EU-HYBNET

SECOND REPORT ON STANDARDISATION RECOMMENDATIONS

DELIVERABLE 4.9

Lead Author: PPHS

Contributors: KEMEA, L3CE, Laurea, RISE

Deliverable classification: Public (PU)

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

D4.9 SECOND REPORT ON STANDARDIZATION RECOMMENDATIONS

Deliverable number :	D4.9	
Version:	V1.0	
Delivery date:	12/06/2023	
Dissemination level:	Public (PU)	
Classification level:	Public	
Status:	Ready	
Nature:	Report	
Main authors:	Małgorzata Wolbach, Magda Okuniewska, Rashel Talukder	PPHS
Contributors:	Athanasios Kosmopoulos Edmundas Piesarskas Päivi Mattila Rolf Blom	KEMEA L3CE Laurea RISE

DOCUMENT CONTROL

Version	Date	Authors	Changes
0.1	24.04.2023	Małgorzata Wolbach Magda Okuniewska / PPHS	First draft
0.2	24.04.2023	Rashel Talukder / PPHS	Review
0.3	27.04.2023	Rolf Blom / RISE	Review
0.4	28.04.2023	Päivi Mattila / LAUREA	Review
0.5	22-29.05.2023	Vanessa Papakosta / KEMEA Edmundas Piesarskas / L3CE Małgorzata Wolbach Magda Okuniewska Rashel Talukder / PPHS	Additional input from KEMEA, L3CE, PPHS based on reviewers comments
0.6	07.06.2023	Päivi Mattila/ LAUREA	Review and text editing
0.7	12.06.2023	Małgorzata Wolbach Magda Okuniewska Rashel Talukder /PPHS	Final review
1.0	12.06.2023	Päivi Mattila / LAUREA	Final review and submission of the document to the EC

DISCLAIMER

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

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

TABLE OF CONTENTS

1. INTRODUCTION

1.1 OVERVIEW

The main goal of task (T) 4.3 within Work Package (WP) 4 “Recommendations for Innovation Uptake and Standardization” is to map the current status and identify needs and possibilities for standardisation in the context of innovations that are seen most promising to fulfil the practitioners’ gaps and needs to counter hybrid threats – as it is described in “Empowering a Pan-European Network to Counter Hybrid Threats” (EU-HYBNET) Grant Agreement.

The main objective of this deliverable is presenting how T4.3 partners have mapped the current status and developed recommendations in the area of standardisation, legal harmonisation and best practices[1], with reference to:

a) gaps and needs identified in Work Package 2 (Definition of Needs and Gaps of Practitioners’ against Hybrid Threats) especially in “Deeper Analysis, delivery of short list of gaps and needs” (Deliverable 2.10);
b) the most promising innovations identified in the Work Package 3 (Surveys to Technology, Research and Innovations) especially in “First Mid-Term Report on Improvement and Innovations (Deliverable 3.4);
c) selected feasible innovation areas and projects that counter hybrid threats and foster hybrid threat situational awareness described in Work Package 4 (Recommendations for Innovations Uptake and Standardization) especially in “Second Innovation Uptake, Industrialisation and Research Strategy” (Deliverable 4.5).

Based on the above outlines, task 4.3 main partners (PPHS, KEMEA and L3CE) started to work on the reports which are presented in this document.

The figure below shows where Work Package 4 is located on the EU-HYBNET structure of work packages and how it is related with other packages.

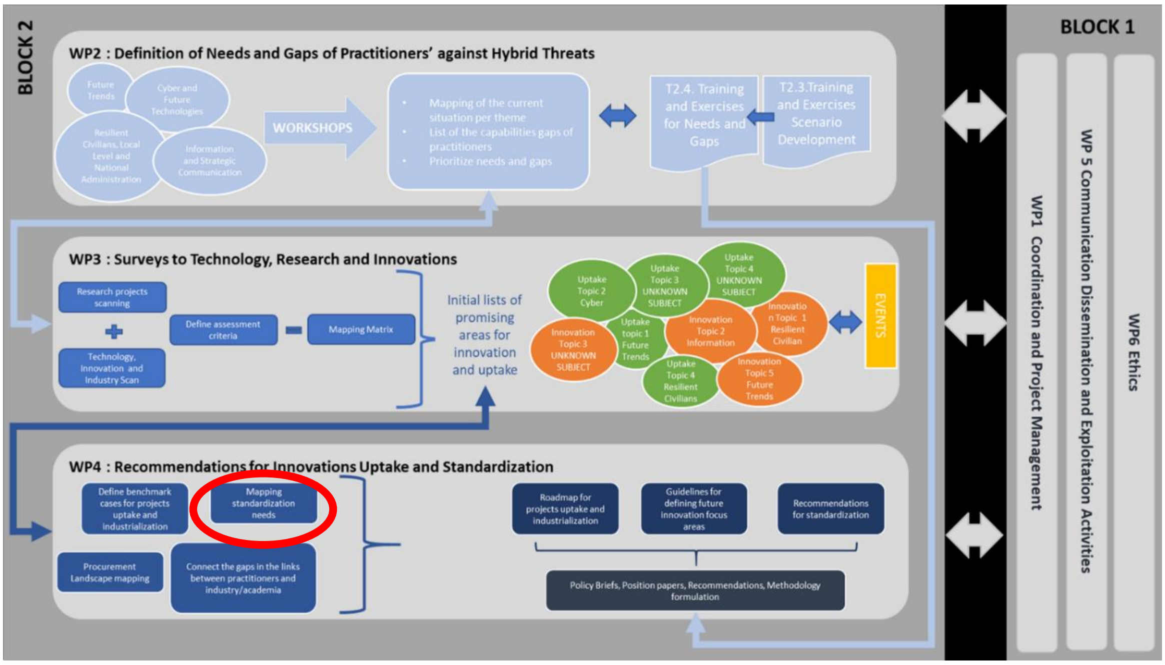
BLOCK 2
WP2 : Definition of Needs and Gaps of Practitioners’ against Hybrid Threats
Future Trends
Cyber and Future Technologies
Resilient Civilians, Local Level and National Administration
Information and Strategic Communication
WORKSHOPS
Mapping of the current situation per theme
List of the capabilities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

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

[1] It is important to underline that official ISO or CEN standards very often are being developed based on best practices.

1.2 METHODOLOGY AND MAIN OBJECTIVES OF TASK 4.3

The main objective of Task 4.3 is the description of the current state of play within the selected areas. The selection of areas to focus on was preceded by a thorough analysis done by Task 4.3 partners of the outcomes of Work Package 2, Work Package 3 and Work Package 4 with major emphasis on:

- Deliverable 4.5 (Second Innovation Uptake, Industrialisation and Research Strategy)
- Deliverable 3.4 (First Mid-Term Report on Improvement and Innovations).

In Deliverable 4.5 four innovations were selected but Polish Platform for Homeland Security (Task 4.3 leader) decided to focus on six innovations which were considered initially to be analysed in Task 4.2. Based on those findings, six areas were selected and the work was distributed among partners:

1. DDS-alpha (Core theme: Information and Strategic Communication) – KEMEA;
2. Multi-stage supply chain disruption mitigation strategies and Digital Twins for Supply Chain Resilience (Core theme: Future Trends of Hybrid Threats) - L3CE;
3. Detection of Disinformation Delivery Proxy Actors (Core theme: Resilient Civilians, Local Level and National Administration) - Polish Platform for Homeland Security;
4. Development of Real-time Rapid Alert System on Disinformation (Core theme: Resilient Civilians, Local Level and National Administration) - Polish Platform for Homeland Security;
5. Identify and safeguarding vulnerable individuals (Core theme: Information and Strategic Communication) - Polish Platform for Homeland Security;
6. What Information Needs to be Shared between CI entities to detect hybrid threats (Core theme: Resilient Civilians, Local Level and National Administration) - Polish Platform for Homeland Security.

During the work in Task 4.2 partners found that no innovation related to core theme Cyber and Future Technology was scored high enough to be suitable for review and hence the area is also omitted in Task 4.3.

Within the aforementioned areas, each partner provided a report which consists of:

- the description of the current state,
- initiatives and documents supported by the relevant links,
- recommendations.

Moreover, within innovations presented in four described areas:

1. DDS-alpha (KEMEA)
2. Multi-stage supply chain disruption mitigation strategies and Digital Twins for Supply Chain Resilience (L3CE)
3. Identify and safeguarding vulnerable individuals (Polish Platform for Homeland Security)
4. Impact and Risk assessment of critical infrastructures in a complex interdependent scenario (Polish Platform for Homeland Security).

Within the above mentioned areas, recommendations presented in Deliverable 4.5 are also included.

Recommendations provided in the reports from Section 2 of this deliverable are accompanied by a type of recommendation (legal, standard, best practice) and a relevant institution which was identified as the primary institution which should receive a given recommendation for their information and possible future actions regarding this area. Additionally, each recommendation is marked with information whether it is most feasible for implementation in the short, medium or long term.

Findings described in this document are a result of ongoing analysis including desktop research, discussion with experts, consultations with consortium partners and network partners within EU-HYBNET project but under no circumstances should be treated as a complete, finished and exhaustive work. The world of hybrid threats, gaps and needs accompanying them is the environment that is constantly changing. Certain features described in the reports were accurate and up-to-date at the time of reports creation.

In each of the reports described in this deliverable, more general or more specific recommendations (in the area of standardisation, legal harmonisation and best practices) were developed for actions to be taken at the level of the European Union and Member States. The purpose of developing the recommendations is to indicate particularly important aspects in each of the topics, which is proceeded by the description of the current state of play within a given area.
One of the points to be carried out within Task 4.3 is the dissemination of the recommendations to relevant entities and experts that a given recommendation refers to directly or with the idea that they might be interested with the solutions proposed in the report.
Each recommendation was addressed to one or more of the institutions operating at the EU level – mostly referring to public institutions, private entities or civil society organisations.
Additionally, the reports will be sent to all EU-HYBNET consortium and network members to see if they would like to contribute to any of the state-of-the-art points or recommendations.
The reports will be sent to the identified institutions by Laurea University, coordinator of the
EU-HYBNET project, and by the Polish Platform for Homeland Security - the leader of Task 4.3 Recommendations for Standardization. Both institutions will monitor feedback from institutions that have received reports with recommendations. Feedback will be consulted among the partners of Task 4.3 and its content will be taken into account, as far as possible, in further project work.

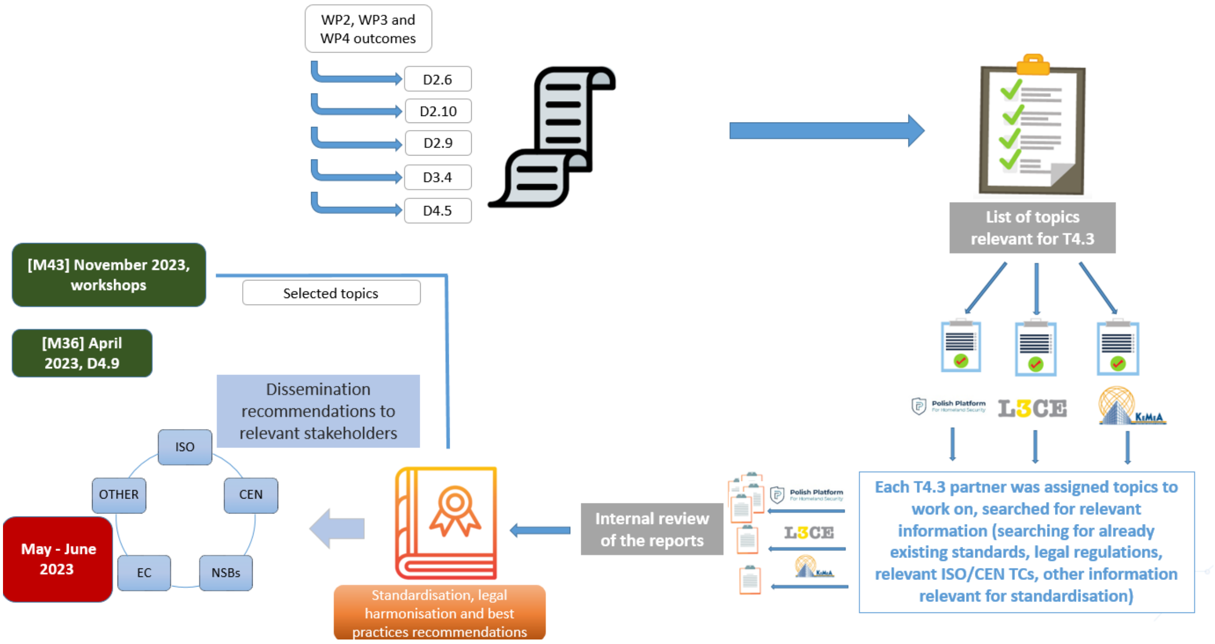
WP2, WP3 and WP4 outcomes
D2.6
D2.10
D2.9
D3.4
D4.5
List of topics relevant for T4.3
Polish Platform for Homeland Security
L3CE
KiMiA
Each T4.3 partner was assigned topics to work on, searched for relevant information (searching for already existing standards, legal regulations, relevant ISO/CEN TCs, other information relevant for standardisation)
Internal review of the reports
Standardisation, legal harmonisation and best practices recommendations
Dissemination recommendations to relevant stakeholders
Selected topics
[M43] November 2023, workshops
[M36] April 2023, D4.9
May - June 2023
ISO
CEN
NSBs
EC
OTHER

Figure 2. EU-HYBNET workflow within Task 4.3 (Cycle 2)

1.3 STRUCTURE OF THE DELIVERABLE

This document includes the following sections:

- Section 1: In this section an overview together with methodology is presented.
- Section 2: In this section all the reports from 6 main areas are presented (state of the art, most important documents and recommendations).

  Section 2 contains following subsections:
  - Description of the Innovation - taken from Deliverable 3.4;
  - State of play related to this specific innovation accompanied by relevant links with the description of state-of-the-art;
  - Recommendations – in the first place, recommendations presented in Deliverable 4.5 (in four out of six innovations) are listed and they are followed by additional recommendations proposed by partners within Task 4.3 along with an indication of type of recommendation (legal/standardisation/best practice) and the most probable term for its implementation (short/medium/long). Each recommendation provides relevant institutions which should receive a given recommendation.

- Section 3: In this section it is explained how this deliverable contributes to three lines of actions.
- Section 4: In this section summary and future work are presented.

2. REPORTS

2.1 DDS-ALPHA

Description of the Innovation
DDS-alpha is the Disinformation Data Space, a common and modular framework and methodology for collecting systematic evidence on disinformation and foreign interference as proposed by the European Democracy Action Plan. We introduce an inclusive set of open tools, frameworks and standards, adapted from the cybersecurity sector and best-case practices on information manipulation and interference (IMI) analysis to provide the most comprehensive database on informational threats. DDS-alpha allows for all stakeholders with information on IMI activities in government, international organisations, civil society, the private sector and academia to pool, extract and recombine those insights to enable a wide range of countermeasures and products, depending on the stakeholders' needs and capabilities. It will also offer new insights on the threat, enabling new and faster means to achieve situational awareness or build new products.

State of play	Relevant links
Foreign Information Manipulation and Interference – also often labelled as "disinformation" – is a growing political and security challenge for the European Union and has been recognised as such in many high level policy documents, such as the Action Plan against Disinformation (2018), the European Democracy Action Plan (2020), the European Strategic Compass (2022), and several Council Conclusions. Given the foreign and security policy component, the High Representative, supported by the European External Action Service (EEAS), has a leading role in addressing the issue. FIMI is a pattern of behaviour that threatens or has the potential to negatively impact values, procedures and political processes. Such activity is manipulative in character, conducted in an intentional and coordinated manner. Actors of such activity can be state or non-state actors, including their proxies inside and outside of their own territory. Foreign actors trying to manipulate and interfere with our information environment use a variety of constantly evolving Tactics, Techniques, and Procedures (TTPs), often in combination with cyber security and hybrid threats. For example, cyber-attacks can be among other things used to obtain sensitive documents, which can then be leaked selectively at politically opportune moments to influence the political agenda, sow distrust, or drown out unwanted political debates. Analysis of foreign information manipulation and interference (FIMI), including disinformation has been conducted by individuals, researchers, civil society organizations and governments. More recently, social media platforms and online service providers have had to step up their work to protect their platforms from such manipulation. The challenge is global, complex and ever evolving. To protect universal values, democracy,	https://www.eca.europa.eu/lists/ecadocuments/ap20_04/ap_disinformation_en.pdf https://ec.europa.eu/info/strategy/priorities-2019-2024/new-push-european-democracy/european-democracy-action-plan_en https://eeas.europa.eu/headquarters/headquarters-homepage_en/106337/A%20Strategic%20Compass%20for%20the%20EU

freedoms and societies, a diverse range of actors has emerged who try to detect, understand and respond – the defender community. Strategic and coordinated use of FIMI in Russia's war of aggression against Ukraine recently focused the attention of the defender community, and saw an unprecedented effort to use open-source intelligence to expose Russia's efforts to manipulate global discourse and opinion. It has also underlined how important cooperation between these stakeholders is; a comprehensive, timely and shared understanding of the threat can lead to effective action denying FIMI its intended effect. This work to collect evidence, to understand the mechanics behind FIMI and share insights forms the basis for effective and appropriate responses taken by every FIMI defender in civil society, private industry and governments. The whole-of-society approach is a key element in the EEAS' work to prevent, deter and respond to FIMI. Therefore, the development of best practices is conceiving as a community-driven process; EEAS offers conceptual perspective and analytical framework, as a (possible) starting point for a constructive conversation within the defender community. The EEAS' goal is to facilitate and contribute to the creation of an open source, decentralised and interoperable framework that increases the efficiency of sharing threat insights between the different stakeholders involved in FIMI analysis and disruption. Intentional attempts to manipulate the information environment and public discourse by foreign actors is by no means a new phenomenon. However, activity which has previously been described as "propaganda" and more recently as "disinformation" has received a considerable new impetus by technological advancements and the propagation of the internet, in particular social media and private messenger services. With this development, new ways of manipulation have become available to malicious actors. In the last years, the term "disinformation", intended as the intentional spread of false and/or misleading information for a specific purpose, has become well-known and broadly used. However, this definition of disinformation captures only part of the problem: the manipulation of the content that is being pushed to distort facts and reality, to foster fear and hatred and to sow division in societies. Other terms have also been developed, such as "computational propaganda", "coordinated inauthentic behaviour" or "information pollution", to name just a few. These either incorporate new aspects in addition to disinformation intended as above or they depict activities that go beyond its focus on content.	https://euvsdisinfo.eu/ https://www.enisa.europa.eu/publications/foreign-information-manipulation-interference-fimi-and-cybersecurity-threat-landscape

Recommendation: Legal/Standardisation/Best Practices	Explanation on recommendation	Relevant Institution
Recommendations proposed within T4.2 (D4.5 Second Innovation uptake, Industrialisation and Research Strategy)		
Best Practices (medium term)	A recommended solution in the context of DDS-Alpha is called MIMI – a Marketplace for IMI information. The innovation DDS-alpha (the Disinformation Data Space – alpha) it is proposed to transform into a solution focusing on how to build a market and a Market place for IMI Information (MIMI). A secure and trusted marketplace for IMII sharing which is embraced by IMI data providers, analysts, and consumers. Aiming to build a European community of IMI data providers, analysts and consumers which embrace the idea of a market based IMII sharing solution. It is necessary to define and agree on the business model, as well as define and agree on functional requirements on the sharing platform for a secure and controlled information exchange supporting the business model. It is recommended to develop a strong and convincing storyline proving the benefits of a general IMI exchange which takes all existing barriers into account. Additionally, after studying existing business models used by stakeholders for existing IMI exchange solutions, it is necessary to synthesize a business model acceptable for all which would stimulate current stakeholders to exchange IMI information. Another aim is to design a service platform on top of DDS-alpha including required DDS-alpha extensions required for charging and service control. The solution should support exchange of IMI information which is required by EU and national regulations. It has been recognized that one barrier is the problem of having access to all required information when aiming for exact and detailed real-time data and situational awareness covering all aspects of IMI activities and campaigns. With the proposed MIMI solution, the barrier would be reduced/eliminated as there would be a direct business value in sharing.	**EEAS** **ENISA** **EU INTCEN**

	Increased sharing of observations and IMII base as well analysed data would improve situational awareness in terms of quality and timeliness and improve the possibilities for speedy mitigating actions and interventions. MIMI will serve the governmental and security sectors, which require in-time and complete information to enable fast reaction. Private sector companies (particularly online platforms) may benefit from a systematic inflow of threats observed and flagged to them for interventions. A market-based solution like MIMI, with a mixture and private companies, organizations and government institutions at different levels as stakeholders, would most likely develop into an efficient market economy solution and thus be driving force behind increased sharing of IMII. The alternative is to regulate sharing, which will remove many incentives as it will mainly be a cost driver. For the establishment of MIMI there is a need to establish an organization which drives the building a European community of interested partners. This could be organized as a time limited project. The project should: • Develop a strong and convincing storyline showing the benefits of using MIMI and elect evangelists to convince stakeholders of the value in using MIMI. • Liaise with the DDS-alpha community/interest group to prepare for future joint developments. • Define and propose a suitable business model. • Define the requirements for the service platform on DDS-alpha, including required DDS-alpha extensions for charging and service control. The solution should support exchange of IMI information which is required by EU and national regulations. It must contain functionality for – Secure and controlled information exchange – Interfaces for control of service level agreements between users and providers • Implement and verify required functional extensions of DDS-alpha. Publish extensions as open source.	

	• Set up a MIMI interest group which can maintain and extend MIMI. • Transfer maintenance operations of the service platform to the organization handling DDS-alpha. When MIMI has been established as a working solution, the required maintenance of the idea would be handled by the interest group.	
Additional recommendations within T4.3		
Standardisation (medium term)	There is a need for implementing a Standard regarding the exchange of Data between the stakeholders The main standards in use are STIX, a language and serialization format for exchange of Cyber Threat Information (CTI) and TAXII, a CTI data exchange protocol. CTI documentation is here. Relative to the DDS-Alpha Innovation we could examine the applicability of already existing standards as per ISO 20614:2017 (Information and documentation — Data exchange protocol for interoperability and preservation), CEN/TS 16157-10:2022 (DATEX II data exchange specifications for traffic management and information|||), where we may observe analogies with the DDS-Alpha operational needs and finally an interesting analysis EU-SysFlex (PROPOSAL FOR DATA EXCHANGE STANDARDS AND PROTOCOLS) conducted in the context of Horizon 2020 (https://eu-sysflex.com/wp-content/uploads/2021/05/Deliverable-5.5-report-FINAL-2021.04.29.pdf) where interesting conclusions are illustrated in section 5.3 regarding Data exchange standards in General.	**ENISA**

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

Description of the Innovation
The COVID pandemic followed by the Russian aggression on Ukraine brought new challenges for various EU sectors. Disruptions in supply chains adversely affected the safe, secure and smooth operations of EU industries and EU society. The study by Chen et al (2022)[2] on a supply chain disruption recovery problem in the context of Covid-19 pandemic proposed a mixed-integer linear programming (MILP) model based on emergency procurement and product design change strategies considering the product life cycle. The implementation of the idea is meant to support the manufacturers in establishing an optimal recovery strategy whenever the supply chain system experiences supply disruptions, which is especially relevant in times of war or considering hybrid threats. The mitigation of supply chain disruptions can be done with visibility, analysis, and planning. Companies employ specific tools that allow a new supply chain modelling – the digital supply chain network (DSN). These new tools can account for problems that can affect a whole supply chain, such as the ripple effect of an exceptional disruption. A digital twin represents the current state of a supply chain, with the actual transportation, inventory, demand, and capacity data. Then, simulation in the digital twin can help show disruption propagation and quantify its impact. In addition, simulation enables efficient recovery policy testing and the adaptation of contingency plans according to the situation. Stress testing a supply chain with "what if" scenarios can reinforce any mitigation strategy and strengthen the resiliency of a critical entity". Such methodologies and tools allow to build more resilient supply management, but there are still questions to be addressed.

State of play	Relevant links
Numerous factors have shaped the environment of the international trade, technological advancement and geopolitical balance. The support of European industry is expressed in the new Global Connectivity Strategy aiming to build sustainable and high quality digital, climate, energy and transport infrastructures and strengthen health, education and research systems across the world, taking into account their needs and the EU's own interests. The approach of increasing resilience through good governance should also be considered in the effort to maintain the competitiveness of European companies. The European Label of Governance Excellence (ELoGE) has already	Global Gateway: up to €300 billion for the European Union's strategy to boost sustainable links around the world' The European Label of Governance Excellence (ELoGE),

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

succeeded in promoting the 12 Principles of Good Democratic Governance, while the Centre of Expertise for Good Governance is supporting the implementation of ELoGE by providing guidance, advice and training. Disruptions in supply chain were one of the results of fluctuating international environment, pandemic and war. The good example of this is recent global chips shortage. It was followed by the European Chips Act, adopted by the Commission on 8 February 2022, that seeks to strengthen the semiconductor ecosystem and develop a resilient supply chain, while setting measures to prepare, anticipate and respond to future supply chain disruptions. There are also numerous other examples of supply chain disruptions with significant impacts for certain sectors. Consolidated efforts to stabilize certain sectors or ecosystems are very helpful, but it will not be expected to cover all aspects of industry with similar initiatives. Significant efforts to cope with supply management issues is made by companies. They employ sophisticated tools to analyse, optimise, build resilience in supply chain management. Currently there are variety of solutions available in the market. A short illustrative list of such tools includes *anyLogistix* (previously proposed in the EU-HYBNET project deliverable D3.4 section 1.1.2), *Shippabo, Magaya Supply Chain, FreightPOP, SAP Supply Chain Management,* and more specialized packages such as *Precoro,* and *Lagiwa WMS*. Differing in their functionalities, these nevertheless allow for the digitization of the procurement process, vendor and supply management, asset and warehouse management, optimization, maximizing productivity, and alternative supply chain modelling capabilities. **Supply chain is** in the scope of current standards. ISO family includes ISO 9001 focusing on the quality of supply chain, ISO 26000 and ISO 20400:2017 focusing on sustainability. ISO 2800 is specifically designed for supply chain security management, but the scope remains on transportation of products. The same can be observed in other recommendations or standards related to supply chain management, provided by Association for Supply Chain Management (ASCM), American National Standards Institute (ANSI). The European Committee for Standardization (CEN) and the European Committee for Electronical Standardization (CENELEC) are developing sectorial standards, that in some cases include supply chain aspects. All the above mentioned initiatives are considering supply chain from the traditional point of view, focusing on goods and transportation.	European Chips Act, Shaping Europe’s Digital Future, European Commission www.anylogistix.com/business-challenges/supply-chain-risk-assesment/ www.shippabo.com www.magaya.com www.freightpop.com www.sap.com/products/scm.html https://precoro.com/ www.logiwa.com ISO - ISO 9001 - What does it mean in the supply chain? ISO 20400:2017 - Sustainable procurement — Guidance

<table>
<tr><td colspan="2">However, challenges remain. For example, understanding and defining the relevant scope of supply chain management in the context of hybrid threats. The current tools are mainly focused on goods but hardly include services. In addition, these lack functionalities that could deal with geopolitical risk, impact assessment and minimization, cascading effects, including recovery planning features, or other threats of a hybrid nature. Current instruments have been developed on a traditional understanding of the supply chain, while the proposed solution is focused on a much wider concept of supply chains and not on expedient optimization procedures.
The EESCM proposes to address these shortcomings.</td><td>ISO 28000 - Supply Chain Security Management | BSI (bsigroup.com)
SCOR Digital Standard | ASCM
SCRM (asisonline.org)</td></tr>
<tr><td><b>Recommendation: Legal/Standardisation/Best Practices</b></td><td><b>Explanation on recommendation</b></td><td><b>Relevant Institution</b></td></tr>
<tr><td colspan="3"><b>Recommendations proposed within T4.2 (D4.5 Second Innovation uptake, Industrialisation and Research Strategy)</b></td></tr>
<tr><td><b>Legal/Standardisation/Best Practices (short/medium/long term)</b></td><td>The innovation Multi-Stage Supply Chain Disruption Mitigation Strategy and Digital Twins for Supply Chain Resilience has been transformed into a solution focusing on how to enhance and extend the supply chain management scope (EESCM, Enhanced and Extended Supply Chain Management) to take more aspects into account, provide a better understanding of the real issues and how to minimize disruption impacts.
The EESCM (Enhanced and Extended Supply Chain Management) concept enhances the scope and functionality of previous supply chain management packages by augmenting supply chain resilience capabilities to minimize disruption impacts, with special attention to Critical Infrastructures (CI), to proposals for new policies, and to changes in legislation and/or relevant regulations. It also involves supporting CI service providers and product suppliers by building capabilities for impact minimization, modelling of cascading effects and rapid recovery, including extension of management practices and improvement of tools to be employed by all relevant organizations to reduce supply chain disruptions.</td><td><b>Council of the EU, European Parliament and European Commission</b>
<b>https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0829</b>
<b>The Critical Entities Resilience Directive (CER) (critical-entities-resilience-directive.com)</b>
<b>EUR-Lex - 32022L2555 - EN - EUR-Lex (europa.eu)</b>
<b>www.eeas.europa.eu/sites/default/files/documents/strategic_compass_en3_web.pdf</b></td></tr>
</table>

	In the short term the recommended actions required for the implementation of the innovation put forward above should address the target audience (for example, policy makers, providers of tools and training) and stakeholders concerned with preserving the integrity of Critical Infrastructures under fire. This should include setting up a governance body that is capable of defining the final scope of an innovative supply chain resilience framework and ensure that the critical components of the framework are consistent with existing legal / standardization and best practice related strategies and directives of EU and EC, which are delineated and explained below and include a Proposal for a DIRECTIVE on the resilience of critical entities; The Critical Entities Resilience Directive (CER); and the Strategic Compass for Security and Defence. More specifically, within the context of the CER, the Commission may also adopt legal acts laying down procedural arrangements necessary for the smooth functioning of the burgeoning **Critical Entities Resilience Group**, which shall support EC and be composed of representatives of the Member States and the Commission, facilitating strategic cooperation and exchange of information. The key recommendation here is to ensure that this **Group** will also address the evolving needs of the extended supply chain management framework. Furthermore, for the medium term, within the context of these EU / EC level actions and the supply chain resilience framework, we recommend strict adherence to supporting the development of enhancements to the aforementioned actions with special attention to: • developing and testing the framework on a sub-set of industries at the EU or regional level to evaluate resilience capacities; • ensuring that the final framework is adequately robust across industry sectors and can also be implemented in education/training environments;	**IBM, What is a digital twin?**

	including a set of newly developed guidelines for the further development of tools and methodologies. Finally, in the long term, to bring the EESCM solution to fruition, providers of supply chain management related services (tools and training) should enhance current instruments with novel concepts. To effectively accomplish this, the strategies and guidance should be set by EU and MS level policy makers. In this context, the Digital Twins approach is crucial and although currently used to model supply chain and optimization techniques, it can also be adopted to widen the scope of its capabilities. This would include expansion of services, geopolitical concerns and hybrid threat challenges; as well as enhanced tools capable of providing reliable, real life based, modelling of cascading effects; including impact minimization and recovery simulation capabilities	
Additional recommendations within T4.3		
Best Practices (medium term)	**Strategic Compass for Security and Defence** (approved 21 March 2022) provides the European Union with an ambitious plan of action for strengthening the EU's security and defence policy by 2030**.** The **Compass** is ambitious, formally approved just after Russia's attack on Ukraine. It covers security and defence strategies in relation to global competition, overall economic security, the space industry, disruptive technologies, and associated risks to EU's supply chains related to Critical Infrastructure.	**Council of the EU and European Commission** **www.eeas.europa.eu/sites/default/files/documents/strategic_compass_en3_web.pdf**

2.3 DETECTION OF DISINFORMATION DELIVERY PROXY ACTORS

Description of the Innovation
Authoritarian regimes are increasingly attempting to undermine the shared democratic values of the EU and its member states and polarise societies for their own strategic purposes using various types of hybrid activities, including information manipulation and lawfare. Hence, the protection of democracy infrastructure against exploitation of political cleavages and foreign interference needs more comprehensive attention.
The main outcome of the innovation proposal could be better situational awareness, more powerful analytical capabilities and better coordinated counter-disinformation actions in both national and EU levels to avoid hostile exploitation of existing political cleavages such as polarization, radicalization and undervalue of democratic institutions as we've seen during the Covid-19 pandemic crises or after the Russian aggression against Ukraine.

State of play	Relevant links
Foreign information manipulation and interference has grown rapidly in the recent years and the examples can be seen in social, political and economic spheres. Foreign interference can be seen whenever there is tension, emotional context, political, social and economic cleavages. The information/disinformation campaign most often origins at one source and is then being spread by proxy actors – including troll networks and bots.	https://www.oecd.org/ukraine-hub/policy-responses/disinformation-and-russia-s-war-of-aggression-against-ukraine-37186bde/
The UK Government found that TikTok influencers were being paid to amplify pro-Russian narratives. Disinformation activities also amplified authentic messages by social media users that were consistent with Russia's viewpoint in an effort to increase the spread of such narratives, giving an artificial sense of support. Efforts to manipulate public opinion on social media took place on Twitter and Facebook, with extensive efforts also concentrated on Instagram, YouTube and TikTok. Evidence also exists of disinformation campaigns taking place in the comments sections of major media. Russian government accounts have also been linked to "typo squatting" (registering websites with deliberately misspelled names of similarly named websites) of popular news organisations containing false information. For example, Russian actors created a fake website of the Polish daily newspaper, Gazeta Wyborcza, to spread disinformation about the atrocities reported in Bucha.	
Experts are concerned about increasingly sophisticated efforts to evade automated detection - for example, by mobilizing authentic digital-platform accounts to engage in inauthentic behaviour. Adversary actors will likely	https://carnegieendowment.org/2020/07/15/eu-s-role-in-fighting-

boost a greater number of accounts with fewer followers to avoid detection, thereby blurring the lines between authentic and inauthentic and between coordinated and uncoordinated behaviour. Experts also anticipate a broader integration of hybrid influence techniques and disinformation. Paid services for boosting digital platform profiles, in conjunction with existing tools allowed by the platforms, will continue to enable platform distortion. Experts also expect continued microtargeting of content, in conjunction with wider manipulation of public discourse. The EU has taken some actions to counter disinformation and is grappling with how to counter its adversaries in the information space. But its current policy on disinformation is characterized by a lack of terminological clarity, unclear and untested legal foundations, a weak evidence base, an unreliable political mandate, and a variety of instruments that have developed in an organic rather than a systematic manner.	disinformation-taking-back-initiative-pub-82286
Strategic Compass for Security and Defence, approved 21 March 2022, mandates the European Union to protect its citizens, values and interests and contribute to international peace and security. The Strategic Compass is setting out concrete actions also in the field of hybrid threats, cyber diplomacy and foreign information manipulation and interference.	A Strategic Compass for Security and Defence - document 2023 Annual Progress Report on the Implementation of the Strategic Compass for Security and Defence
The plan is to develop the EU Foreign Information Manipulation and Interference Toolbox – by 2023. There should be an appropriate mechanism to systematically collect data on incidents, facilitated by a dedicated Data Space, to develop a common understanding of foreign information manipulation and interference. By 2024 all CSDP (Common Security and Defence Policy) missions and operations will be fully equipped with capabilities and resources to deploy relevant instruments of this toolbox.	
In 2022 the Strategic Compass was to further strengthen the Cyber Diplomacy Toolbox, notably by exploring additional response measures and develop EU Hybrid Toolbox that should provide a framework for a coordinated response to hybrid campaigns affecting the EU and its MS. The plan in 2022 was to bring together existing and possible new instruments, including the creation of EU Hybrid Rapid Response Teams to support MS, CSDP missions and operations and partner countries in countering hybrid threats. Strategic Compass sets out an ambitious plan to strengthen EU security and defence policy by 2030.	

The European Regulators Group for Audiovisual Media Services (ERGA) - is an advisory group whose role is to provide technical expertise to the Commission in its work to ensure a consistent implementation of the Audiovisual Media Services Directive (AVMSD) in the Member States, and regarding related audiovisual media matters as well as to facilitate cooperation among the national regulatory authorities or bodies, and between them and the Commission. Originally established by the Commission in 2014, ERGA has been recognised and established by the revised AVMSD which reinforced its role and tasks. Some of the tasks will be: • work within the strengthened EU Code of Practice on Disinformation which was published on 16 June 2022. The Code created a permanent Task-force which includes ERGA representatives and is chaired by the European Commission. The Task-force and its Subgroups will have to, among others, establish a risk assessment methodology, agree on reporting templates and publish a first set of structural indicators in the coming months; • monitor and contribute - where relevant - to the adoption and implementation of the Regulation on transparency and targeting of political advertising	ERGA website ERGA Work Programme 2023
2022 Digital News Report shows that attitudes toward information are changing in media audiences, and in particular trust in professional journalism and traditional media is declining. This is a trend that has been evident for some time, but it is still continuing, and in some countries, it is intensifying. At the same time, the overall consumption of traditional media, radio, television and newspapers, is declining. Interest in news has fallen from 63% in 2017 to 51% in 2022. A growing proportion of respondents also declare that they avoid information from traditional media because it is too depressing or complicated (the latter indication applies mainly to younger people with lower media competence). This type of selective avoidance has doubled in both Brazil (54%) and the UK (46%) over the last five years. At the same time, the demand for subscriptions of paid information from online sources is not increasing, and Facebook remains the main source of information for the global population.	https://www.digitalnewsreport.org/
The Digital 2022 report indicates that while interest in traditional media and the information they offer is declining, the popularity of social media is growing consistently. The number of social media users globally has increased year-on-year by more than 10%. At the same time, more than 90% of the population uses smartphones to access the Internet (including news content). This is significant because the information we receive via mobile	https://datareportal.com/reports/digital-2022-global-overview-report

devices is structured differently. It is shorter, simplified and more emotional - as it has to compete for the recipient's attention in different circumstances. It is also worth noting that TikTok, which is a platform heavily saturated with disinformation content and often used by proxy actors, has recently seen the greatest growth in popularity. Another disturbing phenomenon is that the highest susceptibility to disinformation from social media (which is linked to the highest trust in the content published there) is observed among young and uneducated users, as well as among women. At the same time, this indicator correlates with the greatest criticism of science and the least trust in traditionally recognized authorities and sources of information (Disinformation through the eyes of Poles Report, Digital Poland). A particular challenge in the analysed area is that disinformation campaigns using proxy actors are difficult to detect, and especially difficult to track once they gain popularity on social media. For the most part, they appeal to existing stereotypes and social fears, and take advantage of the spontaneous behaviour of social media users (for example, the tendency to share content). A good example of this is the Tik Tok trend of @.MOMMYJUICY, which triggered huge engagement from young Polish women while tapping into their most widespread fears. Ultimately, the campaigns aroused resentment against young Ukrainian women who had arrived in Poland, who were presented as "more attractive" and thus a "threat" to young Polish women and their relationships. Campaigns of the analysed type certainly have some common mechanisms (e.g. those related to the functioning of social media), but it should be noted that their nature is very different. This means that, in principle, each of these campaigns should be analysed separately, often referring to broad cultural or social contexts (such reports are published, for example, by the Demagog Association). As a result, it is particularly difficult to build public knowledge and resilience has such phenomena.	https://digitalpoland.org/publikacje/pobierz?id=4f2e2116-82a6-47b5-a984-801b5e704b56 https://oko.press/ukrainka-ukradla-meza-mlode-polki-ofiarami-dezinformacji-dzis-widac-skutki https://demagog.org.pl/analizy_i_raporty/w-krainie-kolorowych-matrioszek-jak-dziala-rosyjska-dezinformacja/ https://demagog.org.pl/fake_news/ukraincy-niszcza-mariupol-prorosyjska-propaganda-patricka-lancastera/ https://demagog.org.pl/fake_news/mariupol-oswobodzony-od-nazistow-prorosyjska-dezinformacja/ https://demagog.org.pl/analizy_i_raporty/thank-you-usa-polscy-politycy-w-rekach-rosyjskiej-propagandy/

		https://texty.org.ua/projects/108323/germs-russian-world-who-supports-russia-europe
Recommendation: Legal/Standardisation/Best Practices	**Explanation on recommendation**	**Relevant Institution**
Recommendations within T4.3		
Legal **(medium term)**	Set up a national agency to monitor, detect and analyse the operation used by foreign actors to disseminate and amplify online content hostile to nation with the aim of damaging the nation’s interest. France set up VIGINUM (The Vigilance and Protection Service against Foreign Digital Interference) to combat information manipulation. Formed in 2021 and attached to the General Secretariat for Defence and National Security (SGDSN). The main mission is to protecting digital public debate against information manipulation campaigns involving foreign actors intended to harm France and its fundamental interests. VIGINUM has an ethical and scientific committee, and its mandate is strictly regulated by law. The agency employs mainly analysts, data engineers and digital media experts who work with open sources information. According to Report, VIGINUM has detected 84 potentially inauthentic phenomena as of 22 July 2022 phenomena on digital platforms and 60 of them during the 2022 French election period.	**EU MS governments related to national security and defence**

Legal **(short term)**	Legal solutions to be introduced on the EU level that will increase transparency of online platforms – e.g. sharing of and accessing relevant data of social media platforms, increasing transparency of political advertisements, increasing transparency and understanding of micro targeting, algorithms and content moderation activities	**European Institute for Security Studies** **EEAS** **European Parliament Committees** **Communications Networks, Content and Technology** **European Commission – DG EAC – Education, Youth, Sport and Culture - EAC.B YOUTH, EDUCATION AND ERASMUS+**
Legal **(short term)**	Code of Practice of Disinformation to be signed by relevant players to be signed obligatorily and not voluntarily, as it is currently	
Best Practices **(short term)**	Supporting independent, quality, fact-based journalism, including independent public-service broadcasting, and encouraging media literacy campaigns to develop trust in the media and understanding of what constitutes good information will continue to play important roles	
Best Practices **(short term)**	Promote and support audiences' use of reliable sources of information, including traditional media. Enable young people to access paid news services on preferential terms, for example, through school subscriptions.	
Best Practices **(short term)**	Support the activities of independent fact-checking organizations that publish specific data on disinformation campaigns delivered by proxy actors and whose personnel have the competence and tools to professionally detect and describe such phenomena. In this context, also promote broad cooperation, especially between the journalistic and fact-checking communities with social-media platforms.	

Best Practices (short term)	Aim to ensure that social media users are not only competent in recognizing disinformation messages, but also have the widest possible access to data on, for example, where a message came from, how it spread, etc. The idea would be to make the circulation of messages on social media as transparent as possible.	**European Parliament – Committee on Culture and Education**
Best Practices (medium term)	Media-literacy teaching should be stretched across all age groups including kindergarten groups and seniors. For schoolchildren and students countering disinformation classes should be part of the core curriculum. Teachers who are responsible for those classes should first be thoroughly educated themselves so that they are well prepared to share the knowledge with children and students. As the landscape of disinformation is constantly evolving, teachers should undergo regular up training sessions (also with practitioner e.g. journalists and civil society representatives) to make sure they are updated. For older groups, media-literacy teaching can take different forms – lectures, discussion panels, workshops, awareness campaigns etc. with age and education-appropriate tools. It is important for media-literacy teaching to be rather group specific than include everyone.	
Best Practices (short term)	Creating guides tailored to selected target groups – social and digital media users. Guides in a practical and understandable way should inform on how to recognise fake news and what can be done in this case. Those guides should be consistent within all MSs but taking into consideration different topics specific for various countries/regions. Once created, those guides should be incorporated into media-literacy teaching classes and events (as described above).	

2.4 ALERTING ON AND REACTING TO DISINFORMATION IN REAL TIME (UPGRADE OF RAPID ALERT SYSTEM ON DISINFORMATION)

Description of the Innovation	
European Commission's Action Plan against Disinformation states (p. 6) that 'a Rapid Alert System will be set up to provide alerts on disinformation campaigns in real-time through a dedicated technological infrastructure'. As James Pamment (2020: 14) emphasizes, that 'while the Rapid Alert System was used to share reporting among EU member states, an alert related to the pandemic has not been triggered.' So, this attempt seems like a missed opportunity, which needs to be carefully assessed and further developed to be real-time, rapid and really alerting. Rapid Alert System is not working in the area of countering disinformation. Nowadays we need a modern, more novel tool that will work the way (and beyond) that Rapid Alert System was supposed to – alerting on disinformation in real time which will allow to initiate relevant protocols and respond to it. Works are in progress on FIMI toolbox – a tool that will result in better situational awareness between the EU institutions and its Member States, more powerful analytical capabilities and better coordinated counter-disinformation actions in both national and EU levels via 24/7 operational information exchange platform. It will also help avoid hostile exploitation of existing political cleavages, especially in times of large-scale crises such as pandemics, irregular immigration flows or when political turbulences could spill-over the regions and have negative cascading effects also (in-)between different nationalities and social groups	
State of play	**Relevant links**
The EU response to the hybrid warfare (specifically from the Kremlin side) accelerated after illegal Crimea annexation, COVID-19 infodemic and Russian war against Ukraine. The response involves actions such as: creation of the East StratCom Task Force within the EEAS's Strategic Communications Division (established to effectively communicate and promote EU policies toward the eastern neighbourhood. The task force produces a weekly review of pro-Kremlin disinformation targeting the West as a flagship product on the EUvsDisinfo web platform, and its database features over 8,000 examples of disinformation); Code of Practice on Disinformation, Action Plan Against Disinformation, European Democracy Action Plan, Digital Services Act, Rapid Alert System.	https://epthinktank.eu/2022/04/21/eu-action-against-fake-news/
In January 2015 the European External Action Service's (EEAS) East StratCom Task Force established, as already mentioned above, EUvsDisinfo after the illegal annexation of Crimea by Russia. Its mandate is to forecast, address, and respond to Russia's ongoing disinformation campaigns affecting the European Union, its Member States, and countries in the region.	https://www.eeas.europa.eu/node/59644_en

The European Union provided funding for the European Digital Media Observatory in an effort to connect researchers, fact-checkers, media literacy experts and media organisations. This independent observatory facilitates closer co-ordination for fact-checking organisations, the scientific community, media literacy practitioners, journalists and policy makers via technological platforms, training and co-ordination of independent fact-checking and research activities. Part of the EDMO are regional hubs, among others: CEDMO (Poland, Czech Republic, Slovakia) BECID (Estonia, Lithuania, Latvia), GADMO (Germany, Austria), NORDIS, EDMO Ireland, BENEDMO (Benelux), ADMO, IDMO (Italy), DE FACTO, IBERIFIER, BROD (Bulgaria and Romania), MEDDMO (Mediterranean; Greece, Cyprus, Malta).	https://euvsdisinfo.eu/ https://edmo.eu/
Following the European Commission Communication on tackling online disinformation, SOMA (Social Observatory for Disinformation and Social Media Analysis) has been launched to provide support to a community that will jointly fight disinformation. SOMA is a platform with infrastructure and connections to support experts in their activity against disinformation, with verification tools, algorithms, and processes	https://www.disinfobservatory.org/
The European External Action Service launched the Rapid Alert System in March 2019 to enable common situational awareness related to disinformation spread across EU member states, as well as the development of common responses. The Rapid Alert System (RAS) is an important element of the EU's overall approach to tackling disinformation and is one of the four pillars of the Action Plan against Disinformation (signed by the European Council in December 2018). The Rapid Alert System is set up among the EU institutions and Member States to facilitate the sharing of insights related to disinformation campaigns and coordinate responses. The RAS is based on open-source information and will also draw upon insights from academia, fact-checkers, online platforms and international partners. The system consists of a rudimentary platform for information sharing, as well as a network of points of contact in the various EU member states. The Rapid Alert System is intended to connect to existing real-time monitoring capabilities inside and outside of the EU, such as the Emergency Response Coordination Centre and the EEAS Situation Room, as well as the G7 Rapid Response Mechanism and the North Atlantic Treaty Organization (NATO).	https://www.oecd.org/ukraine-hub/policy-responses/disinformation-and-russia-s-war-of-aggression-against-ukraine-37186bde

The system is therefore, in theory at least, an important platform for information sharing on disinformation activities and campaigns from an international perspective. It is hard (or even impossible) to find any data on the use of Rapid Alert System in countering/alerting on disinformation. However, several sources (links provided in the document) claim that relatively few highly engaged EU member states share information through the Rapid Alert System.	
Rapid Alert System could be used as a major tool in pre-bunking disinformation not allowing disinformation campaign to spread. Pre-bunking and inoculation strategy are being more and more often perceived as essential means of building societal resilience. One of the examples and major successes of pre-bunking took place before Russia attacked Ukraine in February 2022 - the United States noted in November 2021 that it was aware of invasion plans, and in early 2022, the United States and the United Kingdom shared intelligence with allies and the public warning of an imminent attack. While these strategic communication efforts did not prevent Russia from invading Ukraine, publicising intelligence made it more difficult for the Russian government to disguise its intent or confuse the public discourse via disinformation campaigns, and likely supported the rapid and relatively unified response. Inoculation and pre-bunking is about warning people of the possibility of being exposed to manipulative information, with the idea that such activities will reduce susceptibility to mis- and disinformation.	https://gcs.civilservice.gov.uk/publications/resist-2-counter-disinformation-toolkit/#:~:text=RESIST%20Counter%20Disinformation%20Toolkit,Strategic%20communication%2C%20Track%20outcomes
Numerous countries decide to create a special (governmental) unit responsible for countering disinformation. In the United Kingdom, the Government Information Cell was created by the government shortly before the Russian invasion to support the public communication function in debunking and countering Russian disinformation campaigns. The United Kingdom also relies on the Counter Disinformation Unit, part of the Department for Digital, Culture, Media and Sport, to engage directly with social media platforms to flag what it has identified as false and dangerous content published on the platforms – similar 'counter disinformation' units have been created e.g.. in US, Canada and EU countries. In March 2022, European Parliament set up a new special Committee on Foreign Interference (INGE2) - The European Parliament's anti-disinformation team monitors and analyses disinformation, cooperates with other institutions and civil society, and organises training and awareness raising activities.	https://gcs.civilservice.gov.uk/wp-content/uploads/2021/11/RESIST-2-counter-disinformation-toolkit.pdf

Europe and the West are targets of disinformation, influence operations, and foreign interference. Many sources emphasise that the responses of most Western countries to disinformation campaigns is slow, insufficient, late and hampered by legal restraints and bureaucracy. UK government published RESIST-2 counter disinformation toolkit. This toolkit provides a consistent and effective approach to identifying and tackling a range of manipulated, false, and misleading information that government and public sector communicators may experience. The framework has been written by the UK Government with other like-minded organisations in mind. It is a framework to support any communicator looking to protect their audiences and defend their organisation against the threat of mis- and disinformation can use RESIST. As the toolkit website states, the toolkit will: ✓ give you guidance on how to identify a range of different types of mis- and dis- information consistently and effectively ✓ help you prevent and tackle the spread of mis- and disinformation ✓ enable you to develop a response when mis- and disinformation affects your organisation’s ability to do its job or its reputation, or represents a threat to the general public ✓ help you to build audience resilience to the threat of mis- and disinformation. In 2018, the EC adopted a document entitled Code of Practice on Disinformation, under which relevant players agreed on the self-regulatory standards on disinformation. On the 16 June 2022 The strengthened Code of Practice on Disinformation has been signed by 34 signatories. The new code is the revision of the 2018 Code and its goal is to achieve the objectives of the Commission’s Guidance presented in May 2021, by setting a broader range of commitments and measures to counter online disinformation. The signatories of the code are: major online platforms, emerging and specialised platforms, players in the advertising industry, fact-checkers, research and civil society organisations. Signatories committed to take action in several domains, such as; demonetising the dissemination of disinformation; ensuring the transparency of political advertising; empowering users; enhancing the cooperation with fact-checkers; and providing researchers with better access to data. The code is planned as a part of a broader regulatory framework, in combination with the legislation on Transparency and Targeting of Political Advertising and the Digital Services Act. The Code is a tool from the area of self-regulation	https://carnegieendowment.org/2020/07/15/eu-s-role-in-fighting-disinformation-taking-back-initiative-pub-82286 https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation

and includes 44 commitments and 128 specific measures, in the following areas: demonetisation - cutting financial incentives for purveyors of disinformation, transparency of political advertising, Ensuring the integrity of services, Empowering users, Empowering researchers, Empowering the fact-checking community, Transparency centre and Task-force, Strengthened Monitoring framework.	
European Regulators Group for Audiovisual Media Services (ERGA) brings together heads or high-level representatives of national independent regulatory bodies in the field of audiovisual services. Established on 3 February 2014, the general goal of ERGA is to advise the EC on the implementation of the EU's Audiovisual Media Services Directive (AVMSD). ERGA has a group working on countering disinformation (Countering disinformation and strengthening democracy in the digital environment), which purposes are: - to support and advise the Commission in the effective implementation of the strengthened Code of Practice on Disinformation - to prepare capacities for monitoring of the strengthened Code of Practice on Disinformation and to prepare a report on its implementation in 2023 - to contribute to the discussions of the co-legislators for the adoption of the Regulation on transparency and targeting of political advertising - to monitor the evolution of NRAs' competencies in countering disinformation, - to organise workshops/meetings, - to follow the European Democracy Action Plan implementation, - to inform and share expertise on interconnected issues, including on the Digital Services Act and the European Media Freedom Act.	https://erga-online.eu/?page_id=12
International Fact-Checking Network is the organization that was launched in 2015 by Poynter to bring together the community of fact-checkers around the world and advocates of factual information in the global fight against misinformation. IFCN fosters cooperation between fact-checking organizations in Europe and around the world and promotes and strengthens professional fact-checking standards. IFCN monitors the situation in the world as far as disinformation trends are concerned, organizes workshops and trainings for fact-checkers, and supports fundraising for fact-checking activities. The main document to which IFCN refers is International Fact-Checking Network's code of principles.	EEAS

Currently, the IFCN has about 100 members and signatories to the aforementioned document, among which are fact-checking organizations from all over the world. In order to become a member of IFCN, one must meet strict requirements and follow detailed transparency rules. In this way the IFCN contributes to the development and growth of public confidence in the activities of fact-checkers.	
EUFACTCHECK is a project of the European Journalism Training Association (EJTA), which aims to create a sustainable fact-checking curriculum within a European network of journalism schools. This curriculum contains information on methodology, fact-checking flow, warning signs, examples of fact check, evaluation and reflection. By fact-checking and trying to combat disinformation, the project wants the students and the public to have a deeper insight and interest in democratic processes, both at the national and European levels. The goal of EUFACTCHECK is to motivate fact-based debate in the EU and stimulate media and information literacy. About 20 research institutions (universities) from Europe are members of the network.	https://eufactcheck.eu/ https://eufactcheck.eu/wp-content/uploads/2020/02/EUfactcheck-manual-DEF2.pdf
Disarm Foundation promotes DISARM - the Disinformation Analysis and Risk Management framework - the tool which enables users to map, analyse, and respond to disinformation. It helps in coordinating of actions countering disinformation at scale in real-time, as well as coordination on research, analysis, and policy making. DISARM is the open-source, master framework for fighting disinformation (sharing data & analysis and then coordinating effective action). The Framework is developed on the base of global cybersecurity best practices. It is used to - help communicators, - gain a clear shared understanding of disinformation incidents - identify defensive and mitigation actions that are available to them.	https://www.disarm.foundation/framework
EEAS is working to develop the EU FIMI Toolbox to prevent, deter and respond to the threat, these insights are key to understand how to further enhance the instruments to best serve the purpose of countering disinformation. EU MS need a comprehensive tool which will capture both technical (such as TTPs and observables) and non-technical information (such as suggested attribution, victimology etc.) while linking each piece of information to its primary source (a report, new article, etc.).	1st EEAS Report on Foreign Information Manipulation and Interference Threats

		Council conclusions on Foreign Information Manipulation and Interference (FIMI) Open Cyber Threat Intelligence Platform
Recommendation: Legal/Standardisation/Best Practices	**Explanation on recommendation**	**Relevant Institution**
Recommendations within T4.3		
Best Practice (medium term)	Complete and finish the works on the upscale of Rapid Alert System: FIMI toolbox making it 24/7 operational information tool in cause of time-criticality, especially in times of large-scale crises as pandemics, irregular immigration flows, etc. The main outcome of the innovation proposal could be better situational awareness between the EU institutions and its Member States, more powerful analytical capabilities and better coordinated counter-disinformation actions in both national and EU levels to avoid hostile exploitation of existing political cleavages, especially in times of large-scale crises when political turbulences could spill-over the regions and have negative cascading effects (in-)between different nationalities and social groups.	**National Governments – Entities responsible for Public Security Issue Coordination, in Poland: Government Centre for Security** **European Parliament - Special Committee on Foreign Interference in all Democratic Processes in the European Union, including Disinformation** **Association of European Journalists** **International Fact Checking Network**
Best Practice (short term)	'Countering disinformation' units to be established in EU and in each country (national and local levels), making sure those units are consistent, have similar duties, responsibilities, access to the same tools and are in constant contact with one another sharing information	

Best Practice (medium term)	Multisectoral cooperation supporting pre-bunking and debunking efforts to counter disinformation campaigns. Preparing proactive and tailored responses, Creating blueprints and/or best practices that can be initiated in order to predict the likely impact of disinformation campaign and respond accordingly to ongoing disinfo campaigns by initiating the relevant protocol.	**EU fact checking networks** **EU project working on countering disinformation e.g. EDMO** **European Commission: DG Connect: Directorate H Digital Society, Trust & Cybersecurity** **Council of European Municipalities and Regions (CEMR)** **Council of Europe: Congress of Local and Regional Authority Secretary General** **European Committee of the Regions – thematic commission CIVEX: Commission for Citizenship, Governance, Institutional and External Affairs** **European Institute for Security Studies**
Best Practice (short term)	Work on unified terminology for combating disinformation – fake news, misinformation, disinformation, malinformation, FIMI etc. Currently terms “disinformation” or “fake news” are often used as to cover a range of disinformation activities.	
Best Practice (short term)	Cooperation with fact-checking organizations at the national and supra-national level, with the aim of quickly detecting disinformation messages and obtaining full and certain knowledge that a given message is actually disinformation. This kind of cooperation will minimize the likelihood of bias in the evaluation of messages by applying the solutions developed by fact-checkers	
Best Practice (medium term)	Building on scientific knowledge in the detection and recognition of disinformation messages. Thus, continuous cooperation with researchers of disinformation messages on how to detect and recognize such messages, trends in this area, the most important actors and changes in the media that favour the spread of disinformation messages	
Best Practice (medium term)	Creation of a structure that will include entities of different nature - governmental, public, non-governmental organizations, research centers, etc. Adopt common standards of operation and ensure continuous and uninterrupted flow of information between these institutions.	
Best Practice (short term)	It is particularly important to ensure that relationships are built and maintained with entities that will be able to communicate the results of the FIMI toolbox work to the broader public (to the extent established). These entities are primarily the	

	media, but also fact-checking organizations, NGOs, research institutes, local government units, etc.	**EEAS**
Standard **(medium term)**	Incorporate fact-checking curriculum for journalism students within all European higher education schools which offer journalism faculties.	

2.5 IDENTIFY AND SAFEGUARDING VULNERABLE INDIVIDUALS

Description of the Innovation	
Promotion of extremism[3] and violence in different communication channels has variety of purposes. One of them is recruiting and incorporation of new followers. Widening of extremism minded community is mainly made targeting vulnerable individuals. There were significant efforts made to identify and analyse the underlying drivers to violent extremism offline. Online environment provided new possibilities for such activities and experience from kinetic environment were not utilised, so extremist propagandists and recruiters continue to hunt for vulnerable individuals. Vulnerability is considered as lack of individual resilience to be involved or recruited into violent extremism. Lack of resilience can be related to distrust on society / institutions approaches or actions in respect to certain phenome. Such distrust can be reinforced by other vulnerable groups, despite the phenomena in target. Groups of distrusted individuals are formed, leading to further segregation, making resilience weaker. The idea would be to have different methodological / technological solutions (e.g.: algorithms, redirections to less harmful content, etc.) that would put additional thresholds for people accessing content supporting extremism and violence.	
State of play	**Relevant links**
European Democracy Action Plan (EDAP) - presented by the European Commission on 3 December 2020. It is a non-legislative initiative announcing further steps, including legislative ones. The Plan is centred around: protect the integrity of elections and promote democratic participation; strengthen media freedom and media pluralism; counter disinformation, foreign interference and information influence operations. The Commission plans to gradually implement the EDAP with the active engagement of the European Parliament and the Council as well as with the wide circle of national actors, public and private, beyond government authorities. It envisages to have completed its application until 2023 - a year ahead of the elections to the European Parliament, and to assess the progress made and whether next steps are needed.	European Democracy Action Plan – general information European Democracy Action Plan – complete document
The Strengthened Code of Practice on Disinformation 2022 – has been signed and presented on the 16 June 2022 by 34 signatories who have joined the revision process of the 2018 Code. The new Code became part of a broader regulatory framework, in combination with the legislation on Transparency and Targeting of Political Advertising and the Digital Services Act. Users will be better equipped to identify and react to disinformation. In the area of	The Strengthened Code of Practice

[3] "Extremism is the vocal or active opposition to our fundamental values, including democracy, the rule of law, individual liberty, and respect and tolerance for different faiths and beliefs". Source: https://educateagainsthate.com/define-extremism-terrorism-uk-2/

media literacy, the Code contains commitments on tools to improve media literacy and critical thinking, awareness raising campaigns and partnerships. The Code places a special emphasis on involving vulnerable groups in media literacy campaigns and cooperation with entities with relevant expertise, such as the European Digital Media Observatory, ERGA's Media Literacy Action Group and the Media Literacy Expert Group. The Code contains a comprehensive set of commitments to increase fact- checking coverage and to support fact-checkers' work. Relevant signatories commit to a consistent use of fact-checkers' work on their services, with full coverage of all Member States and languages. It also establishes a framework for a structured and financially sustainable cooperation between the platforms and the fact-checking community, in collaboration with EDMO. To improve the quality and impact of fact-checking, the Code foresees enhanced information exchange between platforms and fact-checkers, as well as the creation of a repository of fact-checks.	on Disinformation 2022 – general information The Strengthened Code of Practice on Disinformation 2022 – complete document
Transparency Centre - the mission of the Centre is to counter the threat of disinformation and misinformation. It is designed to serve as a repository of all information on the Strengthened Code of Practice on Disinformation 2022 of and each of the actions implemented by signatories. It was launched in February 2023 by the 34 Code's signatories (online platforms, players in the advertising industry, fact-checkers, research and civil society organizations). The Transparency Centre, accessible to all citizens, will allow for an easy overview of the implementation of the Code's measures, providing transparency and regular updates of relevant information. Signatories had 6 months to implement the commitments and measures to which they have signed up. At the beginning of 2023, they provided to the Commission their first implementation reports. In general, Very Large Online Platforms, will report every six-months on the implementation of their commitments under the Code. Other Signatories will report on a yearly basis. The next round of reports is due in July 2023. Under the DSA (below), platforms (VLOPs and VLOSEs) with more than 45 million users in the EU could start facing investigations on how they tackle major issues on their platforms — such as the spread of disinformation and illegal content or their algorithms' amplification of toxic behaviours like cyberbullying — as soon as September 2023. Companies in violation of the rules face fines of up to 6 percent of their global revenues.	Transparency Centre – official website Transparency Centre – press release
Digital Services Act (DSA) – on 15 December 2020, the European Commission presented a digital services act package with two draft pieces of legislation, a digital services act (DSA) and a digital markets act (DMA), designed to create a fairer playing field and make online platforms more responsible for the content posted on them. The specific aim of the DSA is to promote a transparent and safe online environment, defining responsibilities and	Regulation on a Digital Services Act – complete document

accountability for a range of digital service providers. The new rules, once adopted, will re-shape the rights and obligations of digital service providers, online users, customers and business users in the EU was published on the 19th of October 2022 to ensure and entered into force on 16 November 2022. Very large online platforms (VLOPs) and very large online search engines (VLOSEs) will start being regulated from mid-2023. The DSA puts in place a framework of layered responsibilities targeted at different types of online intermediary services, including network infrastructure services (e.g. cloud and webhosting), online platform services (e.g. app stores and social media platforms), and services provided by very large online platforms and very large online search engines that pose particular risks in the dissemination of illegal content and societal harms. All providers offering such online intermediary services in the EU will have to comply with a range of obligations to ensure transparency, accountability and responsibility for their actions according to their role, size and impact in the online ecosystem. Regulation on addressing the dissemination of terrorist content online – the Regulation applies as of 7 June 2022 and provides a legal framework to ensure that hosting service providers (providers of social media, video, image and audio-sharing services) that make content available to the public, address the misuse if their services for dissemination of terrorist content online. Online platforms are obliged to remove terrorist content online within one hour after receiving a removal order from a competent national authority of an EU Member States and to take proactive measures when they are exposed to terrorist content. The Regulation puts in place strong safeguards to ensure that freedom of speech is protected. Member states are obliged to sanction platforms for non-compliance with the obligation under the Regulation. Better Internet for Kids runs Safer Internet Centres across Europe. The initiative is co-funded by the European Commission in Member States, and also operating in Iceland, Norway, Russia and the United Kingdom. Safer Internet Centres strive to keep children and young people safe online through a range of actions and initiatives. European Strategy for a better internet for kids (BIK+) – published on 11 May 2022 by the European Commission. The main aim is to ensure that children and young people are protected, respected and empowered online. The BIK+ strategy is built around three topics focused on children: safe digital experience, digital empowerment and active participation. It includes concrete actions that the Commission plans to support such as media literacy campaigns and the EU code of conduct on age-appropriate design to ensure privacy, safety and security for children online. A variety of campaigns and events are organized or attended within the framework of BIK+, e.g. Safer Internet Day, Positive Online Content campaign.	Digital Services Act – EU Legislation in Progress Briefing Regulation on addressing the dissemination of terrorist content online – complete document Regulation on addressing the dissemination of terrorist content online - Factsheet https://www.betterinternetforkids.eu/hu/about The new European Strategy for better internet for kids – complete document

Council of Europe leader calls for support for local media and emphasises the "major role" of local and regional authorities in tackling disinformation and hate - The Committee of the Regions as well as the Council of Europe in Strasbourg have called for local media to be better supported by both local and national authorities to ensure that the public has access to quality information about the area in which they live. In 2021 the Council of Europe's Congress of Local and Regional Authorities informed that in 2022 they will present recommendations for fighting disinformation and hate speech in the local and regional context. In July 2022 the document was published	The new European Strategy for BIK+ - Briefing Hate speech against local politicians has "worsened significantly" – press release Developing a handbook on good practice in countering disinformation at local and regional level – complete publication
"The Digital Era? Also my Era! Media and information literacy: a key to ensure senior's rights to participate in the digital era" provided by Council of Europe Guidelines for teachers and educators on tackling disinformation and promoting digital literacy through education and training provided by European Commission. Guidelines does not present ready solutions but focuses on how to create a learning environment, how to use digital technologies critically and responsibly, how to achieve media literacy and how students can be assessed regarding their competences in the field of digital literacy. Guidelines presents practical teaching and learning tips, activity plans for teaching, cautionary notes and other useful insights.	The Digital Era? Also my Era! – Information Society Department Council of Europe document (May 2022) Guidelines – complete document
Activity in the area of media literacy is an important element of EDMO's activity. In this context, the EDMO supports the activities of the Media Literacy Expert Group, maps good practices, coordinates the activities of other hubs, conducts trainings and workshops, and organizes an international meeting on media literacy education.	https://edmo.eu/media-literacy/
Rapid Evidence Assessment on Online Misinformation and Media Literacy Report, commissioned by Ofcom. The report "summarises the results of the Rapid Evidence Assessment (REA) on Online Misinformation and Media Literacy (REA), conducted from November 2020 to April 2021 and commissioned by Ofcom. The review is focused on studies that measure the effectiveness of interventions designed to tackle misinformation, both within the media literacy curriculum and in relation to technological interventions that draw on literacy principles (such as critical thinking, information evaluation and active engagement), even if they are not conducted in an educational setting". Comprehensive report presents findings on interventions in existing research; methodological limitations of existing research and recommendations.	https://www.ofcom.org.uk/__data/assets/pdf_file/0011/220403/rea-online-misinformation.pdf

Other departments of the European Commission that deal with, among other things, the area of media education: - Communications Networks, Content and Technology - Education, Youth, Sport and Culture	
Many activities related to media education, including digital exclusion and education of groups particularly susceptible to disinformation are undertaken by the Council of Europe. These include trainings, workshops, seminars, reports, recommendations, guides, etc.	https://www.coe.int/en/web/freedom-expression/media-literacy
Google Poland “Aces of the Internet” (“Asy Internetu”) initiative, which aims for children to learn the basics of safety and participation in the online community so that they can navigate the online world without fear. The program is aimed at families and parents, schools and teachers, and other educational institutions. It offers audiovisual matrices, games, educational programs, tutorials and lesson plans.	https://beinternetawesome.withgoogle.com/pl_all
Interesting materials for teachers are also prepared by the Demagog Association in Poland. - Educational game "Cool you know!" (https://fajniezewiesz.pl/) - the game allows you to practice your own attention to fake news online. - lesson plans on fake news for teachers (https://platforma.demagog.org.pl/wiedza/) - available free of charge. - short lesson supplements for teachers of specific subjects (https://drive.google.com/drive/folders/1-dBnp8voT55HajbKQtXhIMGrAjHx6_ze) available as part of the "Critical Thinking" campaign (https://demagog.org.pl/analizy_i_raporty/czy-w-polskiej-szkole-jest-miejsce-na-krytyczne-myslenie/). - lesson scenarios for grades VII - VIII (https://platforma.demagog.org.pl/fact-checking-w-klasach-vii-viii/) and high schools (https://platforma.demagog.org.pl/akademia-fact-checkingu-w-szkole-sredniej-czyli-scenariusze-zajec-dla-nauczycieli/).	https://demagog.org.pl/stowarzyszenie-demagog-pierwsza-w-polsce-organizacja-factcheckingowa/
The European Commission is undertaking a number of activities related to the area of media literacy, the essence of which is the training of media competencies, including those related to digital media and resistance to disinformation. Such activities are particularly important with regard to groups and individuals with low media literacy, and therefore particularly vulnerable to disinformation activities. The recently revised Audiovisual Media	https://digital-strategy.ec.europa.eu/en/policies/revision-avmsd

Services Directive (AVMSD) strengthens the role of media literacy. It requires Member States to promote measures that develop media literacy skills (Article 33a).		
Recommendation: Legal/Standardisation/Best Practices	**Explanation on recommendation**	**Relevant Institution**
Recommendations proposed within T4.2 (D4.5 Second Innovation uptake, Industrialisation and Research Strategy)		
Best Practices/Standardisation (medium term)	Develop a sharing and analysis platform for GECHO (Gatekeeping ECHO Chambers). The innovation Identify and safeguarding vulnerable individuals has been transformed into a solution that monitors the online environment, identifies where and how interventions are needed, thereafter launching the appropriate actions to build resilience in vulnerable young people against possible entrapment in violent extremism and terrorism. The solution is called Gatekeeping ECHO chambers (GECHO). GECHO is for countering violent extremism and terrorism, as antagonistic states and organizations may use support of local groups that promote violent extremism and terrorism as one tool in their hybrid threat toolbox. This to widen sociocultural cleavage and reduce trust in the society. GECHO proposes the establishment of a platform for information sharing, monitoring, analysis and joint actions between organizations in the MSs to provide detailed and local situational awareness about activities in online environments related to violent extremism and terrorism. This to allow efficient interventions against recruitment activities and to safeguard young people from such influence. 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	**The European Commission** **Ministry Level** **National and Local Authorities** **Actors specialized in monitoring of online activities by violent extremism and terrorism groups as well as tech companies developing tool** **EU Member States stakeholders (social care workers, police, teachers, NGOs)**

	sharing of situational data between stakeholders. The platform can be based on the CISAE principles proposed to be standardized in the first project cycle. An alternative route would be to use an extended DDS-alpha platform. Develop AI based tools to quickly and accurately discover new sites, new visitors and changes in activity levels at known sites. In this work use of federated learning should be considered and how anonymization and GDPR requirements can be fulfilled. Furthermore, there is a need for research and compilation of training sets to guarantee that AI based solutions easily can be developed and tested. 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	**Europol** **The Radicalisation Awareness Network (RAN Practitioners)** **The VOX-Pol Network of Excellence (NoE)** **European Digital Media Observatory (EDMO**
Additional recommendations within T4.3		

Best Practices (short term)	Join the Transparency Centre signatories. By joining the 2022 Code of Practice on Disinformation, new signatories will be part of an EU-wide forum bringing together a variety of relevant players who seek to strengthen their actions, share best practices and improve cooperation in order to mitigate the risks stemming from disinformation in the EU. Potential signatories can get in contact with the Task-force through the website.	**Providers of online services (social media, private messaging applications, search engines)** **Providers of online advertising industry** **Providers of e-payment services, e-commerce, crowd-funding, donation systems** **Fact-checkers** **Civil society organizations specializing in countering disinformation**
Best Practices/Legal (long term)	Finnish Education System and approach to counter disinformation. According to the Media Literacy Index 2022[4] which assess the potential vulnerability of 41 societies in Europe to disinformation, Finland is first in the ranking and also shows that countries in the Southeast and East Europe are more vulnerable to the phenomenon (in Report takes into account such factors are media freedom, education, trust in people and e-participation). Education as one of essential component in aforementioned Report is also the cornerstone to resist information warfare considering by Finland's government. The curriculum was revised in 2016 to teach children the skills they needed to spot the kind of fabricated information on social media. Wide spreading critical thinking skills among pupils/students along with coherent government response is the main tool to combating disinformation campaigns and creating more resilient society.	**Ministries of Education in EU countries** **The European Education Area**

[4] https://osis.bg/wp-content/uploads/2022/10/HowItStarted_MediaLiteracyIndex2022_ENG_.pdf

	Finnish teachers in maths classes showing how statistics can be manipulated is a good example.	
Legal **(medium term)**	Legislation allowing to verify kids' age in social media. The French government is very close to implementing age verification and parental consent for social media platforms. The aim is to protecting children from harmful online content not intended for their age group. On march 2023 the National Assembly of France voted overwhelmingly in favour of the legislation and then it is up to the Senate to pass the bill into law. That legislation will allow to force social media and adult sites to verify their users' age and request parental consent for anyone under the age of 15. Parents will also be empowered to terminate social media accounts for their children if they're under 15. Such legal arrangements could be an appropriate approach for all EU Member States.	**Legislative authority in UE Member States**
Best Practices **(short term)**	Increasing resilience and reducing vulnerability to disinformation on local and regional level Local media are an important part of the fabric of local communities. They provide news that more deeply concerns readers' day-to-day experience. Quality local media promote transparency and accountability from local government and therefore trust in local politics. When citizens do not have access to local media it pushes them towards getting news through social media and messaging app groups, the latter of which are very hard to monitor because their encrypted nature. Therefore "A handbook on good practice in countering disinformation at local and regional level' was developed for the Committee of the Regions, CIVEX Commission (Commission for Citizenship, Governance, Institutional and External Affairs). A Handbook contains: - A typology of different areas of action to combat online disinformation (awareness raising, development of media literacy, strong public communication, promoting involvement of civil society stakeholders and	**Local and Regional Authorities in EU Member States**

	citizens and support for local media) at local and regional level, including of action already taken; - Three in-depth case studies of intervention undertaken to counter disinformation and identifies lessons that local and regional authorities (LRAs) could use for similar initiatives; - Gathered together lessons learned from research to provide practical recommendations for LRAs going forward. The recommendations aim to provide some guidance to LRAs on how to go about countering disinformation, based on practices that have shown to be successful	
Best Practices (medium term)	Create and support the operation of multidisciplinary research and project teams. Such teams would analyse factors influencing the particular vulnerability of given individuals or environments to disinformation and the media-psychological mechanisms of its impact. Then, on the basis of this knowledge, they would design effective communication tools to influence these individuals or environments.	**Local and Regional Authorities in EU Member States** **European Commission** **Research institutions**
Best Practices (medium term)	Build awareness of social media users on how harmful extremist groups operating on the Internet can be and what consequences their disinformation tactics (especially hate speech) can lead to.	**Local and Regional Authorities in EU Member States** **NGOs**
Best Practices (medium term)	Decentralization of educational processes in the field of media competences, delegating such activities to non-governmental institutions that operate in the local environment and have the best understanding of the needs and opportunities for education in this area. These types of organizations also have the knowledge and contacts that allow them to reach the groups most at risk of disinformation with their educational activities. Involvement of local opinion leaders in these activities	**Local and Regional Authorities in EU Member States** **NGOs**

2.6 WHAT INFORMATION NEEDS TO BE SHARED BETWEEN CI ENTITIES TO DETECT HYBRID THREATS AND ATTACKS

Description of the Innovation
The innovation "*What Information Needs to be Shared between CI entities to detect hybrid threat" (WINS)* has primary context related to exploitation of critical infrastructure (CI) weaknesses and economic dependencies. The cascading effects that can be caused after an attack on a critical infrastructure have raised the concern about the interdependencies of critical infrastructures. However, the strategic dependencies have not been clarified, let alone the aggregated risk and impact implications. A platform to share information between CI entities is often suggested as a solution and the idea of a CI resilience platform is interesting. However, the idea is not new and several platforms do exist in EU Member States (MS). Therefore, this idea needs to be further developed to answer how to detect hybrid threats by discovering anomaly in operational environment (incl. data) and how to share the discoveries between critical infrastructure (CI) stakeholders. The EU-HYBNET's suggested innovation WINS is to make possible a systemic risk assessment, anomaly detection and evaluation of currently unknown CI interdependencies and flag, if an event could be a sign of hybrid threats. If there is a systematic approach with e.g., the same signature (anomaly) repeating (digital or physical attack procedure), we can assume that there is a hybrid case ongoing, if we can also connect this incident to influencing decision-making. Therefore, it is crucial to identify "what information needs to be shared".

State of play	Relevant links
The Critical Entities Resilience Directive (CER) and The Network and Information Security Directive (NIS2) entered into force on January 16, 2023. The new CER Directive replaces the European Critical Infrastructure Directive of 2008. The new rules will strengthen the resilience of critical infrastructure to a range of threats, including natural hazards, terrorist attacks, insider threats, or sabotage. Eleven sectors will be covered: energy, transport, banking, financial market infrastructures, health, drinking water, wastewater, digital infrastructure, public administration, space and food. NIS2 Directive is the first piece of EU-wide legislation on cybersecurity, and its specific aim was to achieve a high common level of cybersecurity across the Member States. NIS2 modernised the existing legal framework to keep up with increased digitisation and an evolving cybersecurity threat landscape. By expanding the scope of the cybersecurity rules to new sectors and entities, it further improves the resilience and incident response capacities of public and private entities, competent authorities and the EU as a whole.	CER Directive – complete document NIS2 Directive – complete document

Until October 17, 2024, Member States must transpose the requirements of the CER and NIS2 Directive into national law Technical Committee ISO/TC 292 Security and resilience works with standardization in the field of security to enhance the safety and resilience of society. ISO/TC 292 was established on January 2015. The actual development of the standards is done in various Working Groups which focus on certain areas within the field of security and resilience. Working Group 6 is responsible for drafting standards in the area of Protective Security which is the framework, policies and processes implemented to identify, respond to and reduce the risk of harm from malicious acts. Working In this field, the Group has ongoing project dedicated to provide Guidelines for the development of a security plan for an organization (ISO 22343:2023). This document gives guidance on developing and maintaining security plans. The security plan describes how an organization establishes effective security planning and how it integrate security within organizational risk management practices. The document is applicable to all organizations regardless of type and nature (in the private, public or non-profit sectors, that wish to develop effective security plans in a consistent manner. The intent of the document is to provide the fundamental elements necessary to improve and sustain the protection of an organization. Other identified relevant standards: • ISO/IEC 27031:2011 Information technology — Security techniques — Guidelines for information and communication technology readiness for business continuity • ISO/IEC 27032:2012 Information technology — Security techniques — Guidelines for cybersecurity • ISO 31000:2018 Risk management – Guidelines • ISO/TS 22375:2018, Security and resilience – Guidelines for complexity assessment process		ISO/TC 292, ISO 22343:2023
Recommendation: Legal/Standardisation/Best Practices	**Explanation on recommendation**	**Relevant Institution**
Recommendations proposed within T4.2 (D4.5 Second Innovation uptake, Industrialisation and Research Strategy)		

Legal/Standardisation/Best Practices (short/medium term)	The innovation Impact and Risk assessment of critical infrastructures in a complex interdependent scenario (Acronym CIRP) has been transformed into a solution which present a methodology for how to establish what information dependent CI entities need to share in order to enhance their resilience against cascading effects and to counter hybrid threats. The solution proposed is called WINS, What Information Needs to be Shared between CI entities to detect hybrid threats and attacks, and to be prepared for them? The vision on the solution is to help CI entities and law enforcement (LE) officials to recognize new forms of hybrid threats/attacks, and further fulfil requirements in this respect given in CER- and NIS-2 Directive. Earlier innovation focusing on CI protection (from EU-HYBNET 1st working cycle) was an innovation called CISAE (A common Information Sharing and Analysis environment), and the CISAE was answering the question of how to share CI information between CI stakeholders. Now, the CIRP innovation is reconsidered and reformulated as an innovation called “WINS” that will build on CISAE. WINS is answering the question: what information needs to be shared? Therefore, the key element in WINS is a suggested methodological approach to discover what information needs to be shared to enhance CI entities resilience to counter hybrid threats. It is recommended to deliver pan-European and cross-sectoral CI methodological (even standardized) approach for analysis of CI entities’ critical vulnerabilities also in the context of hybrid threats/attacks. The collection of CI entities’ vulnerability data is based on risk assessments and stress tests and an attack tree approach. If the CI entities share the data with competent authorities, interconnected services and other relevant stakeholders, this will eventually support CI entities to be more prepared for hybrid attacks/threats. 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,	**European Parliament** **European Commission**

	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. 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, 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 see Deliverable 4.5	
Additional recommendations within T4.3		
Best Practices (short/medium term)	ENISA provides state-of-the-art advice and counsel to EU national authorities on safeguarding critical infrastructure such as power grids, telecoms and mass transportation systems essential to the national and cross-border security of essential services.	**ENISA**
Best Practices (short/medium term)	The Common Information Sharing Environment (CISE) is an EU initiative which aims to make European and EU/EEA Member States surveillance systems interoperable to give all concerned authorities from different sectors access to additional classified and unclassified information they need to conduct missions at sea.	**EMSA**

3. THE THREE LINES OF ACTION

The EU-HYBNET needs to report to the EC on Three Lines of Action. Each deliverable should state and explain how it contributes and have provided input and results to the *EC Three Lines of Action*. Below you will find Task 4.3 contribution:

1) monitoring of research and innovation projects with a view to recommending the uptake or the industrialisation of results

D4.9 contribution: During development of standardisation recommendations in the second EU-HYBNET cycle, partners of T4.3 were analysing also what research and innovation projects are bringing to the practitioners. Many of recommendations or identified best practices are based on research and innovation projects and activities, conducted in Europe but also outside Europe. This analysis is a relevant input to the EU-HYBNET's Objective 4 goal 4.3. in order to develop a mapping matrix connecting gaps and needs of European actors to areas that highlight the most promising innovations in different domains.

D4.9 contributes also to the EU-HYBNET's Objective 4 goal 4.1. T4.3 recommendations refer also to the industrialisation and to public procurement. These recommendations are an important input concerning the appraisal of best innovations (both technical and non-technical).

2) common requirements as regards innovations that could fill in gaps and needs:

D4.9 contribution: Many of described above recommendations are related to technological and non-technological innovations. It should be underlined that even best practices from one country can be innovative in many others. D4.9 contributes also to the EU-HYBNET's Objective 2, goal 2.4. enabling to define common requirements for new research and innovation possibilities that can fill knowledge gaps, and enhance capabilities endeavours concerning hybrid threats. Above recommendations suggested key focus research, innovation areas and actions for the future in the field of countering hybrid threats.

3) priorities as regards of increasing knowledge and performance requiring standardisation.

D4.9 contribution: Many of the above described recommendations are related to increasing (disseminating) knowledge and performance related to standardization, also non-technological and technological innovations linked to the increase of knowledge and skills. It is not necessary to list all examples here, as it would be repeating what was written and described in this deliverable's standardisation recommendations reports.

4. CONCLUSION

4.1 SUMMARY

In “Second Report Recommendations Standardisation” we have described the 6 areas selected to focus on in this deliverable and to construct the reports around them. In Section 2 we provide the most important aspects connected with selected areas happening currently together with offered recommendations linked to the innovations’ recommendations for standardization. Section 3 presents three lines of actions.

Authors of this deliverable would like to highlight that within task 4.3 of EU-HYBNET, we are working not only on recommendations for standards *per se*, but also on recommendations for legal harmonisations and identified best practices, which EU-HYBNET recommend to use or be inspired by the best practices. It is relevant do underline, that very often best practices are the beginning of development the official standard (ISO, CEN or national standard).

Hybrid threats are in the one way very old type of threats (Trojan horse described in the Homer’s Iliad is a great example), but for sure todays risks and hybrid attacks are changing and evolving rapidly. Due the fact that standardisation process is taking at least 2-3 years to develop the standard, we can observe that it is very difficult to keep standards in line with rapid changes in the area of hybrid threats. There are relevant standards related to safety, physical security and cybersecurity in general, but these standards mostly aren’t tailor-made for hybrid threats described in this deliverable.

4.2 FUTURE WORK

In the third project cycle, the state of play will be revised and adapted based on the outcomes of EU-HYBNET reports created in the third cycle within other tasks relevant for recommendations for standardisation, especially updated Gaps and Needs matrix and the update of most promising innovations from T3.1 and T4.2.

Additionally, in M43, consortium partners, network members, experts, practitioners and invited guests will meet in Valencia for the second Innovation Standardisation Workshop. The workshop will be the opportunity for in-depth discussions focused on selected recommendations described in this report.

Moreover, T4.3 partners will share information collected in deliverable D4.9 with relevant stakeholders, in particular CEN, CENELEC and ISO technical committees, as well, through WP5 (communication and dissemination), with all other organisations, agencies, institutions and projects working in the area of fighting hybrid threats.

ANNEX I. ACRONYMS

Term	Definition
AVMSD	Audiovisual Media Services Directive
CI	Critical Infrastructures
CIP	Critical Infrastructure Protection
CER	Critical Entities Resilience
CISAE	Common Information Sharing and Analysis Environment
CIWIN	Critical Infrastructure Warning Information Network
DDS-alpha	Disinformation Data Space
DSA	Digital Services Act
DMA	Digital Markets Act
EDMO	European Digital Media Observatory
EEAS	European External Action Service
EESCM	Enhanced and Extended Supply Chain Management
ENISA	European Union Agency for Cybersecurity
EC	European Commission
EU	European Union
FIMI	Foreign Information Manipulation and Interference
GDPR	General Data Protection Regulation
GECHO	Gatekeeping ECHO chambers
IMI	Information Manipulation and Interference
MS	Member state
NGO	Non-governmental organisation
NIS2	Directive Network and Information Security 2 Directive
STIX	Structured Threat Information Expression is a language and serialization format used to exchange cyber threat intelligence
TTPs	Tactics, Techniques, and Procedures
WINS	What information needs to be shared