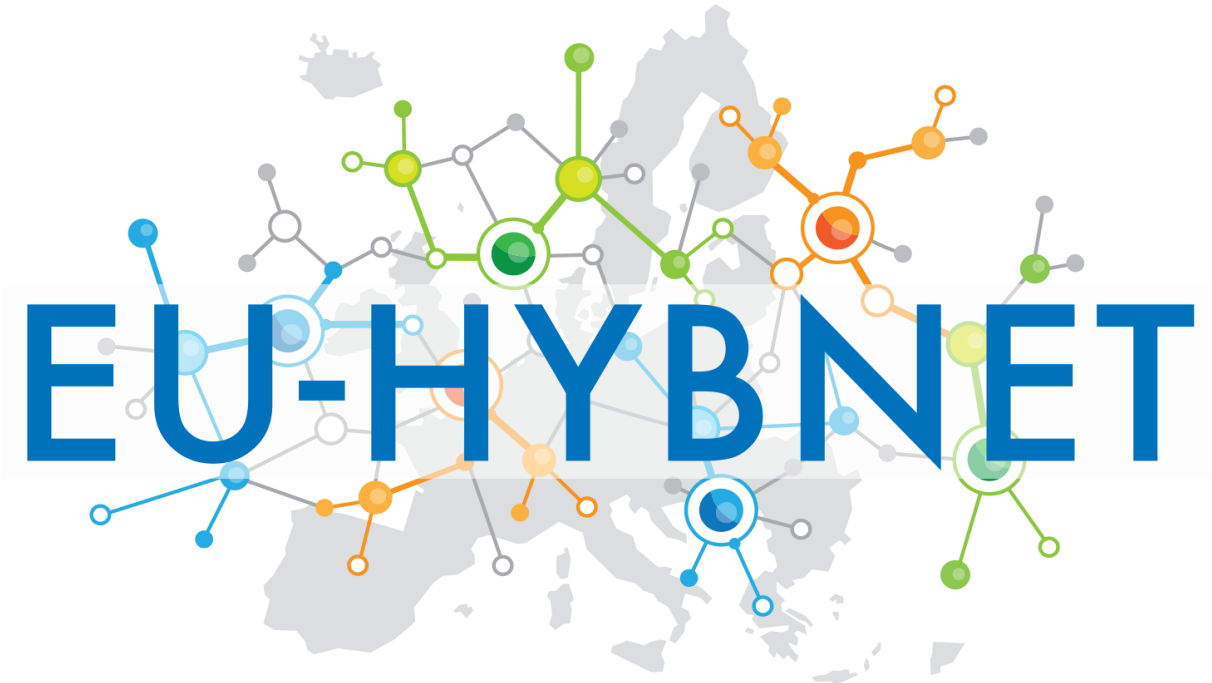


SECOND INNOVATION UPTAKE, INDUSTRIALISATION AND RESEARCH STRATEGY

DELIVERABLE 4.5

Lead Author: RISE

Contributors: KEMEA, L3CE, PPHS, Laurea, UiT

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

D4.5 SECOND INNOVATION UPTAKE, INDUSTRIALISATION AND RESEARCH STRATEGY

Deliverable number	**D4.5**	
Version:	**V1.0**	
Delivery date:	**2023-02-27**	
Dissemination level:	**Public**	
Classification level:	**Public**	
Status	**Ready**	
Nature:	**Activity report**	
Main author:	**RISE**	**Rolf Blom**
Contributors:	**L3CE** **PPHS** **Laurea** **KEMEA**	**Edmundas Piesarskas** **Małgorzata Wolbach** **Isto Mattila, Päivi Mattila** **Athanasios Kosmopoulos**

DOCUMENT CONTROL

Version	Date	Authors	Changes
V01	2023-01-10	Rolf Blom	Report skeleton
V02	2023-01-14	Päivi Mattila, Isto Mattila	First version section 4.1 (WINS)
V03	2023-01-19	Rolf Blom	First version section 4.3 (MIMI)
V04	2023-01-26	Edmundas Piesarskas	First version section 4.2 (EESCM)
V05	2023-01-30	Edmundas Piesarskas	Update section 4.2 (EESCM)
V06	2023-02-01	Päivi Mattila, Isto Mattila	Update section 4.1 (WINS)
V07	2023-02-01	Rolf Blom, Małgorzata Wolbach	First version section 4.4 (GECHO)
V08	2023-02-13	Rolf Blom	Update section 4.3 (MIMI) after review by Pablo Hernández Escayola and Ruben Arcos
V09	2023-02-16	Päivi Mattila, Isto Mattila	Update section 4.1 (WINS) after review by JRC
V10	2023-02-18	Rolf Blom	Update section 4.3 (MIMI)
V11	2023-02-18	Rolf Blom, Małgorzata Wolbach	Update section 4.4 (GECHO) after review by Michael Meisinger and Gunhild Hoogensen Gjørv
V12	2023-02-19	Rolf Blom	Update of all sections except section 4
V13	2023-02-20	Rolf Blom	First “complete” draft (with sections to be updated/inserted)
V14	2023-02-21	Athanasios Kosmopoulos	Section 4.3.6 On prebunking
V15	2023-02-22	Edmundas Piesarskas	Update section 4.2 (EESCM) after review by L3CE
V16	2023-02-23	Rolf Blom	Update after review by Maxime Lebrun and Päivi Mattila
V17	2023-02-24	Rolf Blom	Update after final internal review
V18	2023-02-27	Päivi Mattila	Final review and submission of the document to the EC.

DISCLAIMER

EXECUTIVE SUMMARY

This deliverable (D4.5) is the second report of Task 4.2 (On strategy for innovation uptake, industrialization and research). The objective of Task 4.2 and hence of this deliverable is to, based on the results of WP2 and WP3, select feasible innovation areas and projects that counter hybrid threats and foster hybrid threat situational awareness, and to build concrete roadmaps on strategies for innovation uptake.

The activities in Task 4.2 during this second project cycle has been to apply the methodology developed in the first project cycle

The analysis of the innovations assessed by Task 3.1 has shown that there are important actions to be taken in the areas of increasing resilience in EU critical infrastructures (CI) and building resilience against disinformation campaigns and stop recruitment of young people into groups promoting violent extremism and terrorism.

Two out of the four innovations considered are developed into solutions for building resilience in CI entities. The first one by proposing a method for determining which information that should be shared between CI entities to provide enhanced shared situational awareness and enable detection and mitigation of attacks being part of a hybrid threat situation. The second one by proposing extending the scope of traditional supply chain management to also cover services, geopolitical aspects as well as enhance capabilities to assess cascading effects to allow more rapid recovery and minimisation of impact for critical entities.

The third innovation considered is developed into a solution that proposes to increase stakeholders' willingness to share Information Manipulation and Interference (IMI) information. The main tool to achieve such increased sharing is to create a marketplace with economic incentives.

The fourth solution proposes to provide detailed and local situational awareness about activities in online environments related to violent extremism and terrorism. This to allow efficient interventions against recruitment activities and to safeguard young people from such influence.

The main results presented are the innovation uptake canvases for the four reviewed innovations with clear vision, mission and strategy statements and sketches of roadmaps for their uptake and industrialization. Further results are recommendations for initiation of specific essential research and needed standardization activities.

TABLE OF CONTENTS

TABLES

FIGURES

1 INTRODUCTION

1.1 OVERVIEW

The "Empowering a Pan-European Network to Counter Hybrid Threats" (EU-HYBNET) project Description of Action (DoA)[1] document describes this deliverable (D4.5) as the second report on "Defining a concrete strategic approach for innovation uptake, industrialisation and research". It is part of the overall objective to find common requirements that can fill knowledge gaps, deal with performance needs and enhance capabilities in research, innovation and training concerning hybrid threats. This work is focussed around four core themes, **Future trends of Hybrid Threats, Cyber and Future Technologies, Resilient Civilians, Local Level and National Administration,** and **Information and Strategic Communication**. The core themes are described in Section 1.4.1 Project core themes.

The EU-HYBNET work on "Defining a concrete strategic approach for innovation uptake, industrialisation and research" is part of WP4 (Recommendations for Innovations Uptake and Standardization). WP4 comprises the following objectives:

1. Analysis of the current standardisation and procurement landscape
2. Develop benchmark cases in order to define the cornerstones of the innovation uptake and industrialisation methodologies followed up to now.
3. **Uptake of WP2 and WP3 results and selection of feasible innovations areas and projects of European actors against hybrid threats in order to foster the hybrid threat situational awareness.**
4. **To build a concrete roadmap on innovation uptake.**
5. To compile recommendations for standardisation activities.
6. To deliver Policy Briefs, Position Paper and Recommendations on key innovation and knowledge areas of European actors against hybrid threats

Figure 1 shows WP4 in relation to the other WPs and to the overall EU-HYBNET project.

[1] EU-HYBNET Description of Action, Coordination and Support Action, Grant Agreement No 883054

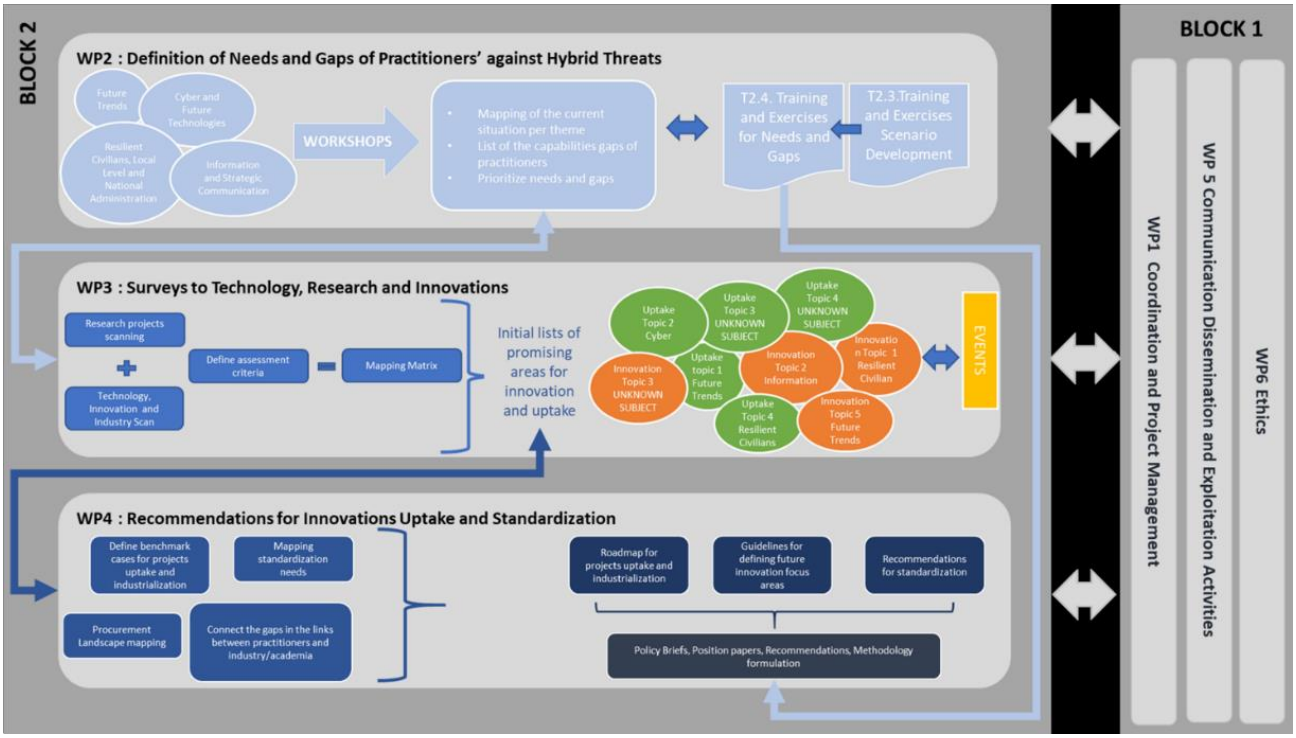


Figure 1. EU-HYBNET Structure of Work Packages and Main Activities

1.2 OBJECTIVES OF TASK 4.2 IN THE SECOND PROJECT CYCLE

Building on the results of WP2 and WP3, Task 4.2 will define concrete strategic approaches for uptake and industrialisation related to the four project core themes. Based on gaps, ongoing research and industrial developments identified by Task 3.1 and Task 3.2, uptake strategies for promising innovations will be developed. Roadmaps, including timeframes, actors and recommended procedures to be followed will be produced. Possibilities for Pre-Commercial Procurements (PCPs) or Public Procurement of Innovations (PPIs) will be reviewed as they are crucial steps in breaching the gap between the buyers and industry. Furthermore, the results from the first project cycle regarding the mechanisms behind good practices and where pitfalls may occur are also taken into account.

In addition to the strategies for innovation uptake, industrialization and research, Task 4.2 results will be fed to Task 4.4 for the preparation of policy briefs, position paper and recommendation.

Figure 2 below, depicts the dependencies between Task 4.2 and WP2, WP3 and other WP4 tasks.

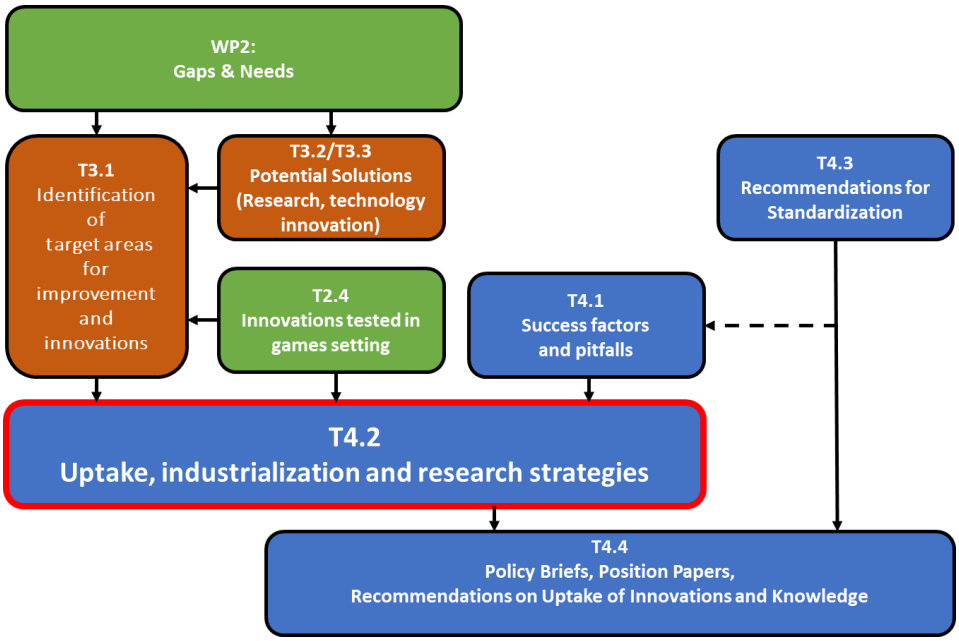


Figure 2. Dependencies between Task 4.2 and WP2, WP3 and other WP4 tasks

1.3 TASK FOCUS AND ACTIVITIES IN THE SECOND PROJECT CYCLE

The main focus of the activities in Task 4.2 during the second project cycle has been to evaluate selected promising innovations and scope them into effective solutions which would contribute to protecting society against hybrid threats.

It is worth noticing that although this is not a research task, the task has had to establish state-of-the art understanding of the innovation areas considered. This to be able to focus the roadmapping work on new and innovative key contributions and solution. An overview of performed the work is:

- Selection of four innovations relating to the EU-HYBNET core themes based on
  - the assessments of proposed innovations performed by Task 3.1, see D3.2[2].
  - The outcome of the trainings (DTAGs) performed by Task 2.4 described in D2.21[3].
- Establishing sufficient state-of-the-art knowledge in the areas covered by the selected innovations. The findings are summarized for each innovation in a section named Setting the scene.
- Application of the framework methodology developed in the first project cycle on the selected innovations.
  - In the review of the four selected innovations the basis has been:
    - The comments from the assessments performed by Task 3.1 and the general and innovation specific recommendations as reported in D3.2[2].

[2] EU-HYBNET D3.2 Second Interim Report Mapped on Gaps and Needs. To be published, see https://cordis.europa.eu/project/id/883054/results

[3] EU-HYBNET D2.21, Training and exercises delivery on up-to-date topics. To be published, see https://cordis.europa.eu/project/id/883054/results

- The review of ongoing research and industrial development performed by Task 3.3 and documented in D3.8[4]
- The uptake success factors and the pitfalls/barriers collected and described by Task 4.1 in D4.1[5].

  - Input and reviews provided by consortium partners and other experts.

- Presenting the uptake strategies for the four selected innovations. Describe barriers, required research and recommend funding solutions in this deliverable.

1.4 EU-HYBNET KEY CONCEPTS AND DEFINTIONS

1.4.1 PROJECT CORE THEMES

For the convenience of the reader we include brief introductions to the projects core themes, fetched from the project web page[6].

1.4.1.1 FUTURE TRENDS OF HYBRID THREATS

To analyse trends has become even more vital than before due to the changed security environment. Hybrid Threats are by character difficult to detect. However, without detection, countering becomes difficult and responses might always be two steps behind. Hybrid threats also have an ever-changing nature. Approach seldom repeats itself and combination of tools is tailor made for the target. For this reason, analysis relating to different security related trends will be essential to be able to have foresight and build early warning systems.

Hybrid threat trend analysis needs to be multidisciplinary and multidimensional using also scenario-based thinking. The future trends of hybrid threats cover also the three other EU-HYBNET themes connecting them to wider security context. This will strengthen situational awareness and identify new and emerging capability needs for countering hybrid threats.

1.4.1.2 CYBER AND FUTURE TECHNOLOGIES

At present, cyber is treated as a domain of activity or knowledge where there are no rules. With regards to hybrid threats specifically, cyber and future technologies are key components through which new developments produce not only new kinds of hybrid threats, but also act as powerful countering measures in the fight against such threats.

Todays' technological upheavals and those of the future suggest that the portfolio of tools used in the realm of hybrid threats will continue to expand rapidly. Computers are ubiquitous, and getting smaller, while processing power is increasing at enormous rates. Other fundamental breakthroughs include robotics, nano- and bio-technologies, artificial intelligence, sensor and 5G technologies. Taken together, these technologies connect symbiotically with people; and they structure society in all spheres – from the interpersonal to the social, and to the military.

[4] D3.8 EU-HYBNET First Report on Innovation and Research Project Monitoring
[5] D4.1 EU-HYBNET First report on the procurement environment
[6] https://euhybnet.eu/

To be sure, communication technologies are driving these developments, there is still a great deal to learn about how an adversary can make use of these new tools and technologies, how cyber is connecting areas previously not connected to realm of security, like hospitals, and how we can in fact use these same tools to detect and counter hybrid threats.

1.4.1.3 RESILIENT CIVILIANS, LOCAL LEVEL AND NATIONAL ADMINISTRATION

Civilians are central as targets and as actors seeking human and societal security. Too much focus has been placed on the state/government level when it comes to hybrid threats. There is still too little research on how this plays out in hybrid threat security environment. Having a better understanding of where the potential vulnerabilities lie within possible target societies enables these same societies – and the diverse civilians within them – to develop measures that can build trust and solidarity within them, making them less vulnerable to such manipulations. This understanding will also help in resilience building that is important for all the EU member states.

Civilians are not passive recipients of information or governmental guidance, and trust levels between the governed and government need re-examination. In a democratic society, political decision-making and the opinions of residents are influenced. Various methods are also combined in order to reach the objective of influencing more effectively. This is a normal, deliberative political activity. Just as there is social or communicative influence that cannot be classified as a threat, there is also governmental influence, i.e., diplomacy. However, outside interference and influence may sometimes be a threat. Classifying something as a threat constitutes normative classification: a threat is something unwanted, i.e., something that is deemed to be wrong or evil. Threats can often easily be classified in the legal sense: in many cases, they are a criminal activity.

1.4.1.4 INFORMATION AND STRATEGIC COMMUNICATION

Information, strategic communication and propaganda are among the areas that, together with cyber, have been linked to hybrid threats most often. The range of hostile and covert influence activities employed in the past include falsely attributed or non-attributed press materials, leaks, the development and control of media assets, overt propaganda, unattributed and black propaganda, forgeries, disinformation, the spread of false rumours, and clandestinely supported organisations, among others. These activities are recognized to be part of the hybrid playbook.

Internet and social media channels have changed the game board for covert influence actions, providing a fertile context for the massive dissemination of overt and covert propaganda by hostile States and non-governmental groups: anyone can produce and disseminate content; connections, funders and identities are blurred; information flows are huge; the speed of information dissemination is breath taking. AI-generated audio-visual forgeries and the likely future improvements in deep fakes technology appear on the horizon as an insidious threat for democracies that will require developing analytic capabilities to detect and counter them. All these require a sound understanding of communication processes and information flows, developing analytic capabilities and skills for assessing open sources and content, raising strong disinformation awareness, critical thinking, and media literacy, and building positive narratives instead of being on the defensive.

While social media networks provide an unprecedented dimension for adversely impacting the potential exposure of target audiences, gathering empirical evidence on disinformation content is

required for a full understanding of the effects of influencing campaigns, and thus developing effective strategies and tactics to counter influence.

1.4.2 THE CONCEPTUAL DOMAIN MODEL

In the report *The Landscape of Hybrid Threats – A Conceptual Model*[7], domains in which hybrid threats may occur are defined. The domains indicate different areas in society and sometimes have overlaps, especially when it comes to threats and risks. Threats often cover more than one domain. Here we list the defined domains and give one or two examples of what threats in the domain could be. For a more comprehensive description we refer to the cited report.

Infrastructure: Physical and or cyber operations against infrastructure.

Cyber: Disinformation, espionage, cybercrime, cyberwar (offensive attacks)

Space: Electronic operations (GNSS jamming and spoofing)

Economy: Sanctions, boycotts, foreign direct investment.

Military/Defence: Border violations, exercises, covert operations (green men), weapons proliferation.

Culture: Exploitation of sociocultural cleavages (ethnic, religion and culture).

Social/Societal: Engaging diasporas for influencing, promoting social unrest, influencing curricula and academia.

Public administration: Promoting and exploiting corruption.

Legal: Leveraging legal rules, processes, institutions, and arguments.

Intelligence: Intelligence preparation, clandestine operations, infiltration Intelligence.

Diplomacy: International relations, diplomatic sanctions

Political: Coercion of politicians and/or government.

Information: Information manipulation and interference. Media control and interference.

1.4.3 DEFINITIONS

All definitions in this section, except for the one of Innovation, are copied from D4.1[8].

[7] Georgios Giannopoulos, Hanna Smith, Marianthi Theocharidou, The landscape of Hybrid Threats: A conceptual model. https://www.hybridcoe.fi/publications/the-landscape-of-hybrid-threats-a-conceptual-model/.

[8] EU-HYBNET Deliverable 4.1 "1st report on the procurement environment. https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e5ded64adc&appId=PPGMS

1.4.3.1 HYBRID THREATS

Hybrid threats aim to exploit a country's vulnerabilities and often seek to undermine fundamental democratic values and liberties [9]. 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[10].

According to the Joint Framework on Countering Hybrid Threats[9], while definitions of hybrid threats vary and need to remain flexible to respond to their evolving nature, the concept of the Framework 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.

1.4.3.2 PRACTITIONERS AT DIFFERENT LEVELS

The EU-HYBNET H2020 project follows the European Commission definition of practitioners which states that "A practitioner is someone who is qualified or registered to practice a particular occupation, profession in the field of security or civil protection." In addition, practitioners in the hybrid threat context are expected to have a legal mandate to plan and take measures, or to provide support to authorities countering hybrid threats.

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. LEAs are an important practitioner group and they are addressed also in the third practitioner category. It should be emphasized that the third category includes researchers and academics, as well as the Centres of Excellence for Hybrid Threats. The third category includes also companies providing critical security and other services for the state e.g., communication networks.

In respect to the I-LEAD project[11], the term practitioners refer to Law Enforcement Agencies. Law enforcement agencies are organisation who respond to, detect, and prevent crime. Within this

[9] European Commission, "Joint Framework on Countering Hybrid Threats", Join (2016) 18 Final, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016JC0018.
[10] EU-Hybnet Description of Action, Coordination and Support Action, Grant Agreement No 883054
[11] Project I-LEAD: Innovation - Law Enforcement Agencies Dialogue, Horizon 2020, https://cordis.europa.eu/project/id/740685.

perspective, it is recognized that police officers play a significant role in adapting and responding to unexpected or unknown situations, as well as recognized situations, such as theft or domestic dispute.

1.4.3.3 GAPS AND NEEDS

The Gaps and Needs analysis that has been completed in the frame of this project aimed to identify, record, and understand the nature of practitioners and other relevant European actors countering hybrid threats' gaps and needs, and the obstacles of developing, maintaining or improving their resilience in the landscape of hybrid threats.

1.4.3.4 TECHNICAL AND NON-TECHNICAL INNOVATIONS

An innovation is defined as the creation or the adoption of new ideas, products, services, programs, technology, policy, structure or new administrative systems and is acknowledged as a source of sustained competitive advantage of many organizations. The concept of newness, crucial in defining innovation, is essential to distinguish the generation of innovation from its adoption. Such a distinction is associated with the differences between the exploration and the exploitation in the organizational learning literature or between the innovation and the imitation in previous innovation research.

The generation of innovation results in the introduction and the use of a product, service, process or practice that is at least new to an organizational population. The adoption of innovation results in the assimilation of a product, service, process or practice that is new to an adopting organization.

In the OECD OSLO MANUAL, Annex 2, The collection of non-technological innovation data[12], an innovation is defined in the following way:

1. An Innovation is defined as the implementation of a new or significantly improved product (good or service) or process, a new marketing method, or a new organizational method in business practices, workplace organization or external relations.

The categorization of technical and non-technical innovations is given as follows (in our wording):

2. **A technical innovation** relates to the introduction of a technologically new or substantially changed good or service or to the use of a technologically new or substantially changed process.

3. **A non-technical Innovation** is, expressed in its simplest form, an innovation which is not a technological innovation. The major types of non-technological innovation are likely to be organisational and managerial innovations, such as
    a. the implementation of advanced management techniques, e.g., Total Quality Management (TQM), Total Quality Service (TQS).
    b. the introduction of significantly changed organisational structures; and
    c. the implementation of new or substantially changed corporate strategic orientations.

[12] OECD, Oslo Manual, https://www.oecd.org/science/inno/2367614.pdf.

1.4.3.5 PUBLIC PROCUREMENT

Public procurement is the process by which public authorities, such as government departments or local authorities, purchase work, goods or services from companies. It is regulated by law to maximise value for money for the public sector and ensure compliance with three key principles:

- equal treatment
- non-discrimination
- transparency

To create a level playing field for businesses across Europe, EU law sets out minimum harmonized public procurement rules. These rules govern the way public authorities and certain public utility operators purchase goods, works and services. They are transposed into national legislation and apply to tenders whose monetary value exceeds a certain amount. For tenders of lower value, national rules apply. Nevertheless, these national rules have also to respect the general principles of EU law.

Every year, over 250 000 public authorities in the EU spend around 14% of GDP (around €2 trillion per year) on the purchase of services, works and supplies. Moreover, in many sectors such as energy, transport, waste management, social protection and the provision of health or education services, public authorities are the principal buyers.

The social gains of the public procurement come from the usage of it by the public sector in order to boost jobs, growth and investment, and to create an economy that is more innovative, resource and energy efficient, and socially inclusive.

Moreover, high quality public services depend on modern, well-managed and efficient procurement. Last but not least is the fact that by improving public procurement big savings can be yield, even a 1% efficiency gain could save €20 billion per year.

1.4.3.6 INNOVATION PROCUREMENT

According to the European Commission's Guidance on Innovation Procurement[13] such procurement is any procurement involving:

- buying the process of innovation – research and development services – with (partial) outcomes; and / or
- buying the outcomes of innovation created of others.

Innovation procurement is a policy instrument whereby policymakers can use the procurement process to foster innovation for the benefit of public authorities, the private sector as well as society at large. Indeed, with innovation procurement public expenditure is used more effectively, as it can harness the private sector's innovation capacity for a number of purposes. Notably, innovation procurement may be used to improve the quality of public services in those areas where the public buyer has a large market share, e.g., healthcare, transport, defence. The increased demand coming from the public sector boosts the private sector's innovative performance, thus increasing overall

[13] European Commission, "Guidance on Innovation Procurement" https://ec.europa.eu/docsroom/documents/45975.

competitiveness. Not least, societal challenges may be tackled through solutions generated via innovation procurement.

Public procurement's primary target is the acquisition of products and services economically. As such, innovation procurement can enhance cost-efficiency by considering life-cycle costs over the long-term and boost performance, thereby producing significant cost savings.

In addition to actual economic demand, innovative products and the provision of services often bestow concrete improvements in administrative procedures and the concomitant enhancement of service quality and user-friendliness. Finally, the government's demand for new products and services stimulates innovative activity in the economy and bolsters the rapid introduction of newer technologies in the market. Small and medium-sized enterprises (SMEs) profit especially, as they require reference projects for their innovative technologies to potential (private) clients and positively influence their purchasing decisions.

1.4.3.7 JOINT PROCUREMENT

"Joint procurement" (JP) means combining the procurement actions of two or more contracting authorities. The key defining characteristic is that there should be only one tender published on behalf of all participating authorities.

2 THE METHODOLOGY FRAMEWORK

The methodology framework[14] was developed in the first project cycle and it provides guidelines on how to derive strategies and evaluate possibilities for uptake and industrialization of innovations but also on identification of barriers, ethical issues, required research, and any needs for new standardization and regulations. The framework's main components are roadmapping and collecting relevant facts in an innovation uptake canvas like the well-known business model canvas[15], see Figure 3. The innovation uptake canvas. The innovation canvas has four columns that describe different aspect of the innovation. The first column, named **The Innovation**, focus on describing important aspects of the innovation itself. The second column named **The solution details** focus on the its functionality, operations and the roadmap for how to realize it. The third column named **Resources** described require resources for the implementation of the solution. Finally the fourth column in the innovation uptake canvas, named the **The uptake environment**,i is about the environment in which the solution will be implemented.

The roadmapping follows standard procedures with vision, mission, strategy and activity statements while the uptake canvas has some EU-HYBNET specific entries. In ANNEX II: The methodology framework, there are descriptions of the roadmapping procedure and the uptake canvas.

Figure 3. The innovation uptake canvas.

[14] EU-HYBNET D4.4 "*1st Innovation uptake, industrialisation and research strategy*" in CORDIS https://cordis.europa.eu/project/id/883054/results

[15] Strategyzer, The business model canvas.

2.1 METHODOLOGY STEPS

The filling in of the Innovation Uptake Canvas and the development of the roadmaps for an innovation is performed in the steps described below. The relevant input and the desired output are depicted in Figure 4.

1. The first, and the most important step, is to instantiate the innovation in a concrete setting by reviewing the scope of the innovation and if needed, redefine it to get a more specific solution to analyse. In this step the findings from the setting the scene work and the recommendations from T3.1 should be taken into account. The result should define the scope of the instantiation of the innovation and roadmapping statements for the 1) vision, 2) mission and 3) strategy. These statements will be the basis for the further analysis.
2. Review the innovation uptake canvas and fill in relevant aspect in the canvas. Identify white spots where more information/analysis is needed. Review and document barriers and success factors.
3. Send the draft canvas for review to project partners, select stakeholders, external experts and the network as applicable.
4. Integrate comments received and finalize the innovation uptake canvas and the roadmap.
5. Document the final canvas and summarize the findings and propose corrective actions, if needed. The resulting final canvases with roadmaps are documented in Section

6. 4 Scoping of and strategy creation for selected innovations.
7. Note all identified barriers and hurdles and recommend strategies / actions to overcome them. These measures could be in the form of required research activities, development of new standards, new policies or changes/updates to current ones. The recommendations are found in Section 5 Recommendations.

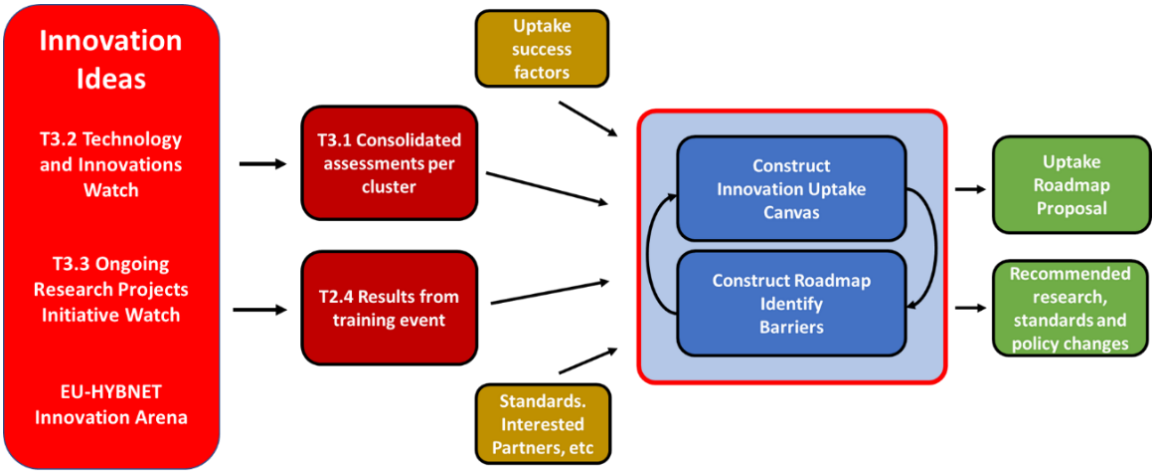


Figure 4. Illustration of the information dependencies for the construction of an Innovation Uptake Canvas, the corresponding Roadmap and Recommendations.

In the following we will use the following phrasing to distinguish between the original innovation and the (scoped) innovation being analysed:

- **The Innovation**: The description of the innovation in the WP3 form.
- **The Solution**: The instantiation of the innovation considered in the uptake and industrialization analysis.

3 SELECTION OF INNOVATIONS

3.1 CRITERIA USED AND RESULTING SELECTIONS

In this second project cycle four innovations were selected for review and scoping, with the ambition to have innovations related to all four EU-HYBNET core themes and also have both technical and non-technical innovations. The selection process is based on

- The assessment and scoring of innovations performed by Task 3.1 and documented in D3.2. The maximum score that an innovation can get is 15.
- The outcome of the training events (DTAGs) organized by Task 2.4, where the attractiveness of the innovations was assessed, see D2.10[16]
- The innovation's relation to the core themes.

Task 3.1 identified a set of 18 promising innovations, i.e., they fulfil the basic assessment criteria defined by Task 3.1. Out of these promising innovations a subset of 6 was identified as "best assessed" and which fulfilled additional evaluation criteria, having score greater than 10.

The T4.2 rationale behind the choice of the four innovations listed below is

1. **Impact and Risk assessment of critical infrastructures in a complex interdependent scenario** belongs a) to the group of the six "best assessed" innovations with a score of 12 and b) it is related to an area judged to be of high importance in the DTAG trainings.
2. **Multi-stage supply chain disruption mitigation strategies and Digital Twins for Supply Chain Resilience** belongs a) to the group of promising innovations with a score of 10 and b) it is related to an area judged to be of high importance in the DTAG trainings.
3. **DDS-alpha** belongs a) to the group of the six "best assessed" innovations with a score of 12 and b) it was judged to be of high importance in the DTAG trainings.
4. **Identify and safeguard vulnerable individuals** belongs a) to the group of the six "best assessed" innovations according to Task 3.1 with a score of 13.

It should be noted that initially, the innovation **Detection of Disinformation Delivery Proxy Actors** with the highest score (14) was considered but it was found to be covered by the scope of innovation **DDS-alpha.**

The innovations' relations to the EU-HYBNET core themes are depicted in Table 1. The reason for not selecting any innovation related to core theme that those innovations were given relatively low scores; the two highest scores were 7.

[16] EU-HYBNET, D2.10 "Deeper analysis, delivery of short list of gaps and needs" in CORDIS https://cordis.europa.eu/project/id/883054/results.

Table 1. Relation between selected innovations and EU-HYBNET core themes according to original innovation descriptions

Innovations	Core Themes			
	Resilient civilians, local level and administration	Cyber and Future Technologies	Information and Strategic Communi-cation	Future Trends and Hybrid Threats.
Impact and Risk assessment of critical infrastructures in a complex interdependent scenario investigations and collective action	X			
Multi-stage supply chain disruption mitigation strategies and Digital Twins for Supply Chain Resilience				X
DDS-alpha			X	
Identify and safeguard vulnerable individuals	X		X	

Here we note that none of the selected innovations relate to core theme Cyber and Future Technology which was aimed for. However, we found that no innovation related to this core theme was scored high enough to be suitable for review in this task.

The selected innovations relation to the target areas defined by T3.1 are given in Table 2. We note that none of the selected innovations are belonging to the target area Low TRL research and innovations**.** The four promising innovations belonging to this target area had low scores and was not considered for this reason.

Table 2. Relation between selected innovations and T3.2 defined target areas

Innovations	Target areas		
	Integration of cyber solutions, AI applications, (dis)information detection, and (fake) news platforms.	Preparation for emerging and disruptive technological developments	Low TRL research and innovations
Impact and Risk assessment of critical infrastructures in a complex interdependent scenario investigations and collective action		X	
Multi-stage supply chain disruption mitigation strategies and Digital Twins for Supply Chain Resilience		X	
DDS-alpha	X		
Identify and safeguard vulnerable individuals	X		

3.2 BRIEF INTRODUCTION TO SELECTED INNOVATIONS

In this section we briefly describe the original innovations assessed by T3.1. We also provide the comments posted by the T3.1 evaluators.

3.2.1 IMPACT AND RISK ASSESSMENT OF CRITICAL INFRASTRUCTURES IN A COMPLEX INTERDEPENDENT SCENARIO.

This innovation is about decision support for critical infrastructure risk assessment with a holistic view on complexity, interdependencies, vulnerabilities and uncertainties. It is proposed to use "What-if scenarios" for impact and risk assessment to build preparedness and to develop risk reduction strategies and implement mitigation actions. It proposes a Critical Infrastructure Resilience Platform to be deployed, i.e., a collaborative software environment that creates new capabilities for policy-makers, decision makers, and scientists by allowing them to use different and diverse modelling and risk assessment solutions.

Comments given in the T3.1 assessment: The envisioned use of the proposed innovation is clear. A major challenge remains: willingness and acceptance by end-users to use the innovation needs to be improved. This could be further strengthened by showcasing the added value of successful implementation use cases.

3.2.2. MULTI-STAGE SUPPLY CHAIN DISRUPTION MITIGATION STRATEGY AND DIGITAL TWINS FOR SUPPLY CHAIN RESILIENCE

This innovation presents an idea to solve a supply chain disruption recovery problem characterized by fluctuating supply disruption risks and manufacturer capacities. Furthermore, it is proposed to use a digital twin representing the current state of a supply chain. Simulations in the digital twin can then show disruption propagation and quantify their impact. In addition, simulations enable testing of recovery policies and adaptation of contingency plans according to the situation.

Comments given in the T3.1 assessment: Whilst this innovation is highly relevant to improve resilience in the supply chain, some challenges include: 1) the high costs for continuous updating of relevant data; 2) the solution space is very narrow (supply chains); 3) whilst it can help improve planning efforts, not everything is plannable.

3.2.3 DDS-ALPHA (EEAS)

This innovation proposes a common and modular framework and methodology for collecting systematic evidence on disinformation and foreign interference as proposed by the European Democracy Action Plan. It is called DDS-alpha, the Disinformation Data Space. It comprises 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.

Comments given in the T3.1 assessment: The proposed solution addresses a key problem in countering hybrid threats and improving resilience, namely sharing information on, and coordinating responses to disinformation campaigns. Whilst the solution shows great promise, it remains a challenge to create enough acceptability and uptake for the innovation to be useful. This can still be considered as a gradual process that can lead to a breaking point once enough entities have taken up the solution. Whilst the solution does address challenges like data management and confidentiality issues related to GDPR, it fails to address potential security problems that might occur resulting from sharing and coordinating databases. Practical issues like differences of language (both by analysts as well as material), and costing remain unclear.

3.2.4 IDENTIFY AND SAFEGUARD VULNERABLE INDIVIDUALS

This innovation proposes to develop different methodological / technological solutions (e.g.: algorithms, redirections to less harmful content, etc.) that would put additional thresholds for people accessing online content supporting extremism and violence.

Comments given in the T3.1 assessment: A clear and precise explanation of the idea of the innovation. The innovation does need to give more details on costs and barriers to implementation.

4 SCOPING OF AND STRATEGY CREATION FOR SELECTED INNOVATIONS

In the following sections we provide the solutions and uptake strategies resulting from the scoping of the original innovations performed by T4.2. As an introduction to the scoping and choices made per solution, we provide some high-level observations. For easy reference the solutions have been named:

- **WINS**, **W**hat **I**nformation **N**eeds to be **S**hared between CI entities to detect hybrid threats and attacks, and to be prepared for them? Based on original innovation *Impact and Risk assessment of critical infrastructures in a complex interdependent scenario investigations and collective action.*
- **EESCM**, **E**nhanced and **E**xtended **S**upply **C**hain **M**anagement. Based on original innovation *Multi-stage supply chain disruption mitigation strategies and Digital Twins for Supply Chain Resilience*
- **MIMI**, A Market place for **IMI** Information. Based on original innovation *DDS-alpha.*
- **GECHO**, **G**atekeeping **ECHO** chambers. Based on original innovation *Identify and safeguard vulnerable individuals*

In the review of innovation DDS-alpha, the importance of having he possibility to do prebunking was identified. In the short to medium term, efforts should be devoted to identifying false stories as early as possible, or even anticipating future narratives. In the longer term, citizens should be provided with the critical skills to distinguish facts from falsehoods and filter out manipulative content. To not lose our findings we have collected them in Section 4.3.6 On prebunking.

WINS and EESCM are non-technical innovations while MIMI and GECHO have technical as well as non-technical components. WINS and EESCM are related to how to build resilience in CI entities. WINS by proposing a method for determining which information that should be shared between CI entities to provide enhanced shared situational awareness and enable detection and mitigation of hybrid threats. EESCM by extending the scope of traditional supply chain management to allow more complete risk analysis and management procedures by a wider consideration of materials and supplies, inclusion of services and the aspect of origin and to extend the depth of the supply chain management to cover end-to-end aspects

The main idea behind MIMI is to increase stakeholders' willingness to share IMI information. The main tool to achieve such increased sharing is to create a marketplace with economic incentives. For this to work, some technical extensions need to be implemented on top of the DDS-alpha platform.

Finally, GECHO proposes the establishment of a platform for information sharing, monitoring, analysis and joint actions between organizations in the MSs to provide detailed and local situational awareness about activities in online environments related to violent extremism and terrorism. This to allow efficient interventions against recruitment activities and to safeguard young people from such influence.

4.1 IMPACT AND RISK ASSESSMENT OF CRITICAL INFRASTRUCTURES IN A COMPLEX INTERDEPENDENT SCENARIO (WINS)

4.1.1 SETTING THE SCENE

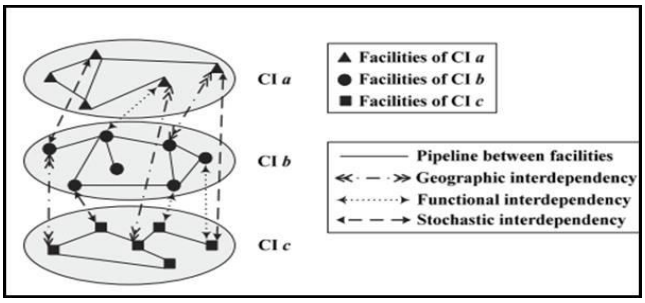
The innovation under review and scoping is based on identified threats under the project Core Theme's "Resilient Civilians, Local Level, National Administration" focus area "**Exploitation of critical infrastructure weaknesses and economic dependencies"**. The innovation is called "*Impact and Risk assessment of critical infrastructures in a complex interdependent scenario"/ CIRP Platform*" described in the EU-HYBNET Task 3.2 deliverable D3.4 "First Mid-Term Report Improvement and Innovations".[17] However, it can be further developed so it will answer the threat above more comprehensive way. The solution proposed is called WINS, **W**hat **I**nformation **N**eeds to be **S**hared between CI entities to detect hybrid threats and attacks, and to be prepared for them?

The original innovation is described in the following way:

> **The Critical Infrastructure Resilience Platform (CIRP)** solution 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.
>
> CIRP creates new capabilities for critical infrastructure (CI) policymakers, 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 minimize the impact of climate change on CIs.
>
> The CIRP idea is based on the article Weilan Suoa, Jin Zhangb, and Xiaolei Suna: Risk assessment of critical infrastructures in a complex interdependent scenario.[18] The paper by Weilan et alia 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.

[17] EU-HYBNET Deliverables D3.2 "First mid-term report Improvement and innovations" in CORDIS https://cordis.europa.eu/project/id/883054/results

[18] Weilan Suoa, Jin Zhangb, and 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).



Concerning the above-mentioned CIRP platform and its analysis, the idea of a critical infrastructure resilience platform is onteresting. However, the idea is not new and several platforms do exist in EU Member States (MS). Therefore, this idea needs to be further developed to answer how to detect hybrid threats by discovering anomaly in operational environment (incl. data) and how to share the discoveries between critical infrastructure (CI) stakeholders.

The overall goal of the EU-HYBNET's suggested innovation WINS is that it will make possible a systemic risk assessment, anomaly detection and evaluation of currently unknown CI interdependencies and flag if an event could be a sign of hybrid threats. **If there is a systematic approach** with e.g., the same signature (anomaly) repeating (digital or physical attack procedure), we can assume that there is a hybrid case ongoing, if we can also connect this incident to influencing decision-making.

Earlier innovation focusing on CI protection (from EU-HYBNET 1st working cycle) was an innovation called *CISAE* (A common Information Sharing and Analysis environment), and the *CISAE* was answering the question of *how to share CI information between CI stakeholders*. Now, the *CIRP* innovation is reconsidered and reformulated as an innovation called "WINS" that will build on CISAE. WINS *is answering the question: **what** information needs to be shared? Therefore, the key element in WINS is a suggested **methodological approach to discover what information needs to be shared** to enhance CI entities[19] resilience to counter hybrid threats.*

Clear identification of infrastructure-related data, and entities operating them, encourages EU MSs to conduct risk assessment of entities operating CI based on a common set of principles developed at the Union level. EU MS may e.g., plan stress test with relevant CI entities in order to augment entities preparedness for disruptions and attacks. However, the EU-level detailed principles are not available for public scrutiny as they are sensitive. Still there is room for novel ideas and views in a further development of the general principles. On the whole, the set of general principles will describe and set out the objectives and modes of cooperation i.e., clarification of *what data is needed to be shared* between CI entities, the MS and EU institutions, bodies, offices and agencies in responding to incidents against CI/critical infrastructure. It's important to recognize that CI in the EU is 93% owned by the

[19] Critical entity definition according to CER Directive Article 2/ (1) is following "Critical entity means public or private entity which has been identified by a Member State in accordance with Article 6 as belonging to one of the categories set out in the third column in the table of in the Annex". CER Directive: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0829.

private sector. Therefore, CI sector involvement in CI protection is essential for defining areas of data and information to be shared.

The core in WINS suggested ***methodological approach*** **to discover** **what information needs to be shared** is based on the establishment of a "**what *if*?"** *scenarios -approach*. In short, the CI entities are encouraged to formulate scenario(s) on possible attacks according to their risks in order to consider in each attack or attack phase what would happen, if in a certain phase of the scenario, the worst would happen, and how this would further affect as an cascading effect, and what is needed to overcome and to prevent the issue to happen? Cascading element are often not only internal but also external (e.g., cyberattack to water purification system and leak of waste/contaminated water to general pipelines and e.g., food industry) due to the wide interconnected environment. According to different scenarios the CI entity would be able to see what the most critical issues are in the "*What If*" situations. This approach also supports focusing on how other related entities need to be alerted for possible damaging effects to come i.e., what data/information needs to be shared between the CI entities (e.g., cyber-attack signatures).

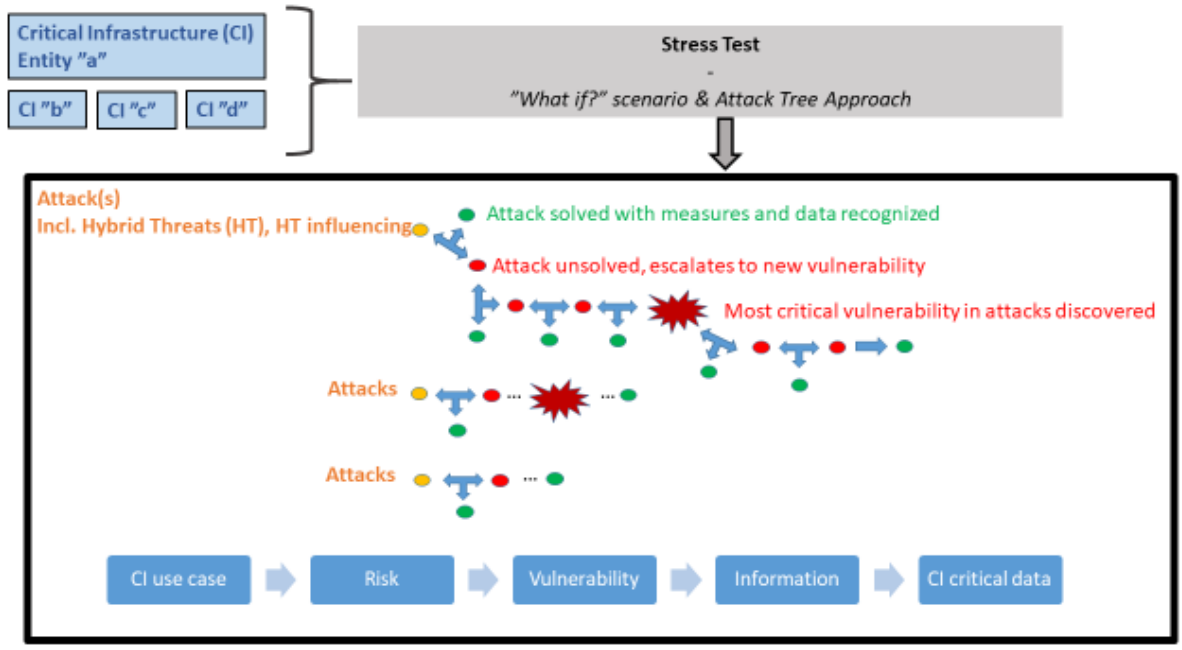


Figure 5 WINS methodological approach, incl. Stress Test and use of "What if?" Scenario

The formulation of the *"What If"* scenario-building should be based on an *"Attack Tree"* approach[20] to define high-priority risks[21]. The novelty of the "*What if*" Scenario and the use of the "*Attack Tree*" approach in WINS innovation is that it would also include the Conceptual Model elements in the scenario building. This enhances CI entities or MS CI authorities to pay attention and categorize security challenges not only in their own but also in other domains (e.g., political, space, cyber, economy). This enables improved ways to counter hybrid threats (in many domains). This would also

[20] Attack Tree approach is especially used in computer science. An overall description of Attack Tee approach is https://en.wikipedia.org/wiki/Attack_tree#Examination

[21] Threats, vulnerabilities and exposure are three components of a risk assessment.

help to create a comprehensive view for the CI entities to counter risks, incl. hybrid threats. The innovation would also support CI entities to implement requirements set by the "Directive 2022/2557 on the resilience of critical entities" (CER) (E.g., Article 7; support to analyse significance of disruptive effect) and "Directive 2022/2555 on measures for a high common level of cybersecurity across the Union" (NIS2) extensively.[22]

4.1.2 THE FIRST COLUMN – THE INNOVATION

- **Description of the solution, i.e., the instantiation of the innovation to be considered.**

  The innovation **Impact and Risk assessment of critical infrastructures in a complex interdependent scenario** has been transformed into a solution which present a methodology for how to establish what information dependent CI entities need to share in order to enhance their resilience against cascading effects and to counter hybrid threats.

  SCOPE: A methodological approach to discover what information CI entities need to share in order to enhance CI entities resilience and to counter hybrid threats.

  VISION: WINS will help CI entities and law enforcement (LE) officials to recognize new forms of hybrid threats/attacks, and further fulfil requirements in this respect given in CER- and NIS-2 Directive.

  MISSION: Deliver pan-European and cross-sectoral CI methodological (even standardized) approach for analysis of CI entities' critical vulnerabilities also in the context of hybrid threats/attacks. The collection of CI entities' vulnerability data is based on risk assessments and stress tests and an attack tree approach. If the CI entities share the data with competent authorities, interconnected services and other relevant stakeholders, this will eventually support CI entities to be more prepared for hybrid attacks/threats.

  STRATEGY: Promote and facilitate discussions of the benefits to use and to implement WINS methodology among CI entities. Initiate a project to in detail define the steps in the WINS methodology and a guide to how it should be implemented. Initiate development of supporting tools. To promote that the WINS methodology uptake is to define *what relevant CI Data and information needs to be focused on and shared* to detect hybrid incidents based on the CER directive requirements so that CI entities may prevent future incidents.

  LIMITATIONS: WINS is based on solely the interest of CI entities to conduct risk assessment (incl. e.g., stress test) with the suggested methodology. Furthermore, WINS is based on solely the information that CI entity/entities provide and voluntary exchange. Based on that analysis, an agreed data-model/methodological approach can be built to have European CI awareness picture as requested in the CER directive. Now CER Directive strives "Critical entities of particular

[22] CER Directive https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0829 ; NIS-2 Directive https://eur-lex.europa.eu/eli/dir/2022/2555

European significance" for information sharing on severe incidents, not on voluntary basis, but sanctions. In short, to avoid sanctions the "Critical entities of particular European significance" would be more inspired to share information voluntarily also with other CI entities to enhance their resilience to crises and disruptions. Sharing CI data and information could be also done by the "data-market-house" -principle, where CI entities agree on data sharing at a certain cost.

RATIONALE: This innovation relies solely on novel methodological approach to gain relevant information and data, and their categorization that CI entities provide from their perspective; when doing their analysis in "What If"-scenarios and according to the "Attack tree" approach the CI entities may realize that they also need open data or restricted data from other domains. In general, to detect signs of hybrid threats and measure that are part of them (e.g. industrial espionage, FDI, creating economic dependencies, territorial water violation) there is a need for data also from other sectors and across borders due to the interlinked CI environment and hybrid threats landscape. Sharing of data for preparedness is not mentioned in CER Directive but this element would empower the directive's goals. Therefore, WINS will support CER Directive's enhanced implementation. In addition, WINS will support EU-level cooperation between different domains. This is seen to provide a more comprehensive resilience picture among pan-European CI entities and pan-European response to hybrid threats via the CI domain. Also, to detect hybrid threats targeted to other domains but also conducted through infrastructure domain.

- **Added value proposition.**

NEED: Existing CI protection (mainly based today on asset protection) has led to a situation where increased interdependencies and related risk of cascading effects across sectors are not sufficiently considered, especially to detect hybrid threats. Today, the used risk management approaches are sector and country-specific, which does not allow the forming of a coherent risk awareness between sectors or countries. There is a need for future wider attention from EU MSs and owners and operators of CI. This has clearly been stated in the new CER Directive and "Strategic Compass for Security and Defence". Identifying the most critical weaknesses in CI resilience (incl. protection) by noticing also other domains (e.g., economy, legal) influence the CI entity's action and sharing CI anomaly detection data/information will enhance CI resilience due to the analysis of what can be made once one has sufficient data available (near real-time).

Most of the critical infrastructure sectors are becoming more and more interdependent on various sectors at the same time and rely on interconnected networks and devices. Due to this interconnectedness, failures in one country or one critical sector may lead to cross-sector and/or cross-

border cascading effects. The lack of awareness makes it difficult for the CI entities to anticipate these risks, which can in turn influence their ability to provide essential services in case of disruptions. Adversaries may be keen to benefit from interconnectedness and cross-sector and/or cross-border cascading effects in forming hybrid threats targeting the CI domain. Indeed, there is a need for large-scale data mining of cross-sectoral and cross-border information from CI entities which is a key enabler for CI resilience and esp. protection against external and internal threats (e.g. FDI, promoting social unrest, electronic operations, creating and exploiting infrastructure dependency incl. civil-military dependency). The focus must shift away from asset protection to one that is more systemic in nature and which recognizes interdependencies across a range of different sectors. Key aspect here is to define the CI external incident data and the hybrid threats element in it.

IMPACT: The main impact of the proposal will allow cross-sectoral and cross-border anomaly information discovery and exchange which will help to build resilience against external threats, identify systemic risks and detect hybrid threats in different CI domains but also in other domains that target to harm CI entities. The purpose is to deliver comprehensive CI awareness that delivers powerful awareness for decision-making at the following levels: domain-specific, national and EU-level in the CER Directive requirements.

VIABILITY: The viability for the solution is linked to the goals of CER Directive. The proposed techniques, use of "What if"-scenarios and attack trees are established methods.

- **<u>Stakeholders and domains</u>**

  Gaps and needs: The solution is related to the following gaps and needs as defined by EU-HYBNET deliverable (D) 2.10 "*Deeper analysis, delivery of short list of gaps and needs*".[23]

  - Threat "**Exploitation of critical infrastructure weaknesses and economic dependencies"** under the project's Core Theme "Resilient Civilians, Local Level, National Administrations"

  Conceptual Model domains: The solution is foremost related to the following domains:

  - Infrastructure
  - Information
  - Cyber

  Stakeholders: CI entities, public and private companies to alert relevant law enforcement (LE) officials and authorities on hybrid threats to prevent escalation.

[23] EU-HYBNET Deliverables D2.10 "Deeper analysis, delivery of short list of gaps and needs" in CORDIS https://cordis.europa.eu/project/id/883054/results.

4.1.3 THE SECOND COLUMN – SOLUTION DETAILS

- **Functional description**

Risk management is key to finding the right data to be shared.

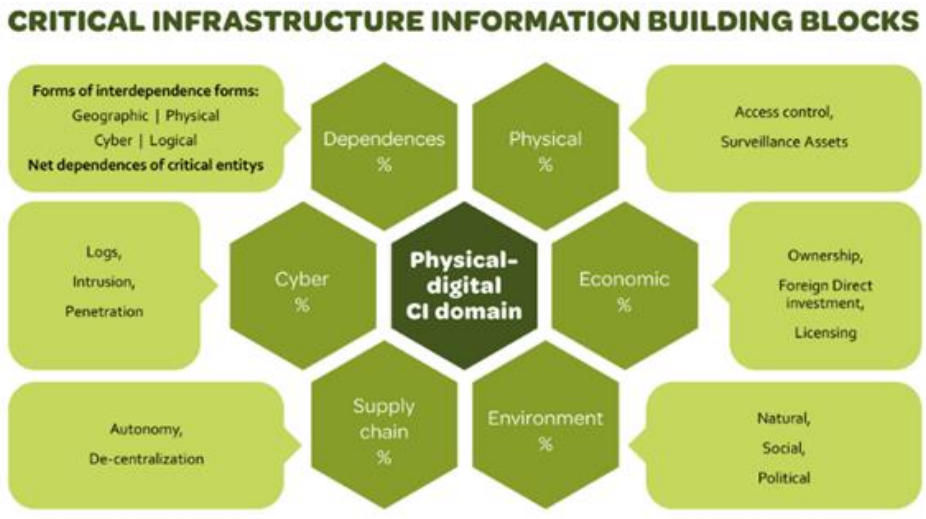
CI risk management is often static and done in silos without a common view or understanding of risks. The data analysis tool is needed to detect and identify risks continuously across sectors, feeding risks for CI assessment on anomaly to data sharing, which was the EU- HYBNET CISAE proposal 2021 answering to the research question on **how** to share information.

This WINS proposal introduces a collaborative multi-criteria data management methodology example for identifying, assessing, analysing, and managing CI risks. This allows the adoption of multiparty interdependency and cross-impact analysis for the EU MS and CI entities.

DATA management

Existing data models are mostly isolated to single organizations or single domains and the overall risk landscape is missing. The state-of-the-art explicitly determines the structured data in relational database frameworks. State-of-the-art data management focuses on an integrated, modular environment to manage organizational application data. Also, corresponding risk prediction tasks are scoped to one domain only. Managing prediction of emerging risk functionality over a multi-organizational domain environment is limited.

After "*What-if*" scenarios and an "Attack tree" approach, each CI community can identify risk areas and their data/information details to be shared. According to the following example, risk related data can be e.g. divided into 6 different risk areas where data is collected from each particular risk category into the one holistic risk data landscape of the critical infrastructure domain.



Picture: example of risk data environment where risk awareness can be built

Critical infrastructure systems and sub-systems continuously generate aggregated data in the format of key performance indicators, counters, events, and alarms from all their components.

It is worthwhile to analyse and correlate all these different types of data to one data environment, where the detection of anomalies gives early indicators of compromise/attack. This systemic anomaly detection solution allows critical infrastructure providers to early detect hybrid threats and early prevent larger effects on the European critical infrastructure. Even though it is not part of CI entities duties to detect that something what occurs is in fact that part of a broader hybrid threat campaign, still this information discovery may now be reached and support CI entities to be prepared for further challenges and/or support to reduce and cut the strength of the hybrid threat campaign.

For example, by knowing that certain foreign direct investments together with cyber espionage and riots have in other similar CI entities cases followed by exploiting thresholds, gaps and uncertainty in law and harming in this way Ci entities functions may provide situational awareness on emerging risk and hybrid threat campaign.

- **Operational description**

  This proposal will classify hybrid threats related incidents. If there is a systematic attack approach with the same signature (anomaly) repeating (digital or operational procedure), we can assume that there is a hybrid threat campaign with various elements ongoing, if we can connect this incident to simultaneous influencing to decision-making; all play their parts. This data-model approach supports the decision-support approach for CI entities' risk (anomaly) findings.

Figure 6. Connecting dots will lead the operator to the roots of the hybrid threat attack/ activity

- **Road-mapping**

The creation of a comprehensive WINS methodology for pan-European CI entities would require the set-up of EU research projects supported by the European Commission.

4.1.4 THE THIRD COLUMN – THE RESOURCES

- **Required development resources**
  The use of the WINS methodology does not require much from the methodology development side because it is to provide the frames for CI entities' own, more specific planning. However, the use and implementation of the WINS methodology by CI entities will ask for resources for planning and testing, and analysing, also to update the plans and views periodically. In short, the use of WINS should be an ongoing activity to be able to cope with new threats and attack vectors - competition for resources may be an issue in this area.

- **Required operating support system**
  EU-HYBNET had suggested during the 1st project working cycle an innovation focusing also on CI protection but called "CISAE" (A common Information Sharing and Analysis environment), and the *CISAE* was answering the question of ***how*** *to share CI information between CI stakeholders*. Now, the WINS *is answering the question and providing a methodological solution:* ***what*** *information needs to be shared to enhance CI entities' resilience to counter hybrid threats.*

  Therefore, to gain the comprehensive benefit of WINS by CI entities and law enforcement authorities pan-European-wide next to a **WINS CISAE** is much welcomed as a CI operating support system.

  In the case of CISAE, the following approach is suggested. A governance body or ENISA which would control the specifications and would oversee the operational procedures of the CISAE (incl. maintenance, updates and upgrades) would be needed. In the case of CISAE the governance body should also provide a forum for the CISAE stakeholders to discuss and share experiences and agree on CISAE improvements and extensions and the possible novelties in the use of WINS methodology. In other words, the governance body could initiate activities and research for the development of new analysis tools and approaches to WINS with CISAE.

- **CAPEX & OPEX**
  EU research projects supported by the European Commission, c. 5 -8 MEURO over 3 - 4 years. Operating costs of the WINS methodology in CI entities would limit under 1 MEURO. However, the development of the CISAE asks for more funding as explained in earlier EU-HYBNET deliverables D4.4. "*1st Innovation uptake, industrialisation and research strategy*".[24]

[24] EU-HYBNET Deliverables D4.4 "*1st Innovation uptake, industrialisation and research strategy*" in CORDIS https://cordis.europa.eu/project/id/883054/results

4.1.5 THE FOURTH COLUMN – THE UPTAKE ENVIRONMENT

- **Competition and market**
  The proposed methodological approach is novel in the sense that it highlights how CI entities may pay attention to hybrid threats/attacks when considering their resilience to critical risks and their key vulnerabilities. Still, there is a need to have a roadmap of how the suggested methodological approach could be accepted by pan-European CI operators widely because only in this case the CI entities may benefit fully from the commonly used methodology. After all, there are several initiatives to increase security in critical infrastructures while, and as said, the hybrid threats focus is now the novelty in WINS.

- **Funding and organization of uptake and industrialization efforts**
  The road mapping indicates that it needs to be an EU initiative behind the realization and development of the proposed CISAE -WINS. The development of a CISAE-WINS will probably never take place without such an initiative and allocation of the required funding. However, we note that the EU already has many actions in the area, and this would only be an add-on to the already ongoing efforts.

- **Barriers**
  Required actions that may become barriers in the work to realize the solution are:

  Barrier 1: Technological barrier
  A technological barrier would involve problems concerning integration or interoperability of sharing the discovery of anomalies related to hybrid threat campaigns as a result of the use of WINS methodology. More specifically, interoperability problems between CI entities could arise from the obsolescence of specific technological components or services, whereas difficulties with integration may come from unexpected delays in subsystem definition or implementation.

  Barrier 2: End-user skills

  WINS methodological approach asks knowledge and understanding of both Attack Tree approach and hybrid threats. However, the knowledge of both can be fairly well achieved and does not require a lot of resources.

  Barrier 3: Regulation, Ethical and Societal acceptance

  WINS methodological approach is to discover vulnerabilities of CI entities and hence the information is often sensitive. However, information on hybrid threat campaigns may also include open data and hence this may be shared between CI entities. Therefore, before sharing the data between CI entities a thorough analysis of societal impact assessment (SIA) and ethical issues needs to be conducted.

Compliance with different types of regulation follows naturally from cooperation with public authorities and integration with existing security data-sharing environments.

Barrier 4: Economic

Notable economic barriers may emerge, if costs from the implementation would climb unexpectedly.

Barrier 5: Operational barrier

To implement the required operational structures and cooperation in information sharing, institutional and legal framework is missing.

Barrier 6: Engagement

To engage the relevant practitioners, end-users, and organizations in all EU MSs and to encourage them all that this is the best way to proceed.

4.2 MULTI-STAGE SUPPLY CHAIN DISRUPTION MITIGATION STRATEGIES AND DIGITAL TWINS FOR SUPPLY CHAIN RESILIENCE (EESCM)

4.2.1 SETTING THE SCENE

The period of the recent COVID pandemic followed by the Russian aggression on Ukraine brought new challenges into sectors that are critical for the safe, secure and smooth operation of our society and industries. Many sectors experienced heavy disruptions in supply chains which constitute a major challenge.

Supply chain management is not a new field within the industrial management scope. It has always been very important to secure operations and provisioning of products to customers and supply chain aspects have always been included in contingency planning. However, during the last 2 years this risk appeared in a new light, and it was realized that the supply change management needs to be extended and enhanced. The main factor behind this need is the new state of affairs in international cooperation, which became visible during the pandemic and especially prominent after the Russian aggression (e.g., the dependence on Russian energy resources in combination with different hybrid operations). The traditional concept of mutually beneficial trade should today be supplemented as new circumstances for trade has evolved. Instead of simply having peace and war periods we must consider hostile periods without real war activities and handle their consequences. Hostile actors might weaponize any component of economy, including supply chains. It is impossible to be fully prepared for such situations. However, to handle their consequences minimizing impact and maximize recovery speed require substantial efforts.

The importance of supply chain in many aspects is described in different EU strategic documents, e.g., the plan of action for strengthening the EU's security and defence policy A Strategic Compass for

Security and Defence[25] highlights the subject in scope of global competition, overall economic security, space industry, disruptive technologies. The document also states that to reduce dependencies "In 2023, we will assess, together with the Commission, the risk for our supply chains of critical infrastructure, in particular in the digital domain, to better protect the EU's security and defence interests." Also, CER- Directive[26] acknowledges the importance of supply chain pointing out the recovery from incidents, including business continuity measures and the identification of alternative supply chains, as one of the key resilience measures of critical entities. The CER-Directive also establishes the governance system, that is very much relevant to the solution proposed.

The above depicted situation shows that there are three main aspects that needs to be covered:

- To increase the resilience of the critical infrastructure by creating an understanding of the need to extend the scope of supply chain management. This aspect includes not only the wider consideration of materials and supplies, but also inclusion of services and the aspect of origin. It is also essential to extend the depth of supply chain management, covering end-to-end chain.

- To model and estimate with greater accuracy the consequences and cascading effects of supply change disruptions and go from theoretical estimates to real and verified developments. Actual disruptions and their impacts must be used for a thorough check models and their calibration. Improved models would offer opportunities not only to evaluate the resilience of supply chains, but also to develop mitigating strategies.

- To support organizations with state-of-the-art instruments to enable proper supply chain management and alternative sourcing. There are existing commercial tools for supply chain management. However, the required broadened scope is not covered. A viable development would be to consider the use of Digital Twin based solutions which can be extended and enhanced to provide the capabilities required in the broadened scope and to make proper optimisations, impact assessments and risk identifications, as described in the EU-HYBNET project deliverable D3.4 section 1.1.2.

The EU-HYBNET project deliverable D3.4 section 1.1.2. proposed on of the tools – anyLogistix[27]. But there are many others in the market. Just to name the few: Shippabo[28], Magaya Supply Chain[29], FreightPOP[30], Precoro[31], Lagiwa WMS[32], SAP supply chain[33] and many more. They have different functionalities, but all provide possibilities to digitalise the procurement process, vendor and supply management, warehouse management, optimization, assets productivity maximisation, alternative supply modelling and many other sector specific or generic components.

[25] https://www.eeas.europa.eu/sites/default/files/documents/strategic_compass_en3_web.pdf
[26] EUR-Lex - 52020PC0829 - EN - EUR-Lex (europa.eu) Article 11.
[27] https://www.anylogistix.com/business-challenges/supply-chain-risk-assesment/
[28] www.shippabo.com
[29] www.magaya.com
[30] www.freightpop.com
[31] Best Procurement Software for Small and Midsize Businesses | Precoro
[32] www.logiwa.com
[33] www.sap.com/products/scm.html

At the same time, we note that even though many tools are available, there are still challenges to understand and define the relevant scope of supply chain management in view of hybrid threats within the chain. Current tools are focused on goods mainly and hardly include services. There is no proper functionalities enabling geopolitical risk and impact assessment, they do not include cascading effects or other threats of hybrid nature, they lack impact minimization and recovery planning features. Current instruments are build based on the traditional understanding of supply chain, while the proposed solution is focused on wider concept of supply chain and not on optimization of current procedures.

4.2.2 THE FIRST COLUMN – THE INNOVATION

- **Description of the solution, i.e., the instantiation of the innovation to be considered.**

  The innovation **Multi-Stage Supply Chain Disruption Mitigation Strategy and Digital Twins for Supply Chain Resilience** has been transformed into a solution focussing on how to enhance and extend the supply chain management scope (EESCM, Enhanced and Extended Supply Chain Management) to take more aspects into account, provide a better understanding of the real issues and how to minimize disruption impacts.

  SCOPE: Supply chain management policies and methods for Critical Infrastructures and industry, followed by enchased tooling.

  VISION: An extended and evolved supply chain management reducing the effects of natural and antagonistic disruptions.

  MISSION: Support CI service providers and product suppliers by building capabilities in impact minimisation and rapid recovery in response to wide supply chain disruptions, including services.

  STRATEGY: Initiate and facilitate discussions for wider understanding of supply chain resilience building by including more components and layers.

  Propose relevant legislation and regulations, as required, to enforce expected CI resilience.

  Evaluate and, if needed, propose changes and extensions of available instruments for supply chain management. Support the instruments availability for all relevant organizations.

  LIMITATIONS: There are no hard limitations. EESMC intends to cover as broad scope as possible. Limitations might appear in the instrument development stage.

  RATIONALE: The period of the recent COVID pandemic followed by the Russian aggression on Ukraine brought new challenges into sectors that are critical for the safe, secure and smooth operation of our society and industries. The experienced heavy disruptions in supply chains were critical**.** Thus, there is a need to build EU autonomy in critical industrial sectors and a key aspect is to understand how supply chains are operating and which interdependencies there are.

- **Added value proposition.**

NEED: Current developments in energy sector clearly shown European dependence on raw materials from Russia. This situation so far resulted in numerous cascading effects (e.g.: providing vast feed for adversary communication, decision making process, potential influence on elections, etc.). There are plenty of other examples, occurring from trade with China or countries under Russia's and China's influence, to illustrate the need to reassess supply chain contingency measures and support industry or even higher-level organizations (associations, groups of interdependent providers of critical products or services) with tools to move to the widened scope of the assessments. The importance of building stability in supply chains are not solely the issue of industry, but also relates heavily to hybrid threats.

IMPACT: The proposed solution (policies, methodologies, followed by relevant tooling) will increase possibilities to react to natural or man-made disruptions in supply chains in general from the current international production interdependencies point of view. The impact of using proper tools to support risk evaluation and alternative supplies, widening supply management scope, will be on impact minimisation and rapid recovery capabilities responding to supply chain disruptions.

VIABILITY: The proposed solution is more of an incremental change than a disruptive step. Thus, it should be relatively straightforward, although not uncomplicated, to develop the proposed EESCM.

There are existing tools, as it is described in the Setting the scene section, that can be taken as a basis for EESCM services. Here we especially consider the use of Digital Twin based solutions which can be extended and enhanced to provide the capabilities required to broaden the scope (including services and geopolitical aspects) and make proper impact assessment, based on real examples. Also strengthen the impact minimisation and recovery components. Even though solutions are available, there is still challenges to understand the scope of supply chain and aspects of hybrid threats within the chain.

The aim of the proposed solution is to provide insights, methodology and frameworks for the industry. New approach of supply chain management then will be taken over by technological solution providers to include new functionalities in their tools.

- **Stakeholders and domains**

Gaps and needs: The solution is related to the following gaps and needs as defined by WP2 in D2.10:

  - Critical threat of Geopolitical heavyweight of domestic policy and the need to Improve geostrategic synergies towards new global frontiers.

Domains: The solution is dedicated for few domains: Infrastructure, Cyber, Space, Economy, Military/Defence, Legal and Political.

Stakeholders: The core stakeholders related to this solution are policy makers and owners/operators of critical infrastructure. In the secondary group other industry and education & training providers should be included.

Policy makers: inclusion of wide scope supply chain in related documents and development of relevant support measures.

Owners / operators of CI: inclusion of wide scope supply chain concept in contingency planning and application of innovative solutions in supply chain risk management.

Other industry: inclusion of wide scope supply chain concept in contingency planning and application of innovative solutions in supply chain risk management were considered relevant.

Education & training providers: conceptualization of the wide scope supply management and provision of relevant training.

4.2.3 THE SECOND COLUMN - SOLUTION DETAILS

- **Functional description**

The proposed solution is to develop easy to follow framework to describe the wide scope supply chain concept. It should include critical services, geopolitical risks, deeper coverage of value chain and other relevant aspects. That can be further used for policy formulation, recommendations and other means to promote and improve it. Relevant legislation on EU and national level can be final stage to anchor the new approach to the supply chain management.

In parallel to the conceptualization efforts methods and tools for wide scope supply chain management should be developed. As was mentioned in the setting the scene, there are innovative solutions already available in the market. There are two aspects to be noted:

- Current available innovative tools and methodologies should be identified, analysed and evaluated on how can they cover additional functionalities, like wider scope, inclusion of services and geopolitical aspects, impact modelling and recovery calculation, including recovery vulnerabilities.

- Support measures, financial instruments in particular, can be established to support CI or other industry if needed to apply extended supply chain analysis tools and methods. This can be done at the national level with EU funding support.

Sectorial initiatives to evaluate and increase resilience are to be considered as well. Most vulnerable industries can be identified, analysed and complex measures can be proposed for sectors, considered critical for national economies.

- **Operational description**

To bring the EESCM solution to practice, providers of supply chain management related services (tools and training) should enhance current instruments with new concept. For doing so the policy and guidance should be set by EU and MS level policy makers. It is presumed that if such recommendations, supported with easy-to-follow framework, are developed and well disseminated, tool and training providers will follow them, adding new capabilities in their instruments.

Digital Twins is the approach currently used to model supply chain and optimisation means and it can be adapted to the widened scope that includes services, geopolitical and other hybrid threats related aspect. Enhanced tools should also be able to provide reliable, real life based, modelling of cascading effects, impact minimisation and recovery simulation capabilities

- **Road mapping**

  The actions required for the implementation of the solution are:

  - Initiate a project and/or set up a governance structure and body to define the final scope of the supply chain resilience building to provide the initial innovative framework, that include above mentioned aspects. Could possibly be the component in some other initiatives and few developments can be initiated in parallel to facilitate the competition and collect different knowledge. It also connects to the activities of Critical Entities Resilience Group, that is expected to be established under the CER-Directive. Supply chain management framework can be in the agenda of the this group.
  - Develop the extended framework to be tested.
  - Launch the testing initiative on the selected industry at EU or regional level to evaluate current resilience level. Few tests can be made in parallel.
  - Develop the final framework that is complete enough to be used in education/training environments and serves as a set of functional requirements for tools and methodologies.
  - Provide recommendations for the target audience (CI, policy makers, providers of tools and training) and evaluate possibilities of inclusion of critical components of the framework in regulatory means.
  - Review available methodologies and tools against the functional requirements of the framework.
  - Initiate the implementation of functionalities projects if considered needed.
  - Organise supporting measures to facilitate the implementation of the framework among CI if needed (can be based on CER Directive).
  - Define how evaluation, maintenance, update, and upgrades will be organized, define responsibilities and set up required bodies to perform the work.

4.2.4 THE THIRD COLUMN – THE RESOURCES

- **Required development resources**

  The set-up of the governance body or to include subject in the agenda of Critical Entities Resilience Group, to be established under CER-Directive, and to define the detailed, evidence based, research program for wide scope supply chain framework should not require any major resources.

  The roadmap proposes to start with the development of the wide scope framework. We find it reasonable to start two-three one-year projects for these tasks with total budget of 4 MEURO. Coordination of research activities should of course be encouraged/enforced.

  Testing can be made in a similar manner, so after two years period the complete enough framework is ready for deployment.

  Assessment of availability and completeness of methodologies and tools can also be done within one-two year with similar funding. At this point it should be decided if additional efforts are needed for functionalities development.

  Governance body or the above-mentioned Group, could start implementation of regulatory measures or recommendations.

  Additional supporting funding requirements in line with CER-Directive can be estimated at this point also.

- **Required operating support system**

  The logic proposed in the roadmap suggests, that initiation of the framework and preparation of tools can be organised at EU level. National supportive funding can later be decided individually by MS.

  The same applies to the tooling issue. If the framework becomes obligatory (as a standard, as a requirement of other form), industry will provide commercial solutions for the market. Those can be developed as bay-in solutions or provided as service.

  The governance body should remain active, mainly focusing on impact assessment and update.

  It might lead to some complex initiatives, requiring EU level interventions, to minimise potential disruptions. Governance body should consider managing such issues as well.

- **CAPEX & OPEX**

  Based on the descriptions of the requirements for development and operational resources we estimate that the CAPEX for the set-up of the organization and the initial research work would be in the order of 8 – 12 MEURO.

It is difficult to assess potential costs for implementation of functional requirements if they appear to be needed. Part of costs can be taken by solution providers.

The same applies to the national level support instruments.

The total cost to launch such an action as proposed here would then be in the order of 10 – 15 MEURO over 3 - 4 years. Other costs can occur at later stages, but expected to be absorbed by solution providers or MS.

4.2.5 THE FOURTH COLUMN – THE UPTAKE ENVIRONMENT

- **Competition and market**

  There are several methodologies and tools for supply management available, as described in the Setting the scene section. Risk of disruptions is also addressed in contingency planning. This proposes that the market is well functioning in the area.

  The proposed change at the high level includes widening the scope by adding services and geopolitical aspects, enabling more precise, real live based, impact assessment, capabilities to assess impact minimisation and recovery time scenarios.

- **Funding and organization of uptake and industrialization efforts**

  There are no specific thresholds for uptake, as innovations considers wider scope and different focus of activities already implemented and services / solutions already available and used by many relevant entities.

  Funding is required at the initial stage to move the subject to other level.

- **Barriers**

  Required actions that may became barriers in the work to realize the solution are:

  - To convince the EU that this is the right way to proceed. Supply chain management is a subject of each organization and might contain confidential information.
  - It might be challenging to agree on the wider scope interpretation, especially inclusion of geopolitical and other aspects related to hybrid threats in the framework.
  - Development of new understanding is rather time consuming while regulatory measures might be not well accepted. Actual resilience should be developed by a big number of organization and probability versus costs should be estimated.
  - Widened scope and shifted focus might require additional funding for organisations. It is not clear how much of new concept of the supply chain management can be implemented on voluntary bases.
  - New concept, especially inclusion of geopolitical aspects, might disclose some sensitive information.

4.3 DDS-ALPHA (MIMI)

4.3.1 SETTING THE SCENE

It has been recognized that a solution for efficient sharing of IMI Information (IMII) between concerned stakeholders is a key element in the MSs' efforts to improve societal resilience against national and foreign IMI activities. This fact is corroborated by the actions and activities by the EEAS Strat.Com. directed at designing and implementing such an IMII sharing platform. It is also communicated in the EU-HYBNET Policy Brief no 3, *Build Societal Resilience – Share IMI* Information.* The need is thus established but the means to ensure wide sharing and exchange of IMII still remains to be comprehended.

IMI activities and campaigns and the mitigation of their effects, affect and involve a large number of stakeholders on domestic, EU and international level. Important examples of stakeholders are the civil society in Member States, Member State and European institutions, research organisations, fact checking organizations, private industry, social media platforms, and other international partners like NATO and the G7.

Today, stakeholders in the IMII arena usually operate in verticals or in limited cooperative setups, that is they collect the base information for the IMI analysis themselves from the open and closed sources they or their partners have access to. This obviously limits the information base which their analysis is based on.

Furthermore, as IMI activities and campaigns propagate across countries and media, the reluctance to share is a limiting factor, especially when it comes to anticipatory work and prebunking. Increased sharing of base information as well analysed data would thus improve the quality and timeliness of possible mitigating actions; the more data, the better output is true also in this context.

With DDS-alpha, a taxonomy and standards for describing and coding of IMI observables is established, which greatly facilitate the sharing of information. The main standards used are STIX, a language and serialization format for exchange of Cyber Threat Information (CTI) and TAXII, a CTI data exchange protocol.

IMII stakeholders currently have very different views on why, what and with whom to exchange IMII. A **first baseline** for cooperation and sharing is that there exists a trust relation between involved stakeholders. IMII may contain very sensitive data, sometimes considered as critical for the national security. Some form of vetting and control may in these cases be needed. This is also the case when data is analysed by national security resources as the resulting product may raise concerns from involved national security organizations. A **second baseline** is that the IMII owner can determine what to share and with whom; there may be e.g., legal restrictions on which information and in which format information may be shared. It is also important to guarantee that shared information is valid. Finally, a **third baseline** is that sharing is of mutual benefit both from an information sharing but also from a financial/economic point of view.

All providers of IMII see the IMII as an asset in their operations and business and thus would providing free access to this asset be problematic for most stakeholders. Furthermore, private companies and

organizations might be hesitant or not at all willing to freely share IMII, either because of the IMII business value (like Cyber Threat Intelligence) or that the information may be business sensitive.

To overcome the above discussed issues and provide a solution which complies with the mentioned baseline requirements we propose that a market and market place for IMII is established. For this to be possible there is a need for a

1. Trusted and secure IMII sharing platform
2. Initial business model which is accepted by all stakeholders
3. Integration of a charging solution in the sharing platform which is compliant with the business model.

The requirement 1) for a trusted and secure IMII sharing platform is satisfied by the DDS-alpha innovation. However, we note that it is important to also implement functionality to make sure that no information leaks to "external agents" or that contaminated information can be entered into the platform. This effort must be sustained during the formation and the operation of the MIMI to ensure that both the functioning of the whole system and the information that moves through it are reliable. This observation is true for MIMI but it is of course also true for the DDS-alpha platform in itself.

Detailed solutions for 2) and 3) would need to be developed in cooperation with the IMII stakeholders to provide a working solution. This proposed solution is called MIMI – a Marketplace for IMI information. We note that business agreements, contracts and payments for services should be handled by standard procedures and are not part of the solution.

Establishment of a MIMI should also promote the building of supply chains in the area. The market place would stimulate the establishment of multiple actors that specialize and compete in different segments of the supply chain with different focus. There may be actors that mine the Internet, others monitor media outlets or the darknet, searching for relevant data and content, and in this way produce baseline IMII. Others may specialize in analysis of such baseline IMII data to detect certain aspects of IMI, like fake accounts, fake media and hate speech, in different cultural regions and languages. Still others, may base their work on already analysed IMII data in order to get an overarching situational awareness or to base decisions on where and how to intervene. If such a market place is established, it would in the best of worlds lead to a market place in which highly competent and specialized competing actors and this would in the end give high quality results and end products.

Finally, we note that although the setting of this innovation is for DDS-alpha, it would be applicable for any other sharing platform like the Common Information Sharing and Analysis Environment (CISAE) for disinformation, proposed in the first EU-HYBNET project cycle, see D4.4[34] and the EU-HYBNET Policy Brief No3.– Information Manipulation and Interference – February 2022[35]

4.3.2 THE FIRST COLUMN – THE INNOVATION

- **Description of the solution, i.e., the instantiation of the innovation to be considered.**

[34] https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e5e29c595e&appId=PPGMS

[35] https://euhybnet.eu/wp-content/uploads/2022/02/EU-HYBNET_Policy-Brief_-Information-Manipulation-and-Interference_Feb-2022.pdf

The innovation **DDS-alpha** (the Disinformation Data Space – alpha) has been transformed into a solution focussing on how to build a market and **A Market place for IMI Information (MIMI)**.

SCOPE: A European IMII sharing solution.

VISION: A secure and trusted market place for IMII sharing which is embraced by IMI data providers, analysts and consumers.

MISSION: Build a European community of IMI data providers, analysts and consumers which embrace the idea of a market-based IMII sharing solution.

Define and agree the business model.

Define and agree functional requirements on the sharing platform for a secure and controlled information exchange supporting the business model.

STRATEGY: Develop a strong and convincing storyline proving the benefits of a general IMI exchange which takes all existing barriers into account. Elect evangelists.

Study existing business models used by stakeholders for existing IMI exchange solutions. Synthesize a business model acceptable for all which would stimulate current stakeholders to exchange IMI information.

Design a service platform on top of DDS-alpha including required DDS-alpha extensions required for charging and service control. The solution should support exchange of IMI information which is required by EU and national regulations.

LIMITATIONS: Compared to the original innovation, this solution is limited in that it only considers the sharing aspects and how to stimulate stakeholders to share their IMII.

RATIONALE: It has been recognized that one barrier is the problem of having access to all required information when aiming for exact and detailed real-time data and situational awareness covering all aspects of IMI activities and campaigns. With the proposed MIMI solution, the barrier would be reduced/eliminated as there would be a direct business value in sharing.

- **Added value proposition.**

NEED: Sharing of IMII is needed to enable production of high quality and detailed situational awareness regarding IMI activities and campaigns.

IMPACT: Increased sharing of observations and IMII base as well analysed data would improve situational awareness in terms of quality and timeliness and improve the possibilities for speedy mitigating actions and interventions. MIMI will serve the governmental and security sectors, which require in-time and complete information to enable fast reaction. Private sector companies

(particularly online platforms) may benefit from a systematic inflow of threats observed and flagged to them for interventions.

A market-based solution like MIMI, with a mixture and private companies, organizations and government institutions at different levels as stakeholders, would most likely develop into an efficient market economy solution and thus be driving force behind increased sharing of IMII. The alternative is to regulate sharing, which will remove many incentives as it will mainly be a cost driver

VIABILITY: That there is a market for threat information is clearly verified by e.g., the business around CTI with several (vertical) companies. Furthermore, the DDS-alpha initiative from EEAS StratCom shows the need and when there is a need there is a market.

- **Stakeholders and domains**

  GAPS AND NEEDS: The solution is related to the following gaps and needs as defined by WP2 in D2.10[36]:

  - Lack of tools to tackle information manipulation / Lack of data on disinformation impact impairs anticipation.
  - Lack of awareness of interference / Lack of horizontal public private governance and risk assessment.

  CONCEPTUAL MODEL DOMAINS: The solution is in the Information domain.

  STAKEHOLDERS: Actors specialized in monitoring of disinformation campaigns or the collection and analysis of IMII will also be important stakeholders. Core stakeholders are of course also the Member States' practitioners involved in monitoring, handling and countering disinformation campaigns. Private platform and media companies will also be important stakeholders in a MIMI solution.

4.3.3 THE SECOND COLUMN - SOLUTION DETAILS

- **Functional description**

  The main technical components, the service platform, to be developed are interfaces towards the technical sharing platform for control of service level agreements between IMI information and data providers and consumers. These service level agreements determine access rights and how services may be invoked on a subscription or pay per use basis. The charging solution has also to be integrated in the access and service invocation functionality.

  Business agreements, contracts and payments for services should be handled by standard procedures and are not part of the solution

[36] EU-HYBNET Deliverables D2.10 "Deeper analysis, delivery of short list of gaps and needs" in CORDIS https://cordis.europa.eu/project/id/883054/results.

- **Operational description**

  For the establishment of MIMI there is a need to establish an organization which drives the building a European community of interested partners. This could be organized as a time limited project. The project should:

  - Develop a strong and convincing storyline showing the benefits of using MIMI and elect evangelists to convince stakeholders of the value in using MIMI.
  - Liaise with the DDS-alpha community/interest group to prepare for future joint developments.
  - Define and propose a suitable business model.
  - Define the requirements for the service platform on DDS-alpha, including required DDS-alpha extensions for charging and service control. The solution should support exchange of IMI information which is required by EU and national regulations. It must contain functionality for
    - Secure and controlled information exchange.
    - Interfaces for control of service level agreements between users and providers
  - Implement and verify required functional extensions of DDS-alpha. Publish extensions as open source.
  - Set up a MIMI interest group which can maintain and extend MIMI.
  - Transfer maintenance operations of the service platform to the organization handling DDS-alpha.

  When MIMI has been established as a working solution, the required maintenance of the idea would be handled by the interest group

- **Roadmapping**

  The roadmap follows the operational procedure described above. The actions required for the implementation of the solution are:

  - Organize EU funding for the project described in the operational description. All types of stakeholders should be involved in the project, either in the actual project work or in project expert and reference groups.
  - Ensure that MIMI extensions are implemented in DDS-alpha.
  - Convince EU and national organizations to use the MIMI to establish a request for provided services
  - Drive the set-up of service level agreements between stakeholder to stimulate MIMI use.
  - Establish an interest group to maintain MIMI when the project establishing the solution has been finalized.

4.3.4 THE THIRD COLUMN – THE RESOURCES

- **Required development resources**

  The roadmap proposes an EU funded project to establish MIMI. Resources will be required for the "marketing" of MIMI, investigation and proposal of relevant business models. Furthermore, the development and a first implementation of the service platform will be

required. We find it reasonable that a three-year 4 MEURO project would be able to perform the required actions and achieve the goals.

- **Required operating support system**
  Organizational support after the establishment of MIMI would be the work performed in the suggested MIMI interest group. The work in the interest group should be financed by its members but would not require any substantial resources. Any required updates of the service platform should be integrated in the future developments of DDS-alpha.

- **CAPEX & OPEX**
  As the roadmap only proposes the set-up of one EU funded projects to establish MIMI the CAPEX would be 4 MEURO. Thereafter operational costs will part of the DDS-alpha operational costs and are hard to estimate, however these costs should be limited.

4.3.5 THE FOURTH COLUMN – THE UPTAKE ENVIRONMENT

- **Competition and market**
  MIMI is a unique solution and there are no similar competing solutions. Possible competition could appear from already established players that work in vertical silos.

- **Funding and organization of uptake and industrialization efforts**
  The roadmap points at that it must be an EU initiative behind the realization and development of MIMI. This solution would most likely never happen without such an initiative and the required corresponding funding. There is also a need that MSs embrace the idea and that national stakeholders are prepared to join in using MIMI. Furthermore, we note that the EU already has a number of activities in the area of handling and understanding disinformation and that MIMI just would be a relatively small extension of the already ongoing activities.

- **Barriers**
  The only identified barrier, which the MIMI solution actively tries to break down is the acceptance to use a marketing solution for IMI sharing.

  There may also be efforts from antagonistic actors, trying to stop the establishment of MIMI by claiming that it would increase the surveyance and control of citizens in MSs and impact and limit their freedom of expression.

4.3.6 ON PREBUNKING

An additional element with regard to the DDS-alpha innovation is the aspect of prebunking, i.e., the practice of countering potential misinformation by warning people against it before it is disseminated. Below a discussion on its importance and use.

From Debunking to Prebunking

If there is one hallmark of the efforts against disinformation in Europe, it is quantity. A huge number of think tanks, consultancies, CSOs, media organisations, academics, start-ups, and fact-checkers are

involved in one way or another in this issue, from all angles and all member states. With such a variety of individual initiatives taking place simultaneously, there is inevitably a certain amount of overlap, duplication of efforts and missing connections.

In the last few years, the EU has started to take a stronger role in facilitating connection between civil society actors, mainly through two overlapping projects: the Social Observatory for Disinformation and Social Media Analysis and the European Digital Media Observatory[37].

Prebunking, in the short to medium term, efforts should be devoted to identifying false stories as early as possible, or even anticipating future narratives. In the longer term, citizens should be provided with the critical skills to distinguish facts from falsehoods and filter out manipulative content.

DDS-alpha may contribute into expanding monitoring activities through coordinated multi-stakeholder initiatives to understand the spread of disinformation narratives and evaluate their potential to spread. Establish early warning systems based on civil society monitoring work to enable fact-checkers and communication professionals to assess the likely reach and impact of disinformation before intervening and craft swift responses where necessary.

Use foresight techniques to anticipate which disinformation narratives might spread in response to particular events and how they might cross linguistic and political boundaries.

Stakeholders and domains

Stakeholders are categorized in providers of data and consumers of data. Public sector entities, private sector end-users, and society actors. They all may play a role into contributing to the idea and benefitting from it at the same time. These actors may operate in different domains such government, media, LE, armed forces, logistics, transport, energy, etc.

Functional description

In order to setup DDS-Alpha into an “up and running” mode including prebunking elements, there has to be an entity responsible for the database in terms of physical equipment, connectivity and security. Relevant platforms are available in the market, and it has to be decided if the platform will run under the auspices of a MS or a private entity. An administrator shall define the users that have access to DDS Alpha and assign the relevant rights and privileges to them.

A dashboard may provide necessary details and info on important events of hybrid nature.

Bearing in mind that information operations - regardless of whether they are labelled as political warfare or influence operations or exercised as an element of a broader hybrid campaign - exploit the vulnerabilities of modern democracies and target both the elites and societies of the western states in order to influence political behaviour and public opinion, the hostile toolkit involves the dissemination of false, misleading and manipulative information in the media - especially the social media. Information operations exploit one of the most challenging characteristics of our era: ambiguity. The lines between virtual and real, domestic and international, public and private have eroded, and the result is far more ambiguity. Planting and disseminating a lie via social media is cheap and easy. On the

[37] From debunking to prebunking: How to get ahead of disinformation, EUROPEAN MIGRATION AND DIVERSITY PROGRAMME EUROPEAN POLITICS AND INSTITUTIONS PROGRAMME, 29 NOVEMBER 2021

other hand, identifying the lie, tracking its origins, and communicating 'your' truth to the same audiences is labour intensive and costly.

Concern about people's general vulnerability to political indoctrination goes back many decades[38], arising at the time from disquietude about persuasive techniques employed by totalitarian states. The larger question of how to go about developing attitudinal "resistance" against unwanted persuasion attempts ultimately led McGuire to develop "inoculation theory", which, for a popular audience, he described as a "vaccine for brainwash" which led nowadays to the "Prebunking Approach".

Inoculation theory[39] closely follows the biomedical analogy. Just as vaccines are weakened versions of a pathogen that trigger the production of antibodies when they enter the body to help confer immunity against future infection, inoculation theory postulates that the same can be achieved with information: by pre-emptively exposing people to a sufficiently weakened version of a persuasive attack, a cognitive-motivational process is triggered that is analogous to the production of "mental antibodies", rendering the individual more immune to persuasion[40].

Prebunking is an effective countermeasure when relentless targeting plays "to the fears and the prejudices of people, in order to alter their opinion and plans" and proves to be "more invasive than obviously false information" contributing to a "democratic crisis"[41] .

Operational description

From the operational point of view DDS-Alpha may be deployed on a subscription basis by an annual or monthly subscription fee for each participant.

An important concern is the possible reluctancy of participants to disclose information considered to be sensitive or confidential for market and reputational reasons.

A participant may be a provider or consumer of information or both, contributing to the common effort of fighting disinformation.

Roadmapping

In the last few years, the EU has started to take a stronger role in facilitating connections between civil society actors, mainly through two overlapping projects.

First, the Social Observatory for Disinformation and Social Media Analysis (SOMA) ran from November 2018 until April 2021. It sought to lay the basis for a Europe-wide network of fact-checking

[38] McGuire, W. J. (1961). Resistance to persuasion conferred by active and passive prior refutation of the same and alternative counterarguments.. The Journal of Abnormal and Social Psychology, 63(2), 326–332. https://doi.org/10.1037/h0048344

[39] McGuire, W. J. (1970). Vaccine for brainwash. Psychology today, 3(9), 36–64.

[40] Compton, J. (2013). oculation theory. In J. Dillard & L. Shen (Eds.), The SAGE handbook of persuasion: Developments in theory and practice. (pp. 220– 236). Thousand Oaks, CA: Sage.

[41] Youyou, W., Kosinski, M., & Stillwell, D. (2015). Computer-based personality judg
ments are more accurate than those made by humans. Proceedings of the National Academy of Sciences, 112(4), 1036–1040. https://doi.org/10.1073/pnas.1418680112

organisations. But in practice, it only attracted a small number of members, most of whom did not appear to make much use of the project platform.

SOMA's activities have largely been taken over since June 2021 by the more ambitious European Digital Media Observatory (EDMO). The latter is a Europewide network of not only fact-checking organisations but also academics, researchers and media institutions.

Built around a European level of partner organisations, with several national and regional hubs that are in the process of being set up, its goal is to strengthen cooperation, raise awareness and empower citizens to respond to online disinformation. To this end, it conducts original research, maps and supports existing fact-checking and research activities, and seeks to build a European community of fact-checkers that will collaborate continually, contributing to a culture of cross-border cooperation.

EDMO's structure is, therefore, by design, cross-sector, cross-border and cross-purpose, in that it aims to develop research and understanding about disinformation while also working practically to counter it. Although each of its national and regional hubs is composed of different organisations working together in different ways, the various national experiences should allow for exchange and mutual learning between countries. This transnational perspective, informed by expertise on national and regional dynamics, helps monitor the spread of disinformation more effectively, regardless of its origin, and contribute to finding and coordinating effective responses against it.

The European-level EDMO partners currently use two main instruments to pursue this goal: in-depth reports, based on surveys among fact-checkers, that shed light on disinformation patterns and narratives prevailing across European countries; and monthly briefs that provide up-to-date situational insights into disinformation narratives dominating at transnational level, examining and identifying cross-border patterns regularly.

In this light, deploying a prebunking DDS-Alpha platform seems to be following the same template and modus operandi as previous initiatives with no substantial effort needed.

Required development resources

It has to be decided which entity will be responsible for the deployment of DDS-Alpha, in terms of public or private character. Evidently, for a public entity will be by far easier to set up and launch the initiative, obtaining the necessary assets and means for this purpose from a MS. If not for a MS to take the initiative to set up the project, then an EU research project could be established to develop the organizational framework, the processes and collaboration methods.

Required operating support system

In order to keep up with threat developments the ENISA's DISARM tool[42] (DISinformation Analysis & Risk Management) which focuses on FIMI/disinformation creation and dissemination behaviours is appropriate. The framework is inspired by the structure of the MITRE's ATT&CK ® framework[43], which is a knowledge-base of cyber adversary behaviour and taxonomy for adversarial actions across their lifecycle. The DISARM Red Framework is a useful tool to describe FIMI TTPs. DISARM is born out of the

[42] https://disarmframework.herokuapp.com/

[43] https://attack.mitre.org/matrices/enterprise/

collaborative effort of individuals from the FIMI defender community, which introduced the concepts of kill chain, tactics, techniques, and procedures (TTPs) and behavioural fingerprints to the FIMI field. Due to its threat-informed, open-source and community-driven nature, the DISARM framework allows to consolidate all known FIMI TTPs. It also introduces a taxonomy for defenders to speak a common language when describing their findings. The DISARM framework is used jointly with MITRE ATTA&CK and specifically ATT&CK for Enterprise, which covers behaviour against enterprise IT networks and cloud.

4.4 IDENTIFY AND SAFEGUARD VULNERABLE INDIVIDUALS (GECHO)

4.4.1 SETTING THE SCENE

Violent extremist groups and terrorists pose a serious problem for democratic societies today. Their actions and propaganda aim at destabilizing and reducing trust in societal institutions and may in the end target the overthrow of current rule of law.

Violent extremism and terrorism are tools in the hybrid threat toolbox used by antagonistic states and non-state actors (e.g., Daesh/ISIS, neo-Nazi/white supremacy movements, and conspiracy groups). Violent extremism and terrorism are in this case often used to exploit and widen sociocultural cleavages (ethnic, religious and cultural). Antagonistic states may support local groups that promote violent extremism and terrorism and, in that way, try to avoid being identified as a complicit and driving force behind actions.

An obvious countermeasure to reduce the threat from extremist groups promoting use of violence and terrorism is to limit and prevent recruitment of followers. With a radically reduced number of members in these groups the motivation and possibility to perform violent actions will clearly be reduced. It is most likely also much easier to stop someone from becoming a follower than to deradicalize a person, who embraces ideologies promoting use of violence.

The expansion of communities promoting violent extremism and terrorism is mainly achieved by targeting vulnerable individuals. Here, personal vulnerability is often related to fear and insecurity resulting in a distrust in society in general, its institutions, or societal approaches or actions in respect to certain phenomena. Angry and marginalized youth, looking for solutions to their own problems, is a vulnerable group of special importance.

Promotion of extremism and violence take place via many different communication channels and physical meetings. Today, online platforms play an increasingly important role in the recruitment process. Platforms promoting violent extremism and terrorism are abundant and easily accessed. To attract new followers, they are often closed, but open for anyone to visit. Thus, online platforms may often serve as an initial place of contact between a vulnerable individual and groups promoting violent extremism and terrorism. However, meetings in real life are also important in recruiting and solidifying commitments to the “cause”. Thus, there is no single “silver bullet” solution to the problem and there is a need to develop programmes/ frameworks containing coordinated actions and activities. Such actions and activities have to be adapted per type of extremism (right-wing, left-wing, Islamic, etc.) and to local conditions (societal issues, language, culture, online platform used, etc.). The way ideas and propaganda are expressed varies between groups in different cultures and languages between women and girls, men and boys and societal situation.

Furthermore, we note that there are many entrance points for becoming radicalized. Extremist music and online games are two and viewing of streamed media of e.g., mass shootings and studies of extremist manifests are two more. These entry points may relate more to lone wolves' radicalization than direct recruitment activities. They are however just as important.

As with countering of Information Manipulation and Interference (IMI, or also called disinformation campaigns), it is important to have good situational awareness on a local but also at regional, national, EU and Global level. To survey the violent extremism and terrorism online environment AI based tools should be used to quickly and accurately discover new sites, new visitors and changes in activity levels at known sites. Early detection would be very valuable in the deployment of timely countermeasures and interventions. An EU standardized platform for (semi-)real-time collection and sharing of such information would be of great importance in this work. One of the key components in the solutions presented here is the establishment of such a platform. Other key components are further research on underlying factors for being attracted to violent extremism and on how interventions and countermeasures should be realised.

Activities in countering violent extremism

EU has adopted the EU Counter-Terrorism Strategy[44] and the Revised EU Strategy for Combating Radicalisation and Recruitment to Terrorism[45]. These strategy documents together with the Final Report[46] from the High-Level Commission Expert Group on Radicalisation (HLCEG-R) and the recent new Counter-Terrorism Agenda[47] provide a number proposals for countering violent extremism and terrorism. We note here that

- There is an EU strategic commitment to prevent people from being drawn into terrorism by tackling the factors or root causes which can lead to radicalisation and recruitment to terrorism, in Europe and internationally;
- The responsibility of combating radicalisation and terrorist recruitment lies primarily with the Member States, but that EU efforts in this field can provide an important framework to share good practices;
- There is a need to develop a strategy to address radicalisation in all of its forms; and
- Measures to counter radicalisation and recruitment need to take account of the diversity of modern society and modern communications.

Furthermore, to fight against terrorism, the European Commission has put forward a series of voluntary and legislative measures and initiatives to help mitigate the terrorist and radicalization threat. One relevant example is the regulation on addressing the dissemination of terrorist content online48 as of 7 June 2022. The regulation sets out EU-wide rules to tackle the misuse of hosting services for the public dissemination of terrorist content online. The regulation sets out a number of measures to address the public dissemination of terrorist content online. Based on the Regulation, terrorist content must be taken down within one hour after it is identified

[44] EU counter-terrorism strategy
[45] Revised EU Strategy for Combating Radicalisation and Recruitment to Terrorism
[46] https://op.europa.eu/en/publication-detail/-/publication/04756927-97bc-11e9-9369-01aa75ed71a1/language-en
[47] Counter-Terrorism Agenda
[48] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32021R0784

online. This applies for online platforms offering services in the EU, to ensure the safety and security of citizens. At the same time, the Regulation puts in place strong safeguards to guarantee that freedom of expression and information are fully protected.

There are many EU activities and organizations that actively operate in the field of countermeasures towards extremist groups and terrorist. One such important organization is The Radicalisation Awareness Network (RAN Practitioners)[49] which has been active since 2011 and funded by the EU Commission's Internal Security Fund – Police. The Network consist of over 6000 frontline practitioners from all EU Member States such as field experts, social workers, teachers, NGOs, civil society organisations, victims' groups, local authorities, law enforcement, academics and other who are focusing on exchange knowledge, experiences and approaches to preventing and countering violent extremism in all its formats, undermine the radicalisation and recruitment of future terrorist, that means vulnerable individuals. Practitioners work in RAN Working Groups and one of them is dedicated to provide both online and offline communications that offers alternatives or that counters extremist propaganda and challenges extremist ideas – Communication and Narratives Working Group (RAN C&N). But in the last years, multiple RAN Working Groups have discussed online Prevention / Countering of Violent Extremism (P/CVE) and what next forward steps should be taken in this area.

The main global actor powering solutions to extremism, hate and disinformation is the Institute for Strategic Dialogue (ISD)50. Worldwide, a wide range of experts from different places work together on pushing back the forces threatening democracy and cohesion around the world today by analysis, action and policy. In previous years they tested innovative programme ("Counter Conversation 51": A model for direct engagement with individuals showing signs of radicalization online) with an experimental approach designed to fill a gap to online extremism by checking if the methods deployed in offline intervention can be brought into the social media. The results demonstrate the positive potential of direct online engagements and point to the need for further exploration into how this model can be deployed in a responsible, effective and scaled fashion, as part of a suite of online risk reduction methodologies.

The Global Internet Forum to Counter Terrorism (GIFCT)[52] plays a very important role in countering extremism and violent content. Their mission is to prevent terrorists and violent extremists from exploiting digital platforms. In line with GIFCT's mission, technology sector marshals its collective creativity and capacity to render terrorists and violent extremists ineffective online. Bringing together various environments central to their efforts is the protection and promotion of the fundamental human rights–to include freedom of expression–that terrorism seeks to undermine. This NGO supports many other initiatives like The Global Network on Extremism and Technology[53], academic research that is trying to better understand

[49] https://home-affairs.ec.europa.eu/networks/radicalisation-awareness-network-ran_en
[50] https://www.isdglobal.org
[51] https://www.isdglobal.org/wp-content/uploads/2018/03/Counter-Conversations_FINAL.pdf
[52] https://gifct.org/
[53] https://gnet-research.org

the ways in which terrorists use technology. GNET is led by International Centre for the Study of Radicalization (ICSR)[54] based in London and cooperates with experts from all over the world.

Moreover, there are many initiatives implemented within EU funded projects:

- **Participation**[55] is project which primary purpose is to prevent extremism, radicalization and polarization that can lead to violence through more effective social and education policies and interventions that target at risk groups to be performed through the establishment of a holistic framework and the involvement of social actors, local communities, civil society, and policymakers;
- **INDEED**[56] builds from the state-of-the-art, utilizing the scientific and practical strengths of recent activities – enhancing them with complementary features to drive advancements and curb a growing rise of radical views and violent behaviour threatening security. Project's methodological framework is based on the '5I' approach i.e. 5 project phases: Identify; Involve; Innovate; Implement; Impact;
- **Dominoes** (Digital Competences Information Ecosystem)[57] is a project dedicated to the investigation of hybrid threats, propaganda and disinformation which overall objective is to reduce societal polarization by combating fake news and online disinformation in two target groups: university professors employed by the partner universities/civil society trainers and M.A. students in the partner universities.
- **VOX-Pol Network of Excellence**[58] is a FP7 started Virtual Centre of Excellence for Research in Violent Online Political Extremism, which still is very active. The aim of VOX-Pol is the comprehensive exploration of the many varieties of Violent Online Political Extremism, its societal impacts, and responses to it. To this end, project partners combine complementary expertise from a range of disciplines (e.g. Communications, Computer Science, Criminology, Ethics, International Relations, Politics).

In the Horizon Europe Work Programme on Civil Security for Society, there is a RIA call[59] on Radicalisation and gender, with focus on improved understanding of motivation for supporting extremist ideologies, by women and girls, by men and boys as well as of the role of group dynamics. Another target is to develop modern and validated tools, skills and training curricula to identify early symptoms of radicalization. This project is well aligned with the proposed solution detailed below.

To conclude, we want to first reference one successfully developed and widely deployed method and then one study report. The first refence is to a solution from Moonshot, the Redirect Method[60]. It 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

[54] https://icsr.info/
[55] https://participation-in.eu/
[56] https://www.indeedproject.eu
[57] https://projectdominoes.eu/
[58] https://www.voxpol.eu/
[59] HORIZON-CL3-2024-FCT-01-04: Radicalisation and gender
[60] https://moonshotteam.com/the-redirect-method/

of countering harm, to challenge narratives which support violent extremism, violent misogyny, disinformation and other online harms.

The study report is a report in Swedish titled *Webbpoliser, gaming och kontranarrativ : Digitalt förebyggande arbete mot extremism och våldsbejakande extremism*[61] (Google translate: *Web police, gaming and counternarratives: Digital prevention efforts against extremism and violent extremism*) by Linda Ahlerup and Magnus Ranstorp at the Swedish Defence University. It discusses the digital arena and preventive measures with respect to violent extremism and reviews 15 innovative and successful methods and tools[62] for how to use the digital arena in preventive work. One conclusion is that there is a need for many different initiatives with different functions and focus areas and that they often need to be integrated in a wider strategy and plan of actions.

Conclusions

The desktop research results summarized above have shown that there are a lot of organizations, initiatives and projects that focus on the main issue, which is fighting against radicalization/terrorism in a global way. However, we have found that what is missing are:

- A platform for online situational awareness with respect to violent extremism and terrorism. The platform should comprise functions for real-time sharing of available information.
- AI based tools for rapid and accurate discovery of new sites related to violent extremism. Monitoring of activity levels at known sites and visits by new users.
- A standardized taxonomy which is accepted by all stakeholders together with standardized formats for descriptions, their coding and communication.
- Automatic identification and rapid launch of automatic countermeasures and human interventions online and IRL, based on validated frameworks and methods.
- Targeted and coordinated research and development to provide systematic knowledge at a European level on all aspects of how to build resilience in vulnerable young people against online entrapment in violent extremism and terrorism.

4.4.2 THE FIRST COLUMN – THE INNOVATION

- **Description of the solution, i.e., the instantiation of the innovation to be considered.**
  The innovation **Identify and safeguarding vulnerable individuals**[63] has been transformed into a solution that **monitors the online environment, identifies where and how interventions are needed, thereafter launching the appropriate actions to build resilience in vulnerable young people against possible entrapment in violent extremism and terrorism**. The solution is called Gatekeeping ECHO chambers (GECHO).

[61] Webbpoliser, gaming och kontranarrativ: Digitalt förebyggande arbete mot extremism och våldsbejakande extremism

[62] The 15 solutions studied are: Gamen met de politie (the Netherlands), Les Promeneurs du Net & Web Citizen Training Program (France), Veebikonstaabel (Estonia), Counter Conversations (England), Seriously (France), Malmö – Trygg och säker digital stad (Sweden), Politiets Online Patrulje (Denmark), Politiets nettpatruljer (Norway), Project RETHINK, The Redirect Method, MoonShot, Islam-ist och Tränen de Dawa (Germany), Jamal al-Khatib, Extremkoll.se, Prevent Duty Training (England), streetwork@online, (Germany)

[63] See D3.4 First Mid Term Report on Improvement and Innovations, Section 4.3.2 p80.

GECHO is for countering violent extremism and terrorism, as antagonistic states and organizations may use support of local groups that promote violent extremism and terrorism as one tool in their hybrid threat toolbox. This to widen sociocultural cleavage and reduce trust in the society.

SCOPE: Building resilience in vulnerable young people against online entrapment in violent extremism and terrorism.

VISION: Young people will be resilient against online content that advocate, incite, promote or justify hatred, violence, terrorism and discrimination.

MISSION: Ensure that young people when traversing online environments promoting ideas of hate, violence, terrorism and discrimination also encounter, absorb and internalise content/information, which counter such ideas.

STRATEGY: Develop an EU standardized platform for (semi-)real-time surveillance and situational awareness of the violent extremism and terrorism online environment comprising a taxonomy for describing situational events and information together with standardize formats for their coding and communication. Enable sharing of situational data between stakeholders.

Develop AI based tools to quickly and accurately discover new sites, new visitors and changes in activity levels at known sites.

Develop easy to follow validated frameworks, methods and tools for creation of practical locally adaptable means for prevention of online recruitment of young people into groups promoting violent extremisms and terrorism.

Ensure that a research networking organization exists which promotes and coordinates required research efforts needed to better understand the drivers behind radicalization, to develop countermeasures and validate their impact.

Establish a systematic knowledge base and means for collecting and sharing of frameworks, methods, tools and research results in a searchable database. Liaise, cooperate and share information with existing practitioner networks.

Initiate training activities for first line practitioners to

1. Get to know the proposed frameworks, methods and tools presented, including online behaviour guidelines.
2. Understand the reasoning behind proposed countermeasures and interventions.
3. Become proficient in their use and how to adapt them to different online environments.

LIMITATIONS: Compared to the original innovation, this solution is limited in that it does not concern direct identification of vulnerable individuals as this most often would be in conflict with GDPR and that it is mainly targeting young people.

RATIONALE: Countering/Preventing violent extremism and terrorism is a wide area and concerns many aspects, but at the core it is about reducing the number of supporters and followers. One way of achieving this is to focus on the most vulnerable groups and counteract on their radicalization. As online platforms play an increasingly important role in the recruitment process and are abundant and easily accessed it is a logical consequence to spend substantial efforts in developing online countermeasures.

- **Added value proposition.**

NEED: There is a need to provide means to reduce the number of followers and supporters of groups that promote violent extremism and terrorism. This need is validated by the many initiatives from different global, EU and national organizations and networks working in the general area preventing/countering violent extremism and terrorism.

IMPACT: In GECHO, the proposed platform for surveillance and situational awareness will allow that countermeasures against recruitment into groups of violent extremisms and terrorism can be launched with high precision, earlier and more effectively than has been possible before. The proposed research will review existing, develop new, and validate efficient and rapid automatic countermeasures together with human intervention strategies. The proposed countermeasures will be integrated in frameworks for deployment in different extremism environments and have easily adaptable methods and tools to become fit for purpose. In the research one strand of actions is targeting a better understanding of drivers and what constitutes effective counter means.

VIABILITY: The viability of the GECHO surveillance and situational awareness platform solution can be deduced from activities in related areas like EEAS Stratcom activities around FIMI[64] and the development of a Disinformation Data Space (the DDS-alpha platform[65]). Another platform was proposed in the first cycle project cycle of EU-HYBNET, the CISAE for disinformation[66] which easily can be adapted for the current target area.

To ensure that a research networking organization would exists it could be possible to delegate this responsibility to an existing body e.g., the RAN (the Radicalization Awareness Network) or expand the VOX-pol network of excellence mandate. If judged more efficient a new networked research organization like EDMO, the European Digital Media Observatory (EDMO) could be initiated. EDMO is a Europe wide network built around a few core partner organisations and several national and regional hubs.

[64] EEAS Stratcom, 2022 Report on EEAS Activities to Counter FIMI. https://www.eeas.europa.eu/sites/default/files/documents/EEAS-AnnualReport-WEB_v3.4.pdf

[65] Innovation the DDS-alpha description can be found in D3.2.

[66] EU-HYBNET Deliverables D4.4 "*1st Innovation uptake, industrialisation and research strategy*" in CORDIS https://cordis.europa.eu/project/id/883054/results

- **Stakeholders and domains**

  GAPS AND NEEDS: The solution is related to the WP 2 defined gap and need *Promoted ideological extremism* in Core Theme *Information and Strategic Communications*, see D2.10. It is also related to Core Theme *Resilient Civilians, Local Level and National Administration.*

  CONCEPTUAL MODEL DOMAINS: The solution is related to the following domains:

  - Cyber,
  - Culture,
  - Social,
  - Legal,
  - Intelligence and
  - Information.

  STAKEHOLDERS: The core stakeholders of course are the Member States first line practitioners, e.g., social care workers, police, teachers and NGOs like RAN, that meet vulnerable individuals in danger of becoming radicalized. Furthermore, local level as well as support functions will be heavily involved in the monitoring of online activities and launch of countering activities. Finally, the research community and ministry level functions will have to be involved in providing resources to research, to develop countermeasures, and to build and maintain overarching situational awareness. The responsibility for the realization of the solution will lie on ministry level and the commission. Actors specialized in monitoring of online activities by violent extremism and terrorism groups as well as tech companies developing tool for such monitoring will also be important stakeholders.

4.4.3 THE SECOND COLUMN - SOLUTION DETAILS

- **Functional description**

  The functionality of the GECHO situational awareness platform is similar to that offered by the CISAE solution presented in D4.4. The core concept would be to have situational awareness entities in all participating Member State that share and exchange information in a common standardized format based on (extensions) to existing standards like STIX and TAXII.

  Monitoring of the online environment need to be supported by AI-based automatic and semi-automatic tools. Where these tools should be deployed, how the information is shared and how the analysis work is distributed needs to be agreed between the stakeholders to limit unnecessary duplication of efforts. The analysis work could be distributed or centralized and possibly be based on federated machine learning principles. To stimulate further developments, research and compile training sets for the AI based solutions taking GDPR requirements for anonymization into account.

  The ultimate objective of GECHO is to develop easy to follow validated frameworks, methods and tools for creation of practical means for timely and efficient prevention of online recruitment of young people into groups promoting violent extremisms and terrorism. To

make it become the powerful tool it should become, there is need for supporting research in several areas related to the factors influencing the radicalisation process:

a) The state-of-the-art of existing frameworks, methods and tools.
b) Methods used by groups promoting violent extremism in their online recruiting activities.
c) Relevant differences in cultural, language and community codes
d) What makes a person vulnerable
e) Frameworks, methods and tools for creation of practical means for prevention.
f) Methods for evaluation and validation of the effectiveness of countermeasures

To make the frameworks, methods and tools usable by the core stakeholders, the first line practitioners, there will also be a need to develop training material.

- **Operational description**

The development of the GECHO platform for surveillance and situational awareness would require the setup of a project organization to formulate detailed requirements and use of standards (or to be standardized formats) for information sharing. An integral part of the project would be to take care of the initial development of the AI-based tools required. A steering group of key stakeholders should oversee the project work. A possible driver for the platform development work could be EUROPOL.

The research and development of GECHO frameworks, methods and tools for creation of the practical means for recruitment prevention should start from the current state-of-the-art. Different components exist today but may need validation and/or updates to become more generic, others need to be developed; what is missing is the overarching framework – the creation of a systematic knowledge base with validated intervention means. The proposed way to proceed is to use an incremental, step-by-step approach in building the frameworks, the tools and methods. However, as the target arena is agile both in the way that the extremist groups behave and appear online, and in the development of knowledge and technology in countermeasure methods and tools continuous development and updates will be required. Also, for this research a project organization is required.

The GECHO solution will target stakeholders at different levels and with different application areas. Dissemination and training activities will be needed for the uptake of the developed working methods and tools.

There will be a need to guarantee continuous updates and developments of the GECHO solution it will be required that there is an organization for discussions on new requirements and a body of experts that regularly review the framework and its methods and tools and propose and implement updates and improvements. There will also be a need for updates of course material and teacher training.

- **Roadmapping**

The actions required for the industrialization of the solution and organize its uptake are:

- Set up a governance structure and body to define the final scope of the work. This body could be tied to EUROPOL or RAN or some other suitable existing organization. The governing body should include key representatives from existing P/CVE organizations and key stakeholder.
- Organize a stakeholders' forum which is tied to the governance structure to ensure adoptions of the GECHO solution as well as influence it's features and functionalities.
- Let the governance body define a detailed, evidence based, research program (see proposal of content above) supporting creation of practical means to prevent online recruitment of young people into groups promoting violent extremisms and terrorism.
- Organize funding for the required research and development projects. All types of stakeholders should be involved in the research activities, either in the actual research and development work or in project expert and reference groups.
- Organize EU funding for a permanent research cooperation community, possibly based on the same ideas that lies behind the establishment of EDMO[67].
- Based on the project results, the governance body should establish and publish recommendations and guidance documents for the developed frameworks, methods, and tools. Set up the searchable database for access to the published recommendations, guidance documents and research results.
- Define how maintenance, update and upgrades will be organized, define responsibilities and set up required bodies to perform the work.

4.4.4 THE THIRD COLUMN – THE RESOURCES

- **Required development resources**

  The roadmap proposes one or more EU finance projects to establish the required knowledge base and to develop the framework, methods, tools and training material. The required development resources for this part of the work will be researchers in P/CVE and related areas. We find it reasonable to start three, three-year 3 MEURO projects for these tasks, out of which one should be on AI tools and methods. The establishment of a more permanent research cooperation community, based on the same principles as for EDMO, would likely have a somewhat lower cost than the EDMO had and could be in the order of 4 MEURO. Extending it with satellite nodes as EDMO has, would be in the same order.

  The set-up of the governance body and to define the detailed, evidence based, research program following the proposed solution should not require any major resources.

  The work on local and regional levels with adaptations of the methods and tools will require involvement of local experts and admin personnel. It is hard to estimate the total efforts required before knowing what the framework, methods and tools will look like. But each adaptation task will most likely require efforts in the order of man-years.

[67] EDMO (European Digital Media Observatory) is EU funded and its mission is to bring together fact-checkers, media literacy experts, and academic researchers to understand and analyse disinformation, in collaboration with media organizations, online platforms and media literacy practitioners. https://edmo.eu/

- **Required operating support system**
  The governance body should ensure that a body is assigned which is responsible for required updates and upgrades of the solution to have it keep up with threat developments and to provide expected performance. This task would require close cooperation between central and local experts and authorities, possibly companies involved in developing the teaching material and the training apps. It is hard to estimate the total efforts required before knowing what the framework, methods, tools, and training material with their local adaptations will look like. But the update and upgrade work will most likely require efforts in the order of several man-years.

- **CAPEX & OPEX**
  Based on the descriptions of the requirements for development and operational resources we estimate that the CAPEX for the set-up of the organization and the initial research work would be in the order of 15 MEURO.

  The initial local adaptions would, if they require 1 - 3 man-years per Member State and end up to about in same order. The same effort would probably be needed for the continues updates and grades the coming years.

  The total cost to launch such a comprehensive action as proposed here would then be in the order of 30 MEURO over 3 - 4 years. Operating costs would, according to the estimates above, be of the same order, that is 3 – 4 MEURO per year but financed by each Member State.

4.4.5 THE FOURTH COLUMN – THE UPTAKE ENVIRONMENT

- **Competition and market**
  There are a great number of initiatives in the field of P/CVE and there are tools and training material available. However, there is no, as far as we understand, ongoing initiative with the vision and scope of the GECHO solution. Examples on ongoing initiatives in can be found in the setting the scene section.

- **Funding and organization of uptake and industrialization efforts**
  The roadmap points at that it must be an EU initiative behind the realization and development of the proposed solution and national support for the required local adaptations. The proposed coordinated work would most likely never take place without such an initiative and the required corresponding funding.

- **Barriers**
  Required actions that may became barriers in the work to realize the solution are:

  - To convince the EU that this is the right way to proceed. This should in general not be a barrier as P/CVE is high on the EU agenda.
  - To engage the MSs in the work and get them involved.

- To attract the right competencies and expertise for the required research and development activities
- To get acceptance from and liaise with already existing groups and initiatives in the area of P/VCE.
- To organize the funding of the research activities and the related local adaptations.

5 RECOMMENDATIONS

5.1 RECOMMENDATION 1: UPTAKE OF REVIEWED INNOVATIONS

In the scoping and development of the innovation uptake canvas for the four solutions

1. WINS
2. EESCM
3. MIMI
4. GECHO

we have not found any blocking issues. We thus recommend that the proposed solutions are promoted for uptake and industrialization.

5.2 RECOMMENDATION 2: PRIVATE SECTOR INVOLVEMENT

The solutions in this second project cycle as well as two of the innovations in the first project cycle rely heavily on access to different types of information. To get access to as much information as possible, the private sector should participate. The recommendation from the first project cycle is thus repeated here.

Set up an EU task force to conclude on how to enable participation by private sector in information sharing and analysis networks.

- How EU external ownership/control of assets should influence possibilities to participate.
- Trust issues in general.
- Barriers against sharing of secret or sensitive information

5.3 RECOMMENDATION 3: RESEARCH AND DEVELOPMENT OF SUPPORTING TOOLS FOR WINS

To make the WINS solution a practical and efficient tool to identify which information to share, supporting tools for handling the required base information about the CI entities, the formation of attack trees and the following sensitivity and risk analysis will be needed. It is thus recommended to start such research and development work.

5.4 RECOMMENDATION 4: CISAE STANDARDIZATION

This recommendation is a repetition of a recommendation from the first project cycle. We include it once again as it a proposed basis for the WINS solution. The recommendation is to develop and standardize a framework for the implementation of information sharing and analysis environments (CISAEs). Build the information sharing functionality on the EMSA CISE[68], solution. Define principles for how analysis functionality can be implemented and analysis results be shared. The work should cover

[68] Common Information Sharing Environment (CISE), http://www.emsa.europa.eu/cise.html

the needs for situational awareness in EU critical infrastructures and for monitoring and handling of disinformation campaigns. For further details se D4.4 [69]

5.5 RECOMMENDATION 5: RESEARCH AND DEVELOPMENT OF SUPPORTING TOOLS FOR EESCM

To make the EESCM solution a practical and efficient comprising the widened scope including services, geopolitical, cascading effects and other hybrid threats, tools and models have to be enhanced. The details of how to efficiently include the new scope in existing models has to be researched and developed. This to allow the EU and MS level policy makers to define extended policies that are supported with easy-to-follow frameworks, tools and training material.

5.6 RECOMMENDATION 6: EXTENSION OF DDS-ALPHA FUNCTIONALITY FOR SUPPORT OF MIMI

To enable a market-based sharing of IMII, the DDS-alpha platform needs to be extended with a service platform on top of DDS-alpha. This service platform should include DDS-alpha extensions for charging and service control.

5.7 RECOMMENDATION 7: DEVELOP A SHARING AND ANALYSIS PLATFORM FOR GECHO

Develop an EU standardized platform for (semi-)real-time surveillance and situational awareness of the violent extremism and terrorism online environment comprising a taxonomy for describing situational events and information together with standardize formats for their coding and communication. Enable sharing of situational data between stakeholders. The platform can be based on the CISAE principles proposed to be standardized in the first project cycle. An alternative route would be to use an extended DDS-alpha platform.

Develop AI based tools to quickly and accurately discover new sites, new visitors and changes in activity levels at known sites. In this work use of federated learning should be considered and how anonymization and GDPR requirements can be fulfilled. Furthermore, there is a need for research and compilation of training sets to guarantee that AI based solutions easily can be developed and tested.

5.8 RECOMMENDATION 8: ESTABLISH RESEARCH NETWORK WITH FOCUS ON GECHO NEEDS

The ultimate objective of GECHO is to develop easy to follow validated frameworks, methods and tools for creation of practical means for timely and efficient prevention of online recruitment of young people into groups promoting violent extremisms and terrorism. To make it become the powerful tool

[69] EU-HYBNET D4.4 "*1st Innovation uptake, industrialisation and research strategy*" in CORDIS https://cordis.europa.eu/project/id/883054/results

it should be, there is a need for supporting research in several areas related to the factors influencing the online radicalisation process:

a) Review state-of-the-art of existing frameworks, methods and tools to prevent radicalization.
b) Methods used by groups promoting violent extremism in their recruiting activities.
c) Relevant differences in cultural, language and community codes
d) What makes a person vulnerable
e) Frameworks, methods and tools for creation of practical means for intervention and prevention.
f) Methods for evaluation and validation of the effectiveness of countermeasures.

6. LESSONS LEARNED

We have found that the framework methodology developed in the first project cycle with roadmapping and an innovation uptake canvas still represents a valid procedure to base the T4.2 work on. However, its use could be simplified if some of the difficulties experienced (see below) could be remedied.

Once again, we note that Innovation descriptions received from WP3 need to better cover State-of-the-Art. Furthermore, EU activities and initiatives related to the scope of an innovation has to be accounted for. The innovation descriptions should also be more specific in scope and more clearly indicate what is new functionality compared with existing solutions. The already proposed innovations from earlier project cycles should be referenced, to not invent the wheel again.

It would have been great if T4.3 and T3.2 would have provided a sound baseline for the setting the scene sections in the solutions descriptions. Now this work had to be done in T4.2 as we had to ensure that we didn't propose something which (almost) already exist. The evaluation of the innovations should also review this aspect.

Another important lesson is that to review, evaluate and synthesize solutions and propose appropriate uptake strategies, there is a need to have area experts participating and contributing in the work. In this cycle the need has partly been fulfilled by review of the resulting uptake canvases.

There is also a need to establish a stricter and more well-defined procedure for how to select the innovations to review for uptake strategies. The selection influences the possibility to achieve defined KPI's.

And finally, the format of the innovation canvas should be used when innovations are described. This means that the template for innovation descriptions produced by Task 3.1 should be replaced by or reformulated according to the innovation uptake canvas. Having one common way of describing innovations would simplify the interactions between WP3 and WP4 and make it more efficient.

The very last remark is that the project partners and persons involved in the Task 4.2 work in this second cycle have been very committed and have contributed their expertise in a most productive way. Special thanks also to the coordinator and the Innovation manager for their contributions and guidance and also to all expert reviewers. Finally, special thanks to Lisa Kaati at Stockholm University for providing valuable input to the scoping of the GECHO solution.

7. CONTRIBUTIONS TO PROJECT OBJECTIVES AND KPI'S

The D4.4 deliverable contributes to some of the overall Project Objectives (OB) defined in the DoA. In the Table 3 the most significant contributions related to OBs and their relevant Key Performance Indicators (KPI) are listed.

Table 3. Task 4.2 contributions to EU-HYBNET objectives.

OB2: To define common requirements that can fill knowledge gaps, deal with performance needs, and enhance capabilities of research, innovation and training endeavours concerning hybrid threats			
Goal		**KPI description and target value**	**Contribution by Task 4.2**
2.2	To define innovations that can overcome the identified gaps and needs in certain focus areas in order to enhance practitioners (priority), industry, SME and academic actors' capabilities	Innovations and innovative solutions (technical and human science based) are detailed in relation to Goal 2.1 above Targets: -At least 3 innovative solution possibilities are defined in relation to each of the four project core themes and fed into the EC procurement process	In this second project cycle, four innovations, with relations to three of the four project core themes, have been reviewed and uptake strategies proposed. So far, we have 1 core theme with 3 innovations, 2 core themes with 2 innovations and 1 core theme with 1 innovation
2.4	To develop a roadmap of the requirements for on-going research and innovation necessary to build the preferred system of the future for confronting hybrid threats	Details of a roadmap containing suggested key focus research/ innovation areas and actions for the future are described Targets: -At least 5 suggestions are put forward yearly on new research and innovation possibilities and compiled into a final roadmap at project's end	In this second project cycle the work has been focussed on roadmapping for the four innovations reviewed. For these innovations, this report includes roadmap / uptake strategies which deals with procurement issues, barriers and aspects that need to be further researched
OB3: To monitor developments in research and innovation activities as applied to hybrid threats			
Goal		KPI description and target value	Contribution by Task 4.2
3.2	To monitor significant developments in technology that will lead to recommending solutions for European actors' gaps and needs	Monitor existing innovations addressing gaps and needs; incl. areas of knowledge/performance Target: -At least 4 reports every 18 months that address technological innovations that are able to fulfil European actors' gaps and needs	In this second project cycle the work has been focussed on monitoring the technical development required for uptake and industrialization of the four innovations that have been under review. The findings will be part of the corresponding strategies for uptake and industrialization

OB4: To indicate priorities for innovation uptake and industrialisation and to determine priorities for standardisation for empowering the Pan-European network to effectively counter hybrid threats			
Goal		KPI description and target value	Contribution by Task 4.2
4.1	To compile recommendations for uptake/industrialisation of innovation outputs (incl. social/non-technical); and provide opportunities for greater involvement from public procurement bodies upstream in the innovation cycle	Appraise best innovations (technical/human science based) for standardisation and innovation uptake, especially industrialisation and procurement. Targets: - At least 3 reports targeting areas for improvement (potentially ground-breaking innovations mapped on gaps and needs) - A list of final recommendations for procurement /industrialization.	The innovations analysed for uptake and industrialization in this second project cycle belong to the group of innovations appraised to have major impact in reducing risks in connection with hybrid threats and attacks. They are mapped to gaps and needs in three of the project core themes.
4.2	To deliver a strategy for innovation uptake and industrialisation based on innovation standardisation needs among practitioners in the same discipline	A strategy on innovation uptake & industrialisation including most innovative solutions is developed. Targets: -At least a report every 20th month on innovation uptake -A strategy for innovation uptake and industrialisation is delivered.	For the four innovations reviewed for uptake and industrialization in this second project cycle, strategies for uptake and industrialization are proposed. Common aspects are noted and are part of the basis for generalized strategies/recommendations.

8. THE THREE LINES OF ACTION

The EU-HYBNET consortium decided on request of the EC to also report on three Lines of Action. Each deliverable therefore states its contribution to these three Lines of Action in order to highlight the importance of the work conducted in the deliverable to the whole success and proceeding of the project. In Table 4, the D4.5's contribution to the three Lines of Action is provided.

Table 4. Deliverable 4.4 contribution to Lines of Action

Lines of Action	D4.4 contribution
Monitoring of research and innovation projects with a view to recommending the uptake or the industrialisation of results.	Task 4.2 has drawn from the work of WP3 which was responsible for the identification of solutions, innovations, research, and innovation projects that might have potential to help counter hybrid threats. As such Task 4.2's work is founded on this Line of Action and builds on it for its review of the selected innovation projects that are recommended for uptake and eventually exploited by the EU and its member states to improve their resilience against hybrid threats.
Common requirements as regards innovations that could fill in gaps and needs.	Based on its review of the proposed innovations Task 4.2 proposes that the State-of-the-Art is collected and summarized for the by Task 3.1 identified and prioritized target areas (1) Citizen and Governmental Resilience, (2) Critical Infrastructure and Flows, (3) Disinformation, and (4) Cyber and Quantum security. In this second project cycle, T4.2 collected State-of-the-Art information relevant for the four selected innovations recommended for industrialization and uptake.
Priorities as regards of increasing knowledge and performance requiring standardisation.	Based on its current and earlier work Task 4.2 proposes that - The CISAE framework is standardized by ETSI to enable broad adoption and industrialization of the solution(s) - Image, video and audio formats to be used by tools for detection of digitally modified or generated content are standardized to allow easy integration in media consumption applications. - The standardizations work performed in the Coalition for Content Provenance and Authenticity is supported to provide an efficient solution for identifying authentic content. - Develop a standardized taxonomy for describing situational events and information related to online violent extremism and terrorism. - Standardize coding and communication for sharing of events and information related to online violent extremism and terrorism.

9. CONCLUSIONS

9.1 SUMMARY

In this second project cycle we have applied the methodology on four innovations representing three of the project core themes and innovation canvases have been produced. Furthermore, recommendations for the uptake of all four solution proposals are stated together with recommendation for initiation of related research, standardization and update of EU initiatives and actions.

9.2 FUTURE WORK

In the next project cycle, the methodology will once again be reviewed and updated according to the outcome of the review. The updated methodology will then be used to assess new innovations assessed and recommended by WP3. In this upcoming review round the standardisation aspects documented in the upcoming Task 4.3 deliverable D4.9, First report for standardisation recommendations, will be studied and taken into account.

ANNEX I. GLOSSARY AND ACRONYMS

Table 5 Glossary and Acronyms

Term	Definition / Description
CAPEX	Capital Expenditure
CIP	Critical Infrastructure Protection
CISAE	Common Information Sharing and Analysis Environment
CIWIN	Critical Infrastructure Warning Information Network
CTI	Cyber Threat Information
DebunkEU	Debunk EU is an independent technological analytical centre and an NGO, whose main task is to research disinformation in the public space and execute educational media literacy campaigns
DoA	Description of Action
DTAG	Disruptive Technology Assessment Game
EDMO	European Digital Media Observatory
EEAS	European External Action Service
ENISA	European Union Agency for Cybersecurity
EU	European Union
IPR	Intellectual Property Right
JP	Joint Procurement
KPI	Key Performance Index
MISP	Open Source Threat Intelligence Platform & Open Standards For Threat Information Sharing (formerly known as Malware Information Sharing Platform)
OPEX	Operating Expenditure
EUvsDiSiNFO	https://euvsdisinfo.eu/about/
PCP	Pre-Commercial Procurement
PPI	Public Procurement of Innovation
SME	Small and Medium Enterprise
STIX	Structured Threat Information Expression is a language and serialization format used to exchange cyber threat intelligence.
SWOT	Strength, Weaknesses, Opportunities and Threats
TAXII	Trusted Automated Exchange of Intelligence Information. An application protocol for exchanging CTI over HTTPS

ANNEX II: THE METHODOLOGY FRAMEWORK

The major component in the methodology framework for strategy creation builds on the use of an innovation uptake canvas and roadmapping developed and defined by Task 4.2. The ideas behind the innovation uptake canvas are based on the findings in Section 2.1. The roadmapping and the innovation uptake canvas is presented below. Both the canvas and the roadmapping approaches are designed to be used for assessment of uptake possibilities and identification of barriers for uptake.

The uptake canvas covers relevant practical aspects to be considered when analysing the conditions for uptake and industrialization while the roadmapping focusses on scoping the innovation and defining a vision, mission and strategies for making it happen. By combining these two approaches it is possible to identify the key aspects for uptake and industrialization and at the same time identify barriers, such as required standardization efforts, new regulations, ethical issues, etc. The work with the canvas and the roadmap proceeds in parallel, the canvas and the roadmap are not independent entities, just two different views of the same problem.

We will use the innovation uptake canvas to present the outcome of the analysis of an innovation.

ANNEX II.1 ROADMAPPING

Roadmapping is the strategic process of determining the actions, steps, and resources needed to take the initiative from vision to reality. But as stated by ProductPlan[70] "Roadmapping is often mistakenly understood as the act of drafting a roadmap. A critical output of roadmapping work will indeed be a roadmap. But a roadmap is a high-level document that articulates the vision and strategic plan. The process of developing a roadmap involves much more strategic thinking and research than what will ultimately appear on the record." A vision and a strategy for how it can be achieved is what is needed in order to deliver a serious assessment of an innovation's uptake and / or industrialization possibilities and barriers.

The basic principle for developing a roadmap is to define the current state of affairs and the wanted state and then analyse and plan the needed actions, steps and resources required for reaching the target state. Ideally, a good roadmap should, according to roadmunk[71] effectively communicate the following strategic pieces:

- Strategic alignment: Why (and how) the initiatives align with higher-level operational goals.
- Resources: How the goals can be reached and what resources are required to achieve them.
- Time estimates: When any important deliverables are due.
- Dependencies with other efforts.

To serve our purpose as a tool for developing an innovation uptake and industrialization strategy, the roadmap should, following Don Hofstrand[72] contain:

[70] Productplan, What is roadmapping. https://www.productplan.com/learn/roadmapping/
[71] Roadmunk, Why Roadmap, https://roadmunk.com/guides/roadmap-definition/.
[72] Don Hofstrand, Vision and Mission Statements -- a Roadmap of Where You Want to Go and How to Get There. https://www.extension.iastate.edu/agdm/wholefarm/html/c5-09.html

Scope: Who are the intended users of the innovation (citizens, practitioners, etc)

Vision: The big picture of what you want to achieve; Which services and functions to make available to the intended users.

Mission: A general statement of how the vision will be achieved; How services and functions are delivered and used.

Strategies: A series of ways of using the mission to achieve the vision; The preferred and required ways/steps to realize the services and functions.

When developing the strategies in the roadmap, all the factors discussed in Section 2.1 on uptake frameworks are relevant.

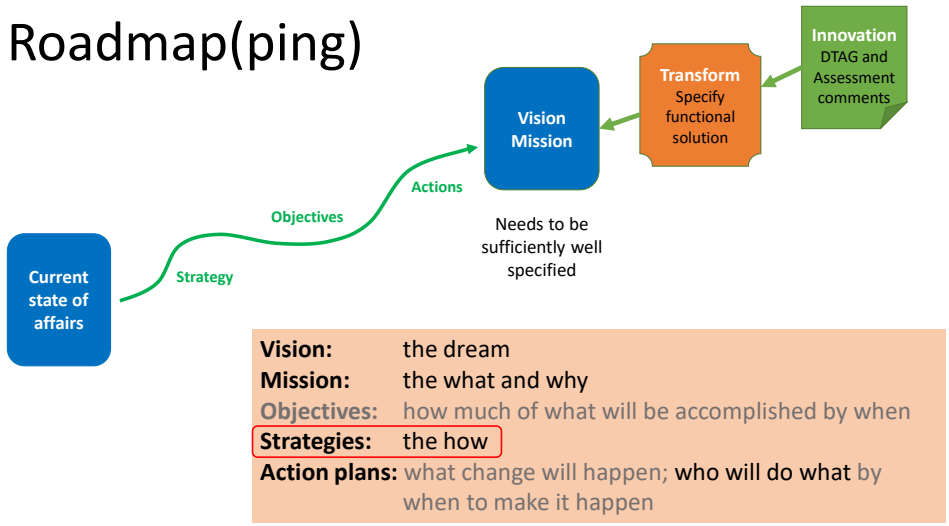


Figure 7. An illustration of the components in a roadmapping exercise of a selected innovation

We note in particular that to perform an analysis of the possibilities for uptake and industrialization of an innovation, its service offering together with the intended users and their needs has to be well defined. There must be a clearly stated vision for what services the innovation should deliver to whom and how. Thus, we find that roadmapping is an essential part of our and any other analysis of possibilities and barriers for innovation uptake and industrialization.

ANNEX II.2 THE INNOVATION UPTAKE CANVAS

The innovation uptake canvas is depicted in Figure 8. The canvas is the result of our research into how to assess and review innovations and is tailored to the EU-HYBNET needs and goals. The canvas has four columns, each covering three important aspects when reviewing the possibilities for innovation uptake and/or industrialization. The first column describes the scope of the innovation, its merits in countering hybrid threats and the involved stakeholders. The second column describes the technical and operational aspects relevant for understanding implementation requirements. The third column depicts the required resources for its implementation and operation. Finally, the fourth column deals with the uptake environment, funding and barriers which are important aspects when assessing uptake possibilities. The canvas is described in detail in the following sections. The canvas is intended to

describe issues relevant both for understanding the benefits of the solution and its implementation and use.

Figure 8. The innovation uptake canvas

ANNEX II: 2.1 THE FIRST COLUMN – THE INNOVATION

- **<u>Description of the solution, i.e., the instantiation of the innovation to be considered</u>.**
  This box shall contain a description of the solution under scrutiny. **The solution shall have a clear scope, vision, mission and high-level strategy**. The solution may, if required, have a narrower scope than the original innovation proposal to make assumptions regarding implementation clearer. Aspects to consider:
  - The solution should be easily identified as of great concern and high importance.
  - Which (aspects of) hybrid threats the solution covers and its advantages and its limitations.

- **<u>Added value proposition.</u>**
  This box shall describe:
  - Why this solution is needed and how it will it benefit practitioners and/or end users.
  - The expected impact of using the solution.
  - The effectiveness of the solution in handling the problem at hand.
  - The viability of the proposed solution.

- **<u>Stakeholders and domains</u>**
  This box shall contain information (fetched from the innovation description but adapted to the scope of the solution) on the:

- Coverage of identified EU-HYBNET Gaps and Needs according to D2.9[73].
- Target JRC domains; Is the solution domain specific or does it apply to a wider sector?
- Benefitting practitioners and end-users (NGO's, private citizens, private companies, media outlets, police, firefighting departments). Are the benefitting organizations aligned with respect to goals, objectives and support of the idea?

ANNEX II: 2.2 THE SECOND COLUMN - SOLUTION DETAILS

- **Functional description**

  This box shall provide a high-level overview of the main functional, procedural and, if a technical innovation, technical components in the solution and how these components interact with users/actors, information sources, sinks and storage in solution internal and external systems / procedures.
  - Which components have to be developed? Which components are off-the-shelf?
  - Are there requirements for interoperation with legacy or other systems?

- **Operational description**

  This box shall provide a high-level overview of how the solution should be introduced for the intended users and integrated (if possible) in their operational environment.
  - Describe the main procedural and human/social aspects to be considered.
  - Describe the requirements for the integration in an organization and/or processes for the set-up of an operational environment. Can resistance from practitioners and end-users be expected due to possible changes of processes or needed introduction of new processes?
  - Review other preconditions for implementation (training, organizational changes, etc).

- **Roadmapping**

  The vision, mission and high-level strategies for the realization of the solution are described in the "Description of the solution" box in the first column of the canvas. This roadmapping box shall describe which maturity level the solution and/or its components exhibit and provide the key actions in the roadmap with details on actions needed, their complexity, and the time required for performing them and to implement a working system.
  - What is the time to market? Discuss the maturity level of key components in the solution.
  - Can a clear specification of the solution be given, based on current knowledge or would this require a substantial effort?
  - Can the solution be used immediately or must it be introduced gradually? Is the solution already tested in an operational environment?

[73] EU-HYBNET Deliverable 2.9 "Deeper Analysis, delivery of short list of gaps and needs]", JRC, October 2020

ANNEX II: 2.3 THE THIRD COLUMN – THE RESOURCES

- **Required development resources**
  This box shall provide estimates on required resources for development, introduction and integration of the solution and how they can become available.
  - Are there or could supply chain issues occur?
  - Will all technical components be available?

- **Required operating support system**
  This box shall provide information on required continuous updates and upgrades of the solution for it to keep up with threat developments and/or to provide expected performance.
  - Who will operate, maintain, update, and upgrade the solution?
  - Review possible cyber security issues to be considered.
  - Review the solution robustness against attacks and changes in threat vectors.

- **CAPEX & OPEX**
  Describe the required resources for the introduction, integration and operation of the solution and how they can become available. We note that this is a complex activity and should be built upon concrete plans to give best estimates. For most innovations this will not be possible and a second best approach would be to base the estimates on comparisons of costs of known similar activities.
  - What are the expected costs (development cost, capital expenditure and operational expenditure) for bringing the innovation into a practically usable technical and operational solution?
  - Has a trustworthy cost/benefit analysis been performed?

ANNEX II: 2.4 THE FOURTH COLUMN – THE UPTAKE ENVIRONMENT

- **Competition and market**
  This box shall describe competing solutions, their maturity level, benefits and drawbacks. Verify the solution's advantages. Review the market situation (if one exists).
  - List the type of solutions that exist on the market and try to address the same need.
  - Why are these solutions not considered adequate? Is there a solution with a dominant "market" share? Is the "industry" characterized by intense competition?
  - Do other business opportunities exist for the solution?
  -
- **Funding and organization of uptake and industrialization efforts**
  This box shall describe the preferred way to organize and fund the development, introduction and integration of the solution.
  - Describe required development and/or implementation resources.
  - Indicate possible solution providers.
  - Have end-users confirmed their interest and have any willing early adopters been identified?
  - Describe the funding opportunities. Will funding constitute a stumbling stone?

- **Barriers**

This box shall review and describe any procedural, regulatory, legal, ethical, financial or procurement issues related to the use and implementation of the solution. Other dependencies should be noted.

- Note any IPRs related to the innovation.
- Is the implementation of this innovation dependent in any respect on the introduction of other innovations?
- Are there any important tasks or decisions that remain to be made before uptake of the solution can start?
- Is there a need for standardization for interoperability to make it useful and/or used across several practitioners?
- Will society accept the consequences of the innovation being implemented? Are there ethical issues to be considered, see section 2.2.2.