EU-HYBNET

FIRST REPORT ON STRATEGY FOR INNOVATION UPTAKE, INDUSTRIALISATION AND RESEARCH

DELIVERABLE 4.4

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

D4.4 FIRST REPORT ON STRATEGY FOR INNOVATION UPTAKE, INDUSTRIALISATION AND RESEARCH

Deliverable number	**D4.4**	
Version:	**V1.0**	
Delivery date:	**29/9/2021**	
Dissemination level:	**Public**	
Classification level:	**Public**	
Status	**Ready**	
Nature:	**Activity report**	
Main authors:	**RISE** **KEMEA**	**Rolf Blom** **Maria Kampa**
Contributors:	**L3CE** **PPHS** **Laurea** **UiT**	**Edmundas Piesarskas** **Bartoz Kozuch** **Isto Mattila, Päivi Mattila** **Gunhild Hoogensen-Gjorv**

DOCUMENT CONTROL

Version	Date	Authors	Changes
V01	2021-02-14	Rolf Blom	Report skeleton
V02	2021-04-20	Maria Kampa	Methodology included
V03	2021-06-07	Rolf Blom	Included definition of non-technical innovations
V04	2021-07-12	Rolf Blom	Updated ToC. Update of introduction, etc
V05	2021-08-05	Maria Kampa, Rolf Blom	Update and inclusion of some new material
V06	2021-08-08	Rolf Blom	Innovation canvases added
V07	2021-08-22	Rolf Blom, Edmundas Piesarskas, Bartoz Kozuch	First complete draft
V08	2021-09-08	Rolf Blom, Maria Kampa	Version for internal review
V0.81	2021-09-09	Isto Mattila	Review and comments for final editing
V0.82	2021-09-19	Päivi Mattila	Review and comments for final editing
V0.83	2021-09-27	Gunhild Hoegensen-Gjorv	Review and comments for final editing
V09	2021-09-28	Rolf Blom	Update after review
V1.0	2021-09-29	Päivi Mattila	Final Review and submission of the D4.4 to the EC

DISCLAIMER

Every effort has been made to ensure that all statements and information contained herein are accurate; however, the Partners accept no liability for any error or omission in the same.

This document reflects only the view of its authors and the European Commission is not responsible for any use that may be made of the information it contains.

EXECUTIVE SUMMARY

This deliverable (D4.4) is the first 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 main focus of the activities in Task 4.2 during this first project cycle has been to develop a methodology framework for creation of innovation uptake and industrialization strategies and test how well the methodology achieves its objectives. The conclusion is that the framework is fit for purpose.

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 and building resilience against disinformation campaigns. In both areas we have seen a need for improving (near) real-time situational awareness to enable timely responses and mitigating actions. To be effective, such responses and actions require cooperation between different stakeholders; stakeholders in one or different member states, stakeholders in the public and private sectors, and that the stakeholders have a common view of the situation at hand. The studies have also revealed that new fully or semi-automatic analysis tools will be required to cope with the increasing amount of information that has to be monitored, scanned and analyses for suspicious activities and/or attacks. As sharing of information may be sensitive, federated machine learning may be one avenue to implement efficient analysis tools without compromising required secrecy of monitored data and events.

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, needed standardization activities and updates of EU initiatives and actions to cover the proposals for increased societal resilience.

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 (D4.4) as a report on “Defining a concrete strategic approach for innovation uptake, industrialisation and research”.

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.

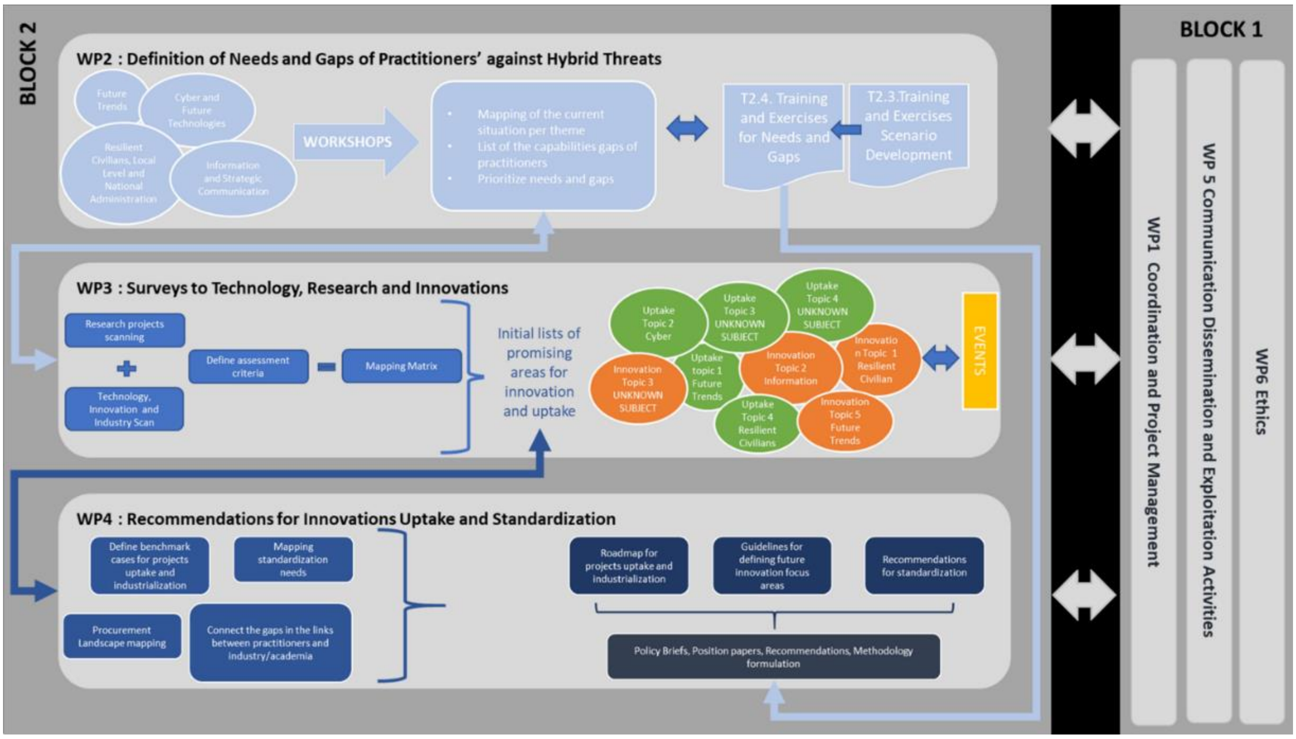

BLOCK 2
BLOCK 1
WP2 : Definition of Needs and Gaps of Practitioners' against Hybrid Threats
Future Trends
Cyber and Future Technologies
Resilient Civilians, Local Level and National Administration
Information and Strategic Communication
WORKSHOPS
Mapping of the current situation per theme
List of the capabilities gaps of practitioners
Prioritize needs and gaps
T2.4. Training and Exercises for Needs and Gaps
T2.3.Training and Exercises Scenario Development
WP3 : Surveys to Technology, Research and Innovations
Research projects scanning
Technology, Innovation and Industry Scan
Define assessment criteria
Mapping Matrix
Initial lists of promising areas for innovation and uptake
Uptake Topic 2 Cyber
Uptake Topic 3 UNKNOWN SUBJECT
Uptake Topic 4 UNKNOWN SUBJECT
Innovation Topic 3 UNKNOWN SUBJECT
Uptake topic 1 Future Trends
Innovation Topic 2 Information
Innovation Topic 1 Resilient Civilian
Uptake Topic 4 Resilient Civilians
Innovation Topic 5 Future Trends
EVENTS
WP4 : Recommendations for Innovations Uptake and Standardization
Define benchmark cases for projects uptake and industrialization
Mapping standardization needs
Procurement Landscape mapping
Connect the gaps in the links between practitioners and industry/academia
Roadmap for projects uptake and industrialization
Guidelines for defining future innovation focus areas
Recommendations for standardization
Policy Briefs, Position papers, Recommendations, Methodology formulation
WP1 Coordination and Project Management
WP 5 Communication Dissemination and Exploitation Activities
WP6 Ethics

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

1.2 OBJECTIVES OF TASK 4.2

Building on the results of WP2 and WP3, Task 4.2 will define a concrete strategic approach for innovation uptake and industrialisation. The strategy will cover the four project core themes. The task will review benchmark cases for innovation uptake in other sectors based on Task 4.1 results and assess them to understand the mechanisms behind good practices and where pitfalls may occur. Then, based on the gaps and ongoing research and industrial development as identified by Task 3.1 and Task 3.2, a strategy for innovation uptake will be formulated. For each project cycle an innovation uptake strategy for the most promising areas will be developed. Special attention will be given to innovation procurement, as it is a crucial step towards breaching the gap between the buyers group and the industry. Furthermore, the most promising areas for future Pre-Commercial Procurements (PCPs) or Public Procurement of Innovations (PPIs) will be identified. Roadmaps will be developed, including timeframes, actors and recommended procedures to be followed.

In addition to the strategy for innovation uptake, industrialization and research, the 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 WP4 tasks.

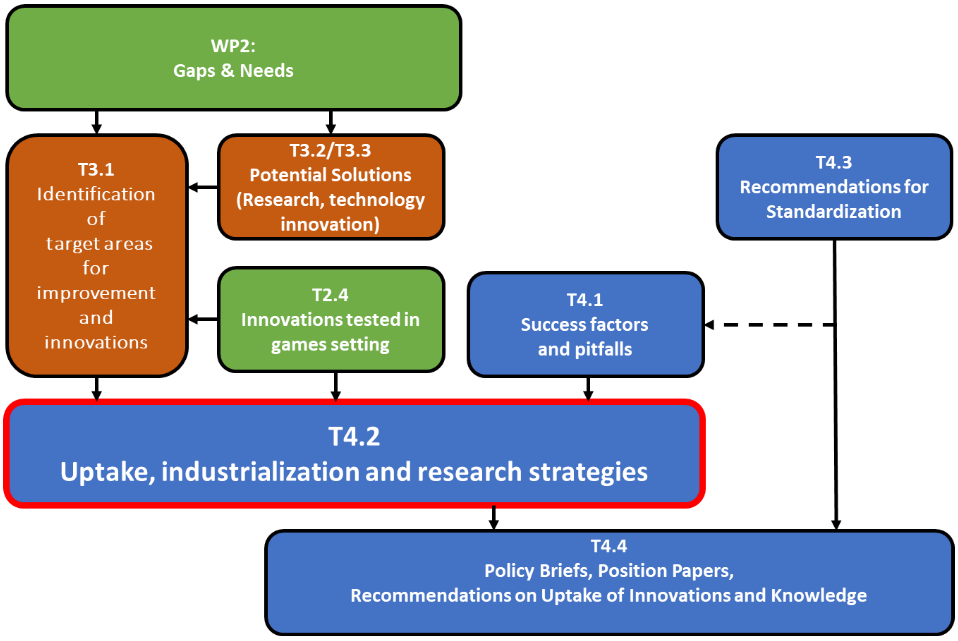

WP2:
Gaps & Needs
T3.1
Identification of target areas for improvement and innovations
T3.2/T3.3
Potential Solutions (Research, technology innovation)
T2.4
Innovations tested in games setting
T4.1
Success factors and pitfalls
T4.3
Recommendations for Standardization
T4.2
Uptake, industrialization and research strategies
T4.4
Policy Briefs, Position Papers,
Recommendations on Uptake of Innovations and Knowledge

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

1.3 TASK FOCUS AND ACTIVITIES IN FIRST PROJECT CYCLE

The main focus of the activities in Task 4.2 during the first project cycle has been to develop the methodology framework for creation of innovation uptake and industrialization strategies and a test of how well the application of the framework methodology achieves the task objectives (the methodology is used to analyse innovations assessed by Task 3.1). This prioritization of work was due to the fact that there were limited resources available for the task efforts and that the development of the methodology framework itself is a major task, which then leads to that less resources are available for the actual analysis of innovations and development of strategies.

It is also worth noticing that although this is not a research project, the tasks in some aspects outpace the research, because some of the project themes and tasks are in themselves quite innovative and do not have a lot of data to offer yet. Therefore, we in some cases do not have extensive information and data to build upon in this first project cycle. Furthermore, the project relies on external research, i.e., externally funded research initiatives, to produce the required data for the tasks.

Furthermore, it was judged to be prudent to use this first project cycle as a test run of the defined methodology. This test run was conducted to establish how suitable and convenient the methodology is to use and to understand which modifications that may be required for the next cycles to make it more efficient and to the point.

The activities conducted in the work to develop strategies for innovation uptake, industrialization and research comprise:

- A review of existing innovation uptake and industrialization frameworks.
- Development of methodology framework for review of innovations with respect to uptake and industrialization possibilities and required research in four dimensions:
    - The scope of the innovation.
    - The defining details of the solution.
    - The required resources.
    - The uptake environment.
- Selection of four Innovations representing the four EU-HYBNET core themes based on
    - The assessments of available innovation descriptions performed by Task 3.1 as described in D3.1, First interim report mapped on gaps and needs [2].
    - The outcome of the trainings (DTAGs) performed by Task 2.4 described in D2.20, Training and exercises delivery on up-to-date topics, [3].
- Application of the framework methodology 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 D3.1 [2].
        - The review of ongoing research and industrial development performed by Task 3.3 and documented in D3.7, First Report on Innovation and Research Project Monitoring, [3].
        - The uptake success factors and the pitfalls/barriers collected and described by Task 4.1 in D4.1, 1st report on the procurement environment, [5].
    - Input provided by Consortium experts during dedicated workshops.
- Presenting the uptake strategies for the four selected innovations and describing barriers, required research and recommended funding solutions in this D4.4

1.4 SOME DEFINITIONS

All definitions in this section, except for the one of Innovation, are copied from D4.1 [5].

1.4.1 HYBRID THREATS

Hybrid threats aim to exploit a country's vulnerabilities and often seek to undermine fundamental democratic values and liberties [6]. 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 [1].

According to the Joint Framework on Countering Hybrid Threats [6], 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.

1.4.2 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 [7], the term practitioners refer to Law Enforcement Agencies. Law enforcement agencies are organisation who respond to, detect, and prevent crime. Within this 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 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.

1.4.4 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 [8], 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.

1.4.5 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.

1.4.6 INNOVATION PROCUREMENT

According to the European Commission's Guidance on Innovation Procurement [9] 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 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.

1.4.7 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.

1.5 STRUCTURE OF THE DELIVERABLE

This document includes the following sections:

- Section 1, Introduction: In this section we introduce the task objectives, the focus of work in the first project cycle and some definitions.
- Section 2, Background on strategies for innovation uptake and industrialization: In this section we present the results from our state-of-the-art in assessing innovations.
- Section 3, The methodology framework: In this section we describe how innovations are reviewed with respect to possibilities for uptake and industrialization.
- Section 4, Innovations selected for review. In this section we describe the reasoning behind the selection of innovations to be reviewed.
- Section 5, Scoping and analysis of selected innovations. In this section we describe the solutions proposed corresponding to the reviewed innovations in the format innovation uptake canvases.
- Section 6, Recommendations. In this section we present recommendations for initiation of research, standardization and updates of EU initiatives and actions.
- Section 7, Lessons learned: In this section we present our lessons learned from the work during the first project cycle and discuss means to improve cooperation and efficiency in the project.
- Sections 8, Contributions to project objectives and KPI’s: In this section we present a table containing our contributions.
- Section 9, The three lines of action: In this section we present a table containing our contributions to the three lines of action.
- Section 10. Conclusions: In this section we present our overarching conclusions and discuss the future work.

2 BACKGROUND ON STRATEGIES FOR INNOVATION UPTAKE AND INDUSTRIALIZATION

The methodology framework shall provide 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.

To set a solid foundation for the development of the methodology framework, a state-of-the-art review of innovation evaluation schemes has been performed. A number of methodologies have been examined and have been taken into account in the formulation of the final methodology framework. The Consortium has invested a significant effort in this development work.

In this section, we summarize the findings of our state-of-the-art review for innovation, industrialization and research strategy creation. We also discuss success factors and possible barriers. In Section 3, our methodology for innovation, industrialization and research strategy creation is described. It is based on roadmapping and a canvas approach and it was developed to serve the specific needs of the EU-HYBNET.

2.1 UPTAKE FRAMEWORKS EXAMINED

Many theoretical frameworks seek to describe the dynamic process of the uptake (adoption and/or implementation) of innovations.

The purpose of the first step of Task 4.2 was to examine different types of studies and to assess the applicability of their findings in the scope of the project. For this review, the first theories to be examined were related to how innovation adoption works and the parameters that could affect it.

In the context of EU-HYBNET project and for the purpose of delivering the uptake strategy of the most promising innovations, several theories were examined. These theories helped the task participants to conclude with the framework that served the needs of the project. In the paragraphs below, the examined frameworks are analysed, providing the advantages and disadvantages for each one of them.

2.1.1 THE INNOVATION ADOPTION PROCESS

Following the reasoning in [10] the innovation adoption process, as a rule, begins with the acknowledgment that a need exists and then is driven by the procedure of looking for solutions. Following this stage, the process of testing the actual selection takes place and finally there is the genuine choice to proceed with the implementation of the solution. There are a few methodologies that one can draw upon to study the adoption process. The stages of the adoption process are:

- The initiation (pre-adoption) stage. The activities associated with perceiving a need, searching for answers, gaining knowledge or understanding of existing innovation, creating an initial attitude toward it, and proposing innovation for adoption are all included in the initiation (pre-adoption) stage. The adoption decision stage entails deciding whether or not to accept the suggested idea by assessing the desired solution from a practical, strategic, financial, and/or technological standpoint, as well as dedicating resources for its purchase. Top managers widen their perceptions of an innovation at this level to determine whether it will help the organization achieve its goals and objectives.

- The implementation (postadoption) stage entails activities such as altering the innovation, preparing the organization for its widespread usage, conducting a trial to check its validity, and providing an organization's and its employees' acceptance of the innovation. The plain conceptualization of the innovation adoption process is illustrated in Figure 3 and seems to be the most representative approach of the models presented in the literature.

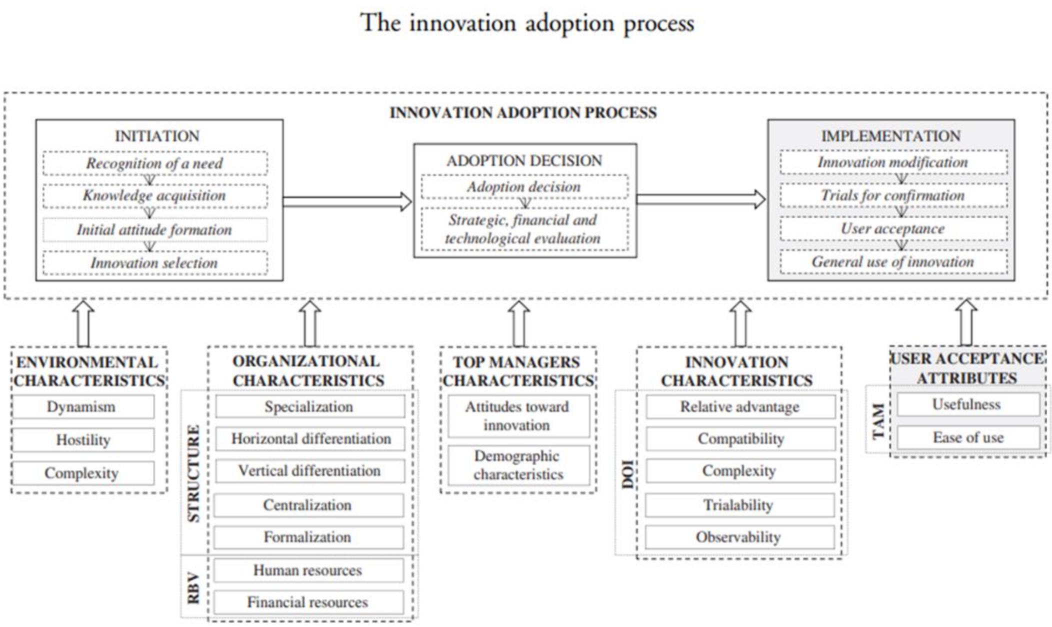


Figure 3. Conceptual framework for the determinants of the innovation adoption process

Pros: The framework provides a good overview for the aspects that can affect the adoption of innovation from an organisational perspective.

Cons: It focuses only on internal factors.

2.1.2 THE TOE FRAMEWORK

To develop an innovation adoption plan, one must first assess the aspects that may influence the adoption process. A framework on the technological innovation decision-making process was established by Louis Tornatzky and Mitchell Fleischer in [11]. It describes the entire innovation process, from the development of innovations by the company / innovation provider to the adoption and implementation of these innovations in the company environment by users. The TOE framework represents one part of this process: embracing and implementing innovation from the end-user perspective. This framework explains the influence of technology, organization, and the external task environment on the decision-making process when implementing new technological innovations.

These parts consider both inherent and motivational factors for an adoption of new technological innovation, see [12]. Each part of the TOE framework affects technological innovation decision making by itself; however, these can also be interlinked with each other.

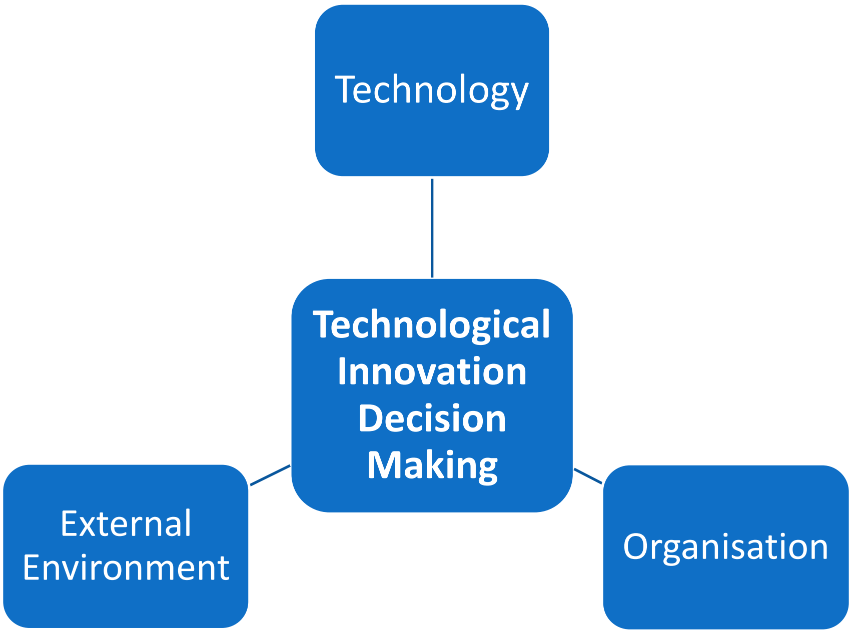


Figure 4. TOE Framework factors.

This framework considers the following factors that influence the innovation uptake:

- The technological context includes all of the technologies that are relevant to the firm – both, technologies that are already in use at the firm as well as those that are available in the marketplace but not currently in use.
- The organizational context refers to the characteristics and resources of the firm, including the firm's size, degree of centralization, degree of formalization, managerial structure, human resources, quantity of slack resources, and linkages among employees.
- The environmental context includes the structure of the industry, the presence or absence of technology service providers, and the regulatory environment.

The abovementioned theoretical framework helps to gain a deeper understanding of the factors that affect the adoption of an innovation in an organisation.

The TOE framework, illustrated in Figure 4, was used as a structured guide to find the relevant factors and to further understand how these factors should be analysed and thus fulfil the purpose of Task 4.2 related to the strategy creation and elaborate the most promising innovation selection. In this context, this is a comprehensive framework, as it considers how the organisations whole context impacts the adoption and implementation of new technological innovations [12], which helped the EU-HYBNET consortium consider all relevant factors without overlooking any important ones.

Pros: The framework describes the factors that could have an impact in the uptake of an innovation in detail.

Cons: The framework does not provide a roadmapping.

2.1.3 T-SHARK GOVERNANCE MODEL

During 2020 the EU-HYBNET and SPARTA [13] projects established a cooperation framework. It included joint discussions and workshops on innovation uptake and governance issues. Specifics of the SPARTA project T-SHARK programme, is that there are several autonomous, mainly technological innovation based, developments (named Sub-cases in the project), that should be integrated and be able to operate in the single ecosystem of comprehensive cybersecurity concept. Sub-cases should be described in a unified way and it should be clear how their activities are triggered, what outcomes they produce and how relevant information should be shared.

During the cross-project workshop, the conceptual model of innovations governance, developed in T-SHARK, was presented. It aims to guide autonomous development towards better integrity and search for functionalities, that are relevant for the whole eco-system. The model presented is not described in any Sparta project deliverable. It is still in a piloting stage, some components are applied, some are in progress.

The focus of the model is on how an innovation is developed in a certain context and is applied during the development, moving through TRL levels. The model is not describing the uptake phase. Even though it includes Innovation type framework, but it is applied more to understand the potential up-take issues in the early stages.

The T-SHARK model is based on the stage gate concept, which is a conceptual and operational roadmap for moving a new-product project from idea to launch.

Pros: It describes a standardised approach for the mapping, cross-integration and comparison of different innovations.

Cons: it focuses mainly on the development side of the innovation. Aspects related to the end users are not considered in-depth. It can be concluded, that T-SHARK innovation governance model cannot be transformed into an innovation's uptake framework. It can well serve other aspects, that might be relevant in how Hybrid Treats related innovations are developed.

2.1.4 INNOVATION'S VIABILITY

The feasibility assessment of an innovation can be evaluated using mainly two assessment models, TELOS and THOR, see below. These frameworks are used to evaluate whether an innovation is actually viable and can be implemented effectively in the long term.

TELOS METHODOLOGY [14]. This methodology can be used in order to assess the viability of an innovation. The evaluator needs to answer the below questions:

1. Technical: What is the technological readiness of the solution – How innovative is the solution?
2. Economic: Is the solution provided by the project expected to save money, time, other assets? How is this potential gain measured?
3. Legal: Is the solution compliant with legal requirements? Are there any legal or ethical constraints?

4. Operational: What is the expected operational impact of the solution? Are there many countermeasures to its implementation? On an operational level how easily the innovation can be implemented?
5. Scheduling: What is the development timeframe till completion of the solution?

THOR METHODOLOGY [15]. The THOR concept was developed by the EU funded project CAMINO [16]. The delivered solution is analysed in four dimensions as follows:

1. Technical: Assess if the implemented innovation will be uptake of the end users, and will provide the required competences to the end users.
2. Human: Evaluate how a series of human factors, behavioural aspects, privacy issues, ethical, societal and raising awareness activities will influence the innovation.
3. Organisational: Examine if the proposed innovation will be influenced by organisational processes, policies and procedures.
4. Regulatory: Inspect the innovation for adherence to law, standards, data protection and legal framework at national and EU level.

Each one of the THOR dimensions is divided into several areas of interest based on the assessment needs.

Pros: Both the TELOS and THOR methodologies can be used to assess innovations from different angles.

Cons: Both cannot provide a roadmap for the actual uptake of the innovation.

2.1.5 RADARS RELATED TO INNOVATIONS

KTH[1] INNOVATION READINESS LEVEL RADAR [17]. This radar examines several aspects related to the readiness of an innovation for its uptake depicted with a visual approach.

- Customer Readiness Level – CRL – confirm customer need and interest
- Technology Readiness Level – TRL – develop and test the technology, product, service, or concept
- Business Readiness Level – BRL – establish that the concept can be financially viable and feasible
- IPR Readiness Level – IPRL – clarify the legal and IP situation and secure relevant IP protection
- Team Readiness Level – TMRL – secure the right competencies and align the team
- Funding Readiness Level – FRL – secure the necessary funding to take the idea to the market

[1] KTH, The Royal Institute of Technology, Stockholm, Sweden

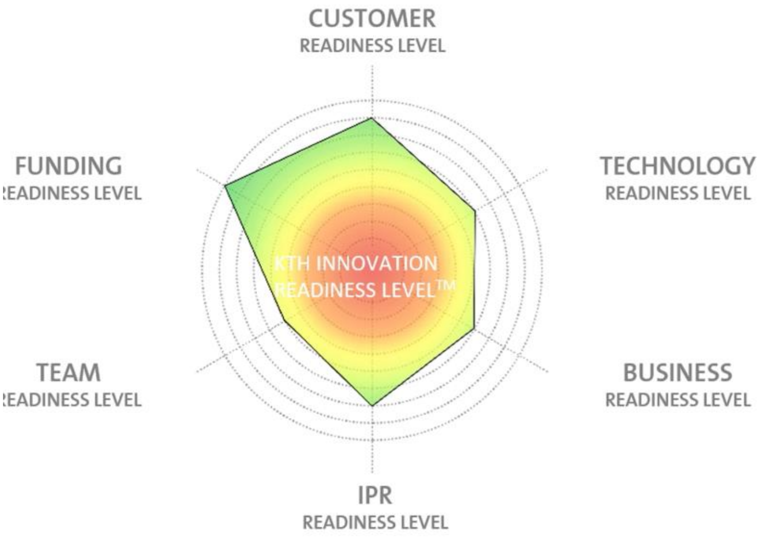


Figure 5. The KTH innovation readiness radar.

THE INNOVATION RADAR [18]. The innovation radar is similar to the abovementioned framework, including several areas that need to be taken into account for the strategy creation of an innovation. These include the technical details, the regulations and standards, the business model and the value network.

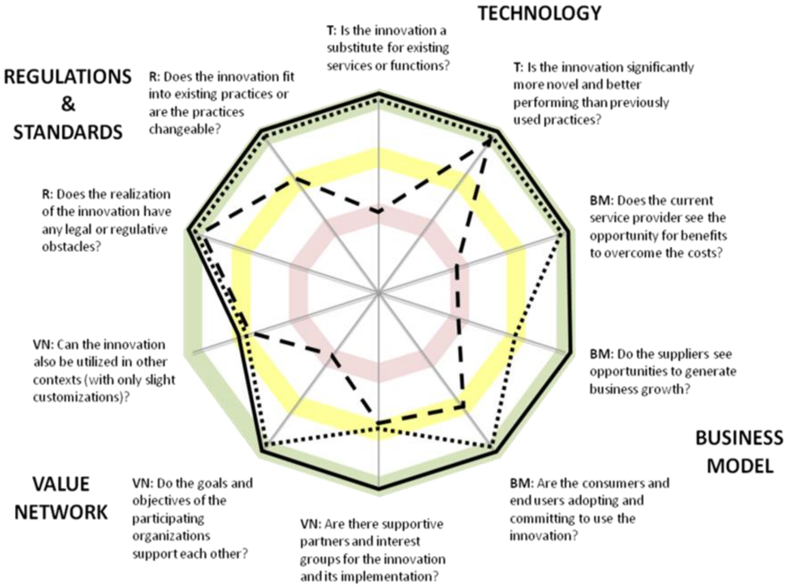

TECHNOLOGY
T: Is the innovation a substitute for existing services or functions?
T: Is the innovation significantly more novel and better performing than previously used practices?
REGULATIONS & STANDARDS
R: Does the innovation fit into existing practices or are the practices changeable?
R: Does the realization of the innovation have any legal or regulative obstacles?
BM: Does the current service provider see the opportunity for benefits to overcome the costs?
BM: Do the suppliers see opportunities to generate business growth?
BUSINESS MODEL
BM: Are the consumers and end users adopting and committing to use the innovation?
VN: Can the innovation also be utilized in other contexts (with only slight customizations)?
VALUE NETWORK
VN: Do the goals and objectives of the participating organizations support each other?
VN: Are there supportive partners and interest groups for the innovation and its implementation?

Figure 6. The innovation radar.

Pros: The framework examines four important areas relevant to the innovation uptake of a specific solution.

Cons: The radar cannot support the creation of a strategy, only the aspects that could influence the implementation of an individual innovation.

2.1.6 SWOT ANALYSIS

SWOT analysis (or SWOT matrix) [19] is a strategic planning technique used to help an organization identify strengths, weaknesses, opportunities, and threats related to business competition or project planning.

This technique is designed for use in the preliminary stages of decision-making processes and can be used as a tool for evaluation of the strategic position of a decision. It is intended to describe, evaluate, and specify the objectives of a decision/ project and identify the internal and external factors that are favourable and unfavourable to achieving those objectives.

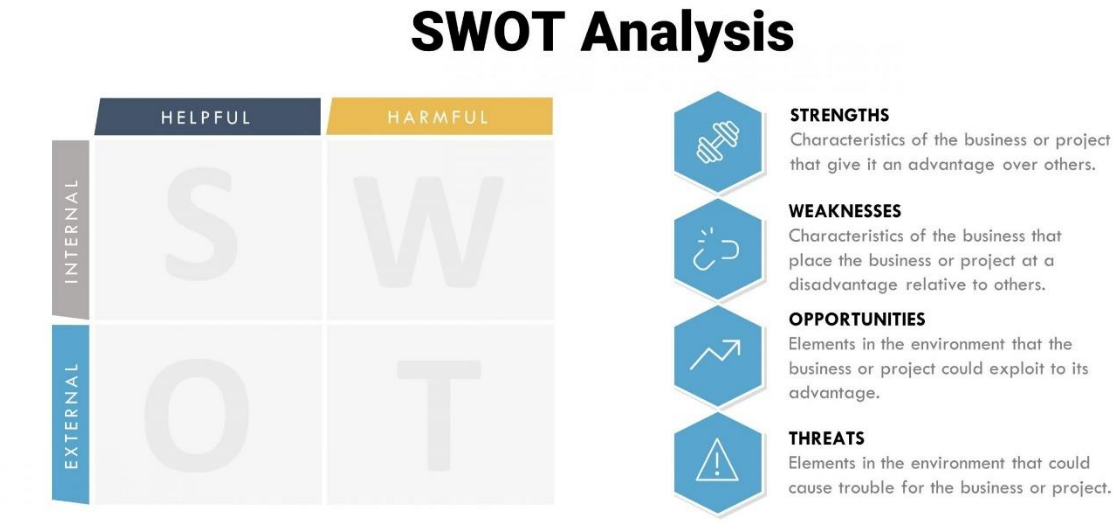

SWOT Analysis
HELPFUL
HARMFUL
INTERNAL
EXTERNAL
S
W
O
T
STRENGTHS
Characteristics of the business or project that give it an advantage over others.
WEAKNESSES
Characteristics of the business that place the business or project at a disadvantage relative to others.
OPPORTUNITIES
Elements in the environment that the business or project could exploit to its advantage.
THREATS
Elements in the environment that could cause trouble for the business or project.

Figure 7. The SWOT analysis explained.

Pros: It takes into account any factor internal or external that can affect a decision.

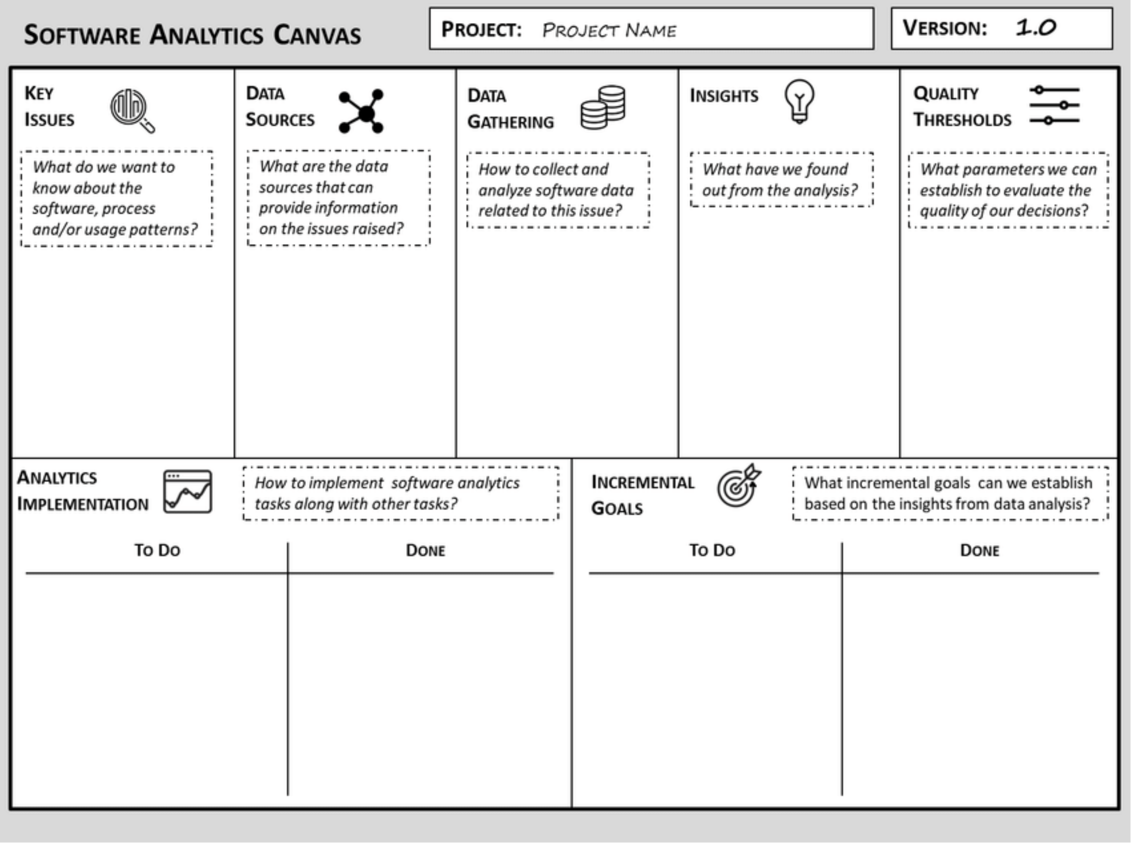
Cons: It is only a starting point for strategy creation.

2.1.7 CANVAS APPROACHES

A canvas model can be used as a shared language for describing, visualizing, and assessing e.g., a business or innovation problem space. It usually describes the rationale of how value can be created, delivered, and captured. In our innovation uptake context three kinds of canvases were taken into account.

THE SOFTWARE ANALYTICS CANVAS [20]. The Software Analytics Canvas is an artifact designed from a set of patterns to support agile teams to plan and manage software analysis activities, see Figure 8.

THE BUSINESS MODEL CANVAS [21]. The Business Model Canvas (BMC) is a strategic management tool to easily define and communicate an innovative idea or concept. It is a one-page document which works through the fundamental elements of a business or product, structuring an idea in a coherent way.



SOFTWARE ANALYTICS CANVAS

PROJECT: PROJECT NAME

VERSION: 1.0

KEY ISSUES
What do we want to know about the software, process and/or usage patterns?

DATA SOURCES
What are the data sources that can provide information on the issues raised?

DATA GATHERING
How to collect and analyze software data related to this issue?

INSIGHTS
What have we found out from the analysis?

QUALITY THRESHOLDS
What parameters we can establish to evaluate the quality of our decisions?

ANALYTICS IMPLEMENTATION
How to implement software analytics tasks along with other tasks?

TO DO	DONE

INCREMENTAL GOALS
What incremental goals can we establish based on the insights from data analysis?

TO DO	DONE

Figure 8. The Software Analytics Canvas.

There are nine building blocks in the Business Model canvas, see Figure 9, and they are customer value proposition, customer segments, channels, customer relationships, revenue streams, key resources, key partners, key activities, and cost structure. A business model canvas is usually filled in by the developers of the idea and meant to provide more comprehensive understanding of the potential issues in further development of business. In the filling in a business model canvas, it is common to brainstorm and conduct research on each of its elements. The data collected can be placed directly in each relevant section of the canvas.

THE INNOVATOR'S CANVAS [22]. The Innovator's Canvas, see Figure 10, is a tool that can assist to identify the most important challenges in developing an innovative product, service or process. It can be used to prioritise next actions, and to seek fresh perspectives, ideas or advice. With the Innovator's canvas a team can have a thorough template for documenting completely new ideas. This forces the individual or team to think through each of the essential building blocks of the idea. In this context, having documented all the aspects of the idea is merely the first step towards strategy creation.

Pros: It can be used to create a strategy for the implementation and uptake of an innovation

Cons: Enables risky assumptions within the model, without offering a clear way to verify them.

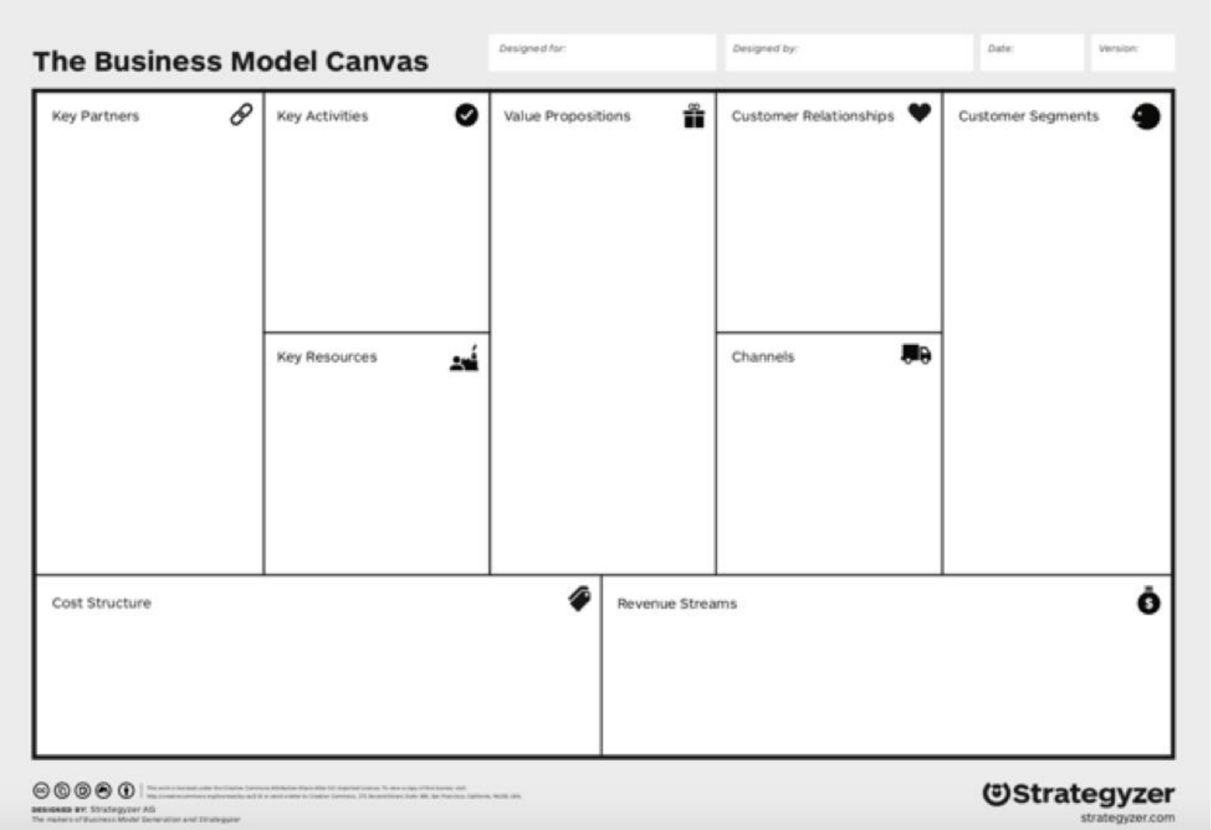
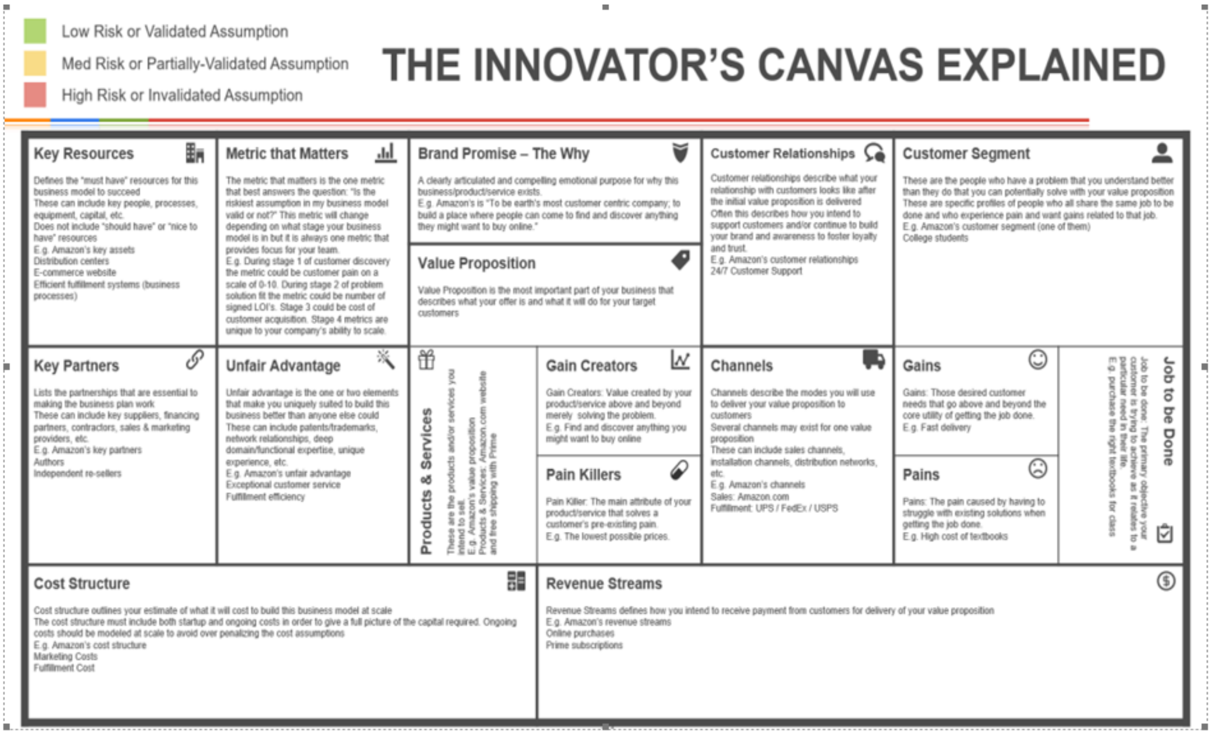


Figure 9. The business model canvas


🟩 Low Risk or Validated Assumption

🟨 Med Risk or Partially-Validated Assumption

🟥 High Risk or Invalidated Assumption

THE INNOVATOR'S CANVAS EXPLAINED

Key Resources

Defines the "must have" resources for this business model to succeed
These can include key people, processes, equipment, capital, etc.
Does not include "should have" or "nice to have" resources
E.g. Amazon's key assets
Distribution centers
E-commerce website
Efficient fulfillment systems (business processes)

Metric that Matters

The metric that matters is the one metric that best answers the question: "Is the riskiest assumption in my business model valid or not?" This metric will change depending on what stage your business model is in but it is always one metric that provides focus for your team.
E.g. During stage 1 of customer discovery the metric could be customer pain on a scale of 0-10. During stage 2 of problem solution fit the metric could be number of signed LOI's. Stage 3 could be cost of customer acquisition. Stage 4 metrics are unique to your company's ability to scale.

Brand Promise – The Why

A clearly articulated and compelling emotional purpose for why this business/product/service exists.
E.g. Amazon's is "To be earth's most customer centric company; to build a place where people can come to find and discover anything they might want to buy online."

Value Proposition

Value Proposition is the most important part of your business that describes what your offer is and what it will do for your target customers

Customer Relationships

Customer relationships describe what your relationship with customers looks like after the initial value proposition is delivered
Often this describes how you intend to support customers and/or continue to build your brand and awareness to foster loyalty and trust.
E.g. Amazon's customer relationships
24/7 Customer Support

Customer Segment

These are the people who have a problem that you understand better than they do that you can potentially solve with your value proposition
These are specific profiles of people who all share the same job to be done and who experience pain and want gains related to that job.
E.g. Amazon's customer segment (one of them)
College students

Key Partners

Lists the partnerships that are essential to making the business plan work
These can include key suppliers, financing partners, contractors, sales & marketing providers, etc.
E.g. Amazon's key partners
Authors
Independent re-sellers

Unfair Advantage

Unfair advantage is the one or two elements that make you uniquely suited to build this business better than anyone else could
These can include patents/trademarks, network relationships, deep domain/functional expertise, unique experience, etc.
E.g. Amazon's unfair advantage
Exceptional customer service
Fulfillment efficiency

Products & Services

These are the products and/or services you intend to sell.
E.g. Amazon's value proposition
Products & Services: Amazon.com website and free shipping with Prime

Gain Creators

Gain Creators: Value created by your product/service above and beyond merely solving the problem.
E.g. Find and discover anything you might want to buy online

Pain Killers

Pain Killer: The main attribute of your product/service that solves a customer's pre-existing pain.
E.g. The lowest possible prices.

Channels

Channels describe the modes you will use to deliver your value proposition to customers
Several channels may exist for one value proposition
These can include sales channels, installation channels, distribution networks, etc.
E.g. Amazon's channels
Sales: Amazon.com
Fulfillment: UPS / FedEx / USPS

Gains

Gains: Those desired customer needs that go above and beyond the core utility of getting the job done.
E.g. Fast delivery

Pains

Pains: The pain caused by having to struggle with existing solutions when getting the job done.
E.g. High cost of textbooks

Job to be Done

Job to be done: The primary objective your customer is trying to achieve as it relates to a particular need in their life.
E.g. purchase the right textbooks for class

Cost Structure

Cost structure outlines your estimate of what it will cost to build this business model at scale
The cost structure must include both startup and ongoing costs in order to give a full picture of the capital required. Ongoing costs should be modeled at scale to avoid over penalizing the cost assumptions
E.g. Amazon's cost structure
Marketing Costs
Fulfillment Cost

Revenue Streams

Revenue Streams defines how you intend to receive payment from customers for delivery of your value proposition
E.g. Amazon's revenue streams
Online purchases
Prime subscriptions

Figure 10. The Innovator's canvas

2.2 SUCCESS FACTORS AND BARRIERS

Under the activities of Task 4.1, an analysis has been made to identify potential blocking points and good practices for the uptake of an innovation from a procurement point of view. The search has been made on the procurement procedures conducted on national level as well as a literature review in the topic on joint procurement procedures and innovation procurement.

2.2.1. PROCUREMENT ASPECTS

Below follows a listing of procurement aspects, problems, extracted from the D4.1 [5]. For more information and details see that report.

2.2.1.1 GENERIC PROBLEMS

The generic problems of procurement refer to the aspects that, if missed, could affect the overall procurement procedure. The following ones have been identified as part of D4.1, [5]:

- Missing involvement of end-users. Tech driven design.
- Missing adoption of solution by policy makers.
- Missing preparedness for upgrades and updates of solution.
- Missing analysis of operational consequences. Required changes in current organization and procedures.
- Missing trustworthy cost benefit analysis.

2.2.1.2 SPECIFICATION ISSUES

The most important step in the preparation of a procurement procedure is the development of the requirements. Based on D4.1 [5] report the following problems could arise:

- Solution not feasible.
- Unclear specifications and requirements. Failure to define needs.
- Incompatibilities with standards.
- Stability in requirements. Change procedures.

2.2.1.3 SUPPLIER AND MARKET ISSUES

Another aspect that needs to be carefully taken into account during the overall procurement procedure is the problematic aspects that could arise in relation to the industry side, and more specifically:

- Unavailability of capable solution providers/developers. Missing supplier assessment and market analysis.
- Competition distortion due to limited number of suppliers. Vendor lock in.
- Deficient supply chain(s).
- No spill over to private markets.

2.2.1.4 CORE PROCUREMENT ISSUES

Strategic aspects of the procurement implementation, may also create several problematic situations. In this context, the following six have been identified under the activities of Task 4.1, [5]:

- Misalignment with procurement strategies and regulations.
- Public sector fragmentation.
- Joint procurement difficulties.
- Insufficient clarity in cost drivers, Capital Expenditure (CAPEX) and Operation Expenditure (OPEX).
- Missing clear award decision design and transparency in procedures.
- Low-cost requirements drive towards poor quality solution.

2.2.1.5 SUCCESS FACTORS

Part of the D4.1 report,[5] was also to identify the success factors in the procurement procedures examined. In this context, the following guidelines have been created:

- Secure involvement of skilled personnel.
- As far as possible, work with open requirements.
- Review procedures and solution. Perform an adequate vulnerability assessment.
- Instigate required IPR provisions.
- Ensure compatibility with legacy systems.
- Use existing standards to the largest extent possible.
- Always perform a market consultation.
- Use open procurement. Rely on available templates.

2.2.2. ETHICAL ASPECTS

In this section we first discuss general ethical and sustainability aspects to consider and then give some more specific issues to consider in the development and use of new solutions and procedures.

2.2.2.1 GENERAL CONSIDERATIONS

Any project that aims be truly successful, whether it aims for market success or success in some other area, needs to take ethical aspects into account. The reason for this is simple as in today's user and business environment, it is not only technical innovativeness and price that drive success, as it is critical to offer solutions that are ethically sustainable and societally acceptable. Today, end-users expect this; ethics is a requirement like any technical one. This is especially important to acknowledge by anyone who wants to enter to the European market, or any other market that has committed to so-called European values, for example, democracy and respecting human right.

Development work should thus, with reference to the above, always start with considering how the work should be performed: an ethically sustainable work ethos will be reflected in the end-results. If and when development work is done ethically, it tends to result in ethical solutions. This means that solutions and/or aimed for end-results should be developed following good research practices and adhering to correct procedures e.g., with respect to human participation, privacy issues etc. However, doing right does not always and automatically result in sought-after and societally acceptable solutions. Thus, specific ethical attention should also be put on the wanted outcomes when they are under preparation, e.g., in the design phase.

Figure 11 provides and diagram depicting that there are three different layers that should be taken into account in an ethical discussion. The first is technology itself. The solution must be ethically sustainable and societally acceptable to begin with. For example, if the technology violates privacy or it is harmful for environment, then it can hardly be successful. Often these ethical requirements are simple to detect as they are often legal requirements too.

The second layer is the use of the solutions, as the use should be ethical too. Therefore, emphasis should be put into the different ways of how the solution is used. An obvious example is that the use of the solution should not harm, discriminate or favour someone. Thus, in this context not only the solutions itself is important, as it is just as important to provide principles for how to use the solution and to provide user guidance and manuals.

The third layer could be labelled as the business and/or governance layer. This refers to the total environment in which the solutions are used. The questions to ask are about the owners of the solutions and their aims with the solutions etc. It is pivotal, for example, that items that have the potential of misuse do not get in the wrong hands. However, since the road to hell is paved with good intentions, it is equally important to examine the aims and ambitions of legitimate organisations too. In short respecting human rights is a default, other case-by-case.

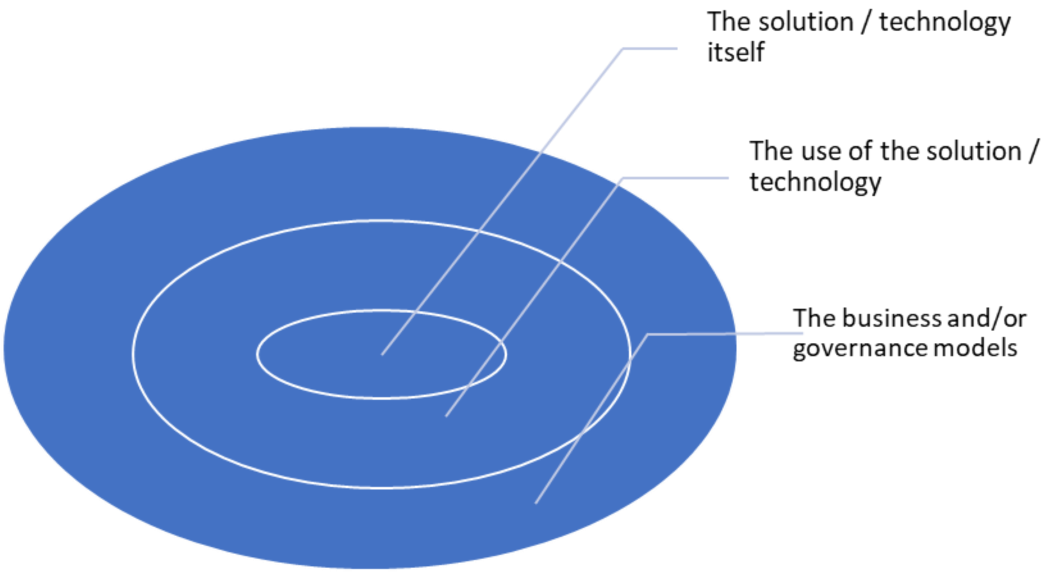

The solution / technology itself
The use of the solution / technology
The business and/or governance models

Figure 11 The different ethical layers

2.2.2.2 SOME SPECIFIC ISSUES

Below we point at some specific aspects when it comes to ethical issues and societal acceptance:

- Freedom of thought is a fundamental right and it must always be respected. This aspect is of special relevance in the design and use of solutions in the areas of information and media surveillance, used to e.g., detect and debunk disinformation. Such solutions must be designed, governed and controlled in such a way that they do not becomes instruments to control and shape citizens' opinions. Special care has to be taken not to influence but only to inform the public.

- Loss of privacy is a severe threat to citizens' right to be left alone, not be tracked and to control which information they want to share with others. This aspect relates to what the General Data Protection Regulation (GDPR) is about (https://gdpr-info.eu/). Key aspects in GDPR with respect to how personal data are to handled are: Lawfulness, Fairness and transparency, Purpose limitation, Data minimisation, Accuracy, Storage limitation, Integrity and confidentiality (security) and Accountability. The GDPR has to be followed together with all other laws and regulations related to the privacy area.
- Gender equality is a fundamental human and a necessary foundation for a peaceful, prosperous and sustainable world right as it is stated in the UN sustainable development goal. Thus, it is essential to assess that all solutions and procedures do not preserve the current inequality between men and women but help to improve the current situation.
- There are a number of ethical issues discussed in connection with the use of AI techniques, e.g., privacy and surveillance, manipulation of behaviour, opacity of AI systems and bias in decision system. For more information, see e.g., [23], [24].

2.2.3 BENCHMARKING CASES

Based on the activities of Task 4.1, several procurement cases have been identified that could serve as a basis for the creation of the uptake strategy. More specifically, the following cases have been examined (for details see [5]):

- National Procurement of government stamps in Sweden conducted in 2018.
- National Procurement of Hardware and Software equipment in Greece conducted in 2020.
- National Procurement for the development of the National Ecosystem for the Recognition and Analysis of the Information Effect Phenomena (NAAS) in Lithuania started in 2020 and will be finalized by 2023.
- National Procurement for the supply of Xray Scanner in Salerno Airport conducted in 2019
- PPI4HPC[2]: This is a joint Public Procurement of Innovative Solutions (PPI) in the area of High-Performance Computing (HPC) co-funded by the European Commission (EC) started in 2020.
- MALMÖ SWEDEN: The procurement was related to innovation in ICT procurement to promote sustainable and fair supply chains in City of Malmö conducted in 2019.
- SHUTTLE[3] /2018: This is a joint Pre- Commercial Procurement (PCP) for the development of an automated machine toolkit which will facilitate the analysis of micro traces collected in crime scenes co-funded by the European Commission (EC) and started in 2018.

The analysis of the abovementioned cases initially led to the recommendations as included in the previous paragraphs of the current section. In this context, the abovementioned recommendations were used to evaluate various aspects of the best ranked innovations. This comparison allowed the task participants to develop a more concrete strategy taking into account potential procurement approaches when relevant.

[2] https://www.ppi4hpc.eu/
[3] https://www.shuttle-pcp.eu/

2.3. EEAS CONTACTS

EU-HYBNET consortium, under the activities of Task 4.2, cooperated with the European External Action Services (EEAS) in order to exchange information and ideas related to the selected innovations. More specifically, the discussions among the task participants, the EU-HYBNET Coordinator and EEAS representatives were focused on the following two innovations:

- Information sharing environment among practitioners in the scope of hybrid threats in a so-called EU Communication Awareness Environment (EUCAE)
- Support to Media Literacy plans and uptake in EU Member States

During the said meetings, the parties also discussed the correlation of the selected innovations with the RAS (Rapid Alert system) that EEAS has developed. The partners also collaborated to conclude on what EU-HYBNET may bring to an EUCAE development and whether this innovation could address EEAS's needs.

The outcome of the discussions mainly helped EU-HYBNET to describe in more depth the innovations and the main advantages that they can bring to the practitioners as well as the challenges that can be faced during their implementation. Finally, it is important to highlight that the planning of EUCAE content continued by the EU-HYBNET project in cooperation with EEAS after the completion of Task 4.2.

2.4. CONCLUSIONS

The current section summarizes the results collected following the literature study, which provided valuable insights to the Consortium on the frameworks used for uptake strategy creation as well as the ones that play a role on the relevant activities.

More specifically, several methodologies have been analyzed summarizing the advantages and disadvantages and highlighting their suitability for the EU-HYBNET activities. In addition, the input from task 4.1. has been presented and further analyzed for the scope of the task 4.2. Finally, the input provided by EEAS to the development of the uptake strategy of the four most promising innovations is also presented.

The overall information collected, and their analysis led to the development of the roadmapping approach and the Innovation Uptake Canvas presented in section 3.

3 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.

3.1 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 [25] “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 [26] 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 [27] contain:

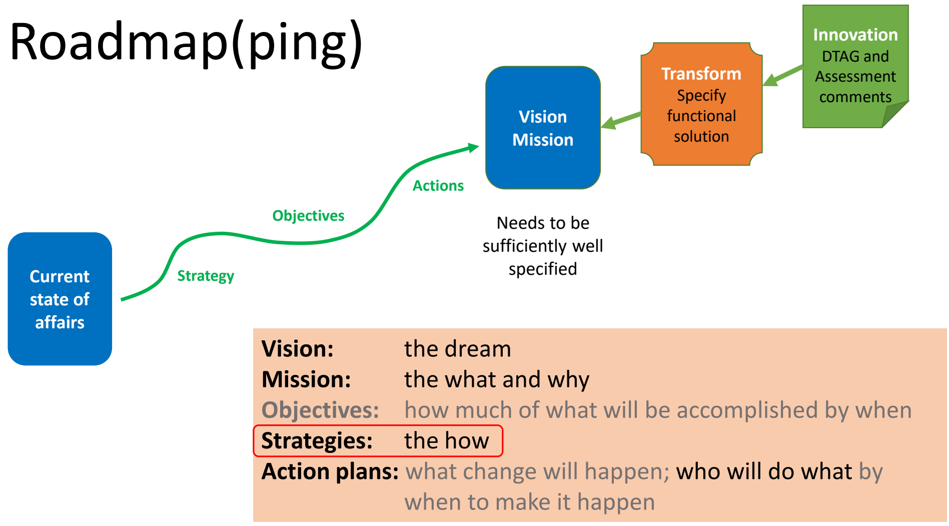
Scope: Who are the intended users of the innovation (citizens, practitioners, etc)

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.


Roadmap(ping)
Innovation
DTAG and Assessment comments
Transform
Specify functional solution
Vision
Mission
Actions
Objectives
Strategy
Current state of affairs
Needs to be sufficiently well specified

Vision:	the dream
Mission:	the what and why
Objectives:	how much of what will be accomplished by when
Strategies:	the how
Action plans:	what change will happen; who will do what by when to make it happen

Figure 12. 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.

3.2 THE INNOVATION UPTAKE CANVAS

The innovation uptake canvas is depicted in Figure 13. 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.

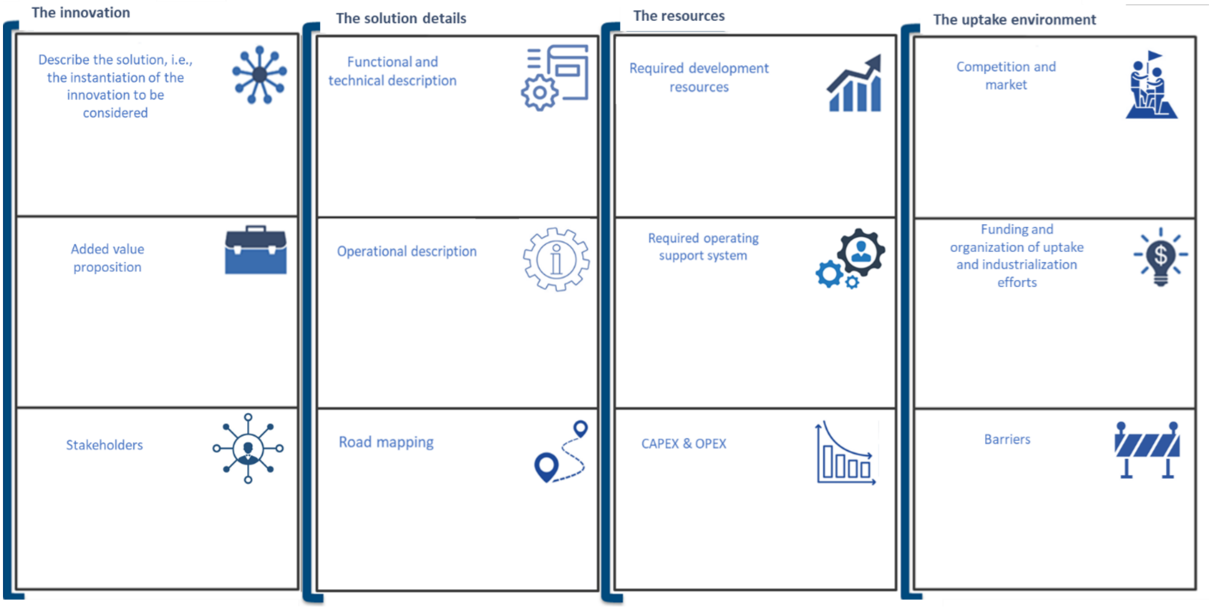

The innovation
Describe the solution, i.e., the instantiation of the innovation to be considered
Added value proposition
Stakeholders
The solution details
Functional and technical description
Operational description
Road mapping
The resources
Required development resources
Required operating support system
CAPEX & OPEX
The uptake environment
Competition and market
Funding and organization of uptake and industrialization efforts
Barriers

Figure 13. The innovation uptake canvas

3.2.1 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 [28].
  - 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?

3.2.2 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?

3.2.3 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?

3.2.4 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.

3.3 APPLYING THE METHODOLOGY – OUR WAY OF WORKING

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 14.

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. The result should be roadmapping statements for 1) vision, 2) mission and 3) the scope of the solution. These statements will the basis for the further analysis.
2. Review the innovation uptake canvas and fill in relevant aspect in the canvas and the roadmap. Identify white spots where more information / analysis is needed. Review and document barriers.
3. In a workshop with participants knowledgeable in the subject matter, discuss and review the draft canvas and roadmap and discuss / resolve the white spots as far as possible. Update the draft canvas and roadmap.
4. Send the draft canvas for review to project partners, the stakeholder group and the network as applicable.
5. Integrate comments received and finalize the innovation uptake canvas and the roadmap.
6. Document the final canvas and summarize the findings and propose corrective actions, if needed. The canvases and the roadmaps are documented in Section 5.
7. Collect 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 6.

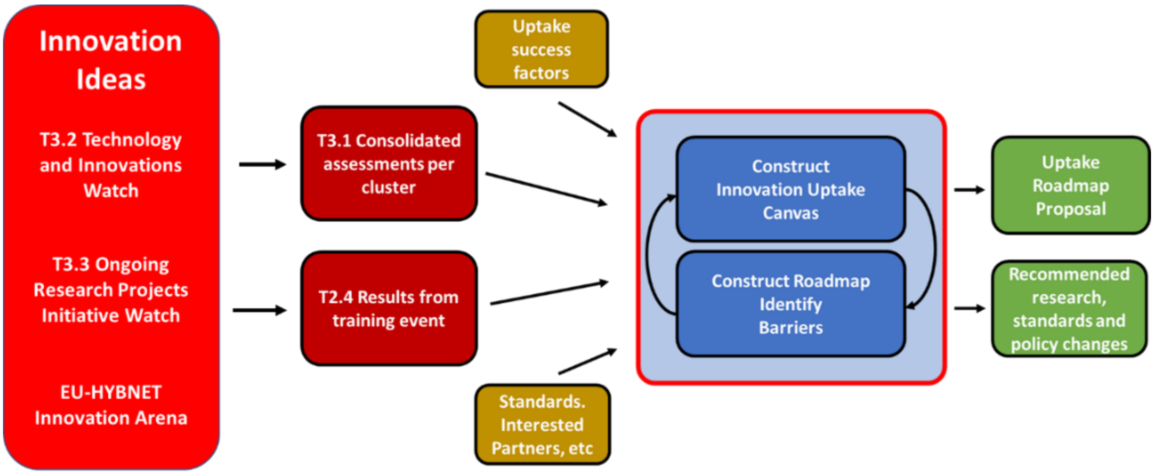

Innovation Ideas
T3.2 Technology and Innovations Watch
T3.3 Ongoing Research Projects Initiative Watch
EU-HYBNET Innovation Arena
T3.1 Consolidated assessments per cluster
T2.4 Results from training event
Uptake success factors
Standards. Interested Partners, etc
Construct Innovation Uptake Canvas
Construct Roadmap Identify Barriers
Uptake Roadmap Proposal
Recommended research, standards and policy changes

Figure 14. 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 innovation analysed:

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

4 REVIEW OF INNOVATIONS

4.1 BACKGROUND ON INNOVATION SELECTION AND EVALAUATION

In this first project cycle, due to limited resources, the number of innovations to review was set to four, with an ambition to have innovations that were related to all four EU-HYBNET core themes and also have both technical and non-technical innovations. This to be able to evaluate how well the developed methodology framework performed for different types of innovations and to understand which modifications that may be required for the next project cycles to make it more efficient and to the point.

For the convenience of the reader, we here first include a short introduction of the four core themes. The introduction is fetched from the project web page [29]:

Core theme 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.

Core theme 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.

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.

Core theme 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.

Core theme 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.

4.2 SELECTION OF INNOVATIONS FOR REVIEW

The selection process was based on

- The assessment of innovations performed by Task 3.1 documented in D3.1 [2]. All innovations can also be found in the EU-HYBNET Innovation Arena [30].
- The outcome of the training events (DTAGs) organized by Task 2.4, where the attractiveness of innovations was assessed.
- The innovation's relation to the core themes.

The Task 3.1 assessment identified a set of promising innovations, i.e., they fulfilled the basic assessment criteria defined by Task 3.1, see [2]. Out of these promising innovations a subset was identified as "best assessed" which fulfilled additional evaluation criteria.

The rationale behind the choice of these four innovations, in addition to that they represent different core themes, are

1. **Public-private information-sharing groups developing collaborative investigations and collective action** belongs a) to the group of the six "best assessed" innovations according to Task 3.1 and b) it was selected in the training exercises.
2. **Debunking of fake news** belongs a) to the group of the six "best assessed" innovations according to Task 3.1 and b) it was selected in the training exercises.
3. **Training application for media literacy** belongs a) to the group of innovations which are promising according to Task 3.1 and b) it exhibits both technical and non-technical features.
4. **Guides to identify fake news** belongs a) to the group of the six "best assessed" innovations according to Task 3.1 and b) it was selected in the training exercises.

The innovations' relation to the EU-HYBNET core themes is depicted in Table 1.

Table 1. Relation between selected innovations and EU-HYBNET core themes

Innovations	**Core Themes**			
	Resilient civilians, local level and administration	Cyber and Future Technologies	Information and Strategic Communication	Future Trends and Hybrid Threats.
Public-private information-sharing groups developing collaborative investigations and collective action		X	X	
Debunking of fake news	X		X	
Training application for media literacy	X		X	X
Guides to identify fakes	X		X	X

4.3 REVIEW OF INNOVATIONS

The review of the selected innovations took place in three regular workshops and an initial test workshop organised to assess the methodology.

- The test workshop considered the innovation Public-private information-sharing groups developing collaborative investigations and collective action. This exercise was very valuable as it showed that the methodology was functional and only needed minor adjustments to serve the purpose for technical innovations. The procedure followed the columns and boxes in the Innovation Uptake Canvas and the discussions were documented in a corresponding table. The review produced a basis for the scoping, vision mission and strategy for the considered innovation.

- The first regular review workshop handled the two innovations:
  - Public-private information-sharing groups developing collaborative investigations and collective action, and
  - Training application for media literacy.

  Due time constraints the discussion on the second innovation could not be finalized and the discussions were to be continued in the third regular workshop. Still, the discussions regarding that innovation showed that the methodology was also useful for review of non-technical innovations. The workshop resulted in scoping, vision and mission statements for both innovations.
- The second regular review workshop handled the two innovations:
  - Debunking of fake news, and
  - Guides to identify fakes.

  The discussions led to agreement on scope, vision, mission and strategies for both innovations.
- The third regular review workshop only considered the innovation Training application for media literacy. The findings from regular workshop number one were reviewed and refined and a more complete Innovation Uptake Canvas was produced.

There are two general observations on the outcome of these review workshops. The first one is that for all innovations handled, the scope of the innovations was reduced to cover a more precise and specific solution. The second is that the workshop format is perfect for discussing and agreeing on the scope, vision, mission, high level strategies and barriers, while other topics covered by the Innovation Uptake Canvas need to be covered by more detailed investigations.

When the Innovation Uptake Canvases had been drafted, a person knowledgeable in the subject matter cover by an innovation was asked to review the canvas to eliminate mistakes and misunderstandings.

The persons that contributed in the workshops and that provided the topics reviews are detailed in Annex III, Table 5

5 SCOPING AND ANALYSIS OF SELECTED INNOVATIONS

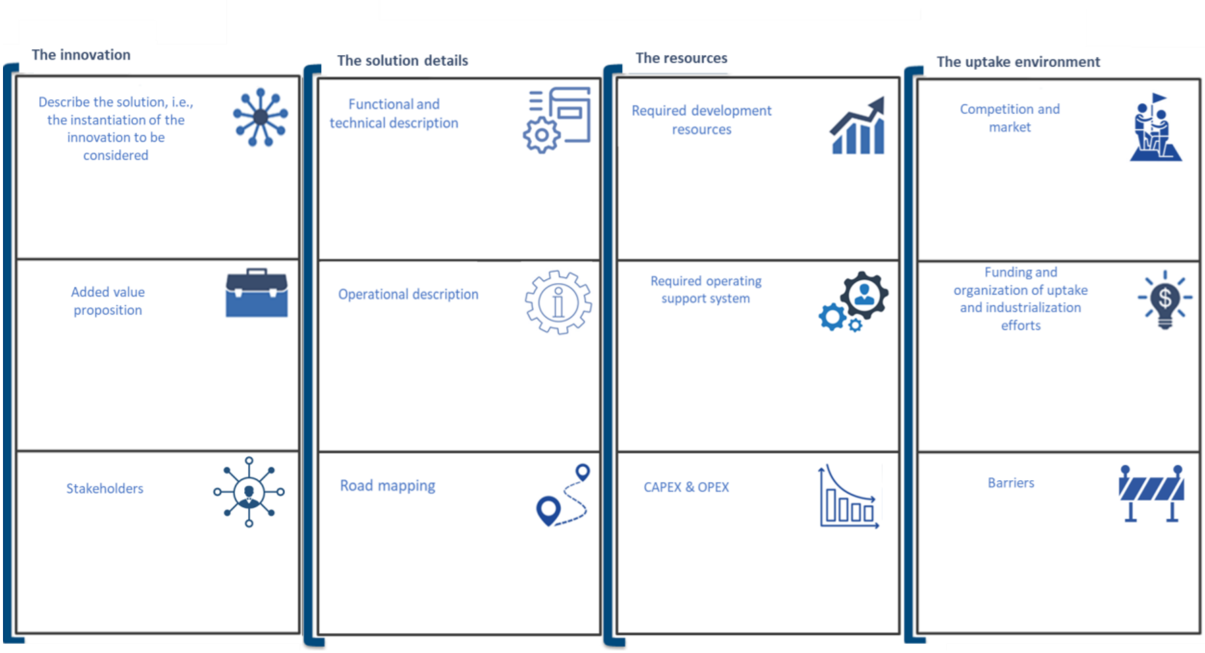
The analysis of the four innovations and the way it was determined to scope them have resulted in two technical innovations and two non-technical innovations. The two technical innovations both are concerned with information sharing, monitoring, analysis and joint actions between organizations in the Member States. The first one of the technical innovations relates to providing situational awareness about threats and attacks in critical infrastructure systems and the second one has the same scope but for disinformation campaigns.

A fundamental precondition for the enhancement of the security and protection of critical infrastructures is a common centre for information sharing, reporting of problems, and exchanging of good practices, [31]. In case of cyberphysical critical infrastructure security, the adoption of a Holistic Security Operation Centre (HSOC) in each critical infrastructure and a National Coordination Centre (NCC), supervising them, which will facilitate the communication and cooperation between the different critical infrastructure operators and stakeholders, in case of an incident, that may have cascading effects to interconnected Infrastructures.

For both of the aforementioned innovations, the proposed way forward builds upon the Common Information Sharing Environment (CISE) [32], developed for EU Member States' need to have a joint situational awareness platform. CISE is hosted by the European Maritime Safety Agency (EMSA), and we will refer to this system as EMSA CISE. The proposed solutions have important extensions for analysis and collective actions.

The two non-technical innovations are related to efforts for increasing Member State citizens' media literacy capabilities and their proficiency in using tools to detect digitally generated or manipulated audio, images and video. This to increase resilience against disinformation campaigns. It should also be noted that three out the four innovations are related to disinformation and so-called fake media. Solutions in this area seems to be most wanted and much needed as was also noted in the work in Tasks 3.1, 3.2 and T3.3.

5.1 PUBLIC-PRIVATE INFORMATION-SHARING GROUPS DEVELOPING COLLABORATIVE INVESTIGATIONS AND COLLECTIVE ACTION


The innovation
Describe the solution, i.e., the instantiation of the innovation to be considered
Added value proposition
Stakeholders
The solution details
Functional and technical description
Operational description
Road mapping
The resources
Required development resources
Required operating support system
CAPEX & OPEX
The uptake environment
Competition and market
Funding and organization of uptake and industrialization efforts
Barriers

5.1.1 THE FIRST COLUMN – THE INNOVATION

- <u>**Description of the solution, i.e., the instantiation of the innovation to be considered**</u>**.**

The **Public-private information-sharing groups developing collaborative investigations and collective action** innovation has been transformed into a solution for a critical infrastructure's (near) real-time sharing and analysis of hybrid and related threat information (a Common Information Sharing and Analysis Environment, CISAE). Situational awareness is key in detecting hybrid threats and mitigate attacks. The more information available, if analysed correctly, the better the situational awareness. We note that the skills, data and capabilities to detect threats and disrupt attacks often reside within the private sector.

In the presented solution the CISAE users are practitioners affiliated with relevant public and private organizations in one critical infrastructure sector. Each critical infrastructure domain(/vertical/sector) can/will implement its own CISAE.

SCOPE: Practitioners in public and private organizations

VISION: All Member State critical infrastructure practitioners and organizations (public as well as private ones) can on a voluntary basis and in a controlled manner share and jointly analyse situational information to enhance their situational awareness related to hybrid threats and launch joint mitigation actions.

MISSION: Define and implement a CISAE. Define information sharing needs. Develop and implement required analysis tools.

STRATEGY: Develop critical infrastructure sector specific CISAEs and analysis tools. In The EC Green paper, [32], 11 infrastructure sectors are listed with a total of 29 subsectors. Build on EMSA CISE [33] (or other existing information-sharing solutions). Include relevant CTI in analysis. Information to be shared on a voluntary basis.

LIMITATIONS: The solution has no major limitations compared to the reviewed innovation.

RATIONALE: Security and resilience of critical infrastructure need to be a shared responsibility among multiple stakeholders because neither governmental nor the private sector alone has the knowledge, authority or resources to handle it alone. Public-private partnerships have been considered the foundation for effective critical infrastructure security and resilience strategies, and timely, trusted information sharing among stakeholders is essential for the security of EU critical infrastructures. Stakeholders involved in such a network should be from EU Member States. Access rights should be assigned according to needs, confidentiality/access level and trust relations.

- **Added value proposition.**

NEED: The complexity of attacks targeting critical infrastructures and the consequences of the large-scale disruptions that may follow in the directly targeted system and other infrastructures relying on it, makes it absolutely essential to provide the best possible means to detect, stop and/or mitigate attacks. The basis upon which such means rely, is on the harvesting and analysis of relevant information about current events and ongoing activities in the critical infrastructure, together with Cyber Threat Information (CTI) and detected hybrid threat activities in the considered critical infrastructure sector as well as in other sectors and domains. This to get an as good as possible situational awareness. Here it is true, that the more information you have, the better it is. However, there is a need for automatic analysis as the sheer amount of information may hide threat and attack traces from human detection.

IMPACT: With shared (near) real-time information about threats and attacks, they can in a trusted way be detected earlier and more securely. With a common situational awareness support system, there can be quick and efficient launch of joint mitigating actions and efforts to stop attacks. In a nutshell, it will greatly improve the resilience of the critical infrastructure.

VIABILITY: The viability of the solution is proven by the successful launch of the EMSA CISE.

- **Stakeholders and domains**

Gaps and needs: The solution is related to the following gaps and needs as defined by WP2 in D2.9 [28]:

- Governmental trust building and situational awareness.

JRC domains: The solution is foremost related to the following JRC domains:

- Critical infrastructure
- Cyber
- Information.

Stakeholders: The core stakeholders are the critical infrastructure operators and providers. But actors specialized in cyber threat information collection and analysis will also be important stakeholders as they provide consolidated related information from other infrastructure sectors and hybrid threat domains.

5.1.2 THE SECOND COLUMN - SOLUTION DETAILS

- **Functional description**

For the CISE part, i.e., the information sharing part of the CISAE, we refer to the documentation of the EMSA CISE specifications, see [35]. The core concept is to have CISAE nodes in each participating Member State to which local systems can be connected. The CISAE nodes exchange information in a common format which is then translated into the formats of the Member States' local systems. Information sharing is discretionary and controlled by the information owner/source. End to end data is used for information sharing.

Data fusion and analysis tools may be implemented locally in each Member State, in joint efforts or as a common system function. Storage tools may be introduced when required for the analysis and/or for logging. These tools can be connected to or implemented in CISAE nodes.

The CISAE will be easily extended to include new users and organizations, while local systems and analysis tools can be connected and integrated stepwise.

The CISAE must have extremely high cyber security. It should build on established principles and best practices for how information exchange between organisations in Member States is protected. The CISAE will not, in the information sharing part, be particularly sensitive to changes in threat vectors. Analysis tools may however exhibit such sensitivity.

Implementation: The system architecture will be similar to the architecture of the EMSA CISE hybrid model as shown in Figure 15. Illustration of how legacy systems are connected in EMSA CISE. In Figure 16 shows a corresponding picture for a CISAE.

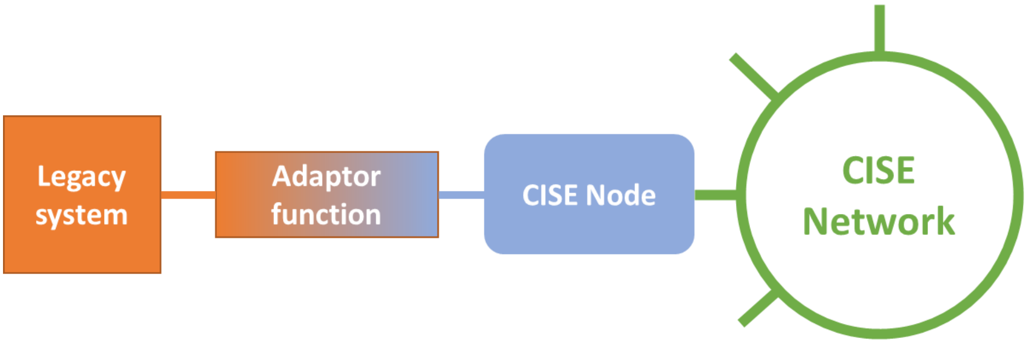


Figure 15. Illustration of how legacy systems are connected in EMSA CISE.

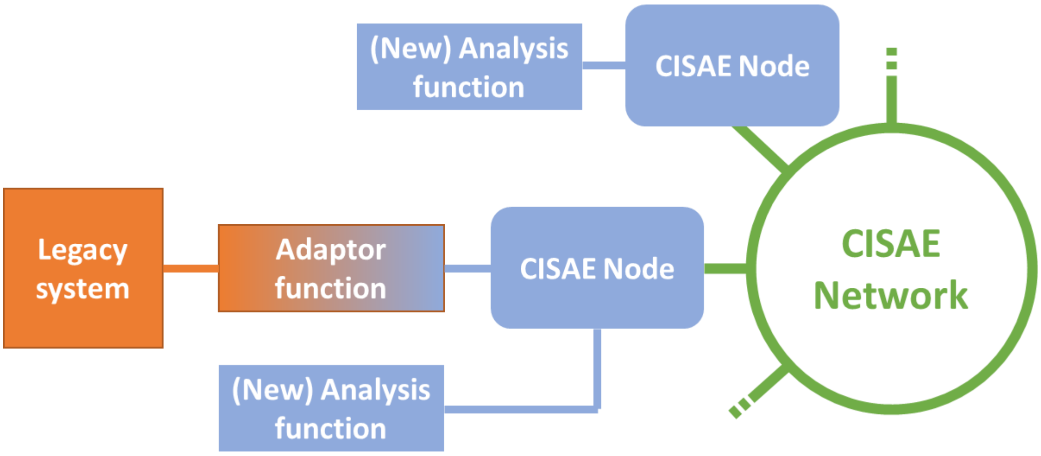


Figure 16. Illustration of CISAE connection with new analysis functions

- <u>**Operational description**</u>

The local services used by the different Member State organizations remain (in principle) the same. Only new services like data fusion, analysis and storage tools have to be introduced. Agreements between Member States and organizations define which information that is shared, based on which protocol or a specific format (e.g. it can be based on existing protocols such as the METHANE, [34], which is used for incident reporting), and with whom. Access control mechanisms are implemented to enforce the sharing rules. For joint services, agreements have to be developed, regarding how results are shared and with whom.

A governance body must be created to initiate and lead the development of the CISAE and define sharing and analysis targets aligned with the European Programme for Critical Infrastructure Protection (EPCIP) [36] and the Directive on European Critical Infrastructures [37]. It should also ensure that needed updates and upgrades of the CISAE are agreed and included in relevant standards and architecture documents. The governance body should also initiate and oversee development of all analysis tools intended for shared use. The governance body should preferably be connected to existing EU activities in Critical Infrastructure protection like the European Reference Network for Critical Infrastructure Protection (ERNCIP) [38] or ENISA [39]. Nevertheless, CISAE should foresee compliance with upcoming directives, such as the Directive on the resilience of critical entities (CER), [40], or the Network and

Information Systems (NIS2) Directive, [41], being also ready to connect with the new EU instruments, such as the Commissions Critical Entities Resilience Group, the European Union Member States Cyber Crisis Liaison Organisation Network (CyCLONe, the operational EU CSIRT network, the strategic NIS cooperation group, etc.

- **Road mapping**

The EMSA CISE is operational and if the CISEA takes the CISE architecture and information sharing principles as a starting point (TRL 6), the CISE part of the CISEA could probably be developed within three plus years. However, the maturity of the analysis tools to be implemented may differ greatly depending on if they build upon established solutions or if they are new developments.

Actions required for the implementation of the solution are:

- Agree and install a governance body as described in the operational requirements above.
- Set up an organization responsible for defining, specifying and implementing the CISAE, including interoperability protocols, data exchange formats and procedures. This is mainly a development and not a research activity.
- Develop a framework and template agreements between Member State organizations to recommend which information to share with whom and how it can be used.
- Set up an organization for defining required analysis tools and the implementation of the required research and development activities.
- Agree on where and how analysis tools should be implemented and operated. Federated learning solutions should be reviewed to investigated with respect to offering efficient distribute analysis without the need to share sensitive information.

5.1.3 THE THIRD COLUMN – THE RESOURCES

- **Required development resources**

The development of the information sharing part of a (sector specific) CISAE, building on the EMSA CISE, will in essence be a straightforward engineering activity. Some resources with sector expertise will be needed to define which information to share and the standardization of exchange formats.

The design and development of the intelligent analysis tools will require sector specific expertise as well as expertise in machine learning and AI and would require the set-up of EU research projects supported by the European Commission. It should be an ongoing activity to be able to cope with new threats attacks. Competition for resources may be an issue in this area.

- **Required operating support system**

A governance body, possibly a part of the European Reference Network for Critical Infrastructure Protection (ERNCIP) or ENISA, which controls the specifications and oversees the operational procedures of the CISAE, including maintenance, updates and upgrades. It should also provide a forum for the CISEA stakeholders to discuss and share experiences and agree on CISAE improvements and extensions. Furthermore, the governance body should initiate activities and research for development of new analysis tools.

- **CAPEX & OPEX**

  Based on the descriptions of the requirements for development and operational resources for we estimate that the CAPEX for the set-up of the organization and the initial development work would be in the order of 7 – 10 MEURO. The required resources for the research in analysis tools would most likely require 2 to 3 research projects with a budget of 3 - 5 MEURO each.

  Maintenance, updates and upgrades of the specifications of the system would be relatively low effort activities which would require no more than 1 to 2 man-years per year. After the initial research work to develop analysis tools, a budget of 1 MEURO per year seems reasonable.

  The total cost to launch the solution as proposed here with the suggested research activities would then be in the order of 20 – 30 MEURO over 3 - 4 years. Operating costs would, according to the estimates above, be in the order, that is 1 – 2 MEURO, after the CISAE has been developed and the initial launch of the solution.

  The cost estimates above reflect our experiences and knowledge about the development efforts and costs for EMSA CISE.

5.1.4 THE FOURTH COLUMN – THE UPTAKE ENVIRONMENT

- **Competition and market**

  There are a number of initiatives to increase the security in critical infrastructures, an overview of work in progress presented by the European Commission Migration and Home Affair can be found in [42]. An existing information sharing network is the Critical Infrastructure Warning Information Network (CIWIN) [43] offering recognised members of the EU's CIP community the opportunity to exchange and discuss CIP-related information, studies and/or good practices across all EU Member States and in all relevant sectors of economic activity. The CIWIN portal, following its prototype and pilot phases, has been up and running since mid-January 2013. However, it does not cover real-time sharing, and as far as we understand, there is no ongoing initiative with the vision and scope of the solution proposed here.

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

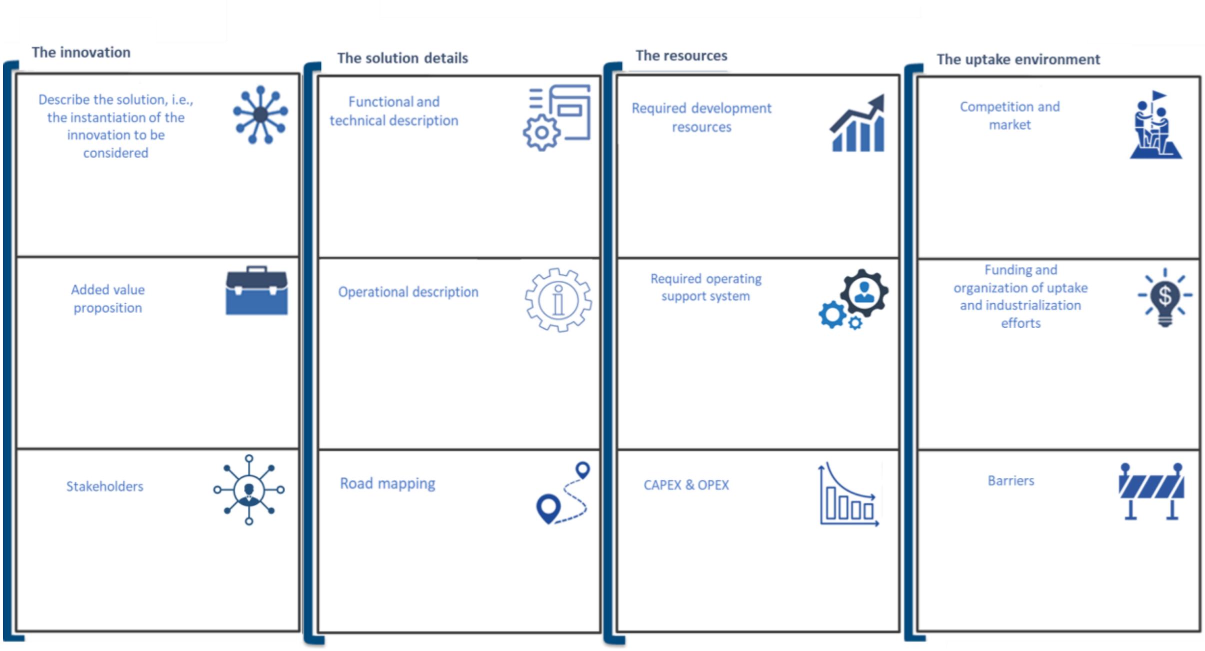
  The roadmapping indicates that it needs to be an EU initiative behind the realization and development of the proposed CISAE. The development of a (sector) specific CISAE will probably never take place without such an initiative and allocation of the required funding. However, we note that the EU already have many actions in the area and this would only be a minor add-on to the already ongoing efforts.

- **Barriers**

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

  - To implement the required operational structures as a concrete and institutional and legal framework is missing.
  - To engage the relevant practitioners, end-users and organizations in all Member States and convince them all that this is the right way to proceed. This should in general not be too hard as it already has been decided that protection of the European Critical Infrastructure must be improved and that sharing of threat and attack information for situational awareness and coordinated responses is key.
  - To develop trust both at EU and Member States level in the context of information-sharing. Trust in other parties' security and operational practices may be missing. Regulations and laws have to be reviewed to find the cases when information cannot be shared.
  - To agree on which information to share with whom and how.
  - To organize the funding of the required development and research work.
  - Availability of sector specific competence and machine learning may be scarce.

5.2 DEBUNKING OF FAKE NEWS


The innovation
Describe the solution, i.e., the instantiation of the innovation to be considered
Added value proposition
Stakeholders
The solution details
Functional and technical description
Operational description
Road mapping
The resources
Required development resources
Required operating support system
CAPEX & OPEX
The uptake environment
Competition and market
Funding and organization of uptake and industrialization efforts
Barriers

5.2.1 THE FIRST COLUMN – THE INNOVATION

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

  The **Debunking of fake news** innovation has been narrowed down into a solution for near real-time situational awareness regarding disinformation campaigns in the public space by monitoring, sharing and analysis of related domestic as well as foreign activities and events in a CISAE. This excludes topics like media literacy campaigns and issues around use of human fact checkers.

Situational awareness is key in detecting campaigns and threats and to be able to mitigate attacks. The more information available, if analysed correctly, the better the situational awareness. We note that the skills, data and capabilities to detect and disrupt what is happening on the Internet often reside within the private sector. In the Action Plan against Disinformation [44], it is stated that "The first hours after disinformation is released, are critical for detecting, analysing and responding to it".

The CISAE users would be practitioners and relevant public and private users and organizations involved in following and trying to control and mitigate disinformation campaigns.

SCOPE: Authorities, practitioners (in public and private sector)

VISION: Practitioners in all MS will be able to have (near real-time information about ongoing disinformation campaigns increasing general and specific situational awareness.

MISSION: Monitor national and foreign digital media and other domains. Perform joint analysis and deconstruction of disinformation in fully and / or semi-automatic manners. Enable information exchange between Member State organizations from the public and private sector in a CISAE. Trust building.

STRATEGY: Build on EMSA CISE [33], Debunk.eu [45], EEAS RAS [46] and similar solutions.

- Deploy information exchange network
- Deploy monitoring tool
- Develop and deploy analysis tools
- Instil measures to build trust

LIMITATIONS: Compared to the original innovation, this solution is limited in that it only considers monitoring, sharing and analysis of disinformation campaigns. It does not integrate identification of disinformation and responses from civilians and / or society in more broad sense.

RATIONALE: Sharing of information from many sources about activities and events related to or indicating disinformation campaigns will increase the possibilities for immediate or at least very early detection such campaigns. It will in also make it possible for to base individual and / or joint counter actions on a collective situational awareness. Identification, sharing and analysis is a pre-condition to debunking and note that early identification may increase chances for pre-bunking.

- **<u>Added value proposition.</u>**

NEED: Provide near real-time common situational awareness in all Member States to allow for alerts and rapid joint mitigation actions.

IMPACT: Countermeasures against disinformation campaigns can be launched earlier and more effectively. It will greatly improve the resilience of the society against such campaigns.

VIABILITY: The viability of the solution can be deduced from the successful operation of DebunkEU.org. DebunkEU.org is a digital platform and an independent crowdsourced analytical centre, whose main task is to research disinformation in the public space and execute educational media literacy campaigns. By employing artificial intelligence, Debunk.EU [45] carries out detailed research on disinformation in the Baltic states and with crowdsourced local experts' involvement, spots and identifies disinformation within 2 minutes from real time.

- **Stakeholders and domains**

GAPS AND NEEDS: The solution is related to the following gaps and needs as defined by WP2 in D2.9 [28]:

- Distinguishing fake from real
- Increase resilience against manipulated information.
- Governmental trust building and situational awareness

JRC DOMAINS: The solution is in the Information domain.

STAKEHOLDERS: The core stakeholders of course are the Member States practitioners involved in monitoring, handling and countering disinformation campaigns. The responsibility for the realization of the solution will lie on them and related EU organizations like the EEAS. Actors specialized in monitoring of disinformation campaigns or collection and analysis of cyber threat information will also be important stakeholders.

5.2.2 THE SECOND COLUMN - SOLUTION DETAILS

- **Functional description**

For the CISE part, i.e., the information sharing part of the CISAE we refer to the documentation of the EMSA CISE [33]. The core concept is to have CISAE nodes in each participating Member State to which local systems can be connected. The CISAE nodes exchange information in a common format which is then translated into the formats of the Member States' local systems. Information sharing is discretionary and controlled by the information owner/source. End to end data is used for information sharing.

Information exchange may use existing standards like MISP[47], STIX [48] and other standards with required extensions to fulfil the needs of the CISAE.

Monitoring of media to detect and follow disinformation campaigns in (near) real-time need to be supported by 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 users of the CISEA to limit unnecessary duplication of efforts. The monitoring should be done where it has best access to media. Analysis could be distributed or centralized and possibly be based on federated machine learning principles. Data fusion and analysis tools may also be implemented locally in each Member State. Storage tools may be introduced when required for the analysis and/or for logging. These functions can be implemented in or connected to CISAE nodes.

The CISAE will be easily extended to include new users and organizations and local systems and analysis tool can be connected and integrated stepwise. The CISAE must have a very strong cyber security infrastructure. It should build on established principles and best practices for how information exchange between organisations in Member States is protected.

The CISAE will not, in the information sharing part, be particularly sensitive to changes in threat vectors. Analysis tools may however exhibit such sensitivity.

Implementation: The system architecture will be similar to the architecture of the EMSA CISE hybrid model as shown in Figure 15 and Figure 16.

- **Operational description**

  A governance body must be created to initiate and lead the development of the CISAE and define monitoring, sharing and analysis targets aligned with EU Democracy Action Plan [49] and the Action Plan against Disinformation [50]. It should also ensure that needed updates and upgrades of the CISAE are agreed and included in relevant standards and architecture documents. The governance body should also initiate and oversee development of all analysis tools intended for shared use.

  Currently used local services used by the different Member State organizations remain (in principle) the same.

  New services like media monitoring, data fusion, analysis and storage tools have to be introduced. Then there is a need for agreements between Member States and organizations which define which information that is monitored and shared with whom. Access control mechanisms are implemented to enforce the sharing rules. For joint services, agreements have to be developed, regarding how results are shared and with whom.

- **Road mapping**

  The actions required for the implementation of the solution are:

  - Set up a governance structure and body to define the final scope of work. The governance body should preferably be connected to existing EU activities in countering disinformation like the Strategic Communications in the European External Action Services (EEAS) [51] or possibly the European Digital Media Observatory (EDMO) [52].
  - Organize a requirement owners' forum which is tied to the governance structure and operates as a reference group for all implementation issues.
  - Set up an organization responsible for defining, specifying and implementing the CISAE, including data exchange formats and monitoring and analysis procedures. This is mainly a development and not a research activity.

- Develop a framework and template agreements between Member State organizations to recommend which information to share with whom and how it can be used.
- Set up an organization for defining required analysis tools and the implementation of the required research and development activities. Federated learning solutions should be reviewed and be investigated with respect to offering efficient distributed analysis without the need to share sensitive information.
- This activity would probably benefit from close cooperation with EDMO [52].
- Agree on where and how monitoring and analysis tools should be implemented and operated.
- Organize EU funding for projects to research the monitoring and analysis issues at hand. 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. It would probably be valuable to have several projects to research the issues at hand.
- Define how maintenance, update and upgrades will be organized, define responsibilities and set up required bodies to perform the work.

5.2.3 THE THIRD COLUMN – THE RESOURCES

- **Required development resources**

  The set-up of the governance body in itself and the work to define the detailed scope of work should not require any major resources.

  The development of the information sharing part of the CISAE, building on the EMSA CISE, will in essence be a straightforward engineering activity. Some resources with specific expertise in the disinformation area and threat intelligence will be needed to define which information to share and for the standardization of the corresponding exchange formats.

  The development of needed and required fully or semi-automatic analysis tools will require resources for their design and implementation. The monitoring of media will have to rely on available interfaces unless new ones can be agreed and their implementation enforced.

  The roadmap proposes several EU funded projects to establish the required knowledge base and the development of the monitoring and analysis tools. The required resources for this part of the work will be researchers with expertise in hybrid threats, disinformation procedures and targets, federated machine learning and AI. We find it reasonable to start two to three three-year 3 MEURO projects for these tasks.

- **Required operating support system**

  A governance body, possibly a part of EEAS Strategic Communications [51] or EDMO [52], should be established, which controls the specifications, the development and oversees the operational procedures of the CISAE, including maintenance, updates and upgrades. It should organize a forum for the stakeholders to serve as a reference group for the CISAE development and to discuss and share experiences and agree on CISAE improvements and extensions.

Furthermore, the governance body should initiate activities and research for development of new analysis tools.

- **CAPEX & OPEX**

  The CAPEX and OPEX estimates in this section follow the same considerations as for the CIP CISAE in Section 5.1.3 and we estimate that the required effort to implement a disinformation CISAE is of the same order:

  - The CAPEX for the set-up of the organization and the initial development work would be in the order of 7 - 10 MEURO.
  - Two to three research projects with a budget of 3 -5 MEURO each.
  - Maintenance, updates and upgrades of the specifications of the system would be relatively low effort activities which would require no more than 1 to 2 man-years per year. After the initial research work to develop analysis tools, a budget of 1 MEURO per year seems reasonable.

  The total cost to launch the solution as proposed here with the suggested research activities would then be in the order of 20 - 30 MEURO over 3 - 4 years. Operating costs would, according to the estimates above, be in the order, that is 1 – 2 MEURO, after the CISAE has been developed and the initial launch of the solution.

5.2.4 THE FOURTH COLUMN – THE UPTAKE ENVIRONMENT

- **Competition and market**

  There are a number of initiatives in the field of understanding and deconstructing disinformation. One could first mention the DebunkEU.org project [45] which inspired the proposed solution. Furthermore, EU has launched a number of activities like the EDMO [52] and the EEAS Rapid Alert System on disinformation [46]. RAS has as target to provide rapid alerts and enable individual or joint counter actions, but has as far as we understand, not been used for such purposes. Furthermore, the EU Hybrid Fusion Cell mentioned in [53], the EDMO [52],the EEAS StratCom task forces, e.g. the East StratCom Task Force [54] and the EUvsDiSiNFO flagship project[55], all perform analysis and debunking activities. However, there is no, as far as we understand, ongoing initiative with the vision and scope of the proposed solution.

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

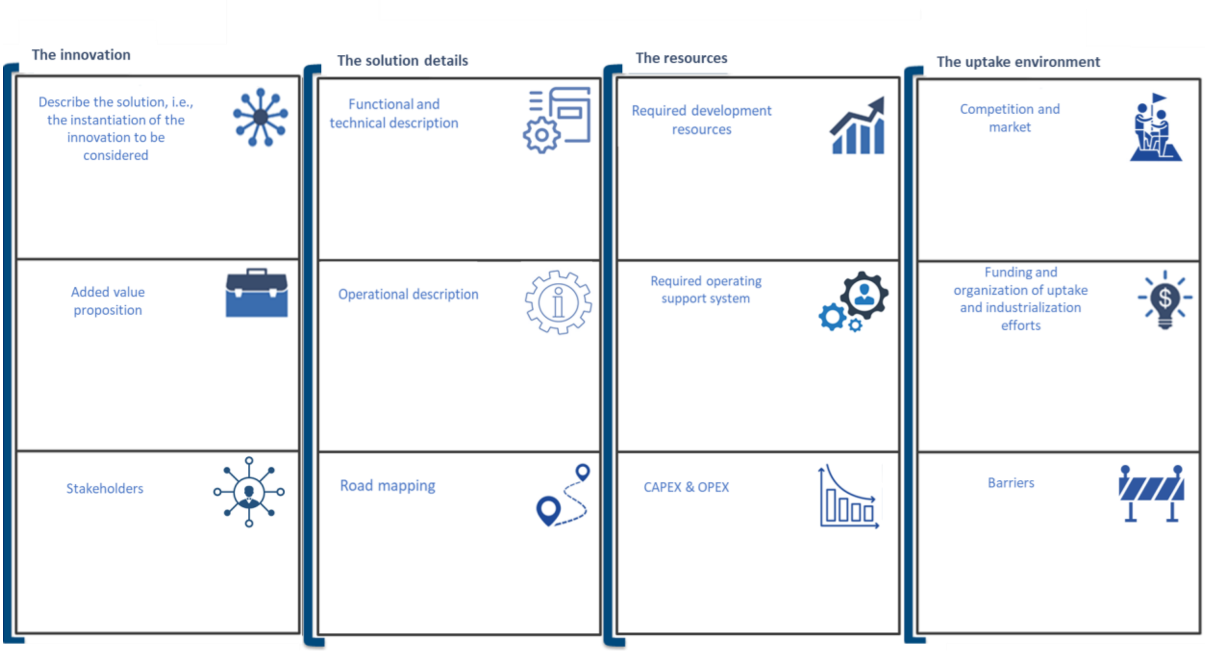
  The roadmap points at that it must be an EU initiative behind the realization and development of the proposed solution. This solution would most likely never happen without such an initiative and the required corresponding funding. In particular, we note that the EU already has a number of activities in the area of handling and understanding disinformation and that the proposal just would be a relatively small extension of the already ongoing activities.

- **Barriers**

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

- To engage the relevant practitioners, end-users and organizations in all Member States and convince them all that this is the right way to proceed. This should in general not be too hard as it already has been decided that the awareness and handling of disinformation campaigns must be improved. However, as has been shown in a special report on disinformation [56], the activity level varies greatly between Member States.
- To develop trust both at EU and Member States level in the context of information-sharing about disinformation campaigns. This will be especially so, if also Member State internal disinformation campaigns are in scope. Then trust in other parties' security and operational practices may be missing.
- To agree on which information to share with whom and how.
- To organize the funding of the required development and research work.
- Availability if sector specific competence and in machine learning may be scarce.

5.3 TRAINING APPLICATION FOR MEDIA LITERACY



The innovation

Describe the solution, i.e., the instantiation of the innovation to be considered

Added value proposition

Stakeholders

The solution details

Functional and technical description

Operational description

Road mapping

The resources

Required development resources

Required operating support system

CAPEX & OPEX

The uptake environment

Competition and market

Funding and organization of uptake and industrialization efforts

Barriers

5.3.1 THE FIRST COLUMN – THE INNOVATION

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

The **Training application for media literacy** innovation has been transformed into a solution which in one way is more generic but in another sense is narrower, as its target audience is smaller. The solutions are concerned with the required foundations for bringing media literacy competence to students. This to increase their and the society's resilience against disinformation campaigns.

SCOPE: Students, 9 -12 graders.

VISION: Young people in EU MS are inoculated against misinformation and fake news.

MISSION: Get media literacy education and training into all 9 -12 graders' curricula in the EU.

STRATEGY: Develop easy to follow frameworks, methods and tools for creation of media literacy course material. Develop engaging gaming models for important course components.

LIMITATIONS: Compared to the original innovation, this solution is limited in that it does not concern direct development of course material and/or training apps.

RATIONALE: Media literacy is a wide area and concerns many aspects, but at the core it is about having the competence to control one owns interpretation of presented media and not uncritically accept any overt message. Media literacy' refers to skills, knowledge and understanding that allow citizens to use media effectively and safely and equip them with the critical thinking skills needed to exercise judgment, analyse complex realities and distinguish between opinion and fact, see [57]. However, the way to express ideas and information varies between cultures, languages and communities, so to reach all citizens with media literacy training it is necessary to have trainings adapted for the respective audiences. Furthermore, it is important to have multiple providers of media literacy training programs to exclude claims that the training is a centralized program for indoctrination about correct opinions and thinking. Thus, we propose to build a profound basis for the production of media literacy training programs on which involved companies and organizations can base their developments.

Added value proposition.

NEED: Improved media literacy will enhance the resilience of citizens against disinformation campaigns which in turn will make society as a whole more resilient against hybrid threats and attacks. We also note that the Audio-Visual Media Services Directive states that Member States shall promote and take measures for the development of media literacy skills. Furthermore, the Special Report on "Disinformation affecting the EU: tackled but not tamed" [56] finds that there is no overarching media literacy strategy that includes tackling disinformation and that there are major differences in activities between MS in the area.

IMPACT: The proposed solution will stimulate production of media literacy training course material and apps for students. By inclusion of media literacy training in the curriculum of 9 – 12 graders the understanding and competence of how to use media effectively and safely will gradually but steadily increase resilience against hybrid threats and attacks in society.

VIABILITY: Within the EU and in many other countries serious work on defining frameworks and tools for media literacy are ongoing. One example of an organization with long experience in the field is the Center for Media Literacy [58] in the US which as a resource provides:

> *The* ***CML MediaLit Kit™****, … , an accessible, integrated, research-based teaching strategy needed to assist schools and districts in organizing and structuring teaching activities using a media literacy lens. Based on longstanding theoretical foundations and a research-based approach, education tools contained in the* ***CML MEDIALIT KIT****™ reflect a philosophy of empowerment through education and articulate the key components of an inquiry-based media literacy education.*

- **Stakeholders and domains**

Gaps and needs: The solution is related to the following gaps and needs as defined by WP2 in D2.9, [28]:

- Increase resilience against manipulated information.
- Media impoverishment, i.e., reduction of media landscape richness.

JRC domains: The solution is in the Information domain.

Stakeholders: The core stakeholders in the actual innovation are requirements owners and researchers and developers. The following groups of stakeholders have been identified:

Requirement owners

1. EU-level media literacy policy makers.
2. Media literacy policy makers, prominently educational departments/organizations on governmental level. National curricula.
3. Media literacy policy makers, prominently educational departments/organizations on local level. Local curricula.
4. Teachers and students.

Researchers and developers

1. Media literacy research organizations and researchers.
2. Companies and organizations developing media literacy course material and training apps.

5.3.2 THE SECOND COLUMN - SOLUTION DETAILS

- **Functional description**

The proposed solution is to develop easy to follow frameworks, methods and tools for creation of media literacy course material and to develop engaging gaming models for important course components. In essence this means to research several areas a) media literacy training with focus on how to handle disinformation, b) media literacy relevant differences in cultural, language and community codes c) efficient models for how to design efficient training apps for different media literacy aspects. Based on this research develop skeletons of tools (automatic or semi-automatic) for creating (adapted) media literacy training curricula and course material according to the requirement owners' specifications. The requirement owners should cooperate and develop common requirements.

- **Operational description**

This solution, i.e., the initial development of an easy-to-follow frameworks, methods and tools for creation of media literacy course material and the development of engaging gaming models will produce a solution which is up-to-date when delivered. Many components and training models exist already today; what is missing is the overarching framework. But this situation also means that it most likely will be possible to use a step-by-step approach in building a coherent framework.

The frameworks and the models need to be continuously updated and follow the developments in different media and in disinformation approaches. There will thus be a need for a forum to discuss new requirements and a body of experts that regularly review the framework and its models and propose and implement updates.

There will also be a need for updates of course material and teacher training. This can most likely take place via introductory courses organized by the companies and organizations involved in the actual production of course material.

Road mapping

The actions required for the implementation of the solution are:

- Set up a governance structure and body to define the final scope of the work. Could possibly be the tied to the Media Literacy Expert Group (MLEG)
- Organize a requirement owners' forum which is tied to the governance structure.
- Let the governance body define a detailed, evidence based, research program for media literacy following the proposed solution.
- Organize EU funding for one or more projects to research the issues at hand. 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. It would probably be valuable to have more than one project research the issues at hand.
- Based on the project results, the governance body should establish and publish recommendations and guidance documents for the frameworks, methods, tools and gaming models to use.
- Define how maintenance, update and upgrades will be organized, define responsibilities and set up required bodies to perform the work.

5.3.3 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, tools and training app skeletons. The required development resources for this part of the work will be researchers in media literacy and app/game developers. We find it reasonable to start two three-year 3 MEURO projects for these tasks. This estimate takes into account the possibilities to cooperate with EDMO and the just launched setup of the eight EDMO local nodes (cost 11 MEURO). Coordination of research activities should of course be encouraged/enforced.

The set-up of the governance body and to define the detailed, evidence based, research program for media literacy following the proposed solution should not require any major resources. The work with local adaptations will require involvement of local media literacy experts and admin personnel. It is hard to estimate the total efforts required before knowing what the framework, tools and apps will look like. But each adaptation task will most likely require efforts in the order of man-years.

- **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 media literacy experts and 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, tools, apps and local adaptations will look like. But the update and upgrade work will most likely only require efforts in the order of 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 6 – 8 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 total cost to launch such a comprehensive action as proposed here would then be in the order of 10 – 15 MEURO over 3 - 4 years. Operating costs would, according to the estimates above, be of the same order, that is 2 – 3 MEURO per year but financed by each Member State.

5.3.4 THE FOURTH COLUMN – THE UPTAKE ENVIRONMENT

- **Competition and market**

  There are a number of initiatives in the field of media literacy and there are tools and educational material available. However, there is no, as far as we understand, ongoing initiative with the vision and scope of the proposed solution.

  Examples on ongoing initiatives in the area are:

  - MLEG, the EU Media literacy expert group [59].

- The Center for media literacy [58].
- A course developed by the Erasmus+ project Crescent [60] in which KEMEA is active. The course is on Strategic Communication to Counter Security Threats in the Disinformation Era [61].
- A web page with best apps for teaching media literacy [62].
- The CommonSenseEducation web page with parental guidance on media literacy training [63].
- The International Society for Technology in Education (ISTE) web page presenting 10 resources to boost student media literacy [64].
- ERASMUS Student Network (ESN) has launched a training program on media literacy [65].
- YLE (Finnish broadcasting company) troll factory training app [66]

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

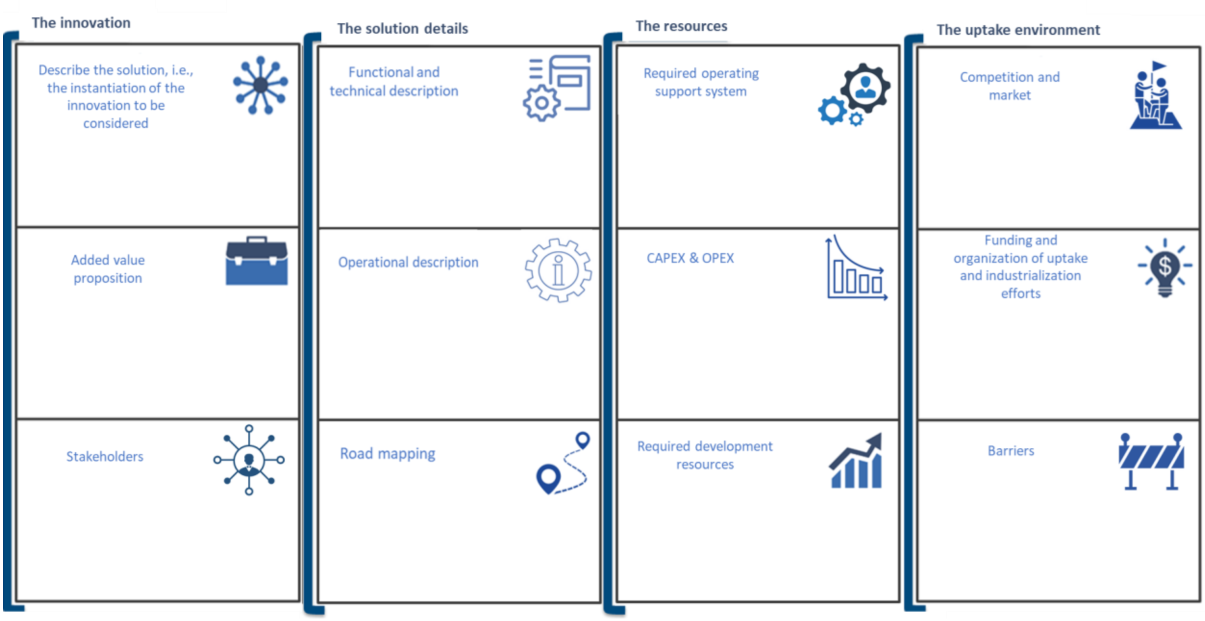
  The roadmap points at that it must be an EU initiative behind the realization and development of the proposed framework, tools and app skeletons and the required local adaptations. This would most likely never take place without that initiative and the required corresponding funding. In particular, we note that the EU already has expressed interest and has tried to initiate work as Member States are asked to rapidly implement the media literacy provisions of the Audio-Visual Media Services Directive.

- **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 it already has been decided that media literacy is an essential competence for EU citizens.
  - To engage the MSs in the work and get them involved. As has been shown in the special report on Disinformation [56], the activity level varies greatly between Member States.
  - To organize the funding of the research activities and the related local adaptations.

5.4 GUIDES TO IDENTIFY FAKES


The innovation
Describe the solution, i.e., the instantiation of the innovation to be considered
Added value proposition
Stakeholders
The solution details
Functional and technical description
Operational description
Road mapping
The resources
Required operating support system
CAPEX & OPEX
Required development resources
The uptake environment
Competition and market
Funding and organization of uptake and industrialization efforts
Barriers

5.4.1 THE FIRST COLUMN – THE INNOVATION

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

The **Guides to identify fakes** innovation has been transformed into a solution for bringing competence to Member State citizens on how they can detect that media is "fake", i.e., digitally generated or that images, video and audio have been altered. The main objective is to increase citizens' and thereby society's resilience against disinformation.

SCOPE: Member State citizens.

VISION: EU Member State citizens know about and are proficient users of tools to detect digitally generated or altered images, video and audio.

MISSION: Publish and distribute guides on how to identify "fakes" and the use of available tools Promote integration of detection tools in media consumption apps. Promote use of reputation systems regarding tools and media sources. Promote development of a multitude of different tools.

STRATEGY: Produce a registry of existing and upcoming methods and tools for identifying "fakes". Review which media channels to use with respect to their effectiveness in reaching different user groups depending on culture, language and media environment. Develop appropriate guides and promotion material for the different channels and user groups. Define and standardize interfaces of detection tools. Propose voluntary and regulatory measures to ensure integration of detection tools in media consumption apps.

LIMITATIONS: Compared to the original innovation, this solution is limited in that it does not concern the development of detection tools or apps, only promotion of their use.

RATIONALE: Being able to detect "fake" media in the form of digitally generated or altered images, video and audio is a first basic step in learning how to reveal and counter disinformation. By making all EU citizens aware of the available tools and methods for detection, it will be much harder for different actors to launch successful disinformation campaigns. Furthermore, it is important to have multiple providers of methods and tools to exclude claims that their use is part of a centralized program for enforcing politically correct opinions and thinking. Integration of tools in media consumption apps should be according to a concept of add-ons so that users can chose a solution which they trust.

- **Added value proposition.**

NEED: Improved competence in revealing "fake" media will enhance the resilience of citizens against disinformation campaigns which in turn will make society as a whole more resilient against hybrid threats and attacks. Tools to reveal fakes and/or establish the true origin of media needs to be easily and trustworthy integrated in the media consumption infrastructure.

IMPACT: It will be much harder for threat actors to launch disinformation campaigns with high penetration and acceptance.

VIABILITY: The viability of the solution can be safely assumed as several training and detection tools are available on the web, see e.g., the 13 tools presented by stopfake.org [67]. Another example is that Maldita.es has integrated a WhatsApp interface and service for fact checking. Efficient means for reaching different consumer groups based on culture, language etc are well research and are directly available from marketing and media companies.

- **Stakeholders and domains**

GAPS AND NEEDS: The solution is related to the following gaps and needs as defined by WP2 in D2.9, [28]:

  - Distinguishing fake from real.
  - Support media literacy of citizens to increase trust in official communication.

JRC DOMAINS: The solution is in the Information domain.

STAKEHOLDERS: The core stakeholders are of course the Member States citizens.

For the realization of the solution and the corresponding information campaign, the responsibility will lie on practitioners in each Member State, in particular the authorities responsible for measures to counter disinformation campaigns.

An EU body, e.g., EDMO, should have the responsibility for maintaining an inventory of existing tools to detect digitally generated or altered images, video and audio.

Local/national authorities should be responsible for developing and maintaining the guides.

An EU body, e.g., EDMO, should promotes activities aiming for the integration of tools to detect “fakes” in media consumption apps and which ensures that there is an associated reputation system.

5.4.2 THE SECOND COLUMN - SOLUTION DETAILS

- **Functional description**

The functional components in the solution are few and standardized. The key component would be a database (centralized or distributed), containing all the identified tools and corresponding guides in all languages and all versions adapted for different target groups.

A second functional component would contain an associated reputation system, if it is deemed necessary to have a dedicated solution for this context.

- **Operational description**

This base of the solution, i.e., the initial inventory of existing tools and guides for their use is a one-time effort of limited scope. The update of the inventory could be integrated in other existing reporting and situational awareness solutions, e.g., EUvsDiSinfo [55] or EDMO, [52].

The development of guides should build upon a philosophy of sharing, both actual guides and best practices, and this also goes for marketing concepts used and developed, the promotion material and the guides for how to reach different groups.

The database of tools and guides needs to be continuously updated and follow the developments in different media and in disinformation approaches. There will thus be a need for a forum to discuss the current situation and review the concepts used in the development of guides, promotion material and outreach.

- **Road mapping**

The actions required for the implementation of the solution are:

- Set up a governance structure to define the final scope of work. Could possibly be the tied to the European Digital Media Observatory (EDMO).
- Organize the development/implementation of the database solutions and a reputation system.
- Have the governance body initiate work in the areas of:
    - Initiate and support national/local activities.
    - Promote joint work and sharing.
    - Inventory of existing tools and guides.

  - Investigations to find the most efficient methods for reaching different user groups.
  - Development of guides and promotion material.
  - Test and rating of guides.
  - Explore and execute actions to have an associated reputation system.
  - Organize regular meetings to review concepts used guides, promotion material and outreach.
- Organize standardization of media formats and interfaces for checking tools.
- Explore possible means and propose a solution for how to get the detections tools implemented in media apps. A possibility might be to include such requirements in the Code of Practice on Disinformation [68].

5.4.3 THE THIRD COLUMN – THE RESOURCES

- **Required development resources**

  The set-up of the governance body and the work to define the final scope of work should not require any major resources, especially if this task can be assigned to an already existing organization like EDMO [52]. The inventory work and the production of guides should be handled by national/local organizations and would also constitute a relatively small task.

  It is hard to estimate the total efforts required to develop locally and group specific promotion material before knowing what the recommendations by market experts /local organizations will be.

  The standardisation of media formats and interfaces should be left to the media app companies. The reputation system should preferably be integrated in already existing solutions.

- **Required operating support system**

  The governance body should ensure that there is a responsible organization for required updates and upgrades of the database and its content. The set-up of regular review meetings must also be supported.

  Test and rating of the detection tools will require some resources. Required resource will likely decrease over time as testing will be most needed when the system is launched,

- **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 work would be in the order of 1 – 2 MEURO.

  Operating expenses are expected to be 0,5 – 1 MEURO per year

5.4.4 THE FOURTH COLUMN – THE UPTAKE ENVIRONMENT

- **Competition and market**

  There are a number of initiatives to develop tools and guides to identify fakes. However, this solution does not compete with those as this is an effort to improve citizens competence in using these tools. As far as we understand, there is no ongoing initiative with the vision and scope of the proposed solution.

  Some examples for already existing guides/web tools are:

  - FotoForensics [69], for the analysis of images.
  - Amnesty International's Citizens Evidence Lab [70], which offers several guides on digital verification.

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

  - How to spot, avoid, and report fake check scams [71], by the US Federal Trade Commission Consumer Information.
  - The SHAREChecklist [72] by the British HM Government
  - Wie Sie Falschmeldungen erkennen [73], by the German Bundesregierung.

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

  The roadmap points at that it must be an EU initiative to support the actions described in the roadmap and implement the solution. This work would most likely never take place without such an EU funded initiative.

- **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 it already has been decided that media literacy is an essential competence for EU citizens.
  - To engage the Member States in the work and get them involved. As has been shown in the special report on Disinformation [56]. the activity level varies greatly between Member States
  - To get media app providers interested in integrating the checking tools interfaces and allow such add-ons.

6 RECOMMENDATIONS

In this first cycle of the EU-HYBNET project we have, by analysing four innovations found that there are important actions to be taken in the areas of increasing resilience in critical infrastructures and building resilience against disinformation campaigns.

In both areas we have seen a need for improving (near) real-time situational awareness to enable timely responses and mitigating actions. To be effective, such responses and actions require cooperation between different stakeholders; stakeholders in one or different member state, stakeholders in the public and private sectors and that the stakeholders have a common view of the situation at hand. The studies have also revealed that new fully or semi-automatic analysis tools will be required to cope with the increasing amount of information that has to be monitored, scanned and analysed for suspicious activities and/or attacks. As sharing of information may be sensitive, federated machine learning may be one avenue to implement efficient analysis tools without compromising required secrecy of monitored data and events.

In the area of disinformation, we have also found that increasing media literacy in the population is an important step in increasing the society's resilience against disinformation. Part of media literacy is to learn how to detect and use tools to detect that digital media has been manipulated. Another more generic media literacy skill is to learn about drivers behind disinformation campaigns and how they are instigated and spread. An important condition is that the media literacy and guide to identify fakes innovations need to work in tandem to be fully effective, as they (potentially) target different parts of the population that, in turn, affect each other (i.e., students impacting families and vice versa). As well, it is important to see the role and influence of civilians/citizens as a stakeholder in many of these innovations (including "Debunking fake news", for example) even if they are not the primary actors implementing the innovation.

6.1 RECOMMENDATION 1: UPTAKE OF REVIEWED INNOVATIONS

In the review of the four innovations

1. Public-private information-sharing groups developing collaborative investigations and collective action.
2. Debunking of fake news
3. Training application for media literacy.
4. Guides to identify fakes.

We have not found any blocking issues for the corresponding solutions defined in section 5. We thus recommend that the proposed solutions are promoted for uptake and industrialization.

6.2 RECOMMENDATION 2: CISAE STANDARDIZATION

This recommendation is based on the two solutions Public-private information-sharing groups developing collaborative investigations and collective action and debunking of fake news. In particular we note that the solutions Public-private information-sharing groups developing collaborative investigations and collective action is relevant for all EU critical infrastructures. The recommendation is to

- Develop a framework for the implementation of information sharing and analysis environments (CISAEs). Build the information sharing functionality on the EMSA CISE [33], solution. Define principles for how analysis functionality can be implemented and analysis results be shared. The work should cover the needs for situational awareness in EU critical infrastructures and for monitoring and handling of disinformation campaigns.

Important non-technical principles are:

- CISAE is a voluntary collaborative process in the EU seeking to further enhance and promote relevant information exchange between different entities. It should bring added value and complementarity to existing (legacy) systems, services and sharing processes.
- CISAE's ultimate aim is to increase the efficiency, quality, responsiveness and coordination of counter operations in its field of operation.
- CISAE's objective is to ensure that relevant threats and activities detected and/or collected by one authority/private entity and considered necessary for the wider community, can be shared and be subject to EU level counter operations, rather than collected and produced several times, or collected and kept for a single purpose in limited network or eco-system in one Member State. Responsibility to share is a driving slogan in this initiative.
- CISAE should neither have an impact on the administrative structures of the Member States, nor on the existing EU legislation.

Important technical principles are:

- CISAE is not replacing or duplicating but building on existing information exchange and sharing systems and platforms.
- CISAE is promoting a decentralised framework for the information exchanges (no-central database, no external access).
- CISAE implements as a data model and a technical reference architecture for public and private services.
- CISAE is not a new system but a set of agreed specifications (for an interoperability layer) that, once implemented, will enable the information sharing e.g., findings exchange and the set of supporting tools (registries, collaboration tools, analysis tools etc.).

It is recommended that the CISAE framework is defined as an ETSI standard following and building on the standardization of the EMSA CISE in an ETSI Industry Specification Group [74]. An important new part in the CISAE compared to the EMSA CISE is the inclusion of the possibility to have joint analysis functions. The standard must thus define how such functions can be controlled, distributed and communicated. Furthermore, to make the CISAE framework generic it is proposed that the standard includes a methodology for creating data models for specific CISAE domains/sectors. This to get consistent data models with the best machine readability as recommended in EU SPARTA project deliverable D4.1 Cybersecurity threat intelligence common data.

6.3 RECOMMENDATION 3: RESEARCH FEDERATED MACHINE LEARNING ANALYSIS TOOLS

In the review of the two CISAE based solutions we have identified a potential barrier in the willingness of participants to share sensitive and/or secret information. We thus recommend that a research program is initiated to resolve which types of analysis tools that can be based on federated machine learning to remove this barrier. The work should also evaluate the effectiveness of such solutions with respect communication and computational needs, handling of large amount data, etc.

6.4 RECOMMENDATION 4: RESEARCH AUTOMATIC DECONSTRUCTION OF DISINFORMATION

In the review of the Disinformation CISAE solutions we have identified that the development of efficient automatic tools for the deconstruction of disinformation campaigns could become a barrier if not properly handled and researched. To allow continuous monitoring and analysis of all media streams automatic tools are needed. Thus, we propose that a research program covering this area is put in place.

6.5 RECOMMENDATION 5: RESEARCH IN MEDIA LITERACY

In the review of the Media Literacy solution, we have identified a need for research that covers how easy to follow frameworks, methods and tools for creation of media literacy course material should be constructed and also a need in the characteristics of engaging gaming models that can be used in media literacy training. This implies that research in several areas is needed: a) media literacy training with focus on how to handle disinformation, b) media literacy relevant differences in cultural, language and community codes c) efficient models for how to design efficient training apps for different media literacy aspects. d) efficient tools (automatic or semi-automatic) for creating (adapted) media literacy training curricula and course material for all age groups and according to the requirement owners' specifications.

6.6 RECOMMENDATION 7: MEDIA FORMATS

Standardization of media formats is recommended to enable simple interfacing towards tools applications that check provenance and authenticity of media in general and images, audio and video in particular.

6.7 RECOMMENDATION 6: UPDATES OF EXISTING EU INITIATIVES AND ACTIONS

Introduce CISAE as a solution in the European Programme for Critical Infrastructure Protection (EPCIP) [76], the Directive on European Critical Infrastructures [77] and as a complement to the Critical Infrastructure Warning Information Network (CIWIN) [78].

Introduce CISAE as a complement to the EEAS Rapid Alert System, [46]. Also introduce it as a tool for information sharing in the EU Democracy Action Plan [49], and the Action Plan against Disinformation [44]. Make it a tool which could be used the European Digital Media Observatory [52] in their work to understand and analyse disinformation and be a platform for cooperation.

Introduce requirements in the Code of Practice [68] on Disinformation for support of tools in media consumption applications that check provenance and authenticity of media in general and images, audio and video in particular.

6.8 RECOMMENDATION 8: PRIVATE SECTOR INVOLVEMENT

Set up a task force to conclude on how to enable participation of 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

6.9 RECOMMENDATION 9: CONTENT PROVENANCE AND AUTHENTICITY

Support and embrace content provenance and authenticity marking of media. As an alternative to the use of detection tools to identify digitally generated or modified media it is possible to rely on reliable media metadata for media attribution giving content provenance and authenticity proofs. Such a solution would in most cases be much simpler and effective than using detection tools.

The Coalition for Content Provenance and Authenticity (C2PA) [79] is a formal coalition for standards development in this area and the drafting of technical standards to form the foundation for a universal provenance solution. C2PA unifies the efforts of the Adobe-led Content Authenticity Initiative (CAI) [80], which focuses on systems to provide context and history for digital media, and Project Origin [81], a Microsoft- and BBC-led initiative that tackles disinformation in the digital news ecosystem.

7. LESSONS LEARNED

We have found that the methodology used with roadmapping and an innovation uptake canvas works well for both technical and non-technical innovations. However, its use could be simplified if some of the difficulties experienced (see below) could be remedied.

The main lesson learned is that the Innovation descriptions need to cover State-of-the-Art in a more profound way and that EU initiatives related to the scope of the 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.

We note that there are important activities in the field of disinformation (e.g., the EU Action Plan against disinformation with associated more specific activities like EDMO) and information sharing (e.g., EMSA CISE, WICIP). All this background information was only discovered in conjunction with the Task 4.2 work to formulate strategies for innovations uptake which meant that the work to the review the innovations took much more time than expected and that the actual time spent on the formulation of uptake strategies thereby was limited. This issue would have been resolved to a great extent if the upcoming deliverable D4.8, First report for standardisation recommendations, from Task 4.3 would have been available earlier. However, due to the project plan, D4.8 could not be changed to earlier delivery month, and the need to have D4.8 earlier was not known in advance

The second most 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 experts participating in innovation uptake workshops and review of the resulting uptake canvases.

The third most important lesson is that there is 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. In the future, the innovation testing in the EU-HYBNET training and exercises event and in T3.1 analysis will be more connected to T4.2 work.

Furthermore, 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. This idea has already been discussed with T3.1 and alignment is ongoing.

Finally, it should be noted that the project partners and persons involved in the Task 4.2 work in this first 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 for the contributions of all innovation Uptake Workshops participants and expert reviewers.

8. 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 2 the most significant contributions related to OBs and their relevant Key Performance Indicators (KPI) are listed.

Table 2. 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 <u>Targets:</u> -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 first project cycle, four innovations, with relations to each of the four project core themes, have been reviewed and uptake strategies proposed.
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 <u>Targets:</u> -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 first 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 <u>Target:</u> -At least 4 reports every 18 months that address technological innovations that are able to fulfill European actors' gaps and needs	In this first 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. As two of the innovation are non-technical, the monitoring has been limited to investigations about existing schemes and

			solutions for building common information sharing and analysis environments. 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 first 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 each of the project core theme.
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 first project cycle, strategies for uptake and industrialization are proposed. Common aspects are noted and will be part of the basis for generalized strategies.

9. 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 3, the D4.4's contribution to the three Lines of Action is provided.

Table 3. 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.
Priorities as regards of increasing knowledge and performance requiring standardisation.	Based on its review of the proposed innovations 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.

10. CONCLUSIONS

10.1 SUMMARY

In this document we have developed and described a framework methodology and a way-of-working for review of innovations, see section 5. Such a review results in an innovation uptake canvas comprising essential roadmapping steps for uptake and industrialization. In section 5, the methodology is applied on four innovations representing the four project core themes and innovation canvases are presented. In section 6, 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.

10.2 FUTURE WORK

In the next project cycle, the methodology will 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 D4.8, First report for standardisation recommendations, will be studied and taken into account.

ANNEX I. GLOSSARY AND ACRONYMS

Table 4 Glossary and Acronyms

Term	Definition / Description
AVMSD	Audiovisual Media Services Directive
C2PA	Coalition for Content Provenance and Authenticity
CAI	Content Authenticity Initiative
CAPEX	Capital Expenditure
CIP	Critical Infrastructure Protection
CISAE	Common Information Sharing and Analysis Environment
CISE	Common Information Sharing 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
EMSA	European Maritime Safety Agency
EMSA CISE	Theh European Maritime Safety Agency Common Information Sharing Environment
ENISA	European Union Agency for Cybersecurity
EPCIP	European Programme for Critical Infrastructure Protection
ERNCIP	European Reference Network for Critical Infrastructure Protection
ETSI	A European Standards Organization (ESO) and a recognized regional standards body dealing with telecommunications, broadcasting and other electronic communications networks and services. (ETSI stands for European Telecommunications Standards Institute)
EU	European Union
EU HYBRID FUSION CELL	The EU Hybrid Fusion Cell is a unit in the EU Intelligence and Situation Centre (EU INTCEN) of the European External Action Service (EEAS)
GDP	Gross Domestic Product is the standard measure of the value added created through the production of goods and services.
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)

MLEG	EU Media Literacy Expert Group
OPEX	Operating Expenditure
EUvsDiSiNFO	
PCP	Pre-Commercial Procurement
PPI	Public Procurement of Innovation
RAS	Rapid Alert System (on disinformation)
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

ANNEX II. REFERENCES

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

[2] EU-HYBNET Deliverable 3.1 "Identification of target areas for improvement and innovations: First interim report mapped on gaps and needs", TNO, July 2021

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

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

[5] EU-HYBNET Deliverable 4.1 "1st report on the procurement environment", KEMEA June 2021.

[6] European Commission, "Joint Framework on Countering Hybrid Threats", Join (2016) 18 Final, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016JC0018.

[7] Project I-LEAD: Innovation - Law Enforcement Agencies Dialogue, Horizon 2020, https://cordis.europa.eu/project/id/740685.

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

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

[10] Pichlak, Magdalena. (2015). The innovation adoption process: A multidimensional approach. Journal of Management & Organization. https://www.researchgate.net/publication/285547373_The_innovation_adoption_process_A_multidimensional_approach

[11] L.G. Tornatzky, M. Fleischer. The Processes of Technological Innovation. 3Publisher: Lexington, 1990

[12] H. P. Borgman, and et al., "Cloudrise: Exploring Cloud Computing Adoption and Governance with the TOE Framework", 2013 46th Hawaii International Conference on System Sciences, pp. 4425-4435, 2013

[13] SPARTA, EU Horizon 2020 project. https://www.sparta.eu/programs/t-shark/

[14] TELOS Methodology, https://en.wikipedia.org/wiki/Feasibility_study

[15] THOR Methodology. https://core.ac.uk/download/pdf/37831592.pdf

[16] Camino project. https://cordis.europa.eu/project/id/607406/reporting

[17] KTH Innovation Readiness Level Radar. https://kthinnovationreadinesslevel.com/

[18] Heikkilä, Marikka & Saarni, Jouni & Kaartemo, Valtteri & Koponen, Aki. (2015). Viability Radar: A Practical Tool for Assessing the Viability of Transformative Service Innovations in a Healthcare Context. Technology Innovation Management Review. 5. 17-30.

[19] SWOT Analysis. https://en.wikipedia.org/wiki/SWOT_analysis

[20] Choma, Joelma & Guerra, Eduardo & Da Silva, Tiago & Zaina, Luciana & Correia, Filipe. (2019). Towards an artifact to support agile teams in software analytics activities. 88-93.

[21] Strategyzer, The business model canvas.

[22] Jake Nielson, IGNITIONframework, The Innovator's Canvas: A Step-by-Step Guide to Business Model Innovation.

[23] Müller, Vincent C., "Ethics of Artificial Intelligence and Robotics", The Stanford Encyclopedia of Philosophy (Summer 2021 Edition), Edward N. Zalta (ed.), https://plato.stanford.edu/archives/sum2021/entries/ethics-ai/

[24] Ethics of artificial intelligence, https://en.wikipedia.org/wiki/Ethics_of_artificial_intelligence

[25] Productplan, What is roadmapping. https://www.productplan.com/learn/roadmapping/.

[26] Roadmunk, Why Roadmap, https://roadmunk.com/guides/roadmap-definition/.

[27] 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

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

[29] https://euhybnet.eu/

[30] EU-HYBNET Innovation Arena. https://euhybnet-innovation.eu.

[31] Mantzana V., Georgiou E., Gazi A., Gkotsis I., Chasiotis I., Eftychidis G. (2021) Towards a Global CIs' Cyber-Physical Security Management and Joint Coordination Approach. In: Abie H. et al. (eds) Cyber-Physical Security for Critical Infrastructures Protection. CPS4CIP 2020. Lecture Notes in Computer Science, vol 12618. Springer, Cham. https://doi.org/10.1007/978-3-030-69781-5_11

[32] European Commission, Green Paper on a European programme for critical infrastructure protection. https://op.europa.eu/en/publication-detail/-/publication/4e3f9be0-ce1c-4f5c-9fdc-07bdd441fb88/language-en

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

[34] Major Incident Management (METHANE), https://www.jesip.org.uk/methane

[35] CISE Technical specifications, http://www.emsa.europa.eu/technical-specifications.html

[36] COMMUNICATION FROM THE COMMISSION on a European Programme for Critical Infrastructure Protection, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52006DC0786&from=EN

[37] COUNCIL DIRECTIVE 2008/114/EC on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF

[38] European reference network for Critical Infrastructure Protection, https://ec.europa.eu/jrc/en/network-bureau/european-reference-network-critical-infrastructure-protection-erncip

[39] ENISA, European Union Agency for Cybersecurity, https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services]

[40] Directive on the resilience of critical entities (CER), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2020:829:FIN

[41] Network and Information Systems (NIS2) Directive, https://digital-strategy.ec.europa.eu/en/library/proposal-directive-measures-high-common-level-cybersecurity-across-union

[42] EC Migration and home affair, European Critical Infrastructure, https://ec.europa.eu/home-affairs/what-is-new/work-in-progress/initiatives/european-critical-infrastructure-eci_en

[43] EC Migration and Home Affairs, Critical Infrastructure Warning Information Network (CIWIN), https://ec.europa.eu/home-affairs/what-we-do/networks/critical_infrastructure_warning_information_network_en

[44] EEAS Action Plan against Disinformation, https://eeas.europa.eu/headquarters/headquarters-homepage/54866/action-plan-against-disinformation_en

[45] Debunk EU, https://debunk.eu

[46]EEAS Rapid Alert System on disinformation (RAS), https://eeas.europa.eu/sites/default/files/ras_factsheet_march_2019_0.pdf

[47]Open Source Threat Intelligence Platform & Open Standards For Threat Information Sharing (formerly known as Malware Information Sharing Platform)

[48] Structured Threat Information Expression, https://stixproject.github.io/about/

[49] EU Democracy Action Plan, https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2250

[50] EU Action Plan against Disinformation, https://eeas.europa.eu/headquarters/headquarters-homepage/area/jobs-funds_en

[51]European External Action Services (EEAS) Stratcom https://eeas.europa.eu/headquarters/headquarters-homepage/100/strategic-communications_en

[52] European Digital Media Observatory (EDMO), https://digital-strategy.ec.europa.eu/en/policies/european-digital-media-observatory

[53] EU HYBRID FUSION CELL, see https://ec.europa.eu/commission/presscorner/detail/it/MEMO_16_1250

[54] EEAS East StratCom Task Force, https://en.wikipedia.org/wiki/East_StratCom_Task_Force

[55] EUvsDiSiNFO, https://euvsdisinfo.eu/

[56] European Court of Auditors, Special Report 09/2021: Disinformation affecting the EU: tackled but not tamed, https://www.eca.europa.eu/Lists/ECADocuments/SR21_09/SR_Disinformation_EN.pdf

[57] Audiovisual Media Services Directive (AVMSD) (EU) 2018/1808.] https://eur-lex.europa.eu/eli/dir/2018/1808/oj

[58] Center for Media Literacy, https://www.medialit.org/

[59] EU Media literacy expert group, https://ec.europa.eu/transparency/expert-groups-register/screen/expert-groups/consult?do=groupDetail.groupDetail&groupID=2541

[60] The Crescent Project, https://crescentproject.eu/

[61] Crescent course on Strategic Communication to Counter Security Threats in the Disinformation Era, https://urjcx.urjc.es/courses/course-v1:URJCx+URJCx113+CCJS/about

[62] Education World, Best Apps For Teaching Media Literacy, https://www.educationworld.com/a_lesson/best_apps_teaching_media_literacy.shtml

[63] Common Sense Education, https://www.commonsensemedia.org/news-and-media-literacy/what-is-media-literacy-and-why-is-it-important

[64] International Society for Technology in Education (ISTE), 10 resources to boost student media literacy, https://www.iste.org/explore/10-resources-boost-student-media-literacy

[65] ERASMUS Student Network (ESN), Media literacy training program, https://esn.org/news/esn-launches-training-program-media-literacy

[66] YLE Troll factory, https://yle.fi/aihe/artikkeli/2020/05/07/yles-troll-factory-game-was-chosen-as-the-best-digital-project-to-engage-young

[67] Stopfake.org, 13 online tools that help to verify the authenticity of a photoghttps://www.stopfake.org/en/13-online-tools-that-help-to-verify-the-authenticity-of-a-photo/

[68] EU Code of Practice on Disinformation, https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=54454

[69] FotoForensics, http://fotoforensics.com/

[70] Amnesty International's Citizens Evidence Lab, https://citizenevidence.org/

[71] US Federal Trade Commission Consumer Information, How to spot, avoid, and report fake check scams https://www.consumer.ftc.gov/articles/how-spot-avoid-and-report-fake-check-scams

[72] The British HM Government, SHAREChecklist, https://sharechecklist.gov.uk/

[73] German Bundesregierung, Wie Sie Falschmeldungen erkennen, https://www.bundesregierung.de/breg-de/themen/mythen-und-falschmeldungen/corona-falschmeldungen-erkennen-1750146

[74] ETSI Industry Specification Group (ISG) European Common information sharing environment service and Data Model (CDM) https://www.etsi.org/committee/1584-cdm?jjj=1629209678094

[75] SPARTA project, Deliverable 4.1 Cybersecurity threat intelligence common data, https://www.sparta.eu/assets/deliverables/SPARTA-D4.1-Cybersecurity-threat-intelligence-common-data-model-PU-M18.pdf

[76] European Programme for Critical Infrastructure Protection (EPCIP), https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0786:FIN:EN:PDF

[77] Directive on European Critical Infrastructures, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF

[78] EU Critical Infrastructure Warning Information Network, https://ec.europa.eu/home-affairs/what-we-do/networks/critical_infrastructure_warning_information_network_en

[79] The Coalition for Content Provenance and Authenticity (C2PA) https://c2pa.org/https://c2pa.org/

[80] Content Authenticity Initiative (CAI), https://contentauthenticity.org/

[81] Project Origin, https://www.originproject.info/

ANNEX III INNOVATION REVIEW CONTRIBUTORS

Table 5. Contributors in the innovation reviews (R = regular review workshop, T = test review workshop, E = expert review).

Participants	Partner org.	Innovations			
		Public-private information-sharing groups developing collaborative investigations and collective action	Debunking of fake news	Training application for media literacy	Guides to identify fakes
Bartosz Kożuch	PPHS	R T		R	
Carlos Hernández- Echevarría	Maldita		R		R
Evaldas Bružė	L3CE		R		R
Gunhild Hoogensen Gjorv	UIT	R		R	
Ilias Gkotsis	KEMEA	E			
Isto Mattila	Laurea	T			
Magda Okuniewska	PPHS			E R	
Maria Kampa	KEMEA	R T	R	R	R
Pablo Hernández Escayola	Maldita				E
Päivi Mattila	Laurea	R T	R	R	R
Rick Meessen	TNO	R	R	R	R
Rolf Blom	RISE	R T	R	R	R
Ruben Arcos	URJC	R	E	R	
Souzanna Sofou	Satways	R		R	