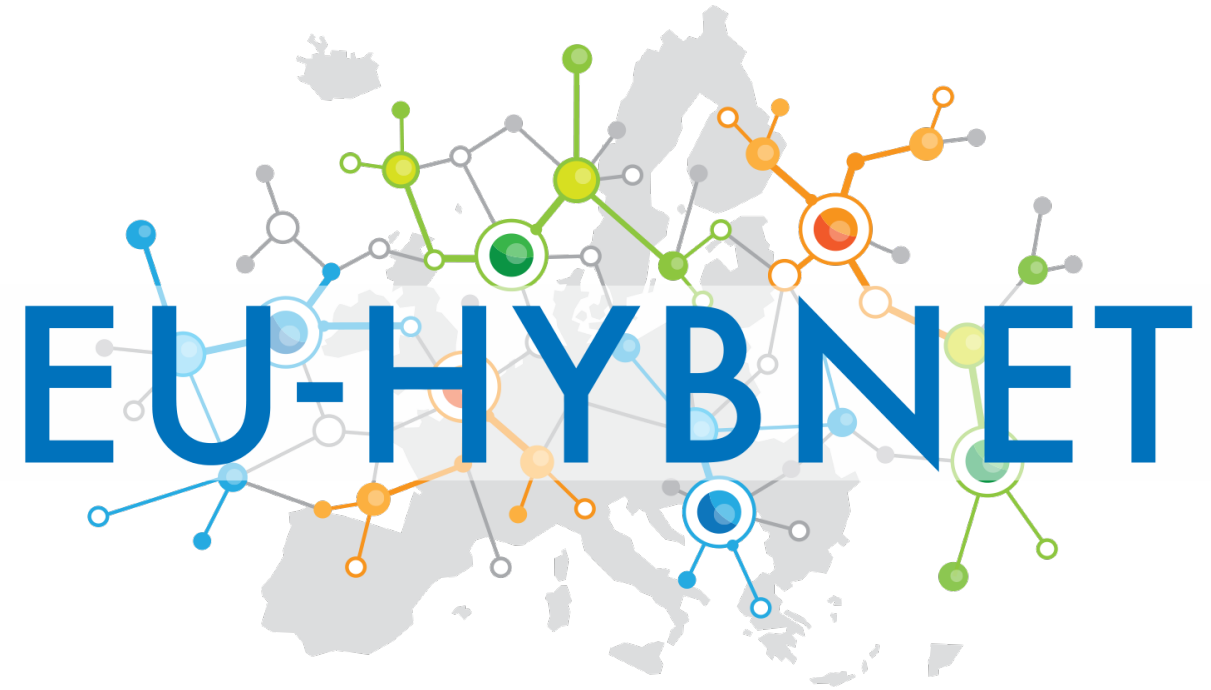

FINAL REPORT ON STRATEGY FOR INNOVATION UPTAKE, INDUSTRIALIZATION AND RESEARCH

DELIVERABLE 4.7

Lead Author: RISE
Contributors: KEMEA, L3CE, PPHS, Laurea
Deliverable classification: Public

This project has received funding from the European Union's Horizon 2020 – Research and Innovation Framework Programme, H2020-SU-SEC-2019, under grant agreement No. 883054

D4.7 FINAL REPORT ON STRATEGY FOR INNOVATION UPTAKE, INDUSTRALISATION AND RESEARCH

Deliverable number	**D4.7**	
Version:	**V1.0**	
Delivery date:	**17.03.2025**	
Dissemination level:	**Public**	
Classification level:	**Public**	
Status	**Ready**	
Nature:	**Activity report**	
Main author:	**RISE**	**Rolf Blom**
Contributors:	**RISE** **KEMEA** **L3CE** **Laurea** **PPHS**	**Efi Papatheocharous, David Eklund, Hendarmawan** **Athanasios Kosmopoulos** **Edmundas Piesarskas** **Isto Mattila** **Małgorzata Wolbach**

DOCUMENT CONTROL

Version	Date	Authors	Changes
V0.1	2024-12-08	Rolf Blom	Report skeleton
V0.2	2024-12-19	Rolf Blom	Skeleton updated for cycle 4. Content added.
V0.3	2024-01-31	Rolf Blom, David Eklund, Efi Papatheocharous, Hendarmawan, Athanasios Kosmopoulos	Content added
V0.4	2024-02-13	Rolf Blom, David Eklund, Efi Papatheocharous, Hendarmawan	Updates and refinements
V0.5	2024-02-23	Rolf Blom	First content wise complete version
V0.6	2024-03-02	Rolf Blom	Updated for internal review
V0.9	2024-03-13	Rolf Blom	Updated after internal review
V1.0	2024-03-17	Tiina Haapanen	Final text modifications, submission to EC

DISCLAIMER

EXECUTIVE SUMMARY

This deliverable (D4.7) is the final report of Task 4.2, focusing on strategies for innovation uptake, industrialization, and research. It builds on the results of WP2 and WP3, refining methodologies and assessing key innovations aimed at strengthening resilience against hybrid threats. The final innovation selected in this project cycle addresses AI-Model Verification and Validation, a critical area ensuring trustworthy, safe, and robust AI-models. This solution provides a framework for validation and verification, evaluating AI systems based on fairness, bias detection, robustness against adversarial attacks, explainability, and aiming for compliance with ethical and legal standards. The Innovation Uptake Canvas was developed to outline a clear vision, mission, strategy, and roadmap for adoption and industrialization. Additionally, key recommendations have been made regarding essential research, standardization, and organisational initiatives necessary for implementation.

A comprehensive review of the thirteen proposed solutions confirms their role in a multi-layered strategy against hybrid threats, addressing governance, civic, and service sectors. These solutions integrate technological innovation, structured governance, and community engagement, forming parts of a resilient ecosystem capable of anticipating, detecting, and mitigating diverse hybrid threats. Many solutions function as enablers, including the AI-Model Verification and Validation Platform and A Common Information and Analysis Environment, which facilitate secure information sharing for real-time situational awareness. The findings highlight that hybrid threats evolve faster than regulatory frameworks, emphasizing the urgency of EU-wide standardization to ensure resilience. AI and Big Data play critical roles in real-time threat analysis, media verification, and crisis response, while early end-user involvement is essential to ensure security tools are practical and effective. Expanding media literacy training and education is also crucial for long-term resilience against misinformation.

To strengthen resilience, cross-sector collaboration between governments, academia, and industry must be enhanced through public-private partnerships and increased citizen engagement. Procurement strategies should focus on leveraging existing solutions, refining innovation descriptions, and incorporating best practices to streamline adoption.

The Methodology for Creation of Uptake, Industrialization and Research has been reviewed and updated, integrating insights from strategy development, innovation uptake, and roadmap creation. The updated Innovation Uptake Canvas incorporates additional components, ensuring better alignment between innovation descriptions and implementation strategies. Moving forward, Proof of Concept development and simulated environments will be crucial for validating solutions before full-scale deployment. Adherence to existing standards should be prioritized, with extensions or new standards developed as needed.

By prioritizing standardization, collaboration, and AI-driven innovation, the EU can build a resilient ecosystem capable of countering evolving hybrid threats in a proactive manner. The updated methodologies and frameworks developed through this project will serve as a foundation for future research and innovation uptake strategies.

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 (D4.7) as the fourth and final report on "Defining a concrete strategic approach for innovation uptake, industrialisation and research". It is part of the overall objective to find common requirements that can fill knowledge gaps, deal with performance needs, and enhance capabilities in research, innovation and training concerning hybrid threats. This work is focused around four core themes, **Future Trends of Hybrid Threats, Cyber and Future Technologies, Resilient Civilians, Local Level and National Administration,** and **Information and Strategic Communication**. The core themes are described in Section 1.4.1 Project core themes.

The EU-HYBNET work on "Defining a concrete strategic approach for innovation uptake, industrialisation and research" is part of WP4 (Recommendations for Innovations Uptake and Standardization). WP4 comprises the following objectives, where the boldface bullets are mainly directed at Task 4.2:

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. The main deliverables referenced in this deliverable are:

D3.1 FIRST INTERIM REPORT MAPPED ON GAPS AND NEEDS
D3.2 SECOND INTERIM REPORT MAPPED ON GAPS AND NEEDS
D3.19 FINAL REPORT MAPPING OF SOLUTIONS ON GAPS AND NEEDS (To be published)
D3.9 SECOND MID-TERM REPORT ON INNOVATION AND RESEARCH MONITORING
D4.4 FIRST REPORT ON STRATEGY FOR INNOVATION UPTAKE, INDUSTRIALISATION AND RESEARCH
D4.5 SECOND INNOVATION UPTAKE, INDUSTRIALISATION AND RESEARCH STRATEGY
D4.6 THIRD INNOVATION UPTAKE, INDUSTRIALISATION AND RESEARCH STRATEGY (To be published)

The following Sections in Chapter 1 contains background, definitions and concepts used. In chapter 2 we introduce the methodology developed for creating strategies for innovation uptake, industrialization and research. Chapter 5 builds upon this introduction and presents a review of the methodology with a number of improvement proposals. Chapter 3 presents a final solution, which is in the area of validation and verifications of AI-models. In Chapter 4 all solutions from the four project cycles are presented and discussed with respect to their coverage of the hybrid threat arena. The relevance and uptake of the Task 4.2 results are reviewed in Chapter 6. and Chapter 7 summarizes the

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

lessons learnt. In Chapter 8 and 9 the contributions to the project's objectives and its three lines of actions are described. Finally, in Chapter 10, overall conclusions and ideas for future work are presented.

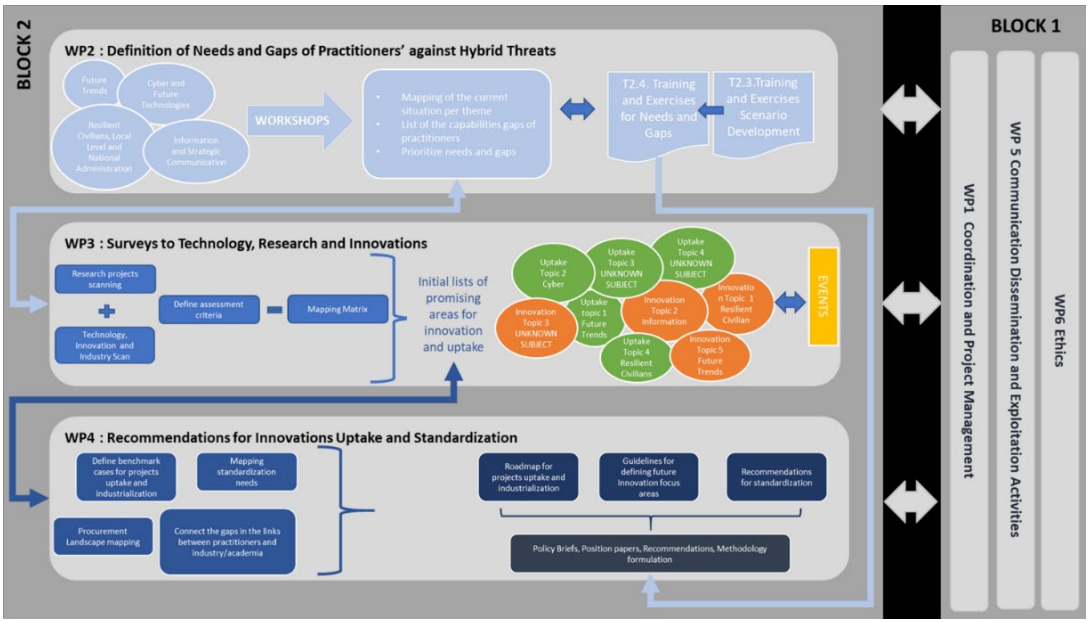

Figure 1. EU-HYBNET Structure of Work Packages and Main Activities

1.2 OBJECTIVES OF TASK 4.2 IN THE FOURTH PROJECT MINI-CYCLE

The main objective for this final deliverable of Task 4.2 is to produce a comprehensive review of the work performed in the earlier full project cycles. The focus of the review is on the coverage of the developed solutions with respect to the hybrid threat arena and on a review of the methodology developed and used for creation of uptake, industrialization and research strategies.

Building on the results of WP2 and WP3, a final solution with concrete strategic approaches for uptake and industrialisation was created. This final innovation is about developing a framework which can help build trust in AI-based tools. There is a need to adopt the view that even if you trust a solution, it should be verified that the trust is warranted.

As in the previous project cycles, our work with the final solution builds the results of WP2 and WP3. Based on gaps, ongoing research and industrial developments identified by Task 3.1 and Task 3.2, an uptake strategy for the innovation is developed. Roadmaps, including timeframes, actors, and recommended procedures to be followed are produced. Possibilities for Pre-Commercial Procurements (PCPs) or Public Procurement of Innovations (PPIs) will be reviewed as they are crucial steps in breaching the gap between the buyers and industry.

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

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

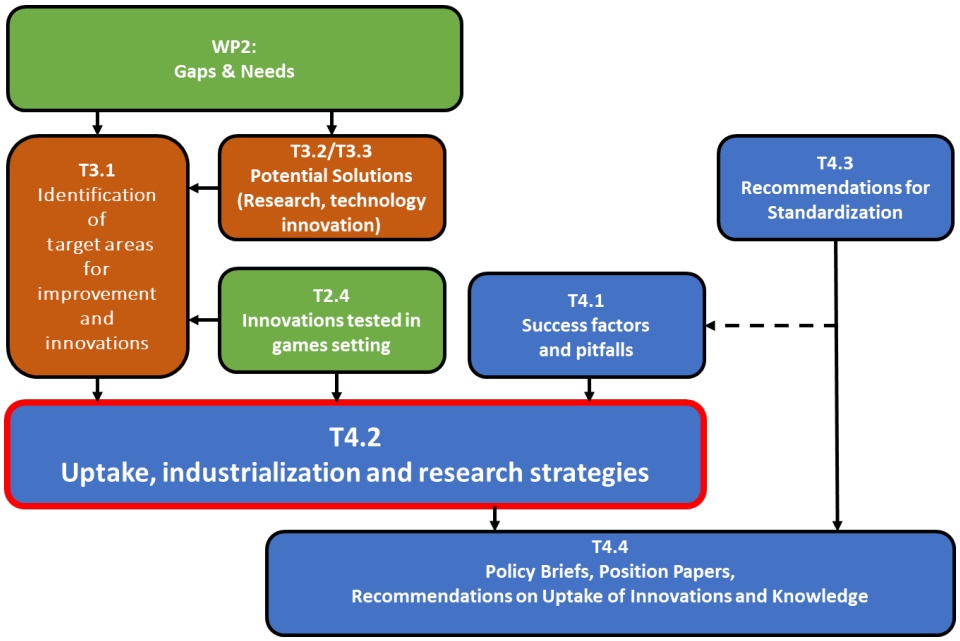

Figure 2. Dependencies between Task 4.2 and WP2, WP3 and other WP4 Tasks

The activities in this project cycle with respect to selecting an innovation to recommend comprise:

- Selection of an innovation relating to the EU-HYBNET core theme Cyber and Future Technology based on
  - the assessments of proposed innovations performed by Task 3.1.
  - The outcome of the trainings (Disruptive Technology Assessment Games, DTAGs) organised by Task 2.4.
  - The added value the innovation would bring to solutions countering hybrid threats.
- Establishing sufficient state-of-the-art knowledge in the area covered by the selected innovation. The findings are summarized in a section named Setting the scene. It is worth noticing that although this is not a Task 4.2 research activity, it was necessary to establish a state-of-the art understanding of the innovation area considered. This to be able to focus the roadmapping work for the selected innovation.
- Application of the framework methodology developed in the first project cycle on the selected innovations.
  - In the review of the four selected innovations the basis has been:
    - The review of ongoing research and industrial development performed by Task 3.3.
    - The uptake success factors, and the pitfalls/barriers collected and described by Task 4.1.
    - The EU and MS public procurement environment as collected and described by Task 4.1 in D4.3[2] and in particular the guidance in D4.3 given on public procurement of the innovations considered for uptake in this deliverable (D4.7).
  - Input and reviews provided by consortium partners and other experts.
- Present the uptake strategies for the four selected innovations. Describe barriers, required research and recommend funding solutions.

[2] D4.3 EU-HYBNET 3rd report on the procurement environment. To be published.

1.4 EU-HYBNET KEY CONCEPTS AND DEFINTIONS

1.4.1 PROJECT CORE THEMES

For the convenience of the reader, we include brief introductions to the projects core themes, fetched from the project web page[3].

1.4.1.1 FUTURE TRENDS OF HYBRID THREATS

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

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

1.4.1.2 CYBER AND FUTURE TECHNOLOGIES

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

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

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

1.4.1.3 RESILIENT CIVILIANS, LOCAL LEVEL AND NATIONAL ADMINISTRATION

Civilians are central as targets and as actors seeking human and societal security. Too much focus has been placed on the state/government level when it comes to hybrid threats. There is still too little research on how this plays out in hybrid threat security environment. Having a better understanding of where the potential vulnerabilities lie within possible target societies enables these same societies – and the diverse civilians within them – to develop measures that can build trust and solidarity

[3] https://euhybnet.eu/

within them, making them less vulnerable to such manipulations. This understanding will also help in resilience building that is important for all the EU member states.

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

1.4.1.4 INFORMATION AND STRATEGIC COMMUNICATION

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

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

While social media networks provide an unprecedented dimension for adversely impacting the potential exposure of target audiences, gathering empirical evidence on disinformation content is required for a full understanding of the effects of influencing campaigns, and thus developing effective strategies and tactics to counter influence.

1.4.2 THE CONCEPTUAL DOMAIN MODEL

In the report *The Landscape of Hybrid Threats – A Conceptual Model*[4], domains in which hybrid threats may occur are defined. The domains indicate different areas in society and sometimes have overlaps, especially when it comes to threats and risks. Threats often cover more than one domain. Here we list

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

the defined domains and give examples of what threats in the domain could be. For a more comprehensive description we refer to the cited report.

Infrastructure:	Physical and or cyber operations against infrastructure.
Cyber:	Disinformation, espionage, cybercrime, cyberwar (offensive attacks)
Space:	Electronic operations (GNSS jamming and spoofing)
Economy:	Sanctions, boycotts, foreign direct investment.
Military/Defence:	Border violations, exercises, covert operations (green men), weapons proliferation.
Culture:	Exploitation of sociocultural cleavages (ethnic, religion and culture).
Social/Societal:	Engaging diasporas for influencing, promoting social unrest, influencing curricula and academia.
Public administration:	Promoting and exploiting corruption.
Legal:	Leveraging legal rules, processes, institutions, and arguments.
Intelligence:	Intelligence preparation, clandestine operations, infiltration Intelligence.
Diplomacy:	International relations, diplomatic sanctions.
Political:	Coercion of politicians and/or government.
Information:	Information manipulation and interference. Media control and interference.

1.4.3 THE CORE MODEL

The description of the CORE (a Comprehensive Resilience Ecosystem) model below consists mainly of citations and a figure from the executive summary [5] of the full report on *Hybrid threats: a comprehensive resilience ecosystem*[6].

The CORE model allows policymakers to estimate how adversaries employ hybrid threats in order to alter democratic decision-making capabilities. It shows how the hybrid threat activity, bit by bit, challenges democratic systems by introducing different types of stress. It also allows monitoring the dependencies and possible cascading effects. This is important for the detection of hybrid threats. Foresight plays a crucial role in this process.

The **Comprehensive Resilience Ecosystem model** is a systemic representation of democratic society as a whole. It is used to analyse and ultimately counteract hybrid threats that seek to undermine and harm the integrity and functioning of democracies, change decision-making processes, and create cascading effects, i.e., a systems-thinking approach to hybrid threats, with representation of society as a whole.

The CORE model is based on the following elements:

1. Seven foundations of democratic systems lie at the heart of the ecosystem. The foundations are the ultimate goals that hybrid threat actors aim to undermine, while scoring some of their own strategic interests. These foundations are (for a discussion of these concepts see the full report on the CORE model):

    I. Civil rights / Liberties

[5] Hybrid threats: a comprehensive resilience ecosystem. Executive summary.
https://publications.jrc.ec.europa.eu/repository/bitstream/JRC129019/JRC129019_02.pdf
[6] Hybrid threats: a comprehensive resilience ecosystem.
https://publications.jrc.ec.europa.eu/repository/handle/JRC129019

II. Feeling of justice / Equal treatment
III. Political responsibility / Accountability
IV. Rule of law
V. Stability
VI. Reliability / Availability
VII. Foresight capability

2. The **domains from the Conceptual model** (see above) also are an integral part of the ecosystem. If resilience is well developed in the domains, they can act as shields against malicious activities. On the other hand, a lack of resilience in the domains can open entry points for hostile actors.
3. The ecosystem consists of **three spaces** – Civic, Governance and Services – which represent the three sectors of society.
4. The layers of the ecosystem represent the different 'levels' that exist in society – from the more local levels to international levels.

The structure of the model and its four types of elements the whole-of-society approach are described in Figure 3.

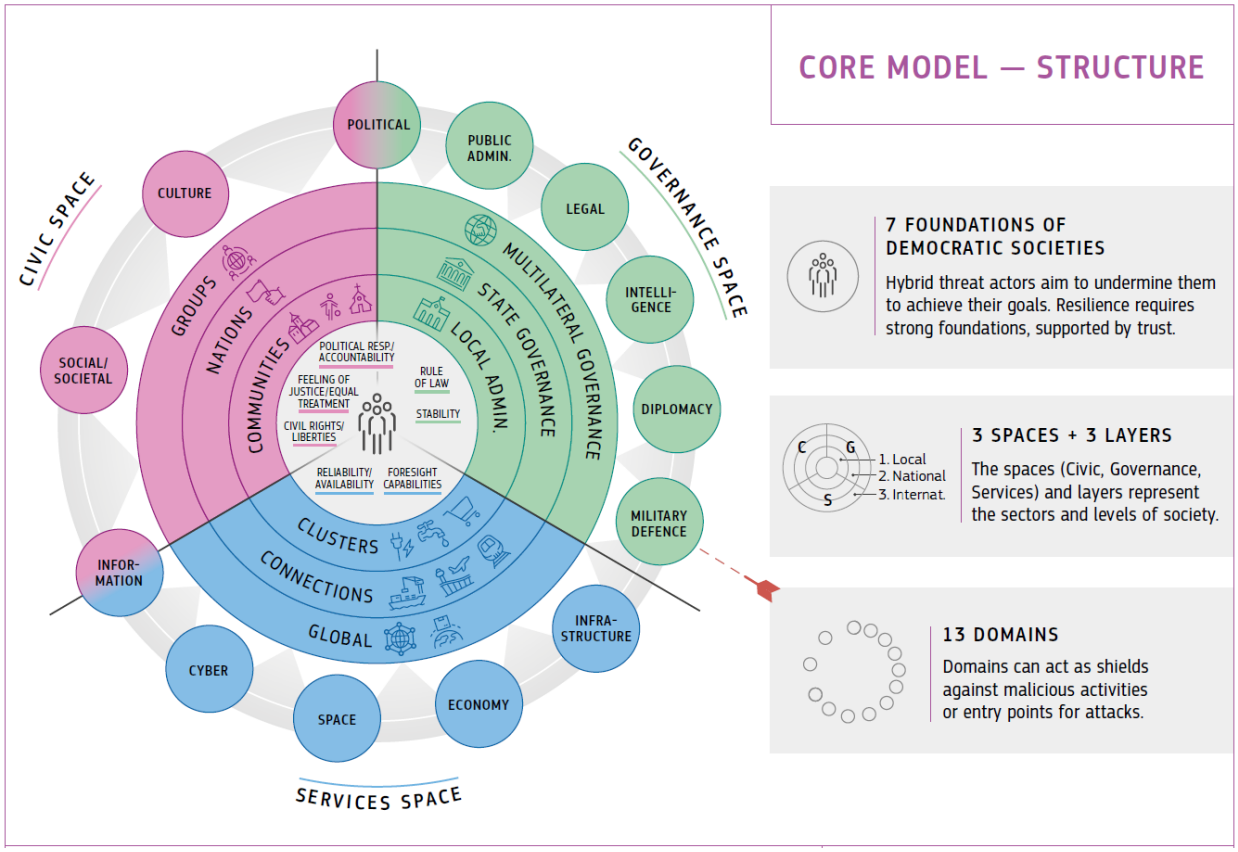

Figure 3. CORE model structures including details of its four types of elements.

1.4.4 DEFINITIONS

All definitions in this section, except for the one of Innovation, are copied from D4.1[7].

1.4.4.1 HYBRID THREATS

Hybrid threats aim to exploit a country's vulnerabilities and often seek to undermine fundamental democratic values and liberties [8]. 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[9].

According to the Joint Framework on Countering Hybrid Threats[9], while definitions of hybrid threats vary and need to remain flexible to respond to their evolving nature, the concept of the Framework aims to capture the mixture of coercive and subversive activity, conventional and unconventional methods (i.e. diplomatic, military, economic, technological), which can be used in a coordinated manner by state or non-state actors to achieve specific objectives while remaining below the threshold of formally declared warfare. There is usually an emphasis on exploiting the vulnerabilities of the target and on generating ambiguity to hinder decision-making processes. Massive disinformation campaigns, using social media to control the political narrative or to radicalise, recruit and direct proxy actors can be vehicles for hybrid threats.

1.4.4.2 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 (including Europe's third sector). EU-HYBNET includes practitioner partners from all of these levels and its primary focus is on civilian security issues. Law Enforcement Agencies (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 European Centre of Excellence for Countering Hybrid Threats[10]. The third category includes also companies providing critical security and other services for the state e.g., communication networks.

---

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

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

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

[10] European Centre of Excellence for Countering Hybrid Threats.

In respect to the I-LEAD project[11], the term practitioners refer to Law Enforcement Agencies. Law enforcement agencies are organisations 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.

1.4.4.3 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.

1.4.4.4 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 organisations. 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 organisational 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 organisational population. The adoption of innovation results in the assimilation of a product, service, process or practice that is new to an adopting organisation.

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

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

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

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

1.4.4.5 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.

1.4.4.6 INNOVATION PROCUREMENT

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

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

Innovation procurement is a policy instrument whereby policymakers can use the procurement process to foster innovation for the benefit of public authorities, the private sector as well as society at large. Indeed, with innovation procurement public expenditure is used more effectively, as it can harness the private sector's innovation capacity for a number of purposes. Notably, innovation procurement may be used to improve the quality of public services in those areas where the public buyer has a large market share, e.g., healthcare, transport, defence. The increased demand coming from the public sector boosts the private sector's innovative performance, thus increasing overall competitiveness. Not least, societal challenges may be tackled through solutions generated via innovation procurement.

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

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.

1.4.4.7 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.

2 THE METHODOLOGY FRAMEWORK

Although that in this final project cycle, a review of the framework is performed and updates are proposed, we use the methodology as applied in the earlier cycles. This is due to the fact that strategy creation for the innovation considered is performed in parallel with the methodology review. So, this section introduces the "old" framework[14] that was developed in the first project cycle and it provides guidelines on how to derive strategies and evaluate possibilities for uptake and industrialization of innovations but also on identification of barriers, ethical issues, required research, and any needs for new standardization and regulations.

The framework's main components are roadmapping and collecting relevant facts in an innovation uptake canvas like the well-known business model canvas[15]. The innovation uptake canvas, see Figure 4, has four columns that describe different aspect of the innovation. The first column, named **The Innovation**, focus on describing important aspects of the innovation itself. The second column named **The solution details** focus on the its functionality, operations and the roadmap for how to realize it. The third column named **The Resources** described require resources for the implementation of the solution. Finally, the fourth column in the innovation uptake canvas, named **The uptake environment**, is about the environment in which the solution will be implemented.

The roadmapping follows standard procedures with vision, mission, strategy and activity statements while the uptake canvas has some EU-HYBNET specific entries. In

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

[15] Strategyzer, The business model canvas.

ANNEX II: The methodology framework, there are descriptions of the roadmapping procedure and the uptake canvas.

Figure 4. The innovation uptake canvas.

2.1 METHODOLOGY STEPS

The filling in of the Innovation Uptake Canvas and the development of the roadmap for an innovation is performed in the steps described below. The relevant input and the desired output are depicted in Figure 5.

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 generic or specific solution to analyse. In this step the findings from the setting the scene work, and the recommendations from Task 3.1 should be taken into account. The result should define the scope of the instantiation of the innovation and roadmapping statements for the 1) vision, 2) mission and 3) strategy. These statements will be the basis for the further analysis.
2. Review the innovation uptake canvas and fill in relevant aspect in the canvas. Identify white spots where more information/analysis is needed. Review and document barriers and success factors.
3. Send the draft canvas for review to project partners, select stakeholders, external experts and network members as applicable.
4. Integrate comments received and finalize the innovation uptake canvas and the roadmap.
5. Document the final canvas and summarize the findings and propose corrective actions, if needed. The resulting final canvases with roadmaps are documented in a *Scoping of and strategy creation for selected innovations* chapter.
6. Note all identified barriers and hurdles and recommend strategies / actions to overcome them. These measures could be in the form of required research activities, development of new standards, new policies or changes/updates to current ones. The recommendations are recorded in a *Recommendations* chapter.

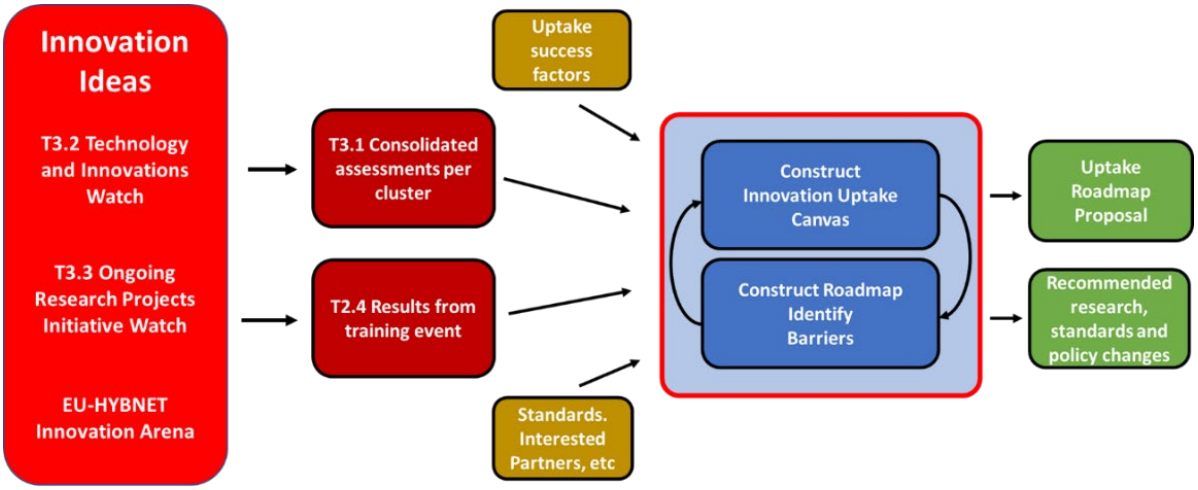

Figure 5. Illustration of the information dependencies for the construction of an Innovation Uptake Canvas, the corresponding Roadmap, and Recommendations.

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

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

3 A FINAL INNOVATION

3.1 CRITERIA USED AND INTRO TO THE SELECTED INNOVATION

In this final project mini-cycle, one innovation was selected for review and scoping. This to ensure that, across all project cycles, at least three innovations are aligned with each of the four EU-HYBNET core themes.

The selected innovation was Commitment to Validating and Verifying AI, initially proposed in the second project cycle. The rationale behind this choice (Task 4.2) is that many previously considered solutions assume the use of AI-based tools. As AI adoption grows, so does our reliance on these tools, making it critical to verify their correct operation.

To build trust in AI, we must ensure that these systems function as intended and comply with relevant regulations. This can only be achieved through rigorous validation and verification processes.

3.2 SCOPING OF AND STRATEGY CREATION

In the following sections we provide a solution and an uptake strategy resulting from the Task 4.2 scoping of the original innovation. As an introduction to the scoping and choices made, we provide some high-level observations. For easy reference the solution has been named AI-Model verification and validation platform (AIMVPP). Below is a short introduction of AIMVPP.

The AIMVVP addresses the growing need for trustworthy, safe, and robust AI-models by providing a standardized framework for their validation and verification. It evaluates AI systems across parameters like fairness, bias detection, robustness against adversarial attacks, explainability, and compliance with ethical and legal standards. By integrating modular tools and sector-specific benchmarks, AIMVVP

ensures AI-models are ready for deployment in critical areas like healthcare, cybersecurity, and public safety.

Key features include bias detection, adversarial testing, explainability modules, and automated compliance checks with regulations such as GDPR and the AI Act. The platform also issues certifications for validated models through a user-friendly dashboard. Challenges include achieving adoption across industries, addressing ethical concerns, and ensuring regulatory alignment across EU Member States.

3.3 AIMVVP: AI-MODEL VERIFICATION AND VALIDATION PLATFORM

3.3.1 SETTING THE SCENE

The innovation under review and scoping is based on identified pan-European security practitioners' gaps and needs in countering hybrid threats under the project core theme Future Trends of Hybrid threats focus area "Digital escalation and AI-based exploitation". The innovation on which our solution is built is called "**Commitment to Validating and Verifying AI**".

The rapid expansion of AI technologies has introduced critical challenges regarding correctness, trustworthiness, safety, privacy, and robustness of AI-models. In the context of hybrid threats, adversaries can exploit vulnerabilities in AI systems, leading to erroneous threat assessments, compromised decision-making, and misuse of sensitive data. At the same time, AI is a key component of cyber defence, playing a vital role in threat detection, anomaly identification, and automated security responses. Ensuring that these AI systems function accurately, securely, and as intended is crucial for national security, crisis response, and public safety.

AI-models are increasingly integrated into mission-critical and safety-critical domains, including cybersecurity, medical diagnostics, autonomous transport, energy infrastructure, and public administration. In these areas, AI-driven decisions impact real-world security, making their verification and validation essential. Hybrid threat actors can target AI biases, manipulate data inputs, or exploit weak model assumptions, leading to malicious disruptions in crisis management, infrastructure security, and intelligence operations.

As AI adoption grows, so does the urgency of ensuring its reliability through verification and testing. Governments, industries, and security agencies require a standardized method to assess AI-models against predefined benchmarks, ensuring they meet requirements for correctness, fairness, transparency, and robustness in high-stakes applications. In addition to these requirements, we find it necessary to have a runtime monitoring system which continuously monitors the use of a high-risk AI systems to assess if events emanate from a real hybrid threat attack or if it is an attack on the AI-system AI-model or a probing attack on the monitoring system. The EU AI Act[16] (Article 15) mandates that high-risk AI systems be accurate, robust, cybersecure, and error-resilient, while privacy laws such as GDPR impose additional constraints on AI-driven decision-making.

Traditional AI testing mostly relies on handcrafted test scenarios, which may fail to expose hidden vulnerabilities in AI behaviour. In contrast, formal verification methods systematically evaluate all possible failure modes, providing mathematical proof that an AI system meets its specifications. If a requirement is not fulfilled, a counterexample is generated, revealing a concrete failure scenario

[16] The Artificial Intelligence Act

where the AI-model misbehaves — such as failing to detect a cybersecurity breach, misclassifying a disinformation campaign, or overlooking an adversarial attack.

Key challenges in AI-model verification include:

1. Requirement formalization and update: Defining clear, testable security and reliability criteria for AI-models in hybrid threat contexts and means for keeping them up to date considering the rapid developments of AI technologies.
2. Computational Complexity: AI verification demands substantial computing.

The proposed solution designated AI-Model Validation and Verification Platform (AIMVVP) directly addresses these challenges by offering a comprehensive validation and verification framework tailored to AI systems used in hybrid threat defence and to security and decision-making support systems in general. The platform provides:

- Bias detection and performance validation – Ensuring AI-models operate fairly and accurately in high-stakes critical applications.
- Explainability and transparency analysis – Making AI based decisions traceable and interpretable for security professionals.
- Adversarial testing – Evaluating resistance to adversarial attacks, data poisoning, and misinformation infiltration.
- Standardized compliance assessment – validating AI systems against EU AI Act, GDPR, and other relevant EU cybersecurity standards.

AIMVVP serves as a centralized environment where AI developers, regulators, security practitioners, and crisis management teams can collaboratively assess, verify, and validate AI-models before deploying them in hybrid threat scenarios. By ensuring AI reliability, security, and compliance, AIMVVP enhances trust in AI-driven critical solutions, making them safer, more resilient, and more effective against evolving threats.

The European Research Executive (REA) Agency[17] consider all aspects, starting from data-related issues and ending with algorithms and use of AI generated results. Despite the active control there are no existing frameworks or tools provided. However, REA already supports projects in the area and two of them, LAGO[18]and TESSERA[19], develop infrastructure for large-scale, trusted, and shareable datasets. So far, they are only in early stages of developing AI assessment mechanism. AIMVVP will of course take the ongoing work into account, but it could also become the REA owned platform for AI-model verification and validation.

3.3.2 THE FIRST COLUMN – THE INNOVATION

- **Description of the solution, i.e., the instantiation of the innovation to be considered**
  The innovation **Commitment to Validating and Verifying AI** has been transformed into a solution which presents a platform and tools to verify correctness, safety, privacy, and robustness of AI-models in the context of hybrid threats. Trustworthy AI-based tools and solutions are of utmost importance as adversaries can exploit vulnerabilities in AI systems, leading to erroneous threat assessments, compromised decision-making, and misuse of sensitive data. The solution is called **AI-Model Validation and Verification Platform** (AIMVVP).

[17] European Research Executive Agency
[18] LAGO: Lessen Data Access and Governance Obstacles
[19] TESSERA: Towards thE dataSetS for the European secuRity dAta space for innovation

AIMVVP is a low technology readiness level (TRL) solution and the covered problem area is under intense study. Thus, the required development work should be regularly reviewed and the roadmap updated.

SCOPE: The AIMVVP ensures the trustworthiness of AI-models by offering a multi-layered assessment framework. It evaluates AI-models for:

- Correctness and robustness.
- Compliance with guidelines, laws and regulations.
- Adversarial attacks.
- Fairness, bias elimination privacy.
- Transparency through explainability metrics.

VISION: To establish a standardized, pan-European platform that fosters trust in AI technologies by enabling thorough validation and verification of AI-models in critical domains eventually resulting in certification schemas.

MISSION: To deliver a robust framework and tools that assess AI-models for correctness, fairness, and regulatory compliance, supporting industries and governments in deploying AI responsibly.

STRATEGY: Key components for the AIMVVP implementation include:

- Developing a multi-dimensional evaluation methodology framework for AI-models, focusing on correctness, robustness, accuracy, and ethical compliance.
- Designing a modular architecture based on open-source software that integrates with existing development environments and regulatory frameworks.
- Creating benchmarks tailored for its application in different hybrid threat domains.
- Incorporating explainable AI-tools to provide insights into decision-making processes.
- Establishing a certification mechanism for validated models.

LIMITATIONS: The solution presented does not include:

- Development and implementation of trustworthy AI-models used in AI based solutions.
- Assessment of the AIMVVPs inherent cybersecurity, the focus is on the development of its services. Nor does the solution evaluate the cybersecurity of the AI-model under assessment as this would be done according to standard security procedures during the model's development.
- Variations in AI regulatory landscapes across EU Member States are not addressed as well as ethical interpretation aspects among different regions across EU.
- Development of runtime monitoring systems used to monitor high-risk AI-systems in order to assess if reported events emanate from real hybrid threat attacks or if they are attacks on the AI-system or a probing attack on the monitoring system.

RATIONALE: AI-models significantly impact decision-making processes in hybrid threat domains and other sectors. Ensuring their trustworthiness is vital to prevent misuse

and errors that could harm society or undermine public trust. The AIMVVP ensures that AI-models align with ethical, legal, and technical standards.

- **Added value proposition.**

NEED: Already today, strategic decision support systems as well as handling of Big Data use AI and ML solutions in critical applications. Trust in them require verification and validation of their correct and secure operation.

IMPACT: With AIMVVP, it will become feasible to efficiently verify and validate AI-models in hybrid threat solutions. AI-models will be / are part of almost all hybrid threat solutions for analysis of observed events and media content to provide situational awareness and proposals for mitigating actions.

By implementing AIMVVP, the EU can lead global efforts in ensuring trustworthy AI, fostering innovation, and protecting societal interests.

VIABILITY: The development of the components in AIMVVP are still relatively immature with examples of components at TRL 2 – 4. However, research and development efforts are progressing and so far, no blocking issues have been discovered.

- **Stakeholders and domains**

Gaps and needs: The solution is related to the primary context *Digital escalation and AI-based exaltation,* as defined by JRC in EU-HYBNET deliverable D2.11 "Deeper analysis, delivery of short list of gaps and needs"

Conceptual Model Domains: The proposed solution is enabler for Hybrid threat tools and methods in all the domains.

Stakeholders: The first- and second-line responders, civil protection authorities, citizens, intelligence services, local admin and national decision-makers, law enforcement and industry.

3.3.3 THE SECOND COLUMN - SOLUTION DETAILS

- **Functional description**

The AIMVVP includes the following features:

- Adversarial testing framework: Tools to simulate adversarial scenarios and assess the model's robustness.
- Bias detection framework: Recommendations on how to identify and mitigate biases in datasets and model predictions.
- Explainability modules: Mechanisms for interpreting model decisions, increasing transparency.
- Compliance checker: Automated tools to verify safety and functionality requirements as well as compliance with the AI Act, GDPR and other legal frameworks.

- Verification and validation dashboard: A user-friendly interface to display evaluation results.

- **Operational description**

The platform follows these operational steps:

1. Upload and register the AI-model for evaluation.
2. Upload of external validations, test results and certifications
3. Select the assessment metrics and benchmarks relevant to the domain.
4. Run automated validation processes.
5. Review detailed evaluation reports, including strengths, weaknesses, and compliance gaps.
6. Issue verification and validation test protocols.'

- **Roadmapping**

Phase 1: Research and development of evaluation methodologies and modular architecture including studies of content and procedures for certification schemas.
Phase 2: Development and validation of the framework.
Phase 3: Pilot implementation in collaboration with key hybrid threat stakeholders, e.g., in Information Manipulation and Interference (IMI) monitoring and analysis.
Phase 4: Full-scale deployment and integration with EU regulatory frameworks.
Phase 5: Continuous updates and incorporation of emerging AI standards.
Phase 6: Creating benchmarks tailored for platform application in other sectors.

3.3.4 THE THIRD COLUMN – THE RESOURCES

- **Required development resources**
  - Multi-disciplinary teams, including AI developers, ethicists, and regulatory experts.
  - Development and testing environments for simulating adversarial attacks and compliance scenarios.
  - Cloud infrastructure for scalability and secure data processing.
  - Computational resources for AI-model verification.

- **Required operating support system**
  - A dedicated governance body (e.g., under the European Commission) to oversee platform standards and operations.
  - Mechanisms for stakeholder feedback to refine evaluation criteria.
  - Partnerships with academic institutions for ongoing research.
  - Dissemination resources.

- **CAPEX & OPEX**[20]
  - Initial development costs: 10 –15 MEURO over 3 years.
  - Annual operational costs: 2–3 MEURO for maintenance, updates, and scaling efforts.

3.3.5 THE FOURTH COLUMN – THE UPTAKE ENVIRONMENT

- **Competition and market**
  Tools exist that address specific AI assessment criteria (e.g., fairness or robustness), but there is no comprehensive, standardized solution which integrates all validation dimensions into a single platform. AIMVVP's unique value lies in its holistic approach, tailored for European regulatory requirements and critical applications. It will incorporate existing and under development recognised tools, methodologies, and compliance validations.

- **Funding and organisation of uptake and industrialization efforts**
  - Initial funding through EU research grants.
  - Collaboration with industry consortia and academic partners.
  - Gradual expansion into global markets after establishing EU-wide adoption.
  - Operational cost should eventually be covered by evaluation fees.

- **Barriers**
  The following challenges have been identified:
  - **Technical:** Addressing interoperability with diverse AI frameworks and systems. Addressing computational complexity challenges in AI verification and validation and securing required computational resources.
  - **End-User acceptance:** Building trust and ensuring user-friendly interfaces for adoption. Leading to wide adoption of the platform by private and public stakeholders.
  - **Regulatory alignment:** Harmonizing standards across EU Member States.
  - **Economic:** Securing sustainable funding for long-term viability.

[20] These estimates are based on the assumption that the development efforts would require 3-4 normal sized Horizon Europe projects.

- **Admin:** Ownership of the solution, including responsibility for maintenance and operations including continuous updates and benchmarking.

3.4 RECOMMENDATIONS

3.4.1 RECOMMENDATION 1: UPTAKE OF REVIEWED INNOVATION

In the scoping and development of the innovation uptake canvas for AIMVVP we see several challenges but have not found any blocking issues. We thus recommend that the proposed solution is promoted for uptake and industrialization.

3.4.2 RECOMMENDATION 2: TAXONOMY AND CODING OF HYBRID THREAT EVENTS

Here we repeat Recommendation 2 from D4.6 as having standardized formats for AI-Models input would simplify verification and validation efforts with respect to AI use in Hybrid Threats applications.

To enable automatic handling of and sending/receiving information about events that (may) relate to hybrid threats it is necessary/highly recommended to standardize:

1. A **taxonomy** for reporting of hybrid threat related events.
2. **Encoding formats** for the events defined in the taxonomy as extensions to STIX. STIX, Structured Threat Information eXpression is a standard language that to express and share threat intelligence information in a readable and consistent format.
3. A **preferred transport protocol** for encoded hybrid threat encoded events, based on TAXII. TAXII defines a protocol for exchanging data, including message formats, communication protocols, and security requirements.

The standards proposed would be beneficial for the proposed solutions in this deliverable as well as for the implementation of earlier proposals and other solutions in the hybrid threat area.

3.4.3 RECOMMENDATION 3: GOVERNANCE FRAMEWORK

Establish a governance framework for AIMVVP initiatives to oversee and assess required development efforts, ensuring stakeholder collaboration and the exchange of information, tools, and results. REA may take this role or the framework could be structured similarly to the European Digital Media Observatory (EDMO).

3.4.4 RECOMMENDATION 4: RESEARCH AND DEVELOPMENT FOR AIMVVP DEVELOPMENT

We recommend that R&D actions are initiated in the following areas in one or two more coordinated projects:

- **AI verification and validation methods for hybrid threats**
  Develop advanced verification frameworks tailored to security-focused AI applications ensuring that AI-models used in hybrid threat intelligence analysis and crisis management meet accuracy, robustness, and reliability benchmarks.

- **Modular architecture and test environment**
  Study requirements on a modular architecture to allow integration of existing verification tools. Build a pilot implementation as a PoC in collaboration with key hybrid threat stakeholders.

- **AI robustness against adversarial attacks**
  Investigate methods to strengthen AI resilience against data manipulation, adversarial inputs, and cyber threats to define AI architectures resistant to misuse, adversarial perturbations, and deceptive data inputs.

- **Explainability and transparency in AI for security**
  Research how to design AI-models to understand how they should be designed to provide clear, interpretable decision-making for practitioners and regulators.

- **AI-model certification and compliance with regulations**
  Develop standardized certification schemas for AI used in critical security applications together with a compliance testing framework for hybrid threat applications.

- **Continuous validation of AI-models**
  Design and develop scalable, automated environments for continuous validation of running operational systems after updates and upgrades (SW and HW).

3.4.5 RECOMMENDATION 5: USE OF THE STARLIGHT DEVELOPMENT MODEL

For efficient and end-user-oriented development of the different tools comprised in the AIMVVP we recommend use of the agile co-development methodology as demonstrated in the STARLIGHT project[21]. Development of solutions together with end-users is considered a good practice, facilitating end-users' interest and involvement.

[21] See Chapters 4 and 5 in D4.6.

4. RECOMMENDED SOLUTIONS AND RESEARCH ACTIVITIES

In this section, we present the thirteen solutions for which uptake strategies have been developed. We also summarize the recommendations for research and other initiatives outlined in the three earlier deliverables (D4.4, D4.5, and D4.6).
The thirteen solutions, covered by the work done in Task 4.2 and the innovations they were based on, are listed in Table 1. In the following sections, the solutions will be referenced by their acronyms. Note that in the first cycle, the solutions were not given acronyms except for CISAE. In this final cycle, we have assigned acronyms to the three that previously did not have one.

To ensure this deliverable is self-contained, we begin with a summary of the solutions, which are presented in Sections 4.1 to 4.4. As outlined in Section 2.1 the following terminology is used to distinguish between the original innovation and the scoped innovation being analysed:

- **The Innovation**: The description of the innovation as presented in WP3.
- **The Solution**: The instantiation of the innovation developed by Task 4.2.

In Section 4.5, we discuss the solutions and their coverage with respect to the project Core Themes, the target groups defined by WP3 and main application areas and end-users. Section 4.6 discusses the insights gained in the three EU-HYBNET Innovation and Standardisation Workshops (ISW).

Details of the solutions can be found in deliverables D4.4, D4.5 and D4.6 (covering the first three project cycles) and this deliverable. Descriptions of the innovations are available in WP3 deliverables D3.1, D3.2, and D3.19.

Table 1. Solutions and the Innovations on which they are based

Project cycle	Solution	Innovation Description
1	**CISAE:** A Common Information Sharing and Analysis Environment	Public-private information-sharing groups developing collaborative investigations and collective action
	SARD: Situational Awareness Regarding Disinformation	Debunking of fake news
	ML4S: Media Literacy for Students	Training application for media literacy
	CiToDeFaMe: Citizens Tools to Detect “Fake" Media	Guides to identify fakes
2	**WINS:** What Information Needs to be Shared	Impact and Risk assessment of critical infrastructures in a complex interdependent scenario investigations and collective action
	EESCM: Enhanced and Extended Supply Chain Management	Multi-stage supply chain disruption mitigation strategies and Digital Twins for Supply Chain Resilience
	MIMI: A Market place for IMI Information	DDS-alpha
	GECHO: Gatekeeping ECHO Chambers	Identify and safeguard vulnerable individuals
3	**CRP:** Citizen - Responder Platform	AI Enhanced Disaster Emergency Communications
	CiReTo: Citizens Reporting Tool	Mobile application to pinpoint acts of harassment/violence on the street and online
	LMHTT: Local Media Hybrid Threat Tracker	Media Pluralism Monitor
	STARLIGHT: Starlight Disinformation-Misinformation Toolset	Starlight Disinformation-Misinformation Toolset
4	**AIMVVP:** AI-Model Verification and Validation platform	Commitment to Validating and Verifying AI

4.1 SOLUTIONS FROM THE FIRST PROJECT CYCLE

4.1.1 CISAE: A COMMON INFORMATION SHARING AND ANALYSIS ENVIRONMENT

The primary aim of this solution is to strengthen situational awareness and response mechanisms against hybrid threats targeting critical infrastructure. The Common Information Sharing and Analysis Environment (CISAE) is designed for near real-time sharing and analysis of threat information among public and private entities involved in critical infrastructure. Each Member State will have CISAE nodes, connecting local systems to a shared network. The system supports voluntary, controlled information sharing, combining local data and cyber threat intelligence for improved situational awareness and coordinated mitigation actions.

The solution proposes leveraging the existing EMSA CISE architecture and developing sector-specific tools for data fusion, analysis, and storage. Governance bodies and interoperability protocols will be established to guide development and ensure compliance with European directives like the CER[22] and NIS2[23]. Initial implementation is estimated to take three-plus years, with a total cost of 20–30 MEURO. The expected impact includes earlier threat detection, rapid joint mitigation actions, and enhanced infrastructure resilience. Key challenges involve building trust among stakeholders, organising funding, and addressing legal barriers to information sharing. The solution's success depends on active engagement and collaboration across all Member States.

4.1.2 SARD: DEBUNKING FAKE NEWS

This solution focuses on countering disinformation campaigns by establishing near real-time situational awareness and enabling rapid responses. Using the CISAE framework, practitioners and relevant organisations in the public and private sectors will monitor, share, and analyse data on disinformation activities. The solution builds on existing tools like DebunkEU.org and the EMSA CISE framework[24] to deploy monitoring systems, analysis tools, and a network for sharing insights on disinformation campaigns.

The strategy includes developing federated machine learning tools for distributed analysis while maintaining data privacy. The governance structure will align with EU initiatives like the Action Plan Against Disinformation and the EU Democracy Action Plan. The roadmap emphasizes the importance of EU-funded research projects to refine tools and methods, estimated to cost 20–30 MEURO over three to four years. Challenges include building trust among stakeholders, coordinating cross-border collaboration, and addressing variations in member states' commitment and readiness. The solution's impact will be evident in enhanced societal resilience against disinformation, early countermeasures, and improved public trust in communication channels.

4.1.3 ML4S: MEDIA LITERACY FOR STUDENTS

This solution aims to improve media literacy among students in grade 9 –12, fostering resilience against disinformation campaigns. By incorporating media literacy education into EU curricula, students will learn critical skills to evaluate media content and resist misinformation. The initiative emphasizes

[22] The Critical Entities Resilience (CER) Directive
[23] The second Network and Information Systems (NIS2) Directive
[24] EMSA Common Information Sharing Environment (CISE)

developing frameworks, tools, and gamified training models tailored to different cultural and linguistic contexts. It aims to provide a foundation for creating comprehensive media literacy programs.

The solution will involve EU-level governance to define research programs and organise funding. Initial development will focus on creating adaptable frameworks, followed by localized implementations guided by experts and educators. Estimated costs for initial development and local adaptations range between 10–15 MEURO, with additional annual operating expenses of 2–3 MEURO. Challenges include convincing Member States to adopt standardized frameworks, coordinating local adaptations, and ensuring ongoing updates to match evolving media landscapes. The initiative's success lies in fostering a media-savvy generation, increasing societal resilience against disinformation, and promoting critical thinking skills across the EU.

4.1.4 CITODEFAME, CITIZENS TOOLS TO DETECT "FAKE" MEDIA

This solution addresses the need for citizens to detect altered or digitally generated media, such as fake images, videos, and audio. By providing accessible guides and promoting detection tools, the initiative aims to enhance individual and societal resilience against disinformation. Key actions include creating a comprehensive database of tools and guides, developing promotion material tailored to different demographics, and integrating detection tools into media apps.

An EU governance body, potentially tied to the European Digital Media Observatory (EDMO), will oversee the solution's implementation. Local and national authorities will develop guides adapted to local culture and language. The roadmap emphasizes using voluntary and regulatory measures to encourage integration of detection tools into media consumption apps. The solution's estimated setup cost is 1–2 MEURO, with annual operating expenses of 0.5–1 MEURO. Challenges include securing support from Member States, convincing media app providers to integrate detection tools, and addressing variations in public awareness. The initiative's impact includes reducing the effectiveness of disinformation campaigns and increasing public trust in media authenticity.

4.2 INNOVATIONS FROM THE SECOND PROJECT CYCLE

4.2.1 WINS: WHAT INFORMATION NEEDS TO BE SHARED

The WINS solution addresses the critical question of what information needs to be shared among critical infrastructure (CI) entities to improve resilience against hybrid threats. Building on earlier innovations like CISAE, WINS proposes a structured methodological approach to identify and categorize critical data necessary for detecting and mitigating cascading effects during attacks or disruptions.

The methodology revolves around a "What-If" scenario-building process, utilizing an attack-tree approach to explore potential risks and their cascading effects. This includes both internal and external threats, such as cyberattacks that cause downstream contamination in interconnected systems. CI entities are encouraged to conduct stress tests to enhance preparedness and identify gaps in information-sharing practices.

Key challenges for implementation include securing cooperation from 93% of CI stakeholders who operate in the private sector. The success of WINS depends on voluntary participation, harmonizing EU directives (e.g., CER and NIS2), and overcoming barriers like technological interoperability, end-user skills, and regulatory constraints. Estimated costs for implementation are 5–8 MEURO over three to

four years. The solution's impact lies in enhanced cross-sectoral and cross-border anomaly detection, enabling better resilience planning and response capabilities.

4.2.2 EESCM: ENHANCED AND EXTENDED SUPPLY CHAIN MANAGEMENT

EESCM aims to broaden traditional supply chain management by incorporating services, geopolitical risks, and deeper value chain analysis to mitigate disruptions in critical sectors. Recent crises, including the COVID-19 pandemic and geopolitical tensions, highlighted vulnerabilities in supply chains that this solution seeks to address.

A significant aspect of EESCM is the use of Digital Twin technology to model and optimize supply chain resilience. By integrating real-world data, cascading effects, and recovery planning, the solution provides a framework for industries and critical infrastructure operators to assess and improve their contingency measures.

The initiative involves developing an EU-wide governance framework, sector-specific testing, and financial instruments to support adoption. Challenges include aligning cross-sectoral interests, addressing funding gaps, and managing sensitive geopolitical information. With an estimated budget of 10–15 MEURO over three to four years, EESCM's outcomes are expected to include faster recovery times, reduced dependency on vulnerable supply chains, and improved operational continuity during crises.

4.2.3 MIMI: A MARKETPLACE FOR IMI INFORMATION

The MIMI solution introduces a secure and trusted marketplace for Information Manipulation and Interference (IMI) data, enabling stakeholders to exchange intelligence on disinformation campaigns. MIMI incorporates economic incentives to encourage data sharing while addressing trust and legal concerns. The solution builds on the DDS-alpha system which is a system for information sharing about events in, and analysis of disinformation campaigns. The full innovation description can be found in D3.2.

MIMI's functional components include service-level agreements, secure access control, and a charging mechanism for information transactions. The initiative fosters collaboration among IMI data providers, analysts, and consumers, supporting the development of situational awareness and mitigation strategies against disinformation.

Challenges include building trust among stakeholders, ensuring compliance with data-sharing regulations, and addressing potential resistance to market-driven information exchange. The initial implementation is estimated at 4 MEURO over three years, with ongoing operational costs integrated into the DDS-alpha platform. The solution's impact includes enhanced situational awareness, improved response times, and the establishment of a robust information-sharing ecosystem.

4.2.4 GECHO: GATEKEEPING ECHO CHAMBERS

GECHO focuses on countering the recruitment strategies of extremist and terrorist groups by identifying and safeguarding vulnerable individuals. The solution includes establishing a shared platform for monitoring, analysing, and intervening in online activities related to violent extremism and terrorism.

The platform leverages AI-based tools for real-time detection of extremist content and recruitment activities, enabling early interventions. It emphasizes research on the sociocultural factors contributing

to radicalization and developing tailored counter-narratives. The solution aligns with existing EU strategies and frameworks like the EU Counter-Terrorism Agenda and the Radicalisation Awareness Network (RAN).

Challenges include managing privacy concerns, ensuring technological interoperability, and securing sustained funding. The estimated cost for implementation is 8–12 MEURO over three years. GECHO's impact lies in reducing the spread of violent extremist ideologies, improving situational awareness for law enforcement, and fostering societal cohesion by addressing root causes of radicalization.

4.3 INNOVATIONS FROM THE THIRD PROJECT CYCLE

4.3.1 CRP: CITIZEN - RESPONDER PLATFORM

The CRP aims to create an Information Sharing Environment (ISE) that enables first- and second-line responders to access real-time, trusted information from a variety of tools used by citizens during crises and emergencies. This platform integrates AI-enhanced capabilities, such as the "Disaster Mode" app, which provides immediate triage assessments and maps emergency requests, helping responders prioritize rescue efforts.

Key features include AI-based analysis tools to detect false alarms and identify hybrid threats, standardized data formats for interoperability, and a language-independent design for pan-European usability. The platform also feeds intelligence services with data on adversaries' hybrid threat campaigns. Challenges include ensuring data privacy, building citizen trust, and addressing ethical concerns about user-generated content. With estimated development costs of 5 MEURO and operational costs under 1 MEURO, CRP's impact lies in improving emergency response efficiency and enhancing societal trust in authorities. Long-term success depends on robust governance, secure integration, and widespread adoption by EU Member States.

4.3.2 CIRETO: CITIZENS REPORTING TOOL

CiReTo provides a mobile application for citizens to report incidents of harassment or violence in real-time, both in physical and online spaces. The app leverages geolocation, multimedia evidence, and timestamps to enhance reporting accuracy and facilitate law enforcement responses. Community engagement features, such as forums and support networks, foster solidarity and promote societal resilience.

Integration with AI tools enables predictive analytics for high-risk areas, while partnerships with authorities enhance credibility and response coordination. Privacy and security are prioritized through anonymized reporting and robust encryption. Estimated development costs range from 85–350 KEURO, with annual operational costs of 160–800 KEURO. Challenges include securing mass adoption, preventing false reporting, and navigating legal and ethical concerns. CiReTo aims to empower individuals, build safer communities, and support law enforcement with actionable data.

4.3.3. LMHTT: LOCAL MEDIA HYBRID THREAT TRACKER

LMHTT addresses risks to media pluralism and the spread of foreign interference and misinformation (FIMI) campaigns at the local and regional levels. This diagnostic tool collects data on media ownership, journalistic practices, and content diversity to identify vulnerabilities and alert security practitioners. The solution builds on the Media Pluralism Monitor but focuses on regional nuances, providing detailed insights into localized risks.

The platform's data is visualized through an interactive interface, enabling authorities to detect patterns and links in hybrid attacks. Key implementation steps include developing a comprehensive methodology, dividing countries into regional zones, and integrating findings with national and European security frameworks. Challenges involve data collection in politically influenced regions and ensuring consistent use across Member States. LMHTT's impact lies in strengthening media pluralism, uncovering hybrid threats, and enhancing societal cohesion through targeted policy recommendations.

4.3.4. STARLIGHT DISINFORMATION-MISINFORMATION TOOLSET

The STARLIGHT [25] toolset is designed to counter disinformation and misinformation through a combination of technical and non-technical solutions. It integrates advanced AI and machine learning technologies to detect, analyse, and combat disinformation campaigns. Tools include real-time media monitoring, automated fact-checking, and sentiment analysis to identify and track the spread of false narratives.

The platform supports law enforcement and policymakers by providing actionable insights and enabling cross-border collaboration. A focus on public education, including training modules and outreach programs, enhances societal resilience against disinformation. Key challenges include ensuring technological interoperability, maintaining data privacy, and addressing public trust issues. With a multi-faceted approach, STARLIGHT aims to safeguard democratic processes, enhance critical thinking, and promote informed decision-making across Europe.

4.4 INNOVATION FROM THE FOURTH PROJECT CYCLE

4.4.1 AIMVVP: AI-MODEL VALIDATION AND VERIFICATION PLATFORM

The AIMVVP addresses the growing need for trustworthy, safe, and robust AI-models by providing a standardized framework for their validation and verification. It evaluates AI systems across parameters like fairness, bias detection, robustness against adversarial attacks, explainability, and compliance with ethical and legal standards. By integrating modular tools and sector-specific benchmarks, AIMVVP ensures AI-models are ready for deployment in critical areas like healthcare, cybersecurity, and public safety.

Key features include bias detection, adversarial testing, explainability modules, and automated compliance checks with regulations such as GDPR and the AI Act. Evaluation results will be accessible through a user-friendly dashboard. In the future, the platform may also issue certifications for validated models when corresponding standards and procedures have been established. Challenges include achieving adoption across industries and addressing ethical concerns.

4.5 ANALYSIS OF THE SOLUTIONS COVERAGE OF HYBRID THREAT AREAS

In this section we look into how the recommended solutions cover the hybrid threat area with respect to the projects core themes, the target areas define by WP3 and our own view on main application areas and end-users.

[25] 2021 STARLIGHT Project

4.5.1 SOLUTIONS AND CORE THEMES

In the DoA it is stated that we should have an even distribution over the EU-HYBNET Core Themes[26]. As shown in Table 2 this is the case considering the four project cycles. The association with the Core Themes is taken from the innovation descriptions. As is seen from the fact that most solutions are associated with secondary Core Themes, there is no strict separation between Core themes and the applicability of the innovations. Thus, the presented solutions will include at least some aspects of use that are relevant for all Core Themes.

Table 2. Solutions per Core Theme as given by the original innovation on which they were based.
A bold **X** indicates the primary Core Theme and an (x) indicates a secondary Core Theme.

Project cycle	Solution	Core Theme			
		Resilient civilians, local level and national administration	Cyber and Future Technologies	Information and Strategic Communi-cation	Future Trends and Hybrid Threats.
1	**CISAE:** A Common Information Sharing and Analysis Environment		**X**	(x)	
	SARD: Situational Awareness Regarding Disinformation	(x)		**X**	
	ML4S: Media Literacy for Students	**X**		(x)	(x)
	CiToDeFaMe: Citizens Tools to Detect "Fake" Media	(x)		(x)	**X**
2	**WINS:** What Information Needs to be Shared	**X**			
	EESCM: Enhanced and Extended Supply Chain Management				**X**
	MIMI: A Market place for IMI Information			**X**	
	GECHO: Gatekeeping ECHO Chambers	**X**		(x)	
3	**CRP:** Citizen - Responder Platform	**X**			
	CiReTo: Citizens Reporting Tool		(x)		**X**
	LMHTT: Local Media Hybrid Threat Tracker			**X**	
	STARLIGHT: Starlight Disinformation-Misinformation Toolset	(x)	**X**	(x)	(x)
4	**AIMVVP:** AI-Model Verification and Validation platform		**X**		

4.5.2 SOLUTIONS AND TARGET AREAS

After analysing the distribution of solutions across Core Themes, we now further examined how these solutions align with broader Target Areas that address specific vulnerabilities and needs. The **definition** of **target areas** is given by Task 3.1 as:

[26] The Core Themes were introduced in Section 1.4.1 Project Core Themes

- A target area is a cluster of equivalent and coherent innovative solutions for a shared specific domain, vulnerability, or purpose.
- Target areas serve (reason-to-be) as a guidance for WP4 to look for standards and best practices in order to foster the development and implementation of like-wise innovations.

The target areas used are the ones defined in D3.19. In summary they are defined as follows:

1. **Integration of Cyber Solutions, (Dis)Information Detection Tools, and (Fake) News Platforms**
   Enhance coordination between existing cybersecurity tools, disinformation detection systems, and media literacy platforms to counter fake news and online manipulation more effectively. Greater integration of innovations is needed to create holistic, user-friendly solutions.
2. **Preparation, Analysis, and Management of Complex Hybrid Threats**
   Develop comprehensive threat analysis platforms to monitor evolving hybrid threat tactics, attack vectors, and vulnerabilities. This requires a cross-domain approach combining risk assessments, information operations monitoring, and critical infrastructure protection.
3. **Improving and Expanding Information Sharing Capabilities**
   Strengthen national and cross-border information-sharing networks to ensure timely, coordinated responses to hybrid threats. Support initiatives like the EU Hybrid Fusion Cell to improve data exchange between agencies, nations, and security stakeholders.
4. **Improving Societal Resilience**
   Enhance public awareness, digital literacy, and crisis preparedness to build resilience against hybrid threats. EU-wide cooperation on education, community engagement, and emerging technology adaptation will help safeguard society from evolving manipulation tactics.
5. **Safeguarding Democratic Processes and Institutions**
   Protect democratic systems from foreign interference, misinformation, and cyber threats. Strengthen media integrity, data privacy, and citizen empowerment while equipping governments and organisations with tools to navigate and counter hybrid threats.
6. **Strengthening Physical Security**
   Address vulnerabilities in critical infrastructure, military bases, and government institutions to prevent physical sabotage and escalation of hybrid threats into violent conflicts. Prioritize security reinforcements and risk mitigation strategies.
7. **Fundamental Research and Low TRL Innovations**
   Support early-stage innovations in AI, quantum computing, and cybersecurity to maintain technological superiority over adversaries. Monitor advancements and invest in future-proof hybrid threat countermeasures before they are exploited by external actors.

presents the promising innovations categorized by Target Area. Innovations highlighted in yellow indicate the foundation of our 13 solutions. The first number in the numbering of the innovations designates the project cycle in which was proposed. The following numbers refer to the numbering in the corresponding deliverable. The innovations on which the presented solutions are based are highlighted in yellow. Innovations highlighted in blue are from cycle 1, in green from cycle 2 and in brown from cycle 3.

We note that:

- **Target Area 1** has the highest number of innovations, with four solutions built upon them.
- **Target Areas 3, 4, and 5** each have two solutions based on their respective innovations.
- **Target Areas 2, 6, and 7** each have one solution based on their respective innovations.

Table 3. The table lists the promising innovations per Target Area.

Target Areas	Innovations the first number indicates which cycle the innovation comes from, followed by the number assigned to the innovation the corresponding deliverable.	Target Areas	Innovations the first number indicates which cycle the innovation comes from, followed by the number assigned to the innovation the corresponding deliverable.
Target Area 1: Integration of cyber solutions, AI applications, (dis)information detection tools, and (fake) news platforms.	1.1.1a Guides to identify fakes	**Target Area 4:** Improving Societal Resilience	1.1.1b Hybrid online dilemma game
	1.1.2a Countering disinformation with strategic personalized adverts		1.3.3 Tools monitoring population's response to information
	1.1.2b Automated detection of hate speech in social media		1.4.1c Non-partisan native-language news channels
	1.2.3a Fake news exposer		1.4.3a Training application for media literacy
	1.3b Factchecker communities		2.15 ResilienceTool (incl. RiskRadar)
	1.4.1b Debunking of fake news		3.8 Code of Practice on Disinformation
	1.4.3b Automated Fact-checker		**3.9 Starlight Disinformation-Misinformation toolset**
	2.3 Digital connected security in response to hybrid tactics		3.18 'Antidote' to hostile messaging delivered by private messaging apps
	2.8 The Development of a Proactive Defensive Framework based on ML and cloud		3.20 "Bad News" Prebunking Game platform
	2.9 A fully automated incident response solution based on CT Intelligence	**Target Area 5:** Safeguarding democratic processes and institutions	1.1.3a A blockchain-based RT info management and monitoring system
	2.10 The Development of a Deepfake Detection System		1.1.3b A crawler and real-time search engine for investors
	2.12 Detection of Disinformation Delivery by Proxy Actors		1.4.1a Journalism Trust Initiative
	2.13 Development of Real-time Rapid Alert System on Disinformation		1.4.2 Fair Trade Data Program
	2.17 Increasing capabilities to systematically assess information validity throughout the lifecycle		2.1 End-to-end Supply Chain Visibility Labels
	2.18 Crowd-sourced verification systems of fake news to counter disinformation in encrypted messaging applications		**2.2 Multi-stage supply chain disruption mitigation strategy and Digital Twins for Supply Chain Resilience**
	2.19 DDS-Alpha		2.5Establishment and reinforcement of political education of democratic values
	2.22 Collection and sentiment analysis of targeted communications		2.6 Installation of rules for mandatory declarations
	2.23 Identify and safeguard vulnerable individuals		2.16 A crawler for correlation of screened FDI with suspicious financial activity
	3.2 Anti agit-prop and hostile conspiracy warning platform		3.12 Expansion of the AVMS Directive
	3.3 WeVerify, a video plugin to debunk fake videos on social media that spread conspiracy theories		3.13 Network of anti SLAPP financial and legal support
	3.5 Breach Guard or Any Other Similar Available Solution		**3.19 Media Pluralism Monitor (MPM)**
	3.6 NordLayer Or Other Similar Solution	**Target Area 6:** Strengthening physical security	2.7 7SHIELD: a holistic framework for European Ground Segment facilities
	3.7 Shield, Watson Studio, Or Any Other Similar Available Solution		2.11 Counter-UAS
	3.21 Real-Time Fact-Checking Browser Extension		2.14 Impact and Risk assessment of critical infrastructures in a complex interdependent scenario
	3.22 Blockchain -based verification		**3.1 Mobile application to pinpoint acts of harassment/violence on the street and online**
Target Area 2: Preparation, analysis and management of complex hybrid threats	1.3.1 Resilient Democracy infrastructure platform		3.11 Advanced Surveillance Systems with Perimeter security
	2.14 Impact and Risk assessment of critical infrastructures in a complex interdependent scenario		3.14 Offline-Face-Secure-Access (OFSA)
	2.20 Integrated monitoring systems against Malware-based Information Operations		3.15 Passive Authentication for Secure Identification (PASID)
	2.21 Integrated monitoring systems against cyber-enabled Information Operations	**Target Area 7:** Fundamental research and low TRL innovations	1.2.1a Open European Quantum Key Distribution testbed
	3.17 Advanced analytical and investigative capabilities via GRACE Platform and approach		1.2.1b A quantum-resistant Trusted Platform Module
Target Area 3: Improving and expanding information sharing capabilities	1.2.2a Cyberthreat information sharing through Hyperconnectivity networks		**2.4 Commitment to validating and verifying AI**
	1.2.2b Cross-sector cyberthreat information sharing		3.4 "EXPERIENCE" The "Extended-Personal Reality": augmented recording and transmission of virtual senses through artificial-Intelligence
	1.2.2c Public-private information-sharing groups for collective action		3.10 AI And Machine Learning Technologies
	1.3.2a Early/rapid damage assessment system		
	1.3.2b Smart message system for sharing interagency OP		
	3.16 AI-enhanced Disaster Emergency Communications		

This distribution approximately corresponds to the number of innovations in each target area. Target Area 1 contains the highest number of innovations, while Target Areas 2, 6, and 7 have significantly fewer. This highlights a stronger focus on cybersecurity and disinformation over physical security and fundamental research.

4.5.3 SOLUTIONS AND MAIN APPLICATIONS AND END-USERS

Table 4 presents another way of categorizing the solutions presented based on their main area of application together with the key end-users. The three application areas chosen are:

- **Information sharing:** Hybrid threats and attacks appear in different domains and may target different stakeholders even in the same domain. Thus, to detect and be able to launch coordinated mitigating actions require that as much information as possible is shared and analysed.
- **Situational awareness:** To understand when and how hybrid threats and attacks appear it is fundamental to have good situational awareness, i.e., to be able to collect as much information as possible from as many sources as possible and have near real-time analysis capabilities.
- **IMI, Information Manipulation and Interference:** Collection and analysis of IMI information could be seen as a joint application of the first two bullets but warrants to be an area of its own as today IMI is a major Hybrid Threat. “Fake” news, conspiracy theories and information bubbles are abundant in social media and on the net and pose a major problem in today’s democratic societies.

The end-user categories are:

- **Citizens:** The general public as receivers of Hybrid Threat information from trusted sources or users if tools for verification of data in unreliable media
- **Public Admin:** Coincides with the definition of local level and national administration int the corresponding Core Theme
- **CE & CI:** These end-users are operators of critical entities and critical infrastructures.
- **LE:** Law enforcement organisations.
- **Developers:** Industries and technical development organisations.

Table 4 shows that the solutions span the application areas and the end-users’ groups relatively even. In the application area Info Sharing, six solutions contribute. The situational awareness area gets input from nine solutions. Finally, the IMI area is related to seven solutions. When it comes to end-users, citizens are targeted by three solutions and developers by two. Public admin, CE & CI and LE are related to six, four and five solutions respectively. Looking at the individual solutions it is noteworthy but also very natural that AIVMPP covers all application areas and all end-users.

There is one Hybrid Threat domain coupled directly to the IMI application area. Other Hybrid Threat domains would benefit from information sharing and maintaining reliable situational awareness and the proposed solutions could be generalized to cover also them. So, in summary, the proposed solutions cover the important area of IMI and propose solutions to advance information sharing to improve situational awareness with respect to Hybrid Threats.

Table 4. Solutions mapped on three main areas of applications and five end-user categories.

- IMI: Information Manipulation and Interference
- CE & CI: Critical Entities and Critical Infrastructure
- LE: Law Enforcement

Project cycle	Solution	Main area of application			End users				
		Info sharing	Situational Awareness	IMI	Citizens	Public admin	CE & CI	LE	Developers
1	**CISAE:** A Common Information Sharing and Analysis Environment	x	x				x		
	SARD: Situational Awareness Regarding Disinformation		x	x		x		x	
	ML4S: Media Literacy for Students			x	x				
	CiToDeFaMe: Citizens Tools to Detect “Fake" Media			x	x				
2	**WINS:** What Information Needs to be Shared	x	x				x		
	EESCM: Enhanced and Extended Supply Chain Management		x				x		
	MIMI: A Market place for IMI Information	x	x	x		x		x	
	GECHO: Gatekeeping ECHO Chambers		x			x			
3	**CRP:** Citizen - Responder Platform	x	x			x			
	CiReTo: Citizens Reporting Tool	x	x		x	x		x	
	LMHTT: Local Media Hybrid Threat Tracker			x		x			
	STARLIGHT: Starlight Disinformation-Misinformation Toolset			(x)		x		x	x
4	**AIMVVP:** AI-Model Verification and Validation platform	x	x	x	x	x	x	x	x

4.5.5 PROJECT RECOMMENDATIONS

In this section we present the key take aways from an analysis of the project recommendations. The project's recommendations are listed in ANNEX III.

The recommendations span the four project cycles and focus on innovation uptake, standardization, AI-driven solutions, private sector involvement and required research in addressing hybrid threat applications. The recommendations show a clear evolution from initial research-based proposals to more structured, implementation-focused strategies. While standardization and AI remain central themes, the emphasis on private sector collaboration, media authenticity, and procurement strategies increases over time.

We note that across all project cycles the promotion and industrialization of reviewed innovations is recommended. No blocking issues were found in the proposed solutions. We also note that CISAE standardization is promoted in all of the first three cycles. This to support increased information sharing to provide better situational awareness in critical infrastructure (e.g., cyber and physical threats), disinformation campaign monitoring (e.g., IMI and media manipulation), etc.

Use and development of AI driven tools is another recurring topic. They are proposed to e.g., detect disinformation campaigns, analyse situational data across multiple domains and jurisdictions, detect false reporting and misinformation operated as hybrid attacks.

Research in Media Literacy and training materials for the general public should be supported and increased; frameworks and gaming models for effective media literacy training should be developed. For detection of IMI, it is proposed that standardized media formats should be introduced for provenance and authenticity verification and that automatic and AI driven tools for deconstructing disinformation campaigns should be developed.

The need for private sector involvement and public-private collaboration is highlighted and it is recommended that a Task force should be set up to explore private sector participation in hybrid threat monitoring. This with the target to eliminate trust barriers and information ownership issues. Federated machine learning is recommended to address security/privacy concerns while allowing data analysis across organisation. Here we add that privacy requirements may be fulfilled by use of other privacy preserving techniques as discussed in section 3.1 Research Area: Stealing data attacking individuals in D3.9.

Finally, there is a need for increased EU and national procurement support to facilitate the funding of hybrid threat solutions. In summary, the following findings are provided as recommendations and conclusions:

1. CISAE Standardization is a core recommendation and that information sharing is key for successful situational awareness regarding hybrid threats. There is a need for a unified EU-wide framework for hybrid threat monitoring and countermeasures.
2. AI is an essential tool for analysis of massive information flows and hybrid threat detection. However, the robustness and trustworthiness of used AI solutions needs to be verified and validated.
3. The need for media literacy training and easy to use tools for fake media detection / fact-checking is strong.
4. Public-private collaboration needs to be increased in a structured way as trust and legal barriers in private sector involvement are prevalent.
5. Procurement challenges persist and financial and regulatory constraints need urgent attention.

4.6 INSIGHTS FROM THE ISWS

The three EU-HYBNET Innovation and Standardisation Workshops (ISW) have covered the following key areas related to hybrid threats: crisis communication and responder platforms, cyber threats and disinformation, citizen reporting and engagement, and law enforcement innovations.

4.6.1 CRISIS COMMUNICATION & RESPONDER PLATFORMS

A primary function of crisis communication and responder platforms is to enhance communication between citizens and emergency responders during crises. These solutions incorporate AI-driven verification processes to process and authenticate citizen reports, ensuring that relevant agencies (law enforcement, intelligence, emergency responders, local administrations) receive accurate and timely information.

Benefits:

- Improved situational awareness, allowing authorities to assess crises in real-time.
- Faster emergency response times, enhancing overall crisis management.
- Establishment of a common operational picture, ensuring coordinated interventions.

Challenges:

- Standardization barriers: Different regulatory requirements across EU Member States necessitate harmonized governance policies.
- Risk of misinformation: Citizen reports may be manipulated or inaccurate, leading to potential overload on emergency responders.
- Privacy concerns: Balancing anonymous reporting with security measures is crucial to maintaining trust and integrity.

The main conclusion is that standardization and coordination at both national and EU levels must be prioritized, ensuring interoperability and cross-border cooperation.

4.6.2 INFORMATION MANIPULATION & INTERFERENCE (IMI)

IMI solutions focus on detecting and countering both foreign and domestic disinformation campaigns, leveraging AI-driven analysis of regional and national media streams. Cross-sector collaboration between governments, fact-checkers, and media organisations is crucial to effectively combat IMI threats.

Key strategies:

- Proactive defence over reactive policies: Strengthening digital literacy programs to reduce public susceptibility to disinformation.
- Citizen-friendly verification tools: Enabling individuals to independently verify media authenticity.
- Standardized information-sharing protocols: Enhancing cooperation across EU Member States.

Challenges & Risks:

- Censorship concerns: Stricter monitoring measures could be perceived as restrictions on free speech.
- Social media jurisdictional challenges: Many platforms operate outside EU regulations, complicating enforcement efforts.

- Rapid evolution of disinformation tactics: AI-based solutions must be continuously updated to detect emerging threats.

Future strategies should focus on harmonizing AI-driven IMI detection, strengthening fact-checking networks, and establishing EU-wide regulatory frameworks.

4.6.3 CITIZEN REPORTING & ENGAGEMENT IN HYBRID THREATS

Secure citizen reporting platforms play a critical role in identifying early signs of hybrid threats. Anonymous reporting mechanisms, combined with AI-powered verification, can enhance public participation in security efforts.

Opportunities:

- Real-time threat detection, allowing law enforcement to proactively mitigate risks.
- Integration of AI-models to detect coordinated disinformation efforts.
- Predictive analysis based on citizen reports to identify emerging hybrid threats.

Challenges & Risks:

- Manipulation by trolls and false reporting campaigns, potentially overloading security agencies.
- Balancing anonymity with security, ensuring that credible reports are prioritized.
- Legal compliance (GDPR & data protection laws) regarding citizen-contributed intelligence.

Future implementations should prioritize security, accuracy, and ease of use, ensuring that citizen participation enhances security without creating new vulnerabilities.

4.6.4 KEY INSIGHTS & BROADER CONSIDERATIONS

The key insights from the ISWs are summarized in the following bullets:

- Hybrid threats evolve faster than regulatory frameworks**, making** standardization a top priority**.**
- AI and Big Data solutions **are crucial for** real-time threat analysis, media verification, and crisis response**.**
- Early end-user involvement **ensures that** security tools are operationally effective **and** meet real-world needs**.**
- Media literacy programs **must be expanded within** education systems **to build** long-term resilience against misinformation**.**
- Cross-sector collaboration (government, academia, industry) **is essential for** successful hybrid threat mitigation**.**

Key actions for ensuring a sound development of future strategies and solutions would be to:

- Standardize security frameworks across EU jurisdictions.
- Strengthen ethical & legal oversight for AI-driven security tools.
- Promote public-private partnerships for disinformation monitoring.
- Enhance citizen engagement & digital literacy programs.

By focusing on standardization, collaboration, and AI-driven innovation, the EU can effectively counter hybrid threats and enhance security resilience.

4.7 SOLUTIONS THROUGH THE CORE MODEL LENS

A comprehensive description, according to the CORE model, of the solutions presented show that they address hybrid threats across governance, civic, and service domains at international, national, and local levels. For instance, CISAE will create a common information sharing and analysis environment that connects local nodes in every Member State, allowing for near real-time exchange of threat intelligence and improved coordinated mitigation actions. By leveraging the EMSA CISE architecture and establishing governance bodies to ensure compliance with European directives like CER and NIS2, CISAE would enhance technical services and fosters trust among stakeholders.

Building on CISAE, SARD focuses specifically on countering disinformation. By using similar frameworks and incorporating federated machine learning tools for distributed and privacy preserving analysis. SARD offers rapid situational awareness against disinformation campaigns. The solution aligns with EU initiatives such as the Action Plan Against Disinformation, thereby strengthening governance and public trust despite potential cross-border coordination challenges. In parallel, the ML4S initiative proposes to embed media literacy into EU curricula for high school students. By developing adaptable, culturally sensitive frameworks and gamified training models, it empowers a new generation to critically assess media content, thereby reinforcing civic resilience and laying a foundation for sustained democratic engagement.

CiToDeFaMe contributes to societal resilience by providing citizens with tools to detect digitally altered or fake media. Oversight by an EU governance body possibly linked to the European Digital Media Observatory would ensure that local and national authorities can tailor guides and detection tools to diverse local and national environments. This effort not only reduces the effectiveness of disinformation but also builds trust in media authenticity. However, its success relies on broad adoption by media app providers as well as citizens.

The WINS solution takes a methodical approach to information sharing among critical infrastructure entities by employing a “what-if” scenario-building process. The core is to understand what information that needs to be shared to detect and be aware of hybrid threats and operations. WINS is an enabler for enhancing cross-sectoral and cross-border anomaly detection, thereby improving overall resilience planning despite. Challenges are found in engaging private sector stakeholders and overcoming technical interoperability barriers.

EESCM addresses vulnerabilities in supply chains by integrating geopolitical risks and deeper value chain analysis through Digital Twin technology. This framework, which should be supported by an EU-wide governance structure and sector-specific testing, optimizes recovery strategies and reduces dependency on fragile supply chains.

MIMI establishes a secure marketplace for exchanging IMI information. By incorporating economic incentives, secure access protocols, and service-level agreements, MIMI strengthens an information-sharing ecosystem that is critical for rapid response.

On the front of countering extremist narratives, GECHO leverages AI-based tools to monitor and intervene in online recruitment activities by extremist groups. The proposed platform, which aligns with EU counter-terrorism agendas, would improve law enforcement situational awareness and at the same time address the sociocultural factors that contribute to radicalization, thereby reinforcing both national security and societal cohesion.

The CRP, or Citizen-Responder Platform, amplifies an integrated approach by connecting first- and second-line responders with real-time trusted citizen data during emergencies. Its AI-enhanced

features, including an “Disaster Mode” app, ensure that emergency response is both efficient and coordinated across diverse administrative levels.

Complementing CRP, the CiReTo mobile application empowers citizens to report evidence of hybris threat operations, incidents of harassment or violence in real time. By utilizing geolocation, multimedia evidence, and anonymized data, it can enhance community engagement and supports law enforcement while maintaining robust privacy safeguards.

The LMHTT diagnostic tool addresses regional risks to media pluralism by collecting data on media ownership and published content. It assists authorities in detecting local vulnerabilities to foreign interference and information manipulation operations, and the need for reinforcing policy recommendations that bolster societal cohesion.

STARLIGHT, among other solutions, offers a multifaceted disinformation and misinformation toolset. Through real-time media monitoring, automated fact-checking, and sentiment analysis, STARLIGHT supports law enforcement. Its cross-border collaborative framework is essential for safeguarding democratic processes, even as it navigates technological interoperability and trust challenges.

Finally, AIMVVP establishes a standardized framework for AI-model validation and verification. By assessing AI systems on parameters such as fairness, bias, robustness, and ethical compliance, AIMVVP not only ensures that critical AI applications in hybrid threat operations, healthcare, cybersecurity, and public safety are trustworthy but also sets new benchmarks for industry-wide adoption.

Together, these solutions exemplify a multi-levelled strategy against hybrid threats, each reinforcing key societal spaces—governance, civic, and services—across various levels of operation. By integrating technological innovation with structured governance and community engagement, the initiatives collectively build a resilient ecosystem capable of anticipating, detecting, and mitigating diverse hybrid threats in today’s complex security environment.

4.8 CONCLUSIONS

The proposed solutions cover important hybrid threat areas and benefit many end-users. Many of them can be characterized as enablers, e.g. the final solution AIMVVP and CISAE.

Project solutions and recommendations present both research-based ideas as well as structured, implementation-focused strategies. Core themes include CISAE standardization for improved information sharing, the use of AI-driven tools for detecting disinformation and analysing complex data flows, and the development of media literacy training and tools for fake media detection. Additionally, increased private sector participation and targeted procurement support are necessary to secure funding and address regulatory constraints. Overall, by prioritizing standardization, collaboration, and AI-driven innovation, the EU can build a resilient ecosystem capable of effectively countering diverse hybrid threats.

Our analysis also reveals that hybrid threats evolve faster than regulatory frameworks, underscoring the need for standardization across the EU. AI and Big Data are vital for real-time threat analysis, media verification, and crisis response, while early end-user involvement ensures that security tools are practical and effective. Expanding media literacy within education systems is also essential for long-term resilience against misinformation. Furthermore, cross-sector collaboration among government, academia, and industry is critical, with recommendations urging public-private partnerships and enhanced citizen engagement to overcome trust and legal challenges.

Together, these solutions exemplify a multi-layered strategy against hybrid threats, each reinforcing key societal spaces—governance, civic, and services—across various levels of operation. By integrating technological innovation with structured governance and community engagement, the initiatives collectively build a resilient ecosystem capable of anticipating, detecting, and mitigating diverse hybrid threats in today's complex security environment.

Furthermore, we conclude that the solutions mainly are independent except for the CISAE upon which SARD and other sharing solutions could be built. This means that a roadmap for development of the solutions should have CISAE in an early stage while the other innovations can be developed in parallel.

5. REVIEW OF THE METHODOLOGY OF THE INNOVATION UPTAKE FRAMEWORK

5.1 INTRODUCTION

In this chapter, the methodology used to review and analyse the Methodology for Creation of the Uptake, Industrialization and Research strategies (MCUIR) is introduced. The first version of MCUIR was initially designed in the first project cycle and subsequently applied in all the three full project cycles, as well as for the one in the fourth project mini-cycle. The only significant change to the methodology was the introduction of the "Setting the scene description" in the second full project cycle. Details on how it should be applied ca be found in chapter 2.

Lessons learned from the previous project cycles showed that MCUIR has been effective in guiding the creation of roadmaps and uptake strategies. However, it was also noted that better alignment of the methodologies used in WP3 with the Task 4.2 developed framework could have streamlined the strategy and roadmap creation processes. Such an alignment is explored in section 5.3.

This chapter explains the research methodology for MCUIR and summarises relevant input from the third and fourth mini-cycles, including procurement, ISWs, and TASK 4.2 lessons learned. It also discusses potential improvements to make the methodology more widely applicable for evaluating innovation and industrialization. Finally, it covers ongoing work to develop a more general and updated version of the methodology.

5.2 RESEARCH METHODOLOGY FOR ASSESSMENT OF MCUIR

In this subsection we describe the research methodology followed for carrying out an assessment of the current methodology. The presentation and analysis of MCUIR is tales its description in Chapter 2 as a starting point.

5.2.1 DESCRIPTION OF USED METHODOLOGY FOR STRATEGIES DEVELOPMENT

The main purpose of MCUIR process was to go through a series of steps to provide exploitation strategies and recommendations for how innovations within the hybrid threat domain can navigate the path to market adoption, uptake, industrialisation and exploitation across the EU.

A high-level description of the MCUIR process is shown in Figure 6. It is a more general and detailed description than Figure 5 in Chapter 2.

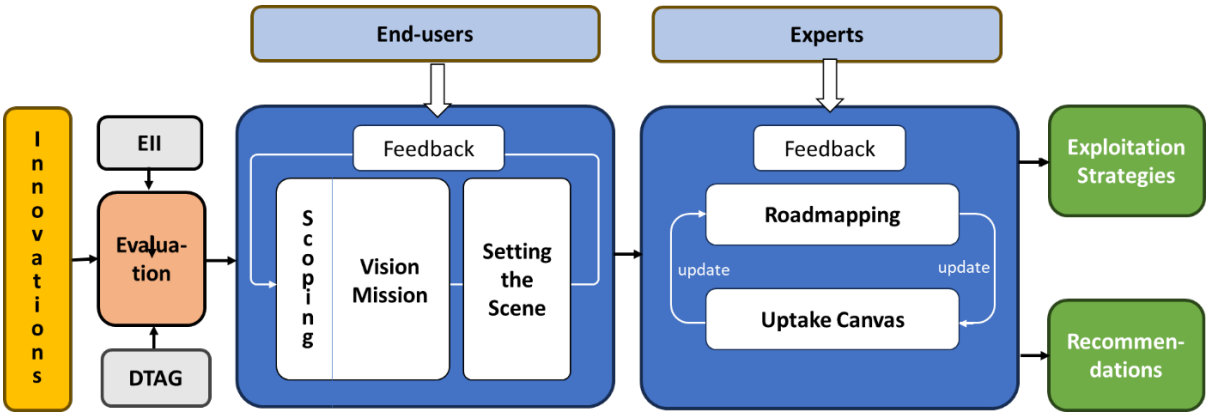

Figure 6. High-level description of the followed process to innovation uptake, MCUIR.

The MCUIR methodology in Figure 6 is a structured and comprehensive approach for innovation uptake that involves feedback and review cycles from multiple stakeholders and phases.

The process begins with defining the "Innovations" (shown in yellow). The format for presenting an innovation is given in a template called the Innovation Description. The innovation Description comprises a number of so-called boxes which should be filled with descriptions of different aspects of the innovation. The innovations are then are fed into an evaluation stage that utilises input from the EII[27] (Excellence, Impact and Innovation assessment used by WP 3) assessment processes and the DTAG (Disruptive Technology Assessment Game organised by Task 2.4). The result of these assessments forms the basis for the next phases.

Following the assessments, the innovations to be handled are selected and two feedback loops involving stakeholder groups are carried out. In the first loop, three components are developed/described:

- Scoping of the solution: Instantiate the innovation in a concrete setting by reviewing the scope of the innovation and if needed, redefine it to get a more generic or specific solution to analyse.
- Vision and Mission: Clear statements of what is to be achieved and how.
- Setting the Scene: Includes the broader context and background of the innovation.

In the second loop, experts are engaged to focus on creating an Innovation Uptake Canvas for the scoped solution by iteratively define and refine:

- A Roadmap for industrialization of the solution in Roadmapping exercises, i.e., creating a strategic plan for the implementation (short-term and long-term)
- The Innovation Uptake Canvas which should be a holistic framework for analysis of the solution details, innovation uptake environment and resources.

These two components are defined, updated and improved with the help of experts in the relevant domains of the solution and the IUC aspects.

The process finally, results in two main outputs: 1) Exploitation Strategies: concrete plans for industrialisation, commercialisation and exploitation uptake, and 2) Recommendations: specific guidance for successful uptake and lessons learnt.

5.2.2 THE DOUBLE DIAMOND

For our review of the process used to evaluate innovations and develop uptake strategies, we used a widely recognized and accepted approach, the Double Diamond.

The selection of the Double Diamond as an evaluation framework, was made after considering the history and development of innovation models, often divided into generations (Berkhout et al., 2006)[28]. We considered models from the first generation (whose main characteristics were technology push, linear process with markets at the end of the pipeline, scientific freedom, no strategic goals, no chain management). We also considered second generation models (whose main characteristics were the market pull, linear process with science at the end of the pipeline, contract research, weak ties with corporate strategy and little emphasis on chain management). Also, we looked at third generation

[27] For details on EII see D3.1

[28] Berkhout, A. J., Hartmann, D., Van Der Duin, P., & Ortt, R. (2006). Innovating the innovation process. International journal of technology management, 34(3-4), 390-404.

models (that combined technology push and market pull, innovation projects are linked to R&D and company goals "open R&D", strong emphasis on chain management), and also we considered fourth generation models (whose characteristics include the innovation is embedded in partnerships "open innovation", attention is given to an early interaction between science and business, the technical knowledge of emerging technologies is complemented by "soft" knowledge of emerging markets, new organisational concepts are acknowledged emphasizing skills for managing networks, with specialized suppliers and early users, and entrepreneurship plays a central role) (Berkhout et al., 2006). The Double Diamond lies within the last generation of models, and while other models also offer valuable insights, the Double Diamond's flexibility and wide applicability made it a strong candidate for innovation process evaluation, among the ones we investigated.

We found that employing the Double Diamond model provided a solid foundation for our analysis. According to the Design Council in the UK, "The Double Diamond is a visual representation of the design and innovation process. It's a simple way to describe the steps taken in any design and innovation project, irrespective of methods and tools used".

More specifically, the framework originating from Design Science[29] offers the following objectives and benefits:

1. **Comprehensive evaluation**: Provides a holistic assessment of the current process.
2. **Thinking outside traditional boundaries**: Encourages thinking and working more like a designer, emphasizing the understanding and capturing of user needs or problems.
3. **Strategic improvement**: Identifies specific areas for improvement.
4. **Iterative process**: Allows for iterative refinement based on empirical insights.

The Double Diamond Design Process, introduced by the British Design Council, comprises four distinct phases:

1. **Discover**: The primary goal is to discover and explore the idea, user need, or problem.
2. **Define**: Involves clearly articulating and prioritizing the needs or problems, while planning for potential solutions.
3. **Develop**: Focuses on developing prototypes to visualize the solution idea, testing, and refining the solution.
4. **Deliver**: The final product or solution is launched to the user.

Figure 7 illustrates the Double Diamond framework for innovation, as defined by the British Design Council[30]. The figure below illustrates the application of the Double Diamond adapted for EU-HYBNET and is used for describing the methodology for innovation uptake, industrialization, and research uptake, using existing project results as a basis. Key aspects included are understanding how to improve the approach, identifying areas for possible improvements, revising the methodology, making concrete recommendations, and suggesting best practices.

[29] Hevner, A. R., March, S. T., & Park, J. (2004). Design science in information systems research. MIS Quarterly, 28(1), 75-105.

[30] https://www.designcouncil.org.uk/our-resources/framework-for-innovation/

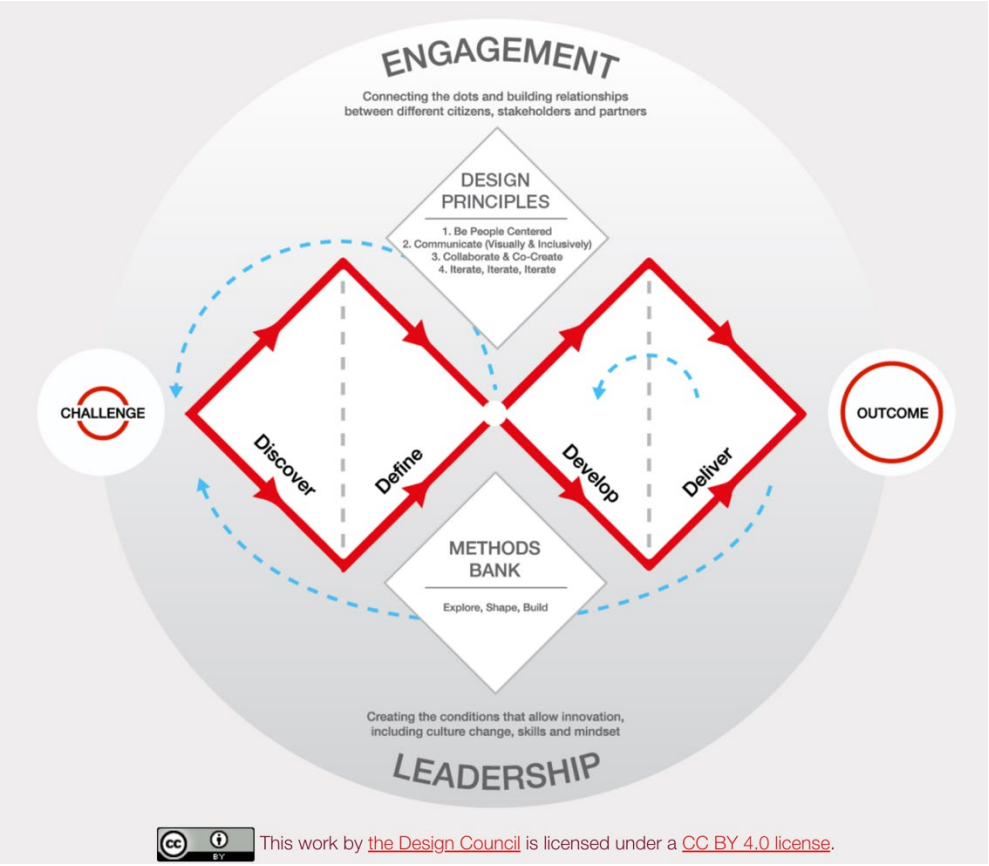

Figure 7. Double Diamond framework process model for innovation.

The Discover phase involved a comprehensive exploration of State-of-the-Art frameworks for innovation uptake. These included different methodologies, frameworks, canvases and radars (such as TOE, TELOS, THOR, SWOT, BMC, etc. see D4.4) and were analysed considering different conditions like the existing market, standardization, innovations' descriptions, procurement landscapes and competitive dynamics. The analysis helped in defining a clear vision, mission and strategy, as well as crystallizing the problem to be solved.

The vision included: "to create a tool for evaluating innovation uptake possibilities" and the problem was identified "no single framework is sufficient for comprehensive evaluation". The mission was formulated as "to develop an evaluation tool for innovation uptake". Finally, our Strategy included: "to evaluate different methodologies, based on a set of evaluation criteria (as described in Subsection 5.2.1 using the EII (Excellence, Impact and Innovation assessment) and DTAG (Disruptive Technology Assessment Game) and select the methodologies to synthesise the solution".

Following the Define phase, the Develop phase involved synthesising various methodologies, using the Innovation Uptake Canvas in combination with the Roadmapping procedure (as described in

ANNEX II: The methodology framework). The developed solution underwent iterative design cycles, included evaluation and refinement, as well as instantiation, to ensure effectiveness. In the Delivery phase, the solution, the final tool was introduced, accompanied by lessons learnt and practical guidelines for its application.

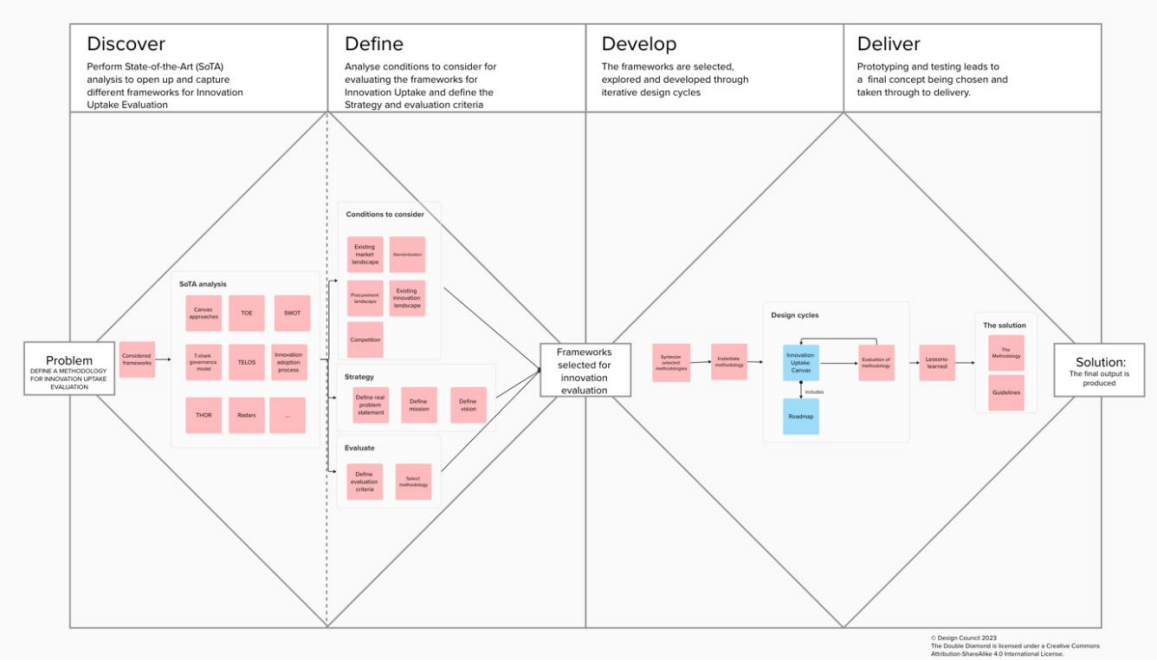

Figure 8. High-level view of the Double Diamond method[31]

[31] Access to the Double Diamond diagram is provided via the following link for the interested reader: https://app.mural.co/t/rise9766/m/rise9766/1732264770856/47f151adbe227efdd4ab2ca2aa58e593ea04ccd9

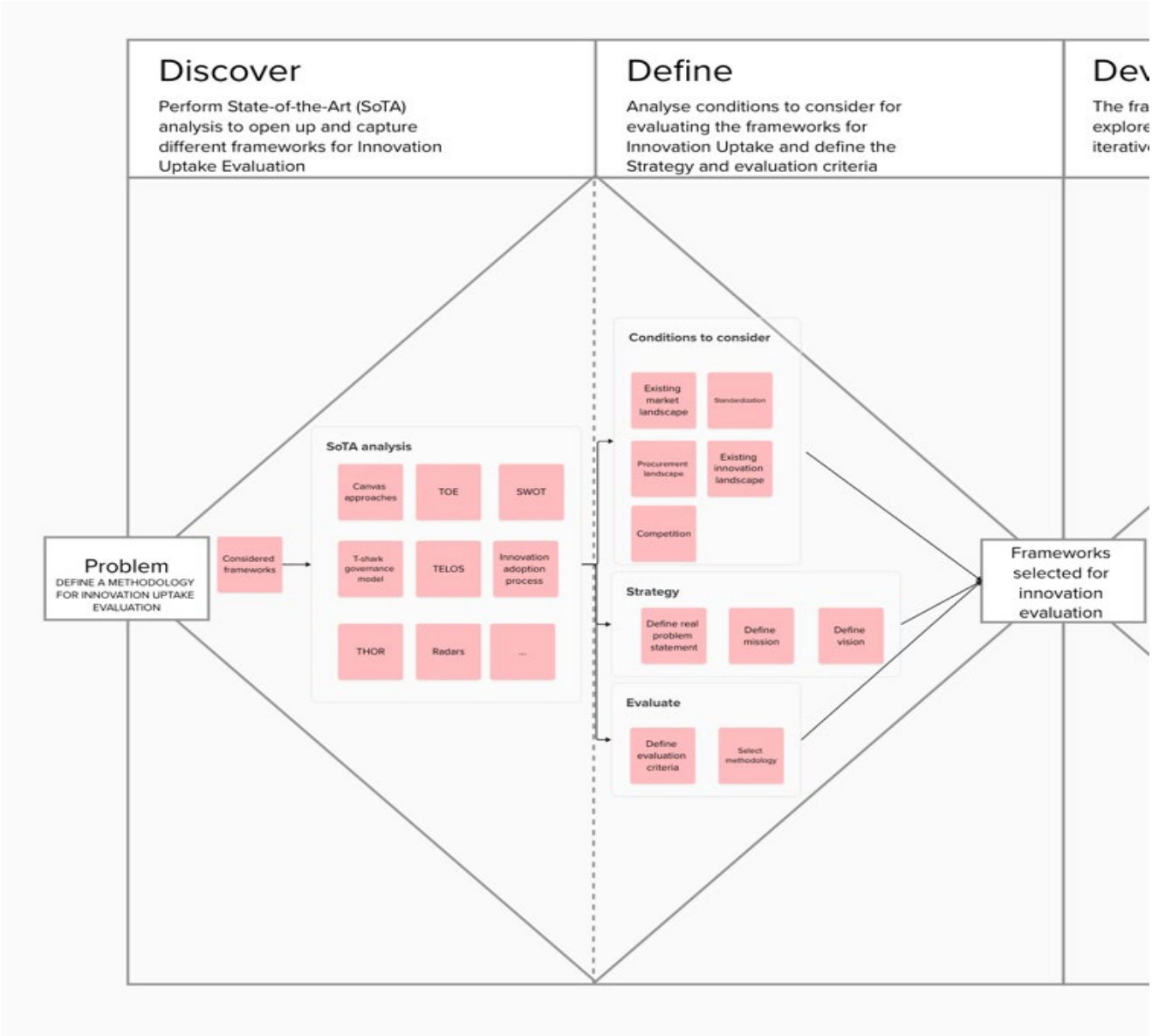

Figure 9. The first diamond, detailed view of the Double Diamond (part 1/2)

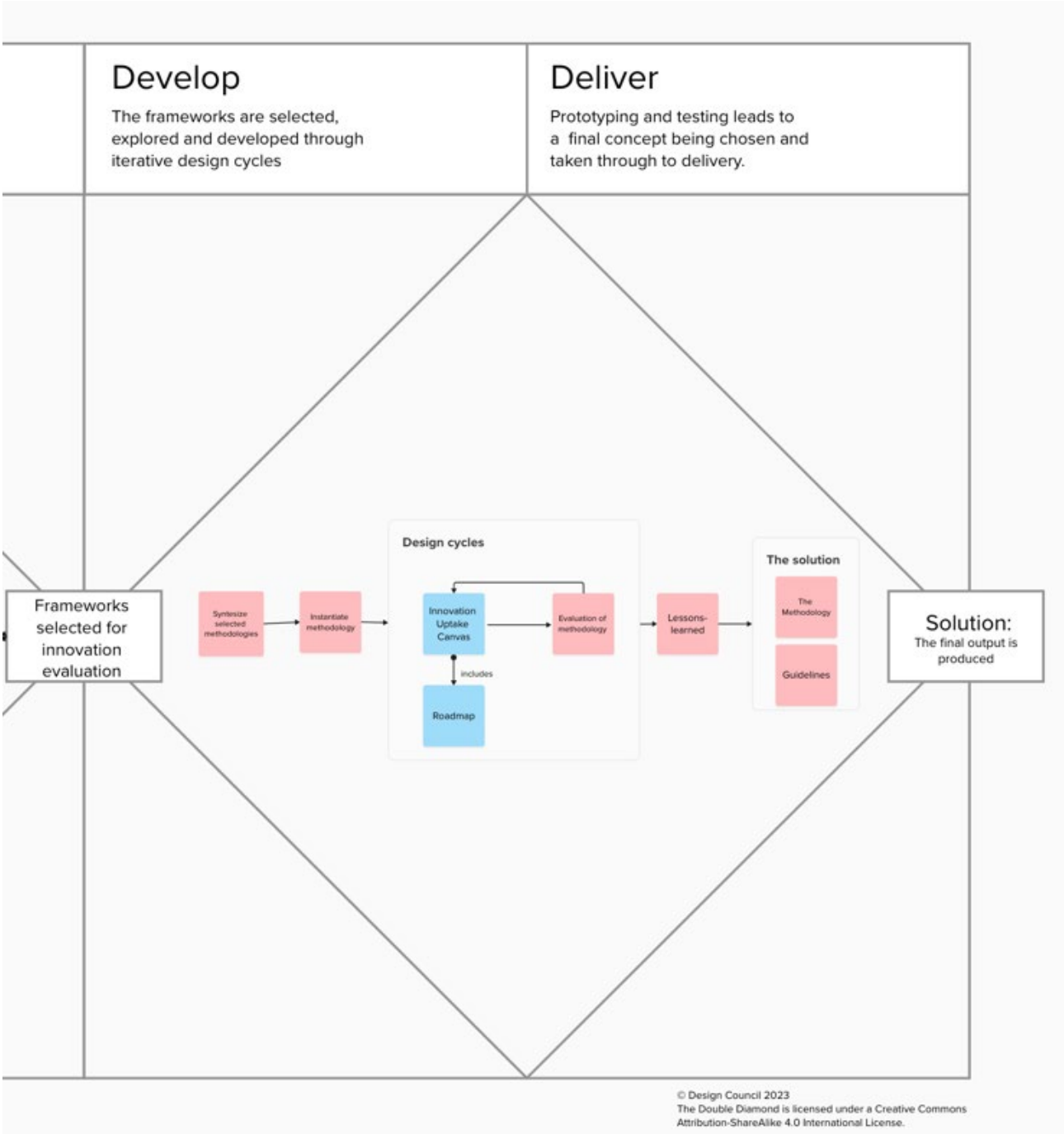

Figure 10 The second diamond, detailed view of the Double Diamond (part 2/2)

As final output, we provide a detailed analysis of the refined, revised, and improved innovation uptake process, with respect to strengths and potential additional improvement areas, and concrete and actionable best practices for future innovation management.

The application of the Double Diamond as a process to evaluate our innovation process was efficient and practical, and suitable due to its structured approach and flexibility to be applied in various contexts. It allowed the systematic evaluation through its four stages, making it a valuable tool for both design and innovation evaluation.

5.3 MAPPING BETWEEN THE INNOVATION DESCRIPTION AND THE CANVAS

In order to fill-in the gap between the innovators' initial concept and current industrial/market needs, Innovation Uptake Canvases were developed for each of the innovations (see D4.4-D4.6). This helped to align the innovators' perceptions on the possibilities of their innovations with exploitation ideas and overall vision, with the rapidly evolving technological market landscape and innovation uptake strategies.

However, the problem that there are gaps and misalignments between the original ID and the IUC, primarily due to differences in the level of detail provided, has been acknowledged from the first cycle of the project. There is as well a need for complementary innovation information which could provide insights on strategies on marketing, further development and outreach. While there was interest from the stakeholders to align and update the IDs, due to lack of time and resources, this was not done.

In this section we investigate how to streamline the development of IUCs based on the IDs. We leverage Generative AI (GenAI) tools such as ChatGPT 4.0, Co-Pilot, and Claude 3.5 Sonet to align and enhance the templates for both the IUC and the ID without relying on requiring use of extensive human resources Generative AI (GenAI) tools like ChatGPT 4.0[32], Co-pilot[33] and Claude 3.5 Sonet[34] were utilised to streamline the process in. The tools enabled an automated, efficient, explainable, and traceable process by identifying specific gaps, resolving misalignments, and highlighting areas requiring more detailed complementary information. Additionally, they facilitated the creation of a structured mapping between the innovation description elements and the innovation uptake canvas components, as outlined in Table 5 below. The table includes a reasoning column to increase explainability.

The process followed is explained as follows:

- Step 1: Extracted the information from the instruction manual for assessing the innovations
- Step 2: Used the template used for Innovation descriptions together with the instructions to create simplified version of the template to feed to the GenAI tools
- Step 3: Extracted the innovation uptake canvas description into a template to feed to the GenAI tools
- Step 4: Asked for bi-directional mappings among the templates, from the innovations to the canvas, and from the canvas to the innovations
- Step 5: Asked for explanations of the mappings, and reasonings justifying the found matches or the mismatched sections
- Step 6: Human experts consolidated and evaluated the mappings and made revision to the final mapping. The mapping is shown below.
- Step 7: Provided an example innovation description and tried to create the canvas based on the mapping and validated the result.
- Step 8: Made any necessary changes to the canvas and to the mapping accordingly.

[32] https://chatgpt.com/
[33] https://copilot.microsoft.com/
[34] https://claude.ai/

5.3.1 RESULTING MAPPING TO BRIDGE CONCEPTUAL GAPS

"Setting the Scene" information, which is collected before the canvas creation, could be mapped with the Innovation Description BOX 6: DESCRIPTION OF USE CASE(S).

Table 5. Mapping between Innovation Uptake Canvas and Innovation Description boxes

Innovation Uptake Canvas (IUD)	Innovation Description (ID)	Reasoning for mapping
BOX 1: Description of the solution	BOX 1: NAME OF THE IDEA BOX 3: TYPE OF SOLUTION	Direct alignment with the initial description of the innovation.
BOX 2: Added value proposition	BOX 2: REFERENCE TO CAPABILITY GAPs/NEED BOX 7: IMPACT ON COUNTERING HYBRID THREATS (BOX 6: DESCRIPTION OF USE CASE(S))	Cover the solution's benefits and effectiveness. Describe the gaps and needs and where they are applicable.
BOX 3: Stakeholders and domains	BOX 4: PRACTITIONERS BOX 2: REFERENCE TO CAPABILITY GAPs/NEED	Match the detailed breakdown of practitioners and end-users.
BOX 4: Functional description	BOX 8: ENABLING TECHNOLOGY BOX 1: NAME OF THE IDEA	Describe the technical components and requirements.
BOX 5: Operational description	BOX 6: DESCRIPTION OF USE CASE(S) BOX 12: PRECONDITIONS (OPTIONAL) BOX 13: LIFE CYCLE MAINTENANCE (OPTIONAL)	Cover implementation aspects, restrictions, and operational considerations.
BOX 6: Roadmapping	BOX 5: STATE OF THE ART BOX 12: PRECONDITIONS (OPTIONAL) BOX 13: LIFE CYCLE MAINTENANCE (OPTIONAL) BOX 9: IMPLEMENTATION	Address technology readiness levels, stage of solution, and time to market.

Innovation Uptake Canvas (IUD)	Innovation Description (ID)	Reasoning for mapping
BOX 7: Required development resources	BOX 10: IMPLEMENTATION EFFORT BOX 8: ENABLING TECHNOLOGY	Discuss resources and associated costs.
BOX 8: Required operating support system	BOX 13: LIFE CYCLE MAINTENANCE BOX 11: COUNTERMEASURES	Focus on maintenance, updates, and on-going support.
BOX 9: CAPEX & OPEX	BOX 10: IMPLEMENTATION EFFORT (Costs section)	Provide detailed cost analysis.
BOX 10: Competition and market	BOX 6: DESCRIPTION OF USE CASE(S)	Help contextualize the solution in the existing market landscape.
BOX 11: Funding and organisation	n/a	Covers additional organisational and funding aspects.
BOX 12: Barriers	BOX 9: IMPLEMENTATION (Restrictions)	Addresses potential legal, ethical, and implementation barriers.

5.3.2 RESULTS AND RECOMMENDATIONS

The mapping between the ID and the IUC boxes showed a strong alignment in many areas, but some gaps and need for improvements were identified. While most concepts matched well, three canvas boxes—#4 (Functional Description), #10 (Competition and Market), and #11 (Funding and organisation)—did not fully align. We were unable to completely map these IUC boxes with corresponding content in ID boxes.

There were 8 specific areas identified where the ID could be strengthened and complemented. These include more comprehensive analysis for stakeholders, roadmapping, resource planning, operational support, cost analysis, market/competitive landscape, funding strategies, and barrier assessment. Overall, the IUC template provides a more holistic and detailed approach to innovation assessment, suggesting that the ID boxes could be enhanced by incorporating these additional dimensions of analysis.

The following proposals for enhancements could be made to both ID and IUC:

1. “Setting the scene” should include use case descriptions as background for the reader to understand the foundation of the proposed solution. Such a box could be added to the IUC template to describe the setting the scene as background and state-of-the art description.
2. The innovation descriptions could add a section with functional descriptions.
3. Expand Box #4 (Practitioners) on IUC to include more detailed stakeholder alignment.
4. Add new box in ID boxes or expand existing ones to cover:

- Detailed road mapping
- Comprehensive resource planning
- Operational support system considerations
- More in-depth market and competitive analysis
- Funding and uptake strategies
- Comprehensive barrier analysis

These recommendations could provide a more complete understanding and analysis of each innovation's potential, challenges and implementation resources required.

The analysis performed in this section bridges the conceptual gap between ID and IUC and addresses the main motivation of this work, which was to create a robust methodology for understanding and positioning technological innovations within broader strategic uptake contexts.

The use of GenAI and human experts in the process to improve our methodology has offered several key advantages. We had been able to rapidly process complex information and instructions within the descriptions and we were able to identify nuanced connections even in cases where there was misalignment in the terminology used. The process we followed was iterative and allowed us to make gradual improvements and revisions that improved the quality and helped us understand the resulting mapping, making it reproduceable and increasing trustability. We were able to be efficient in mapping technical, non-technical and strategic elements and insights of the innovations by analysing detailed innovation descriptions, matching them to canvas elements and generating a comprehensive and structured mapping. There was also increased traceability, involvement of experts and high explainability in the mapping process used.

5.4 RECOMMENDATIONS ON PROCUREMENT ASPECTS

This section includes the most important recommendations from D4.3 which will be taken into account in the update of the canvas and MCUIR.

Market Consultation. Before starting the public procurement process, public institutions are advised to engage with the market to explore state-of-the-art and commercially available solutions. Transparent market engagement plays a crucial role in evaluating the feasibility of a tender by assessing institutional needs, determining appropriate standards and technical specifications, and identifying existing solutions that can be reused, thereby avoiding the need to "reinvent the wheel."

At the European level, several repositories, such as Joinup, the European Federated Interoperability Repository (EFIR) and the European Interoperability Framework (EIF)[35], can be consulted to address these points.

Use available templates. Officials responsible for preparing public procurement specifications and documents can greatly benefit from using readily available templates as a starting point. General procurement templates are often available on the TED[36] platform, while for innovation procurement, public entities can refer to the EAFIP toolkit[37]. At the national level, various initiatives support this process. For example, in Poland, the Public Procurement Office (PPO) is responsible for drafting public procurement policies, regulating and coordinating the national procurement system, and preparing standardized tender documents along with guidance materials. Similarly, in Luxembourg, the Business

[35] European Interoperability Framework (EIF) for European public services
[36] EU Tenders: Standard forms for public procurement
[37] European Assistance for Innovation Procurement (EAFIP): Toolkit

Process Management Office (BPMO) offers tools and templates to assist contracting authorities in preparing tenders.

Include skilled personnel. It is strongly advised to involve experts in the field in the process. Their participation is essential for identifying needs, developing (technical) specifications, monitoring solution development, and conducting testing to ensure that performance and operational aspects are adequately addressed. In this regard, hybrid and cybersecurity threats should be taken into account when planning the procurement of a new system or service, with threat identification being an ongoing consideration throughout the entire procurement lifecycle.

Carry out adequate vulnerability assessment. Vulnerabilities should be assessed prior to procuring new products or services, and the vulnerabilities of existing products or services should be continuously monitored throughout their lifecycle. Additionally, the procuring organisation should define a minimum set of security tests to be conducted on acquired products or systems, based on their type and purpose. It is also crucial that any newly acquired or configured product undergoes a penetration test within its actual installed environment. Similarly, any remedial actions taken must align with the operational parameters of the specific environment.

IPR provisions. To ensure that a procured solution can be reused by other public authorities or redistributed, it is essential to include appropriate IPR provisions in the procurement documents. This is particularly important when procuring ICT solutions that will be accessed by citizens and businesses. One approach is to include requirements in the tender documents that promote maximum public access for citizens and businesses. This can be achieved by specifying that the procured solution should be accessible to a variety of systems, without reliance on specific branded products or applications. Additionally, accessibility requirements for people with disabilities should be carefully considered.

Open requirements. Requirements should be outlined in an open and flexible manner as far as possible with respect to the intended use and the environment in which the solution will be used. There may be a tendency to request highly specific solutions to ensure that a product meets the exact expectations of the procuring entity. However, this approach poses several risks and drawbacks. First, customized solutions are typically more expensive than standard, off-the-shelf alternatives. Additionally, they are less likely to be reusable. Furthermore, suppliers who develop and manage custom systems often retain all critical system information, making it difficult to migrate to another supplier or to maintain or upgrade the system in the future. Excessive customization can result in supplier dependency, which should be avoided. In general:

a. Benchmarks should be utilized to ensure that products meet or exceed overall performance standards.
b. Functional or performance-based requirements should be used to define specifications in a vendor-neutral way.
c. Reference standards and technical specifications to avoid naming specific processes or trademarks.
d. Specific references should only be used in exceptional cases where no other sufficiently precise and clear descriptions are available for potential bidders.

Compatibility with legacy systems. A common mistake made by contracting authorities is failing to request compatibility with previously purchased proprietary solutions, often referred to as legacy systems. Lock-in is a well-documented issue with negative consequences for procuring organisations. To mitigate these issues, several countermeasures have been implemented, including the adoption of open source and open standards, as well as the creation of procurement guidelines.

Public procurements should, if possible, only include standards that are widely supported in the market and recognized by formal standardization organisations or technical specifications identified by the European Commission or national organisations.

Another effective measure to avoid lock-in is to incorporate exit costs into procurement agreements, ensuring a clear pathway for transitioning to alternative solutions in the future.

Open procurement procedure. Open procurement procedures are generally recommended for the procurement of goods and services. However, different procedures may be selected based on specific circumstances. For example, restricted procedures are often preferred when procuring services with unique features provided by a single operator, such as for military purposes, personal data protection, public connectivity services, or specialized activities in strategic locations. Restricted procedures are also useful when the number of potential vendors is too large to manage effectively. Conversely, negotiated procedures may be more appropriate when there are strict time constraints or when a supplier offers unique services. Lastly, opinions on competitive dialogue are mixed, particularly regarding its cost-effectiveness, with some highlighting its benefits while others raise concerns about potential drawbacks.

Make-or-buy. Cost considerations, quality control, supplier expertise, and the need for direct oversight are key factors influencing "make-or-buy" decisions. Similarly, these factors can serve as "motivational drivers" to encourage the adoption of "standards" that effectively reduce costs while ensuring a high level of quality.

5.5 CONCLUSIONS AND RECOMMENDATIONS FOR CANVAS UPDATE

Taking the above recommendations and improvements into account a final canvas update was made, as shown in Figure 11 below.

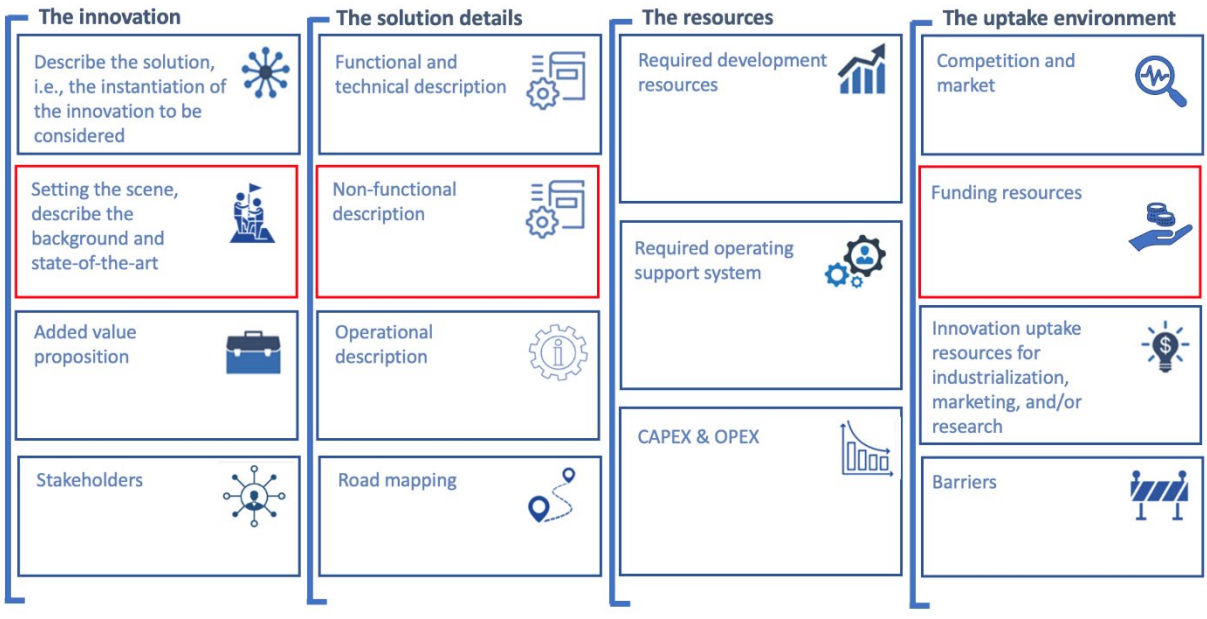

Figure 11. The updated Innovation Uptake Canvas.

The changes comprise three additional boxes in the canvas, containing the following:

- Setting the scene, describe the background and state-of-the-art:

The box shall describe the background of the innovation from the state-of-the-art, including prior research, technical background, standards, or technological baselines to support the innovation.

- Non-functional description:
  The box shall provide a high-level overview of the main extra-functional/quality properties of the innovation, explaining how well the functions are performed. For example, this concerns quality attributes like availability, reliability and performance. The standard ISO/IEC 25002:2024 describes quality models composed of software and system quality characteristics and sub-characteristics.
- Funding resources:
  This box shall describe the available or required funding resources for the innovation.

The procurement guidance should also be taken into account in the IUC boxes considering requirements stemming from organisational and legal aspects, as well as from the non-functional (quality) aspects. Examples could be GDPR, defining controls, best practices and measures, reliability, compliance to legacy, service agreements, licencing, etc.

Hence, we summarise key recommendations for procurement and these involve:

- **Market Consultation:** Engage with the market to find existing solutions and avoid unnecessary development.
- **Use Templates:** Utilize available templates for procurement documents to save time and ensure consistency.
- **Refine innovation descriptions**: Include state-of-the-art and consider EU initiatives to lay the foundation for the innovations.
- **Involve Stakeholders:** Include professionals to ensure technical accuracy and cover cybersecurity concerns.
- **Assess Vulnerabilities:** Regularly assess and test for vulnerabilities in procured products.
- **IPR Provisions:** Ensure intellectual property rights allow for reuse and accessibility of solutions.
- **Avoid reinventing the wheel**: Specify the new functionality and added value from the existing solutions and reuse as much as possible from previously proposed solutions or innovations.

The review carried out has led to improvements and update of the MCUIR for the EU-HYBNET. This advancement incorporates valuable lessons from strategy development methodologies, roadmaps creation, and innovation uptake strategies. The updated version of MCUIR is now ready for application in future projects and research. The enhancements to the innovation uptake canvas will serve as important lessons for both research and industry. The canvas remains a valid approach for capturing the innovation process, as do the innovation descriptions. We have proposed a mapping that requires further validation before being adopted by innovation producers/providers.

As a final note, the development of the updated Innovation Canvas is recommended to be used as a starting point in developing strategies for innovation uptake by the stakeholders. The descriptions can be further detailed as the different stages of the innovation development progresses and matures. The framework can be used in future projects adapted accordingly to their needs.

6. RELEVANCE AND UPTAKE

6.1 PROPOSED SOLUTIONS AND THE NIINISTÖ REPORT

We first note that in the preface of the so-called Niinistö Report [38] it is stated (Citations are indicates by … and the **boldface** in the cited text is done by us)

> … Evolving threats, such as the sabotage of critical infrastructure and cyberattacks, continue to bring private and public actors' security interests ever closer. The systematic sharing of information and experiences is crucial for further deepening trust between different actors to prepare for and address these threats together.

In chapter 3 of the report titled Ensuring speed of action with structures and procedures that are fit for purpose we find the following statements

> **… Data matters**
> … **Situational awareness is vital** to ensuring that decision-makers can **take informed decisions in a timely manner**. Here, there is still room to improve the sharing and fusion of relevant information streams …
>
> … Despite significant advances in terms of gathering and processing of information at the EU level, across numerous domains, there are still **deficiencies concerning the availability of data and information gaps** in others. In particular in some domains that are critical for preparedness, **governmental or private sector actors remain reluctant to share relevant information**, …
>
> … **Trust and mutual understanding** among the main crisis preparedness and response actors at the EU level and across Member States **should be continuously nurtured and reinforced** ...
>
> **… Coordination matters**
> … Multiple and multidimensional crises require **close coordination at the operational level**, for example to effectively deliver civil protection and humanitarian assistance where needed.
>
> … most fundamental coordination challenges during a multidimensional crisis of European scale: how to coordinate – and ultimately arbitrate – the effective use and distribution of scarce resources when their demand surges exponentially. Building in buffers, **resilient supply chains**, stocks and redundancies is one step …

In chapter 4 on Empowering citizens as the backbone of societal resilience and preparedness we find the following statements

> … Comprehensive preparedness must **put citizens at its core.** The EU and Member States can best protect citizens by **enhancing their resilience and agency**.
>
> … **enabling citizens** – in different capacities – **to play an active role** in ensuring crisis preparedness and first response.
>
> **… Media literacy**
> … **effective media and digital literacy will be essential** to upholding fundamental tenets, such as trust in institutions, fair elections, social cohesion, and national security.

[38] Safer Together. Strengthening Europe's Civilian and Military Preparedness and Readiness

> … to bolster citizens' ability to recognise authoritative sources of crisis response information and **to dismiss disinformation and Foreign Information Manipulation and Interference**.

In chapter 5 on Leveraging the full potential of public-private cooperation we find:

> … Private businesses and the public sector as preparedness partners
>
> … interdependencies between different sectors and across borders create the potential for severe knock-on effects in …
>
> **… Closing the gaps in the EU's resilience ecosystem**
> … Insufficient coordination and communication between public authorities and private entities: In particular, lacking channels for the timely, secure, and mutual exchange of information hinder effective crisis response and preparedness action. This includes the **exchange of sensitive information**, for instance the sharing of intelligence and early warnings by intelligence services and other public authorities, as well as the sharing of information on vulnerabilities, stocks, and production rates by private operators. An **insufficient capacity to share information** at the EU level in a secure and trusted manner undermines the ability of both public and private entities for effective risk management.

Here we see that our proposed solutions are aligned with the cited points from the report. In *Table 4. Solutions mapped on three main areas of applications and five end-user categories*. There we have information sharing, situational awareness and IMI (information Manipulation and Interference) as main areas of applications. We also have citizens, public admin and critical entities and infrastructures as targeted end-users which also are in line with the statements in the report. This shows that the proposed innovations are relevant with reference to the Niinistö Report.

6.2 THE CER DIRECTIVE

In the same way as for the Niinistö Report our work is in line with the CER (Critical Entities resilience) Directive[22] many of the proposed solutions and recommendations support CER measures required. In particular we note

> … Member States shall facilitate voluntary information sharing between critical entities in relation to matters covered by this Directive, in accordance with Union and national law on, in particular, classified and sensitive information, competition and protection of personal data.

6.3 COOPERATION WITH THE EEAS

Together with EEAS StratCom[39] a policy brief based on the proposed solution SARD: *Situational Awareness Regarding Disinformation* based on innovation *Debunking of fake news* was published. The policy brief was titled *Build Societal Resilience – Share IMI* Information.*

EEAS StratCom proposed an innovation *DDS-Alpha* on FIMI (Foreign Information Manipulation and Interference) on how to analyse counter hybrid threats in (dis)information domain. Based on this innovation the solution MIMI: A Market place for Information Manipulation and Interference information was produced and EU-HYBNET report on the subject was published.

[39] EEAS StratCom

The above-mentioned policy brief and report has been shared widely to EU-HYBNET Network members, consortium and to EU-HYBNET event participants. The policy brief was referenced in the *2022 Report on EEAS Activities to Counter FIMI*.

We also note that in the call for proposals - HORIZON-CL2-2023-DEMOCRACY-01 - the above-mentioned policy brief was referenced.

6.4 CONCLUSIONS

The sections above show that the solutions and recommendations proposed by Task 4.2 are well aligned with the Niinistö Report and contributes technological solutions in line with the CER directive. The cooperation with EEAS StratCom has been fruitful for both parties and contributed to making related IMI and FIMI activities very relevant.

7. LESSONS LEARNED

We have found that the framework methodology developed in the first project cycle with the roadmapping and the innovation uptake canvas still represents a valid procedure to base the Task 4.2 work on. The process of the review of the methodology evaluated whether the objectives and activities carried out were clearly defined, which they were found to be. However, some clarifications of who the end-users, recipients or practitioners are and who could benefit from the methodology were needed. Simplification of the methodology steps was also carried out and relevant input and desired output better depicted. Moreover, the review of the methodology verified that an alignment of the content in the innovation description with the required content in the uptake canvas would simplify the work to fill in the canvas. In particular the innovation descriptions should better cover the State-of-the-Art including EU initiatives related to the innovation's scope. Furthermore, more specificity is needed to distinguish new functionality from existing solutions.

A better project timeline would also have been helpful. The following timeline had allowed for a more structured and well-defined procedure to select innovations on which to base solutions. It would also allow for a better integration of tests, providing complementary standards considerations and experts' review:

1. WP3 proposes and evaluates innovations and relevant research activities and selects the innovations for which solutions with uptake and research strategies are to be developed.
2. Task 4.2 scopes the innovations into proposed solutions.
3. WP2 performs an assessment of the solutions in DTAG exercises as such training events and practical trials help assess a solutions fit-for-purpose rating.
4. Task 4.3 reviews the solutions from a standardization perspective.
5. Task 4.1 reviews the solutions from a procurement point of view.
6. Task 4.2 develops the uptake strategies.

When solutions have high TRLs, such as TRL 8 or 9, efforts should focus on developing proof-of-concept implementations for test-before-invest trials and market studies. Bringing innovations closer to the market at an early stage can significantly benefit innovators by enhancing competitiveness, creating niche opportunities, and improving innovation capability, outreach, and excellence.

To obtain reliable results in evaluating and synthesizing solutions, as well as in developing adoption strategies, the involvement of domain experts is crucial.

Overall, our experience suggests that engaging end-users and stakeholders earlier in the process leads to more refined innovations and effective adoption strategies.

To have a more efficient review and evaluation process it would today be possible to automate parts of the processes and leverage AI tools to pre-screen innovation descriptions for completeness and relevance.

8. SUMMARY OF CONTRIBUTIONS TO PROJECT OBJECTIVES AND KPI'S

The D4.4, D4.5, D4.6 and D4.7 deliverables contribute to some of the overall Project Objectives (OB) defined in the DoA. In Table 6, the most significant contributions related to the Project OBs and their relevant Key Performance Indicators (KPIs) are listed.

Table 6. 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. Targets: -At least 3 innovative solution possibilities are defined in relation to each of the four project core themes and fed into the EC procurement process	In total, 13 innovations/ solutions have been developed. Three innovations per core theme 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 Targets: -At least 5 suggestions are put forward yearly on new research and innovation possibilities and compiled into a final roadmap at project's end	More than 30 recommendations for actions, research and standardization have been presented. The solutions are mainly independent except for the CISAE upon which SARD and other sharing solutions could be built. This means that a roadmap for development of the solutions should have CISAE in an early stage while the other innovations can be developed in parallel.
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 recommen-ding solutions for European actors' gaps and needs	Monitor existing innovations addressing gaps and needs; incl. areas of knowledge/performance Target: -At least 4 reports every 18 months that address technological innovations that	Four reports on strategy for innovation uptake and research has been published (D4.4, D4.5, D4.6, D4.7).

		are able to fulfil European actors' gaps and needs	
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 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 all four project core themes. A comprehensive list of 9 recommendations on procurement/industrialization has been presented in Section 5.4 (based on D4.3)
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 13 innovations reviewed for uptake and industrialization, strategies have been proposed. Common aspects are noted and are part of the basis for generalized strategies/ recommendations.

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 success and proceedings of the project. In Table 7, the TASK 4.2 contribution to the three Lines of Action is provided.

Table 7. Task 4.2 contributions to Lines of Action

Lines of Action	TASK 4.2 contributions
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 to innovations that could fill in gaps and needs.	Based on its review of the proposed innovations Task 4.2 has developed 13 solutions covering generic components for information sharing, situational awareness and handling of IMI as well as important enablers like development work models and validation of AI-models State-of-the-Art information relevant for most of the innovations recommended for industrialization and uptake. A general overview per innovation is given in the corresponding Setting the scene sections.
Priorities as regards of increasing knowledge and performance requiring standardisation.	Based on its current and earlier work Task 4.2 proposes that: • A taxonomy and a coding scheme for hybrid threat related events are standardized to enable simple and efficient sharing of such information. • APIs/interfaces for AI-based tools used in geolocation and other verification-of-information-authenticity services are standardized. • 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. • A framework for citizens' event reporting to first-line responders, including formats and procedures for applications in mobile phone apps. • The CISAE framework is standardized by ETSI to enable broad adoption and industrialization of the solution(s).

10 CONCLUSIONS

10.1 SUMMARY

In this final project cycle, we have applied the Task 4.2 developed methodology (MCUIR) on one innovation representing the project core theme *Cyber and Future Technologies*. The innovation is about verifications and validation of AI-models and the solution is named *AI-model verification and Validation platform.* An innovation uptake canvas has been produced together with recommendations for the solution's uptake and needed initiation of related research and standardization.

The solution described in this deliverable and the twelve solutions proposed in the earlier project cycles have been reviewed with respect to coverage of the hybrid threat arena and relevance for increasing resilience against hybrid threats. We found that the recommended solutions would be important contributions in building a multi-levelled strategy against hybrid threats. By integrating technological innovation with structured governance and community engagement, the solutions collectively would contribute to a resilient ecosystem capable of anticipating, detecting, and mitigating diverse hybrid threats. Many of them act as enablers, supporting broader security efforts through AI-driven disinformation detection, media literacy training, and advanced data flow analysis. Information sharing and near real-time situational awareness are key. For information sharing and situational awareness, standardization of interfaces and protocols is a foundational requirement.

The analysis further revealed that hybrid threats evolve faster than regulatory frameworks, emphasizing the urgency of EU-wide standardization. AI and Big Data play essential roles in real-time threat analysis, media verification, and crisis response, while early end-user involvement ensures security tools remain practical and effective. Expanding media literacy education is critical for long-term resilience, alongside fostering cross-sector collaboration between governments, academia, and industry. Recommendations include promoting public-private partnerships, securing targeted funding, and addressing regulatory constraints to enhance trust and legal compliance.

The MCUIR review carried out led to suggested improvements and update of the methodology. The suggestions incorporate valuable lessons from strategy development methodologies, roadmaps creation, and innovation uptake strategies. An updated version of MCUIR is now available and could be applied in future projects and research. The enhancements to the innovation uptake canvas will serve as important lessons for both research and industry. The canvas approach remains valid for capturing the innovation process, as do the innovation descriptions.

Inn our review of our works relevance we found that the solutions and recommendations proposed by Task 4.2 are well aligned with the Niinistö Report and that they contribute technological solutions in line with the CER directive. The cooperation with EEAS StratCom has been fruitful for both parties and contributed to making related IMI and FIMI activities very relevant.

10.2 FUTURE WORK

For future work in the area finding and defining solutions that can be of service in detecting and mitigating hybrid threats and operations we propose

- Define new innovations by starting from Gaps and Needs and follow the Double Diamond steps.
- Use the updated MCUIR and align the ID with the IUC (or use the updated IUC as ID)

- To “sell” the solutions to practitioners and end-users, provide for developing POCs (Proof of Concept) and simulated environments.
- Build on existing standards or extend / develop new when required.

ANNEX I. GLOSSARY AND ACRONYMS

Table 8 Glossary and Acronyms

Term	Definition / Description
AI	Artificial Intelligence
AIMVVP	AI-Model Verification and Validation platform (a solution)
CAPEX	Capital Expenditure
CiReTo	Citizens Reporting Tool (a solution)
CISAE	Common Information Sharing and Analysis Environment (a solution)
CISE	Common Information Sharing Environment
CiToDeFaMe	Citizens Tools to Detect “Fake" Media (a solution)
CORE model	Comprehensive Resilience Ecosystem model
CTI	Cyber Threat Information
CRP	Citizen - Responder Platform (a solution)
DoA	Description of Action
DSA	Digital Service Act
DTAG	Disruptive Technology Assessment Game
EII	Excellence, Impact and Implementation. The method for assessment of innovations defined by WP3, see D3.1.
EACTDA	European Anti-Cybercrime Technology Development
EDMO	European Digital Media Observatory
EESCM	Enhanced and Extended Supply Chain Management (a solution)
ENISA	European Union Agency for Cybersecurity
EU	European Union
F)MI	Foreign Information Manipulation and Misinformation
GECHO	Gatekeeping ECHO Chambers (a solution)
ID	Innovation Description
IMI	Information Manipulation and Misinformation
IPR	Intellectual Property Right
IUC	Innovation Uptake Canvas
JP	Joint Procurement
KPI	Key Performance Index
LEA	Law Enforcement Agency
LMHTT	Local Media Hybrid Threat Tracker (a solution)
MCUIR	Methodology for Creation of innovation Uptake, Industrialization and Research strategies
MIMI	A Market place for IMI Information (a solution)
ML4S	Media Literacy for Students (a solution)
MS	Member States
OPEX	Operating Expenditure
PCP	Pre-Commercial Procurement
POC	Proof of Concept
PPI	Public Procurement of Innovation
SARD	Situational Awareness Regarding Disinformation (a solution)
SME	Small and Medium Enterprise
STARLIGHT	Starlight Disinformation-Misinformation Toolset (a solution)
STIX	Structured Threat Information Expression, a language and serialization format used to exchange cyber threat intelligence.

TAXII	Trusted Automated Exchange of Intelligence Information. An application protocol for exchanging CTI over HTTPS
WINS	What Information Needs to be Shared (a solution)

ANNEX II: THE METHODOLOGY FRAMEWORK

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

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

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

ANNEX II.1 ROADMAPPING

Roadmapping is the strategic process of determining the actions, steps, and resources needed to take the initiative from vision to reality. But as stated by ProductPlan[40] "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[41] 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[42] contain:

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

[40] Productplan, What is roadmapping. https://www.productplan.com/learn/roadmapping/
[41] Roadmunk, Why Roadmap, https://roadmunk.com/guides/roadmap-definition/.
[42] 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

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

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

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

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

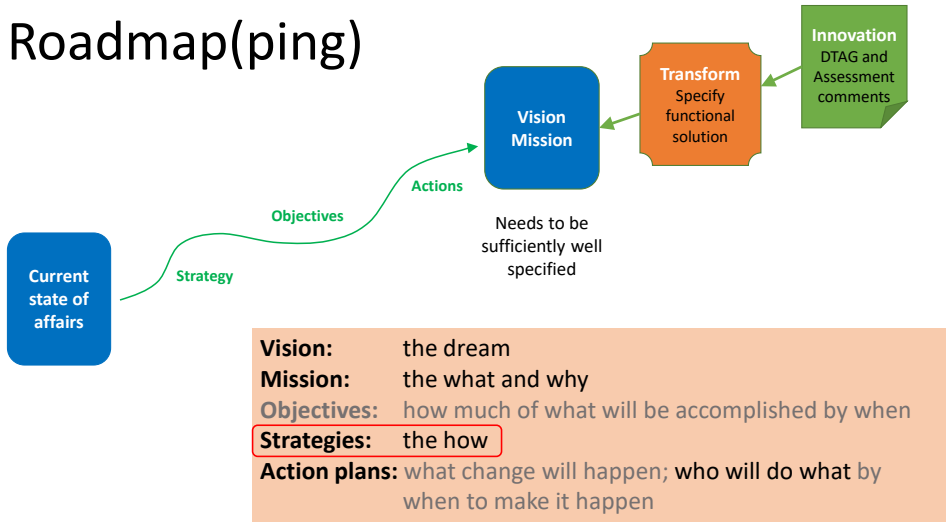

Figure 12. An illustration of the components in a roadmapping exercise of a selected innovation

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.

ANNEX II.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.

Figure 13. The innovation uptake canvas

ANNEX II: 2.1 THE FIRST COLUMN – THE INNOVATION

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

- **Added value proposition.**
  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.
- **Stakeholders and domains**
  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[43].
    - Target JRC domains; Is the solution domain specific or does it apply to a wider sector?

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

- Benefitting practitioners and end-users (NGO's, private citizens, private companies, media outlets, police, firefighting departments). Are the benefitting organisations aligned with respect to goals, objectives and support of the idea?

ANNEX II: 2.2 THE SECOND COLUMN - SOLUTION DETAILS

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

- **Operational description**
  This box shall provide a high-level overview of how the solution should be introduced for the intended users and integrated (if possible) in their operational environment.
  - Describe the main procedural and human/social aspects to be considered.
  - Describe the requirements for the integration in an organisation 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, organisational 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?

ANNEX II: 2.3 THE THIRD COLUMN – THE RESOURCES

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

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

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

ANNEX II: 2.4 THE FOURTH COLUMN – THE UPTAKE ENVIRONMENT

- **Competition and market**
  This box shall describe competing solutions, their maturity level, benefits and drawbacks. Verify the solution's advantages. Review the market situation (if one exists).
    - List the type of solutions that exist on the market and try to address the same need.
    - Why are these solutions not considered adequate? Is there a solution with a dominant "market" share? Is the "industry" characterized by intense competition?
    - Do other business opportunities exist for the solution?
    -
- **Funding and organisation of uptake and industrialization efforts**
  This box shall describe the preferred way to organise 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.

ANNEX III LIST OF PROJECT RECOMMENDATIONS

This annex lists the recommendations emanating from the strategies and roadmaps for the solutions in the four project cycles. The solutions are summarized in Section ZZZ and for their full descriptions we refer to deliverables D4.4, D4.5, D4.6 and Section WWW.

ANNEX III.1 FIRST PROJECT CYCLE 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.

ANNEX III.1.1 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.

ANNEX III.1.2 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 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. 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.

ANNEX III.1.3 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.

ANNEX III.1.4 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.

ANNEX III.1.5 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.

ANNEX III.1.6 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.

ANNEX III.1.7 UPDATES OF EXISTING EU INITIATIVES AND ACTIONS

Introduce CISAE as a solution in the European Programme for Critical Infrastructure Protection[44] (EPCIP), the Directive on European Critical Infrastructures (CER) and as a complement to the Critical Infrastructure Warning Information Network [45](CIWIN).

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[47], and the Action Plan against Disinformation[48]. Make it a tool which could be used the European Digital Media Observatory[49] (EDMO)in their work to understand and analyse disinformation and be a platform for cooperation. Introduce requirements in

[44] European Programme for Critical Infrastructure Protection
[45] Critical Infrastructure Warning Information Network
[46] Factsheet: Rapid Alert System
[47] EU Democracy Action Plan
[48] Action Plan against Disinformation
[49] European Digital Media Observatory

the Code of Practice on Disinformation[50] for support of tools in media consumption applications that check provenance and authenticity of media in general and images, audio and video in particular.

ANNEX III.1.8 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

ANNEX III.1.9 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[51] (C2PA) 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[52] (CAI), which focuses on systems to provide context and history for digital media, and Project Origin[53], a Microsoft- and BBC-led initiative that tackles disinformation in the digital news ecosystem.

ANNEX III.2 SECOND PROJECT CYCLE RECOMMENDATIONS

ANNEX III.2.1 UPTAKE OF REVIEWED INNOVATIONS

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

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

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

ANNEX III.2.2 PRIVATE SECTOR INVOLVEMENT

The solutions in this second project cycle as well as two of the innovations in the first project cycle rely heavily on access to different types of information. To get access to as much information as possible,

[50] The 2022 Code of Practice on Disinformation is now integrated in the Code of Conduct on Disinformation.
[51] The Coalition for Content Provenance and Authenticity
[52] Content Authenticity Initiative
[53] Project Origin

the private sector should participate. The recommendation from the first project cycle is thus repeated here.

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

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

ANNEX III.2.3 RESEARCH AND DEVELOPMENT OF SUPPORTING TOOLS FOR WINS

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

ANNEX III.2.4 CISAE STANDARDIZATION

This recommendation is a repetition of a recommendation from the first project cycle. We include it once again as it a proposed basis for the WINS solution. The recommendation is to develop and standardize a framework for the implementation of information sharing and analysis environments (CISAEs). Build the information sharing functionality on the EMSA CISE[54], 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. For further details se D4.4 [55]

ANNEX III.2.5 RESEARCH AND DEVELOPMENT OF SUPPORTING TOOLS FOR EESCM

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

ANNEX III.2.6 EXTENSION OF DDS-ALPHA FUNCTIONALITY FOR SUPPORT OF MIMI

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

ANNEX III.2.7 DEVELOP A SHARING AND ANALYSIS PLATFORM FOR GECHO

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

[54] Common Information Sharing Environment (CISE), http://www.emsa.europa.eu/cise.html
[55] EU-HYBNET D4.4 "*1st Innovation uptake, industrialisation and research strategy*" in CORDIS https://cordis.europa.eu/project/id/883054/results

on the CISAE principles proposed to be standardized in the first project cycle. An alternative route would be to use an extended DDS-alpha platform.

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

ANNEX III.2.8 ESTABLISH RESEARCH NETWORK WITH FOCUS ON GECHO NEEDS

The ultimate objective of GECHO is to develop easy to follow validated frameworks, methods and tools for creation of practical means for timely and efficient prevention of online recruitment of young people into groups promoting violent extremisms and terrorism. To make it become the powerful tool it should be, there is a need for supporting research in several areas related to the factors influencing the online radicalisation process:

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

ANNEX III:3 PROJECT CYCLE THREE RECOMMENDATIONS

ANNEX III:3.1 UPTAKE OF REVIEWED INNOVATIONS

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

1. CRP
2. CiReTo
3. LMHTT
4. STARLIGHT

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

ANNEX III:3.2 TAXONOMY AND CODING OF HYBRID THREAT EVENTS

To enable automatic handling of and sending/receiving information about events that (may) relate to hybrid threats it is necessary/highly recommended to standardize:

1. A **taxonomy** for reporting of hybrid threat related events.
2. **Encoding formats** for the events defined in the taxonomy as extensions to STIX. STIX, Structured Threat Information eXpression is a standard language that to express and share threat intelligence information in a readable and consistent format.
3. A **preferred transport protocol** for encoded hybrid threat encoded events, based on TAXII. TAXII defines a protocol for exchanging data, including message formats, communication protocols, and security requirements.

The standards proposed would be beneficial for the proposed solutions in this deliverable as well as for the implementation of earlier proposals and other solutions in the hybrid threat area.

ANNEX III:3.3 PROCUREMENT RECOMMENDATIONS

Procurement of new and advances hybrid threat solutions is often cumbersome as the required funding may be hard to get. We thus recommend the following actions to minimize barriers in this respect:

1. Promote the procurement recommendations in D4.3, 3rd Report on the Procurement Environment[2]. See sections Recommendations for procurement and Specific recommendations for EU-HYBNET uptake strategy.
2. Promote the use of national and EU procurement support for funding of uptake and industrialization of hybrid threat related solutions, services and products. An extensive overview of available funding instruments can be found in D4.3 section Procurement Overview.

ANNEX III:3.4 RESEARCH AND DEVELOPMENT OF SUPPORTING TOOLS FOR CRP

We recommend that an R&D action is initiated to define standards for interfacing existing tools that would be useful in the CRP context and also develop missing tools.

1. Develop AI-supported tools for verification of authenticity. Design standardized APIs/ interfaces for the tools. Examples of needed tools are:
    a. Geolocation of events – pictures and videos
    b. Verification of time stamps
    c. AI-EDEC services
    d. Verified integrity of reporting application
    e. Detect indications of ongoing hybrid threat attacks

    We note that some of the tools developed in the Starlight project would have required functionality. If possible, these tools should be tailored for use in CRP and be equipped with the standardized interfaces proposed.
2. Standardise and define principles for how AI analysis results can be shared to the first and second responders, and in case of indicated false, fake alarms as part of a possible hybrid threats campaign should be shared with relevant intelligence services. The work should cover the needs for situational awareness in EU crises response and for monitoring and analysis of disinformation from large amount of data.
3. Initiate an innovation action to implement a proof of concept and use it to evaluate/demonstrate the solutions benefits for first- and second-line responders.

ANNEX III:3.5 RESEARCH AND DEVELOPMENT OF SUPPORTING TOOLS FOR CIRETO

We recommend that an R&D action is initiated to

1. Develop and standardize an architecture for how current and future tools for citizens reporting of emergencies and hybrid threat related events can be integrated in an efficient central service.
2. Develop guidelines on how to ensure a user-centric design, providing multi-platform accessibility of a citizens mobile reporting app and at the same time ensure that security and adequate privacy can be maintained.

3. Study how users' (citizens') consent for the use of a reporting app can be obtained and registered.
4. Use standardized taxonomy, encoding formats and transport protocols defined.
5. Initiate an innovation action to implement a proof of concept for evaluation/demonstration of the CiReTo concept.
6. Foster community engagement and forge partnerships and collaborations with law enforcement agencies, advocacy groups, and other stakeholders to enhance the effectiveness of incident reporting, response and support services.

ANNEX III:3.6 RESEARCH AND DEVELOPMENT OF SUPPORTING TOOLS FOR LMHTT

We recommend the following too ensure the implementation of LMHTT:

1. Initiate a research and innovation action to investigate the situation of local and regional media in the MSs. Involve end-users (security practitioners) to understand their exact needs.
2. Design a comprehensive LMHTT diagnostic tool by defining standardized procedures for data collection and reporting in a questionnaire.
3. Develop comprehensive data analytics tools and an interactive dashboard for data visualisation.
4. Delegate the maintenance of the LMHTT tools to a competent body, possibly ENISA.

ANNEX III:3.7 STARLIGHT DEVELOPMENT MODEL

It is noted that using agile co-development is a rather novel approach for the security sector, especially LEA's, as they traditionally tend to be part in a rather closed ecosystem. Uptake of innovative solutions and co-development is not a common practice in those institutions. There are other possibilities as well, like pre-commercial procurement and concept of "test before invest" is also gaining popularity in many sectors. Early involvement and co-development are essential for the uptake process and is at heart of those practices. To initiate and increase use of co-development of tools in the field of hybrid threats we recommend:

1. Promote use of an agile co-development methodology as demonstrated in the STARLIGHT project. Development of solutions together with end-users is considered a good practice, facilitating end-users' interest and involvement.

ANNEX III:3.8 STARLIGHT TOOLS

To increase the use of the developed Starlight tools we recommend that:

1. LEA's, also outside of the Starlight project, should take part in the Starlight ToolFest events and get acquainted with the tools and get access to the development information[56].
2. The possibility to widen the availability of the tools developed should be reviewed after the project has been ended. The tools obviously are relevant and interesting for different stakeholders in the (F)IMI and hybrid threat related areas.

[56] For access to development information contact the project directly. After project has been finished, some tools will be made available via different platforms (e.g.: EUROPOL, EACTDA or others.)

ANNEX III:3.9 CISAE, A COMMON INFORMATION SHARING AND ANALYSIS ENVIRONMENT

This recommendation is a repetition of a recommendation in D4.4, the first report on strategy for innovation uptake, industrialization and research. It is repeated as it has become clear in our work that the possibility for early detection of hybrid threats often relies on the extensive sharing of seemingly unrelated events. CISAE was developed in the context of sharing evets for CIP but sharing is key also for e.g., the successful use of the solutions CRP and CiReTo in this document as well many others. The key points in the recommendation are:

1. Develop a framework for the implementation of information sharing and analysis environments (CISAEs). Build the information sharing functionality on the EMSA CISE[57], 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.).
2. 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. 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

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

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.

ANNEX III.4 PROJECT CYCLE FOUR RECOMMENDATIONS

See section 3.4 Recommendations in this deliverable, D4.7.