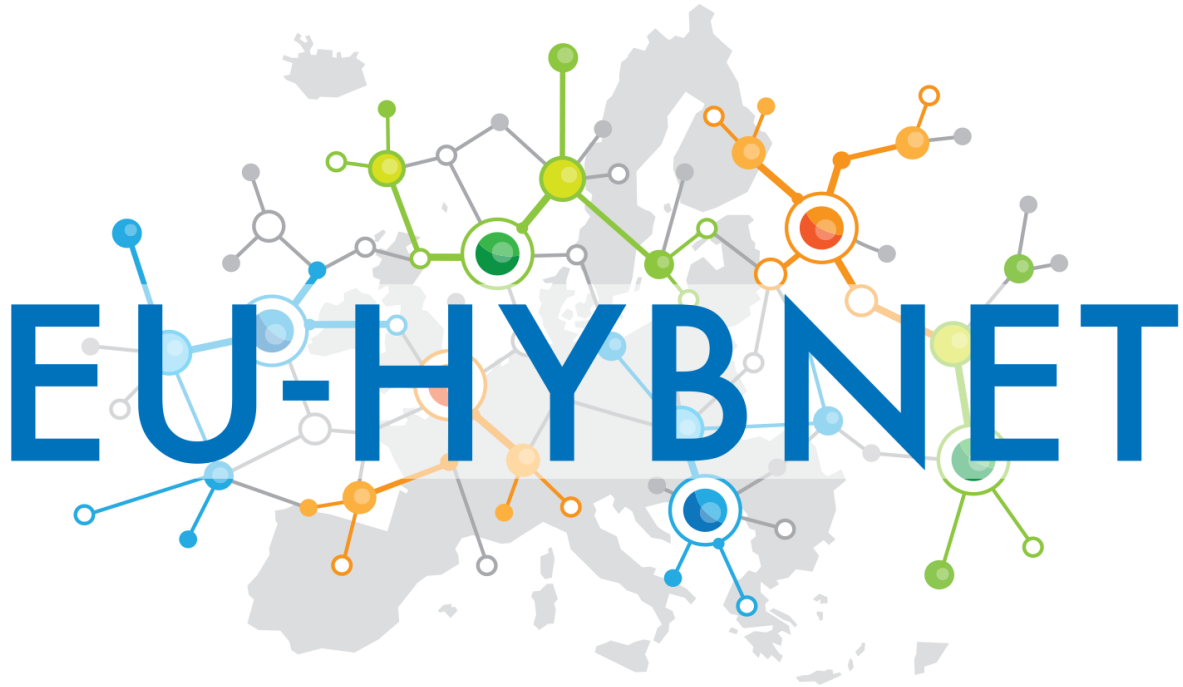


SECOND MID-TERM REPORT ON INNOVATION AND RESEARCH MONITORING

Lead Author: L3CE

Contributors: Laurea, PPHS, RISE, KEMEA, COMTESSA, TNO, Satways
Deliverable classification: PUBLIC

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

D3.9 SECOND MID-TERM REPORT ON INNOVATION AND RESEARCH MONITORING

Task number	T3.3	
Deliverable number	D3.9	
Version:	1.1	
Delivery date:	30/10/2023, resubmitted 4/12/2023	
Dissemination level:	Public (PU)	
Classification level:	Public	
Status	FINAL	
Nature:	Report	
Main authors:	Rimantas Zylius	L3CE
Contributors:	Jarmo Seppälä, Päivi Mattila	LAU
	Malgorzata Wolbach, Magda Okuniewska	PPHS
	Rolf Blom	RISE
	Athanasios Kosmopoulos, Alexios Koniaris	KEMEA
	Son Pham	COMTESSA
	Edmundas Piesarskas	L3CE
	Souzanna Sofou	Satways

DOCUMENT CONTROL

Version	Date	Authors	Changes
0	07-10-2023	L3CE/ Rimantas Zylius	Table of Contents, structure of the document, descriptions of gaps&needs Initial contributions of partners reviewed
0.1	13-10-2023	All partners	Updated contributions of partners reviewed
0.5	17-10-2023	L3CE/ Rimantas Zylius	Initial draft prepared, all partners' contributions structured
0.6	18-10-2023	L3CE/ Rimantas Zylius	Prepared for review
0.9	19-10-2023	L3CE/ Rimantas Zylius	All contributions incorporated, submitted for EU-HYBNET review
1.0	27-10-2023 30-10-2023	L3CE/ Rimantas Zylius Laurea/ Päivi Mattila	Incorporated comments from the EU-HYBNET peer review. Final review. Document prepared for submission to EC. Document submitted to the EC
1.1	04-12-2023	Laurea/ Päivi Mattila	Document re-submitted to the EC for review again. From KEMEA team a name of a colleague who also contributed to the D3.9 delivery (Mr. Alexios Koniaris) was missing and the name was now added to the document history.

DISCLAIMER

CONTENTS

1. INTRODUCTION

The Empowering a Pan-European Network to counter Hybrid Threats (EU-HYBNET) project's Description of Action (DoA) Part A document describes this deliverable (D) 3.9 "Second mid-term Report Innovation and Research Monitoring" as part of EU-HYBNET Task 3.3 *"Ongoing Research Projects Initiatives Watch"* as follows:

Task focuses on gathering the information of research and innovation projects relevant to EU-HYBNET with a view of delivering material for T3.1 and finally WP4 to compile recommendations for an uptake or industrialization of innovations and standardization. Innovation and Research Projects Monitoring will be performed e.g. with partners information exchange actions and gathering relevant information from available entities, organizations and RTO Networks accessible through the partners networks in the ways of targeted surveys and where possible by exploiting existing solutions for technology driven research and innovation scanning and monitoring. (T3.3) contributes strongly to the GM-01 call medium term impact Nr1 and Nr2.

The importance of this Deliverable in the context of U-HYBNET Work Package (WP) 3 "*Surveys to Technology, Research and Innovations*" for EU-HYBNET and the interactions with other Tasks is depicted in the Figure below.

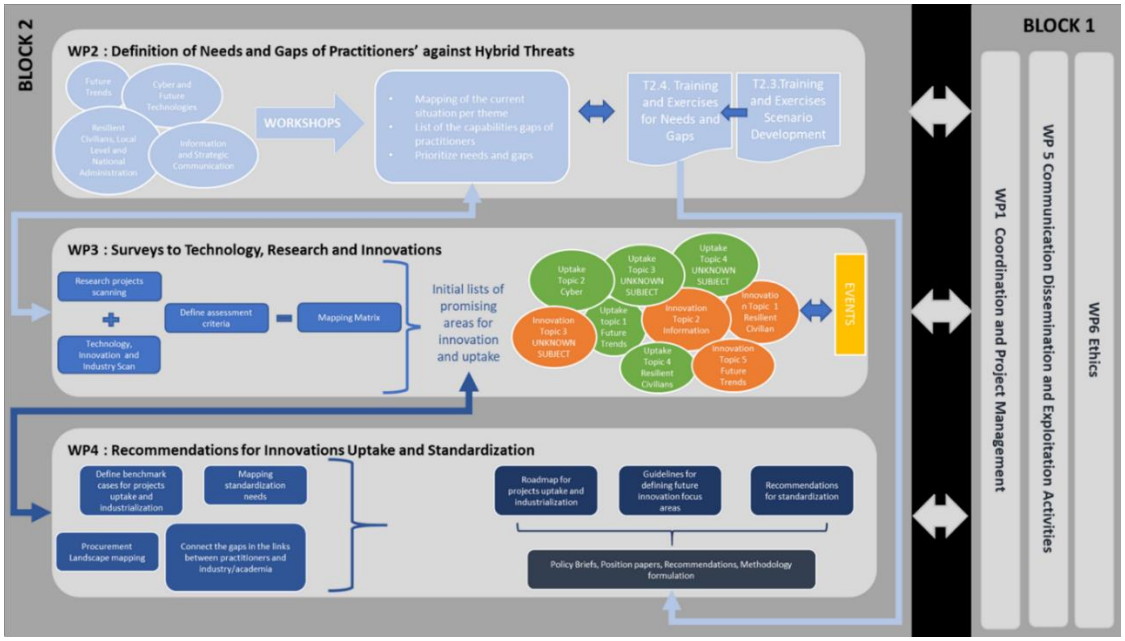


Figure 1 : EU-HYBNET structure of Work Packages and Main Activities

1.1 OVERVIEW

OBJECTIVES OF THE DELIVERABLE

EU-HYBNET's Task (T) 3.3 "*Ongoing Research Projects Initiatives Watch*" deliverable "Second Report on Innovation and Research project Monitoring" (D3.9) focused on scanning scientific research area, defining the status of the knowledge of the researched phenomena, which were identified in the EU-HYBNET's Gaps and Needs deliverable (D2.11) "Deeper analysis, delivery of short list of gaps and needs".

It aims to build understanding on the activities of EU funded projects related to identified areas, possible cooperation areas with EU-HYBNET.

D3.9 extends the method used in D3.8, second iteration of *Ongoing Research Projects Initiatives Watch*. Innovation scan will discuss state of play in the field, identify concepts, tools, technologies, or solutions which were developed or are under development in EU funded research projects that have potential of addressing identified gaps.

Note: focus of this deliverable are the innovations under development or testing. Therefore, only innovations before the widespread adoption in their field would be considered, as otherwise they become a subject matter of EU-HYBNET Task (T) 3.2. "*Technology and Innovations Watch*".

The material that was used in T3.3 is "open access" and generally available, in other words, EU-HYBNET will not use classified or restricted project and research material.

STRUCTURE OF THE DELIVERABLE

This document describes scan results for hybrid threats on the following core areas:

- Section 1: Introduction to the deliverable and work conducted
- Section 2: Core Theme: Resilient Civilians, Local Level and Administration
- Section 3: Core Theme: Cyber and Future Technologies
- Section 4: Core Theme: Information And Strategic Communications
- Section 5: Core Theme: Future Trends of Hybrid Threats
- Section 6: Conclusions

METHODOLOGY

EU-HYBNET "Deeper Analysis, Delivery of Short List of Gaps and Needs" document (D2.11) (further in the text – Gaps & Needs) serves as an input for the scan. D2.11 is structured according to the EU-HYBNET project four Core Themes (Future Trends of Hybrid Threats; Cyber and Future Technologies; Resilient Civilians, Local Level and National Administration; Information and Strategic Communications). In D2.11 three areas and dimensions to each of the Core Themes has been identified. These areas and three dimensions are:

- Critical Threat discusses context and dynamics which create playing field for the threat.
- Critical Gap defines what capabilities are missing which would allow to mitigate this treat
- Critical Need defines what innovations, be they technological, organizational, societal or other, are needed in order to build capability, which was discussed in "Critical gap" section.

Gaps & Needs document defines overly broad areas, which encompasses a variety of intertwined phenomena, complex dynamics of specialized subject matter and hybrid threats. Furthermore, Gaps and Needs document is restricted, so it cannot be quoted in this deliverable, which has classification of "Public".

Thus, as a starting point, for the purposes of this deliverable, broadly described areas and phenomena in Gaps & Needs document were redefined to narrow down to specific aspects, to which scanning was further focused.

In general process of this deliverable consists of the following steps:

1. Areas defined in Gaps and Needs document with Critical Threat / Critical Gap / Critical Need, were narrowed down to specific phenomena on which further research has to be performed. Deliverable sticks to the Critical Threat / Critical Gap / Critical structure but focuses on specifically chosen phenomena which preferably would have substantial "hybrid" angle.
2. This redefined subject area was operationalized into relevant searchable keywords.

3. The description keywords were then used to scan EU funded research projects in The Community Research and Development Information Service (CORDIS) and other relevant sources.
4. Relevant projects were selected, analysed and relevance to the research area described, linking research phenomena to the project deliverables or planned deliverables of the project.
5. Recommendations on observations of project development produced.

2. CORE THEME: RESILIENT CIVILIANS, LOCAL LEVEL AND ADMINISTRATION

Focus of this Project Core Theme in the current iteration is increasing fragility of democratic countries by habituating spread of violence in the political process, disrupting social structures and undermining institutions.

2.1 RESEARCH AREA: SPREADING VIOLENCE

DEFINITION OF THE RESEARCH AREA

Today, society experience violence to express political and religious dissent and violence has in certain situations become more or less accepted and can sometimes even be considered mainstream in the public sphere and as consequence has led to a gradual habituation. This is true for violence in all its forms e.g., verbal, physical or symbolic.

The multiplicity and various natures of violence make it difficult to grasp the full extension of its use. It extends from private behaviors of citizens on the Internet, honor-based abuse/oppression, incendiary political speeches, to violent extremism and terrorism. This reveals a common and worrying radicalization of social behaviors, challenging the cohesion1 of European societies and undermining trust in their social contracts2.

THE CRITICAL THREAT

The threat is the escalating recourse to violence as a means of conveying political dissent, aggravating social divisions, and causing more severe political conflicts with the intent of destabilizing society. Violence is often used in combination with other tools in the hybrid threat toolbox, aiming for destabilization of democratic societies and potentially push societies to the brink of collapse, dismantling representative democracy and replacing it with alternative governance paradigms.

THE CRITICAL GAP

Lack of

- societal in depth understanding at all levels (civilian, local level, administration) of what makes societies more susceptible to violence,
- situational awareness of ongoing and planned violent activities to express political dissent,
- institutional capacities to respond to the threats and activities.

This is true in general, but in certain areas and for certain aspects in these areas such awareness exists, e.g., in the areas of radicalization, violent extremism and terrorism.

THE CRITICAL NEED

The three gaps described brings the following needs:

[1] Social cohesion is a state of affairs concerning both the vertical and the horizontal interactions among members of a society, as characterized by a set of attitudes and norms that include trust, a sense of belonging, and the willingness to participate and help, as well as their behavioral manifestations, in *Reconsidering Social Cohesion: Developing a Definition and Analytical Framework for Empirical Research*

[2] Social Contract Theory is the idea that society exists because of an implicitly agreed-to set of standards that provide moral and political rules of behavior, see https://ethicsunwrapped.utexas.edu/glossary/social-contract-theory

- Handling of the root causes for why todays' societies are more susceptible to violence. Here we need more knowledge with respect to how to build social cohesion and strengthen the social contracts. This knowledge would then allow improving institutional design and governance of societal services which in the long run, hopefully, prevent the adoption of violent behaviour and actions in society.
- Establish situational awareness solutions, networks of information sharing, in which planned and ongoing violent activities of political dissent are monitored. There is a need to, in real time, observe events of violence, analysing and categorizing their intent, proposing and implementing suitable interventions and continuously present the results in formats adapted for all relevant stakeholder groups. Situational awareness is a prerequisite for the possibility to intervene.
  To collect relevant violence related events and to build situational awareness it is especially important to monitor what is happening in the information domain as it the mayor means (hybrid) threat actors use to cause disruptions and instigate violence. Special attention should be given to social networking services, online platforms and chat fora, and the Darknet as well as mobile phone communications.
- Establish institutional capacities to respond to the violent threats and activities. Most of the countries do have legislation to which criminalizes violence, but experience shows that it practically can be applied too late, when violence is out of control. To achieve this the anti-violence legislation in all member states should be updated and aligned and law enforcement would need to have the resources for necessary interventions. This tends to be results of policymaking process rather than research, thus, will not be further considered in this review.

RESEARCH AND OTHER RELEVANT OBSERVATIONS

To stop the adoption of violent behaviour and actions in society is a very difficult task and relies on actions in many different domains. Direct actions, e.g., to try to stop recruitment into extremist groups is one way to go and is necessary in the short term. Such activities are already implemented. But on a longer term there is a need to strengthen the social contract between citizens and society. Here the *EC 2023 Strategic Foresight Report*[3] points at the following challenges relevant in this context:

- **Increasing cracks in social cohesion**: eroding social cohesion will threaten trust in governments and the viability of the transitions;
- **Threats to democracy and existing social contract**: democracy is increasingly challenged as the main form of governance to deal with growing socio-economic issues, while the existing social contract is not fully fit for the new socio-economic reality.

We note that there are important initiatives within the EU to promote social cohesion and strengthen the social contract across its member states: 1) The *EU Cohesion Policy*[4] helps to ensure there are no gaps between countries and between different areas and regions in the same country. It supports key EU goals, such as the green and digital transition. 2) *The European Committee for Social Cohesion*[5] (CCS) is a Council of Europe intergovernmental committee mandated to work in the area of social cohesion. It conducts activities aimed at building inclusive societies in which everyone can enjoy their social rights, especially those guaranteed by the *European Social Charter*[6]. The Committee's work places a particular emphasis on vulnerable groups, persons with disabilities and young people.

[3] https://commission.europa.eu/strategy-and-policy/strategic-planning/strategic-foresight/2023-strategic-foresight-report_en

[4] https://ec.europa.eu/regional_policy/2021-2027_en

[5] https://www.coe.int/en/web/european-social-charter/european-committee-for-social-cohesion

[6] https://www.coe.int/en/web/european-social-charter/about-the-charter

To strengthen the social cohesion and the social contract a number of research domains/directions have to be considered. General aspects on these issues can be found in the following papers/sites:

- Social Cohesion in Europe, Literature Review[7]
- Measuring and validating social cohesion: a bottom-up approach[8]
- Social Cohesion Radar[9]
- The Concept of the "Social Contract"[10]

Below we provide a list of such research areas with references to some relevant project:

- **Trust and Social Capital** are key ingredients in strengthening the social contract. Studies have shown that societies with higher levels of trust and social capital tend to have robust social contracts. Chapter 10 in the OECD publication *For Good Measure Advancing Research on Well-being Metrics Beyond GDP* is on *Trust and Social Capital*[11]
- **Institutional Design** is important as institutional capacity to promote cohesion is strengthened when organisations are representative and take collaborative and co-productive approaches to developing whole community responses. Studies relate to the impact of government policies, the legal framework, and the role of institutions addressing societal needs and ensuring fairness and justice.
- **Civic Engagement, Political Participation and Community Involvement** are ways to strengthening the social contract. Studies have shown that active participation in civil society help individuals feel connected to society and have a voice in shaping its direction.
- **Economic Conditions** are strongly related to social cohesion. Studies on income and wealth inequality shows their relevance in maintaining a strong social contract.
- **Social Justice and Human Rights**: Legal scholars and human rights experts have conducted research on the principles of social justice and human rights, which are foundational to the social contract. This research often focuses on the protection of individual rights and freedoms, equal access to opportunities, and the promotion of justice and fairness.
- **Cross-Cultural and Cross-National Studies**: Comparative research across different countries and cultures has provided valuable insights into variations in the social contract and the factors that influence it. Such studies help identify best practices and policies that can be adapted to different contexts.
- **Behavioural Economics** explores how individuals make decisions and choices. Understanding human behaviour and decision-making processes in a cultural and psychological context of issues such as poverty, use of public goods, implementation of new programs, and so on, can be more effective both in terms of successful design and adoption of policies and interventions as they can be aligned with individuals' motivations and preferences.

SOCIAL COHESION

Search of the Cordis database produced limited number of projects that have overarching objectives in the areas of social cohesion and social contracts. Below a few relevant projects.

[7] https://www.britishcouncil.org/research-insight/social-cohesion

[8] https://www.oecd.org/dev/pgd/46839973.pdf

[9] https://www.socialcohesion.info/concepts/concept/bertelsmann-stiftung

[10] https://www.idos-research.de/en/social-contract/

[11] Algan, Y. (2018), "Trust and social capital", in Stiglitz, J., J. Fitoussi and M. Durand (eds.), *For Good Measure: Advancing Research on Well-being Metrics Beyond GDP*, OECD Publishing, Paris, https://doi.org/10.1787/9789264307278-12-en

UNI_SEL, Universalism or selectivism? What citizens think about the institutional design of the future welfare state?

Start date 1 October 2021, End date 31 May 2024
Web: https://cordis.europa.eu/project/id/101023631

The social legitimacy of universal vis-à-vis selective welfare provision systems remains very much an open question. UNI-SEL explores cross-national, experimental and longitudinal data to identify under which circumstances (when, where and why) one social policy design option is more popular than the other.

The findings will benefit the institutional design of the future welfare state as it will clarify the social legitimacy of universal vis-à-vis selective welfare.

ENGAGE, Engage Society for Risk Awareness and Resilience

Start date 1 July 2020, End date 31 December 2023
Web: https://cordis.europa.eu/project/id/882850

ENGAGE contributes to the target to make cities and human settlements inclusive, safe, resilient and sustainable. The setting is that society have to cope with hazards, requiring that all individuals specifically and the civil society at large, acquire the ability to rapidly respond to natural disaster and to man-made risks. The ability of societies to adapt and prosper depends on the collective action of the whole society. ENGAGE will show how individuals and local practices can interrelate effectively with planned preparedness and response, practitioners and technology and study the significant role citizens and communities play at the grassroots level. It will create innovative new ways of fostering trans-disciplinary collaboration and learning across disciplines.

The ENGAGE results will have relevance for how to build civic engagement, political participation and community Involvement as well as for institutional design.

POLAR: Polarization and its discontents: does rising economic inequality undermine the foundations of liberal societies?

Start date 1 April 2020, End date 31 March 2025
Web: https://cordis.europa.eu/project/id/833196

POLAR studies if the trend of increasing economic inequality in Western societies is leading to societal problems, and when, to which extent and in what respects rising inequality may affect the nature of our societies. POLAR specifically examines patterns of social mobility, the extent of social cohesion, and the level of trust in democratic institutions. It also investigates to which extent rising inequality may interfere with societies' capabilities to allocate positions according to merit and talent, to engage in cooperative social relations, and to decide on political matters through fair and transparent democratic processes.

The POLAR results will thus be relevant for understanding the role of economic conditions as the project will provide new empirical evidence on the purportedly negative relationship between inequality and social mobility, support for democracy, and social cohesion in the West.

PERGAP: The (Mis)Perception of Economic Inequality: The Impact of Welfare State Institutions on Social Perception and Preference Formation

Start date 1 December 2022, End date 30 November 2027
https://cordis.europa.eu/project/id/101042125

PERGAP will create a unique country-comparative dataset on institutional disparities and expand knowledge of the (self-)legitimizing mechanisms of public institutions. Different countries' social security systems provide

different answers to the questions “who receives what and why?”, and “who should get what and why?”, which ultimately shape the way citizens see and justify the existing inequalities in society. Ultimately, it will lead to a comprehensive theoretical and empirical understanding of the impact of public institutions on social perceptions and preference formations.

The rise of economic inequality in countries around the globe is causing societal and political concern. The project results will contribute to cross-cultural and cross-national studies, bringing a better understanding of how individuals’ perception and response to inequalities varies between societies and social groups and how it influences civic engagement and community involvement.

Finally, we point at the CORDIS Result Pack on *Challenges to democracy in Europe: Insights into a complex and turbulent political climate*[12]. There, issues related to the challenges to globalisation, personal freedoms, the reliability of information and, ultimately, the ability of democratic institutions to cope with the rapidly changing societal demands are discussed. These issues added up to a tumultuous decade for European democracy, that saw the rise of populist movements, anti-European sentiments fuelling disintegration pulsion, and growing grassroots protests over a number of issues, ranging from racism to economic disparity. The result pack includes references to a number of projects related to building social cohesion and robust social contracts.

SITUATIONAL AWARENESS ON VIOLENCE

The second area in which actions are required to cope with political violence and violence in general is focussed on situational awareness of where, when and how violence is used. There are a many organizations, initiatives and projects that focus on fighting against radicalization and violent terrorism within the EU and globally. In EU-HYBNET deliverable D4.5, *Second Innovation uptake, Industrialisation and Research Strategy*[13] , the *Setting the scenes* section in chapter 4.4 *Identify and Safeguard Vulnerable Individuals* describes EU initiatives, activities and research projects, gives an overview of the area fighting against radicalization and violent terrorism. Drawing on the conclusions from that work we found that stakeholders trying to cope with political violence and violence in general are missing:

- A platform for online real-time situational awareness of use of violence. The platform should comprise functions for real-time sharing of available information.
- AI based tools for rapid and accurate discovery of new sites related to use of violence. Monitoring of activity levels at known sites and visits by new users.
- A standardized taxonomy which is accepted by stakeholders together with standardized formats for descriptions, their coding and communication.
- Automatic identification and rapid launch of prepared countermeasures and human interventions online and IRL, based on validated frameworks and methods.

That AI based techniques for identifying activities on the internet by analysis of text-based speech is e.g., proven by the work reported in the paper *A Machine Learning Approach to Identify Toxic Language in the Online Space* by Lisa Kaati et al. We also found two services for that track conflicts around the world. The International Crisis Watch publishes *Crisis Watch* an online map indicating where the conflict levels change. It also publishes an EU Watch List, updated twice per year, that identify where the EU and its member states can help enhance prospects for peace. ACLED, the Armed Conflict Location & Event Data Project is a disaggregated data collection, analysis, and crisis mapping project. ACLED collects information on the dates, actors, locations,

[12] https://cordis.europa.eu/article/id/422249-challenges-to-democracy-in-europe-insights-into-a-complex-and-turbulent-political-climate

[13] To be published

fatalities, and types of all reported political violence and protest events around the world. The ACLED team conducts analysis to describe, explore, and test conflict scenarios, and makes both data and analysis open for free use by the public.

In the CORDIS database, we have found the following relevant projects related to the above-described needs.

PaCE: Populism And Civic Engagement – a fine-grained, dynamic, context-sensitive and forward-looking response to negative populist tendencies

Start date 1 February 2019, End date 30 April 2022
Web: https://cordis.europa.eu/project/id/822337

PaCE will analyse the causes, rise, specific challenges to liberal democracy, transitions related to leadership changes and consequences of these movements. PaCE will propose responses and develop risk analyses for each type of movement and transition by employing an agent-based simulation of political processes and conducts.

The project developed an open source tool relying on machine learning algorithms for identifying and tracking populist narratives. The tool is not limited to populist narratives, it can be used to search for any topics in any language e.g., use of violence. It is also will result in specific interventions aimed at: the public, politicians, activists and educators. It also looked into the future and developed new visions concerning how to respond to populism.

ViEWS – a political Violence Early Warning System

Start 1 September 2022, End date 29 February 2024
Web: https://cordis.europa.eu/project/id/101069312

ViEWS is a political violence early warning system. Predicting political violence is useful for first responders and policymakers and ViEWS is a tool for research on high-quality forecasts of political violence. The project will design a plan to explore the system's societal potential and financial viability and will describe how to maximise the system's functionality for conflict prevention and mitigation, preserve and strengthen transparency and open-access publication strategies.

This project is interesting as it is an example of how prediction methods can be developed and used for conflict prevention and mitigation.

ODYCCEUS: Opinion Dynamics and Cultural Conflict in European Spaces

Start date 1 January 2017, End date 30 June 2021
Web: https://cordis.europa.eu/project/id/732942

ODYCCEUs sought conceptual breakthroughs in Global Systems Science, including a fine-grained representation of cultural conflicts based on conceptual spaces and sophisticated text analysis, extensions of game theory to handle games with both divergent interests and divergent mindsets, and new models of alignment and polarization dynamics.

The project gives an interesting example of an open modular an open-source platform that integrates tools for the complete pipeline, from data scraped from social media and digital sources to visualization of the analyses and models developed by the project.

2.2 RESEARC AREA: ATTACK ON SOCIAL STRUCTURES

DEFINITION OF THE RESEARCH AREA

The intensified geopolitical tensions and competition between superpower for economic and military hegemony has brought about several changes in the security environment. In the current situation, nations are trying to influence rival nations in many ways. A particularly effective means is to influence the rival nations from within, i.e. via social institutions, which enable adversaries to shake the foundations of society.

One of the foundational elements of democratic societies is academic freedom. That is, people working in academia have freedoms of "research, teaching, learning and communication in and with society without interference nor fear of reprisal" (European Commission, 2022, p. 21). Additionally, researchers are committed to several other principles of good research practice, such as research integrity and research ethics. Recently academic freedoms and principles have become more threatened due to radically changed geopolitical situation and intensifying competition for power and influence between democratic and authoritarian countries (China, Russia, Iran). Authoritarian governments have exploited the openness and naivety of Western European higher education institutions (HEIs) to infiltrate their agents into the core institutions of European society.

THE CRITICAL THREAT

Higher education institutions are targets and channels of diverse hybrid interferences by foreign actors, such as influencing on-campus activities (topics, speakers, etc.), obtaining sensitive information, online targeting (based on undesirable research themes) and pressuring the administration of HEIs. Institutions are vulnerable because of the open nature of campuses and the ubiquity of research collaboration. HEIs are respected institutions, which exert considerable authority in societies. Affecting their operation could serve the objectives of adversaries in several ways. The objectives of the adversaries include retrieving information, influencing decisions and undermining values (European Commission, 2022, p. 16).

Potential means consist of pressuring and exploiting individuals in strategic positions, who can be students, researchers, staff, authorities or politicians; cyber-attacks on digital networks or databases of HEIs to acquire access to sensitive information; dissemination of disinformation to have an influence on the topics of research and issues under discussion; participating in joint projects to gain access to sensible or intellectually valuable information; and granting financial donation to create economic dependencies to leverage later at a strategically opportune situation to affect decisions.

THE CRITICAL GAP

HEIs are not properly prepared to identify and act against hybrid interference as the threat is not seen as relevant or topical for them. Therefore, there is a lack of capability to recognize and prepare for such incidents. In addition, HEIs do not have sufficient tools to monitor this kind of activity. The EC, individual Member States and several HEIs have published various guidelines on how to manage cooperation with international partner HEIs and how to counter foreign interference in research and innovation activities. The guidelines are an important stepping stone to improved security of HEIs, but they are insufficient as such. Their main shortcomings are that they focus on official international cooperation, such as student exchange, inter-organizational partnerships or focus exclusively on interference originating from China. These perspectives ignore the unofficial and unlawful interference as well as operations coming from other countries (e.g., Russia).

THE CRITICAL NEED

The main needs are to produce comprehensive guidelines for HEIs to tackle foreign interference that take into account the changed security environment and the wide variety of hybrid threats. The guidelines should be

complemented with a Europe-wide database of cases of hybrid interference within HEIs as well as a library of best practices to tackle foreign interference. These tools would allow security practitioners, particularly intelligence and police authorities, to be more informed about the current situation and give advance warnings to HEIs at times of increasing hybrid interference activity.

RESEARCH AND OTHER RELEVANT OBSERVATIONS

In order to identify related projects, we conducted several searches (search terms: foreign/hybrid interference, academic/scientific espionage) in the Cordis database with the following search terms: "foreign interference", "hybrid interference", "academic espionage", and "scientific espionage". The searches did not result in the identification of any relevant projects. However, a search "foreign interference" directed us to two relevant topics in Horizon Europe Work Programmes: *Detecting, analysing and countering foreign information manipulation and interference,* and *Protection of Higher Education Institutions and research organisations against conventional and non-conventional threats*. The former is a topic in this year's (2023) Horizon Europe Work Programme 2023-2024 (HORIZON-CL2-2023-DEMOCRACY-01-01) and its funding decisions were made in July. However, no information about the funded projects is yet (on 19 September 2023) available. The latter was a topic (HORIZON-WIDERA-2021-ERA-01-50) in the Horizon Europe Work Programme 2021-2022. Based on the title of the topic, the funded projects under this call would have been highly interesting for our research purposes but surprisingly no proposals were submitted to this call.

To widen our perspective outside Cordis, we conducted many searches by using Google to find other relevant projects. Those searches provided further confirmation to our previous understanding by showing that the topic of foreign interference in HEIs is important and highly topical following the recent exposures of researchers working for Russia. That said, we could find only a few projects and initiatives on the topic, which is confusing considering the attention that has been paid to the threat of malign foreign activities in the form of published guidelines as discussed above.

The Countering Foreign Interference (CFI) project

It is an EU-funded project (funded by the Service for Foreign Policy Instruments) that started at the beginning of this year. The FCI project focuses on improving understanding of potential threats in the information space. It will utilize accumulating knowledge for developing improved tools and methods to identify, monitor and counter those threats. More specifically, the project will contribute to enhancing the EU's and Member States' capabilities and resilience towards foreign information manipulation and interference to support the European way of life and fundamental values. Thereby, the aims of the CFI project could involve matters related to interference in research and innovation but since the project has not produced publications, it cannot be verified[14].

Mutual Learning Exercise (MLE)

During this year MLE has started based on the European Commission's publication ***Tackling R&I foreign interference***[15]. The MLE is funded by EC's Policy Support Facility for Horizon Europe and has three focus areas, which all are relevant to the topic of this analysis: Awareness raising and stakeholder engagement, Understanding and identifying foreign interference threats, and Measures to counter foreign interference threats. Due to the relatively short running time so far of the MLE, it has not yet published reports

[14] https://www.iss.europa.eu/projects/countering-foreign-interference

[15] https://www.zsi.at/de/object/project/6522

on its progress. The MLE of foreign interference will organize a dissemination event in the spring of 2024 and it will end in November 2024[16].

In the meantime, we suggest that the progress and outputs of the MLE should be monitored. The MLEs produce typically several thematic reports that will offer up-to-date information about their progress. Therefore, we expect the upcoming reports of the MLE on Tackling R&I Foreign Interference will present additional insights on the identification of foreign interference and new innovative means to tackle such hybrid threats.

The EU Knowledge Network on China (EU-KNoC)

EU-KNoC initiative's objective was "to create an R&I Knowledge Network on China that connects European networks, centres, and experts working on China." It was launched by the EC's DG for Research and Innovation in the summer of 2020 and ended in autumn 2021. The initiative's work has continued in a follow-up project for EU-KNoC. The concrete outcomes of the original EU-KNoC initiative were a list of recommendations for future collaboration with China[17], which could be used as a benchmark for other partner countries as well. The recommendations included topics such as: information sharing considering specific needs of EU-MS, strengthening transparency of European cooperation activities with China, identifying common priority areas for cooperation, and toolbox for supporting STI [Science, Technology and Innovation] cooperation with China. In addition, EU-KNoC published a study *Annotated Collection of Guidelines and Meta-Checklist supporting the safe and successful international science and technology cooperation* in 2021 (Klueting et al., 2021). The latter publication has been updated by DLR in 2022 (Heinrichs & Klueting, 2022[18]C:\Users\paikuos\Downloads\ "https:\www.science-diplomacy.eu\wp-content\uploads\2022\09\annotated-collection-2022.pdf"). The follow-up project of EU-KNoC collected information about the security measures in the European HEIs and RPOs through a survey at the beginning of 2023[19]. The results of the survey have not been published so far, or they are not publicly available, but they will be very interesting for their potential usefulness for countering hybrid threats in research and innovation.

As the EU-KNoC's review of guidelines (and DLR's updated version) has found out, there are dozens of different manuals published by individual higher education institutions, governments, and the EU. Most of the existing guidelines to tackle foreign interference in R&I have focused on China or been country-neutral with a general view on internationalization or a limited view on human rights, dual-use or export control (see DLR's document, Heinrichs & Klueting, 2022). Considering the recent cases of foreign interference, there is a specific and urgent need to produce guidelines for R&I interference from Russia. It has turned out that Russian spies have been able to develop credible fake identities that have not been detected before they have started employment or even worked longer time in European HEIs. This implies that the EU and the Member States must take the threat of foreign interference in HEIs more seriously because the cases are not always easily recognized. The EC's Staff Working Document *Tackling R&I Foreign Interference* (European Commission, 2022, p. 20) suggests that "additional tools may need to be developed (including context-specific risk assessments, checklists, screening mechanisms, and best practices) to support HEIs and RPOs in identifying and addressing gaps." These efforts would benefit from at least one of EU-KNoC's recommendations (slightly modified from the original EU-KNoC recommendation, see list of recommendations for the future collaboration with China above), which is building a continuous monitoring mechanism of foreign interference activities in

[16] https://era.gv.at/governance/era-forum/mutual-learning-excercises/; https://www.zsi.at/de/object/project/6522

[17] https://data.consilium.europa.eu/doc/document/ST-1204-2021-INIT/en/pdf

[18] https://www.science-diplomacy.eu/wp-content/uploads/2022/09/annotated-collection-2022.pdf

[19] https://eua.eu/partners-news/1001-survey-on-existing-approaches-for-responsible-international-r-i-cooperation-by-higher-education-institutions-and-research-performing-organisations-in-europe.html; https://survey.dlr-pt.de/index.php?r=survey/index&sid=596249&lang=en

the EU. The monitoring would entail information sharing between the Member States. Over time the monitoring mechanism would develop into a database of known cases of foreign interference in R&I in the European HEIs. This kind of database would also benefit from a collection of best practices that will be done in the MLE on foreign interference. A comprehensive database would serve the information needs of the pan-European security practitioners, in particular intelligence and police authorities.

REFERENCES

European Commission (2022), Tackling R&I foreign interference: Staff working document. Directorate-General for Research and Innovation Publications Office of the European Union. (https://data.europa.eu/doi/10.2777/513746)

Heinrichs Gerold & Klueting Laura (Eds.) (2022), Annotated collection of guidance for secure and successful international R&I cooperation. 2022 update. DLR-PT. (https://www.kooperation-international.de/fileadmin/user_upload/annotated-collection-2022.pdf)

Klueting Laura, Skorzinski Ena, Dierkes Nicola & Heinrichs Gerold (Eds.) (2021), Analysis of current and publicly available documents on securing international science cooperation. EU Research and Innovation Knowledge Network on China. (https://www.kooperation-international.de/fileadmin/user_upload/GuidelinesAnalysis-2021.pdf)

2.3 RESEARCH AREA: UNDERMINING INSTITUTIONS' INTERNAL ORGANISATION

DEFINITION OF THE RESEARCH AREA

Undermining institutions' internal organisation focuses on mistrust of personnel to share information in strategic security institutions, not only inside the institution but also with other relevant institutions and agencies, ministries and authorities. Next to mistrust, lack of motivation caused by the organizational culture and esp. culture of secrecy may harm the most successful proceeding in the strategic institutions' work and pathway for adversary's influence inside the organization.

THE CRITICAL THREAT

If organizations do not have traceability in information sharing or well identified or established work flow and processes, it leaves room for less precise and prompt measures that may harm the organization inside. Furthermore, unclear processes and being acknowledged of achievements may lead to lack of motivation and to prevent organizations' internal development to more precise and prompt actions. This may further prevent cooperation between various of institutions and organization that is much asked in countering hybrid threats.

THE CRITICAL GAP

On the whole, culture of secrecy and lack of clear processes of strategic institutions may support hostile foreign actors to introduce, conduct and expand their malevolent actions inside the organizations and in this way also to harm the security institution(s) and whole society. What is asked for is less politicisation of the administration, more openness in information sharing and workflow in organizations but also between strategic institutions and trust in cooperation and gaining jointly results.

THE CRITICAL NEED

It is seen that empowered cooperation between different strategic institutions and in internal working flow processes is needed in order to minimize risks deriving from organizations' internal structures and manners. Therefore, best practices on strategic institutions or multi-Agency/ministry/authority cooperation may deliver requested solution (e.g. there could be question of institutional security frameworks designed by national intelligence communities according to specific threats to fill). Also enhanced information sharing possibilities (technological and non-technological solutions) between the actors inside the organization but also with other relevant organizations is seen to deliver needed solutions - this may include information sharing platform alike better exchange of information, evaluation of risks, training and control between traditional security ministries. Also new approaches from legal perspective to enhance the cooperation may deliver needed answer to the identified threat – when mandate to information sharing exists it will support the cooperation.

RESEARCH AND OTHER RELEVANT OBSERVATIONS

We researched projects from the Cordis database by using several terms relevant to the topic (Collection: Projects; Domain of Application: Security/Society; Programme: H2020, horizon Europe), yielding several relevant results. In addition, we looked for relevant projects funded by European Union Members States and European Union different Agencies and Offices. After an initial analysis of the potential projects, we selected the following projects that had a fruitful fit with our point of view and thereby offered a notable potential for further development and co-creation.

RELEVANT PROJECTS – ENHANCED INFORMATION SHARING BETWEEN STRATEGIC SECURITY INSTITUTIONS – TECHNOLOGICAL SOLUTIONS

It is expected that information sharing platforms for strategic security institutions would provide not only needed tools for information sharing inside the organization but also between the institutions. The platforms are also to increase cooperation between actors and to increase traceability and trust alike motivation for the cooperation due to enhanced results.

This type of platforms for various security authorities and institutions and to their internal alike joint use have been developed in various EC funded projects in different security domains. The projects mentioned below provide insights what type of platforms have been successfully developed and how they are seen to support enhanced information and workflow(s) inside and between the institutions.

EUCISE2020/ European test bed for the maritime Common Information Sharing Environment in the 2020 perspective. GA No. 608385

Duration: 2014 – 2018
Web: **https://cordis.europa.eu/project/id/608385**

The main goal of EUCISE2020 has been to develop and to build a "Common Information Sharing Environment" (CISE) to European Union Member States (EU MS) various security maritime authorities in order to support their cooperation by using a dedicated platform for information sharing. In short, CISE is a service platform that is able to ensure interoperability among the legacy systems of EU MSs and maritime sectors of EU MS authorities based on agreed roles and rules. The CISE has been involving c. 60 European maritime authorities from 16 states, and the international and cross-sectorial information exchange network is currently operating among 12 nodes both national and European. Furthermore, the CISE has supported to (i) improve the harmonisation of intersectoral maritime awareness (ii) ensuring the EU MSs the direct control in the management of the information shared through the CISE intersectoral node and national nodes. Present CISE is hosted by EMSA/ European Maritime Security Authority and its' development will continue as mentioned in the "Strategic Compass for Security and Defence". This all speaks on behalf of its

valuable approach to support multi-sectoral and multi-agency/institution information sharing needs in order to gain better awareness and cooperation in maritime security. While CISE has been focusing on maritime authorities' information sharing needs, the CISE approach can also be copied and developed to serve other security authorities' needs too. Due to the successful use of maritime CISE, the EC has granted funding also to other projects to build CISE for authorities focusing on security concerns in land borders and custom. The projects are ANDROMEDA and CONNECTOR.

ANDROMEDA/ An EnhaNceD Common InfoRmatiOn Sharing EnvironMent for BordEr CommanD, Control and CoordinAtion Systems. GA no. 833881

Duration: 2019 – 2021
Web : **https://cordis.europa.eu/project/id/833881**

The main goal of ANDROMEDA has been to benefit on the European Union's Common Information Sharing Environment (CISE) approach, and how with the support of CISE information may be shared seamlessly with a range of third actors, including police agencies and defence forces. In ANDROMEDA CISE is making different systems interoperable so that data and other information can be exchanged easily via modern technologies. ANDROMEDA will leverage on the developments, results and experience of CISE that is also partly gained in EC projects such as PERSEUS, CloseEye, MARISA, RANGER.

Due to the success in CISE (maritime security authorities) and ANDROMEDA (land borders), also pan-European custom authorities has been interested in having similar system. Due to this noticed need a project called CONNECTOR has just been grant EC Horizon Europe funding. The CONNECTOR will kick off during October 2023.

CONNECTOR - Customs extended interoperable Common information sharing environment.
GA No. 101121271

Duration: 2023 – 2025

CISE is not only to support various pan-European security authorities to increase their cooperation, but it also empowers the cooperation in national level due to the development of national nodes. In short, without the cooperation between the national security institutions and authorities in the specific security domain (e.g. in maritime domain/ border guards, navy, police, customs) development of the solution/CISE national node would not have been possible. In short, the pan-European CISE has pushed national security authorities and institutions to find and definite new ways of cooperation and information sharing reducing partly also the culture of secrecy between institutions and inside the institutions. An example of increased cooperation between national *strategic security institutions* is a FINCISE project from Finland **FINCISE 2.0 Project** CISE | The Finnish Border Guard (raja.fi) (Duration: 2022 -2024) where all Finnish Maritime Cooperation (FIMAC) authorities joined to CISE development and finding new ways for future cooperation.

On the whole, the takeaway from the above mentioned CISE projects' is that the approach seems to work in various security domains and hence also hybrid threats related security authorities could consider to develop CISE for their purposes. Furthermore, CISE seems to support cooperation between strategic security institutions and diminish culture of secrecy between institutions, also in the institution.

What comes to platforms that support especially strategic security institutions' internal information sharing culture in different positions and parts of administration to proceed, esp. in a case of crises, a platform developed in an EC funded project STOP-IT, aims to this. Even though STOP-IT focuses on delivering a solution for authorities in water security and management, still the STOP-IT platform may provide an example to any other security domain and their institutions and authorities incl. hybrid threats.

STOP-IT - Strategic, Tactical, Operational Protection of water Infrastructure against cyber-physical Threats GA No. 740610

Duration: 2017 – 2021
Web: https://cordis.europa.eu/project/id/740610

STOP-IT has delivered an integrated, modular platform that supports strategic/tactical planning, real time operational decision making and post-action assessment for the key parts of the water infrastructure. Furthermore, the platform is scalable (scaling from small utilities to large ones); adaptable (including various modules addressing different needs, with expandability for future modules); and flexible (the utility managers can decide how to use it and it will be usable by experts, novices, and even non-technical staff). On the whole, the platform support to enhance cooperation skills and trust between the users because its use provides exercise(s) that may then ease the cooperation in the future in real cases. The platform has been developed to three different user categories in and organizations, but it can also host multi-agency/ institutions discussion and planning. The categories in the platform are: Decision Makers; Risk Officers and Modellers; Real Time Operators and Maintenance Managers.

RELEVANT PROJECTS – ENHANCED INFORMATION SHARING BETWEEN STRATEGIC SECURITY INSTITUTIONS – NON-TECHNOLOGICAL SOLUTIONS SUCH AS TRAININGS & EXERCISES, BEST PRACTICES, LEGAL MANDATE, ETC.

As highlighted in the chapters above, technological solutions may be part of the solution how to decrease barriers in information exchange and culture of secrecy and to increase cooperation, but still also solutions that will bring real connections between the authorities to work together are also called for. Such solutions are trainings and exercises in order to learn on different security institutions' ways to work. Moreover, legal aspects such as mandates for cooperation may deliver needed solution too.

As mentioned above CISE has delivered a technological solution to increase cooperation in information sharing between various security authorities, as well as supported joint exercises and multi-authority trainings in order to enhance the joint actions for the security concerns. The trainings and exercises normally also increase trust between the actors and ease the cooperation in the future. This kind of best practice on Multi-Agency Cooperation between maritime security practitioners (border guard, police, custom, various ministries and agencies) can be recorded from Finland next to CISE[20]. Furthermore, the cooperation has been supported by updates in the legal operational mandate for the enhanced cooperation between various authorities[21]. Therefore, all these issues are much needed to empower the cooperation, share information and to build trust between various security institutions. In a case of hybrid threats, this lesson is also recorded from Finland where multi-agency cooperation has been highlighted as a central tool to counter hybrid threats[22].

Third Phase of the Consultation Forum for Sustainable Energy in the Defence and Security Sector, EDEN, (CF SEDSS III

Duration: 2019 – 2023
Web : https://eda.europa.eu/what-we-do/eu-policies/consultation-forum/phase-iii
Web: https://eda.europa.eu/docs/default-source/events/eden/annex-a-conf-prog-23-24-11-21.pdf

Similar positive experiences on enhanced cooperation and trust, also possibility to learn other organizations' manners to react have been part of European Defence Agency (EDA) EDEN project that included exercise based

[20] https://merivoimat.fi/-/merireittiemme-toimivuuden-varmistajat-saman-poydan-ymparilla
[21] https://raja.fi/monialaisiin-merionnettomuuksiin-varautumisen-yhteistoimintasuunnitelma
[22] https://intermin.fi/en/national-security/hybrid-threats

on approaches in CORE Model[23]. According to the training & exercise experience, the CORE Model was seen much to support the understanding between various authorities and enhancing their cooperation. Therefore, approaches and methodologies to support strategic institutions to enhance their cooperation and information sharing, also building trust among actors, are much underlined are solid innovations to counter hybrid threats.

NOTIONES - Interacting network of intelligence and security practitioners with industry and academia actors GA No. 101021853

Duration: 2021 – 2026
Web: https://cordis.europa.eu/project/id/101021853

Security frameworks designed by national intelligence communities according to specific threats to strategic institutions may also support to overcome the challenges in cooperation and information sharing. An EC funded project NOTIONES may deliver some views to this while at present the project merely focuses on technological solutions to security practitioners', and especially needs of intelligence services. After all, the key activities in NOTIONES are to build and maintain a pan-European ecosystem of security and intelligence practitioners in order to (**1**) monitor technologic opportunities and advancements and best practices and (**2**) define and refine requirements and standardization needs. NOTIONES project will last until 2026 and hence solutions that will serve to build security framework by national intelligence may be gained through the project.

[23] https://joint-research-centre.ec.europa.eu/jrc-news-and-updates/new-method-help-policymakers-defend-democracy-against-hybrid-threats-2023-04-20_en

3. INNOVATION AND RESEARCH PROJECTS MONITORING. CORE THEME: CYBER AND FUTURE TECHNOLOGIES

3.1 RESEARCH AREA: STEALING DATA ATTACKING INDIVIDUALS

DEFINITION OF THE RESEARCH AREA

Broadly speaking, privacy is the right to be let alone, or freedom from interference or intrusion. Information privacy is the right to have some control over how your personal information is collected and used[24]. Here we are interested in informational privacy. To maintain informational privacy, this information should be stored so it can only be accessed, by authorized parties, i.e., information and cybersecurity solutions must be used. With access to personal information there are risks for identity theft, credit card fraud, getting access to private and/or work-related confidential data and doxing.

Kaspersky[25] defines doxing as: Doxing is the act of revealing identifying information about someone online. That information is then circulated to the public — without the victim's permission. Examples of doxing information are: Real name, Home addresses, Workplace details, Personal phone numbers, Social security numbers, Bank account or credit card information, Private correspondence, Criminal history, Personal photos, Embarrassing personal details. Doxing attacks can range from the relatively trivial, such as fake email sign-ups or pizza deliveries, to the far more dangerous ones, like harassing a person's family or employer, identity theft, threats, or other forms of cyberbullying, or even in-person harassment. Not to forget the risk of credit/debit card and investment frauds by criminals. Doxing is also used as threat in coercion activities against politicians and Civil Society Organization activists and is one tool in the hybrid threat toolbox.

We first note that personal data is becoming massively available and transparent due to voluntary sharing in social networks and in different other for a, as well as by the personal information requested by authorities in their services and which then is made available in public directories. To collect this information is what is known as an OSINT (Open Source INTelligence) operation. OSINT is defined as intelligence produced by collecting, evaluating and analysing publicly available information with the purpose of answering a specific intelligence question.

Secondly, we note that some personal information should, as stated above, be stored securely and only be accessible by authorized persons. To get access to such stored information, some kind hacking activity must be performed. One could say that an INTelligence operation has to be performed and here INT means that you try to find information which should be kept confidential.

To provide privacy there need to be a legal framework and techniques and solutions to support its implementation in all information systems handling personal information. Within the EU, we have GDPR which goals are to enhance individuals' control and rights over their personal information and to simplify the regulations for international business. Most countries also have strict laws on how personal health data should be handled. We also note that specific laws against doxing are being implemented in e.g., some US states, Hong Kong and are under discussion in Europe.

When it comes to supporting techniques, we see two strands of solutions. The first is to implement standard information and cybersecurity solutions. This area has been researched for many years and there are a large variety of research projects in the CORDIS database covering most aspects. The second area is to use privacy enhancing techniques (PET), technologies that embody fundamental data protection principles by minimizing

[24] From International Association of Privacy Professionals: https://iapp.org/about/what-is-privacy/
[25] From Kaspersky: https://www.kaspersky.com/resource-center/definitions/what-is-doxing

personal data use, maximizing data security, and empowering individuals and privacy preserving techniques (PPT). That PPT is seen as an important technique is corroborated by the existence of the UN Handbook on Privacy Preserving Computational Techniques[26].

THE CRITICAL THREAT

The threat posed by obtaining and using sensitive personal information is that the right to privacy is violated and that this information can be made public on the Internet, i.e., used for doxing, coercion, criminal and fraudulent purposes. Doxing and coercion are known tools in the hybrid threat toolbox.

THE CRITICAL GAP

The gap is insufficient cybersecurity and privacy protection in many IT systems handling personal and sensitive information. Access to sensitive personal information is often achieved by hacking, giving rise to large data leaks. The root cause of a hacking success may be insufficient security controls in the information handling system and in operational procedures, which sometimes depend on the use of old systems. To achieve the necessary security level, it may be required to upgrade the computational environment and the operational procedure to current state of the art.

Although legal restrictions may not stop all publication of private and sensitive information, an EU common legal framework for investigating and taking action against such publication of private information and doxing is missing. This as an addition to the existing GDPR legislation. Here it should be noted that to be effective, laws have to be enforced and sufficient resources for investigations and prosecution has to be in place.

THE CRITICAL NEED

The most important need is the implementation of up-to-date industrial standards for cybersecurity in all IT systems and in particular for those handling personal and sensitive information. The required knowledge to do this already exists. What is missing is awareness, resources and willingness.

The second most important need is to bring awareness to the population about the risks on the internet and of voluntary sharing of sensitive information on social media and other platforms.

The third need is to develop and deploy available and new PET and PPT to increase the resilience against leaking sensitive personal information from registers and databases.

RESEARCH AND OTHER RELEVANT OBSERVATIONS

In the cordis database thematic packs of topics highlighted. The packs include reference to the projects on which the theme is based.

For the implementation of up-to-date industrial standards for cybersecurity in in all IT systems and in particular for those handling personal and sensitive information the thematic pack we first refer the pack named *Securing cyberspace: Concrete results through EU research and innovation*[27] (Last update: 17 December 2018). This pack also includes results within the area of online privacy. As stated in the end of the description: These projects, of course, provide just a glance at what EU researchers are currently working on. Many cybersecurity related projects have been started after the pack description was published. Searching the Cordis database for projects mentioning privacy with start date from 2020-01-01 and onwards gives a list of more than 500 projects. There are more the 80 projects starting in 2023. The same search for cybersecurity results in more than 380 projects

[26] ibid

[27] https://cordis.europa.eu/article/id/400141-securing-cyberspace-delivering-concrete-results-through-eu-research-and-innovation

while a search with privacy and cybersecurity gives 135 projects. Thus, the available knowledge base is huge and increasing and the results will improve privacy cybersecurity solutions in the future. Still, the guidance needed for implementing high cybersecurity is readily available in industrial standards and best practices, e.g., from ENISA and CISA[28] (Cybersecurity & Infrastructure Security Agency) in the US.

In this context of we also want to point at all cybersecurity related information and activities available at ENISA[29] and in particular their efforts to develop cybersecurity certification at EU level[30], with the goal to harmonise the recognition of the level of cybersecurity of ICT solutions across the Union. Ongoing work are the following three schemes: 1) The European Certification Scheme on Common Criteria (EUCC), which initially targets ICT products such as hardware and software products and components. 2) The European Certification Scheme for Cloud Services (EUCS). 3) The European Cybersecurity Certification Scheme for 5G (EU5G) and a first draft should be available for public consultation at the end of 2023. Related regulations, proposed and in force, are e.g., 1) the Directive for a High Level of Cybersecurity across the Union (NIS2), focusing on critical infrastructure, 2) the proposed regulation on electronic identification and trust services for electronic transactions in the internal market (eIDAS Regulation) with the Wallet regulation, 3) the proposed Cyber Resilience Act (CRA) which adds cybersecurity to criteria for obtaining a CE marking, and 4) the proposed Artificial Intelligence Act.

In the EU, ENISA drives awareness raising campaigns[31] pointing at the need for safe and secure use in our digital world the development of safe and secure IT products and services. The ENISA stated aim is to raise cybersecurity awareness and promote behavioural change. An interesting guide from ENISA is the ENISA Do-It-Yourself Toolbox: AR-in-a-Box[32] – A guide to creating your own awareness raising program. Another example of such a program is the CISA driven Secure Our World Cybersecurity Awareness Campaign[33] which aims to make all Americans across the cyber ecosystem part of their national cyber defence by adopting essential cybersecurity habits. A search in the Cordis database shows that no projects with focus on raising cybersecurity and/or privacy have started after 2020.

The development of PET and PPT solutions to improve the privacy of personal data are of great interest and is supported by the EU. There are several different techniques explored in the research out of which we see the following as important: 1) Use of homomorphic ciphers to allow operations on ciphered data in registers and databases to e.g., allow collecting statistics without knowing the data in plaintext format (for more information on homomorphic ciphers, see Wikipedia[34]. 2) Use of secure multi-party computation has the goal of creating methods for parties to jointly compute a function over their inputs while keeping those inputs private (for more information on secure multi-party computations, see Wikipedia[35]. Finally, we note that federated learning, i.e., training an AI machine learning algorithm, for instance a deep neural network, on multiple local and private datasets contained in local nodes without explicitly exchanging data samples (for more information on federated learning, see Wikipedia[36]. In the area of PET and PPT we have identified the following relevant research projects:

[28] https://www.cisa.gov/topics/cybersecurity-best-practices

[29] https://www.enisa.europa.eu/

[30] https://certification.enisa.europa.eu/

[31] https://www.enisa.europa.eu/topics/cybersecurity-education/?tab=details

[32] https://www.enisa.europa.eu/topics/cybersecurity-education/awareness-raising-in-a-box

[33] https://www.cisa.gov/secure-our-world

[34] https://en.wikipedia.org/wiki/Homomorphic_encryption

[35] https://en.wikipedia.org/wiki/Secure_multi-party_computation

[36] https://en.wikipedia.org/wiki/Federated_learning

FLUTE, Federate Learning and mUlti-party computation Techniques for prostatE cancer

Start date 1 May 2023, End date 30 April 2026
Web: https://cordis.europa.eu/project/id/101095382

FLUTE will demonstrate the practical use of federated learning and multi-party computation techniques having health data hubs located in three different countries.

Flute will provide an example of a novel federated AI toolset to provide privacy protection, pushing the performance envelope of secure multi-party computation, used for diagnosis of clinically significant prostate cancer.

SECURED, Scaling Up secure Processing, Anonymization and generation of Health Data for EU cross border collaborative research and Innovation

Start date 1 January 2023, End date 31 December 2025
Web: https://cordis.europa.eu/project/id/101095717

SECURED demonstrate technologies developed in health-related use cases like real-time tumour classification, telemonitoring for children and access to genomic data. It will do this by increasing efficiency, scaling up multi-party computation, data anonymisation and synthetic data generation, focusing on private and unbiased AI and data analytics.

The results on how to increase efficiency in multi-party computation to allow private and unbiased AI and data analytics will be of great interest.

HARPOCRATES Data analytics and cryptography for privacy preservation

Start date 1 October 2022, End date 30 September 2025
Web: https://cordis.europa.eu/project/id/101069535

HARPOCRATES will design and demonstrate several practical cryptographic schemes (functional encryption and hybrid homomorphic encryption) for analysing data in a way that preserves privacy and enables a comprehensive approach where data analytics and cryptography are associated with increased privacy.

This project will advance the encryption techniques used for privacy protection and can become part of generic solutions.

PAROMA-MED, Privacy Aware and Privacy Preserving Distributed and Robust Machine Learning for Medical Applications

Start date 1 July 2022, End date 30 June 2025

Web: https://cordis.europa.eu/project/id/101070222

PAROMA-MED aims to develop novel technologies, tools, services and architectures for patients, health professionals, data scientists and health domain businesses so that they will be able to interact in the context of data and machine learning federations according to legal constraints and with complete respect to data owners' rights to privacy protection to fine grained governance, without performance and functionality penalties of ML/AI workflows and applications.

The project will develop a hybrid-cloud based delivery framework for privacy and security assured services and applications in a federative environment, in particular presenting privacy preserving processing and trusted data storage.

ENCRYPT, A Scalable and Practical Privacy-Preserving Framework

Start date 1 July 2022, End date 30 June 2025
Web: https://cordis.europa.eu/project/id/101070670

ENCRYPT will, based on different use cases, evaluate and validate Differential Privacy, Multi-Party Computation, Full Homomorphic Encryption (FHE) and Local Differential Privacy. The project will develop a scalable, practical, adaptable privacy-preserving framework, allowing researchers and developers to process data stored in federated cross-border data spaces in a GDPR-compliant way.

The project will address the limitations of the studied Privacy Preserving (PP) technologies in several aspects such as scalability and performance issues, by going beyond the single-key FHE paradigm. Furthermore, it will investigate the combinations of several of these PP methods. The improvements will be of general interest in the implementation of privacy preserving solutions.

SPATIAL: Security and Privacy Accountable Technology Innovations, Algorithms, and machine Learning

Start date 1 September 2021, End date 31 August 2024
Web: https://cordis.europa.eu/project/id/101021808

SPATIAL will address the challenges of black box AI and data management in cybersecurity. To do this, it will design and develop resilient accountable metrics, privacy-preserving methods, verification tools and a system framework to pave the way for trustworthy AI in security solutions.

SPATIAL will design and develop required critical building blocks to achieve trustworthy AI in security solutions. In particular, it will develop systematic verification and validation software/hardware mechanisms that ensure AI transparency and explainability in security solution development and system solutions that enhance resilience in the training and deployment of AI in decentralized, uncontrolled environments. Results will be of interest when designing future privacy preserving solutions.

3.2 RESEARCH AREA: ONLINE MANIPULATION ATTACKING DEMOCRACY

DEFINITION OF THE RESEARCH AREA

Cybersecurity of critical infrastructures is important vector for hybrid attacks. Disrupting functioning of critical infrastructures may be very important stepping stone of larger plan of hybrid attack.

Subject of protection of Critical infrastructure against cyberthreats is a well-established area with detailed regulation at national and EU levels, supported by huge professional knowledge base, advanced tools, fast growing cybersecurity profession, etc.

But for the disruption to occur, attack does not necessarily be successful. The reaction that defending party takes to the threat may cause disruption itself.

For hybrid perpetrators disruption of one or another infrastructure or service may not be an aim in itself, but only intermediate step which sets events in motion. What they are looking for is a specific impact to decision makers or society/public opinion. They may seek specific reaction, to incident rather than disruption of service itself.

They seek to destroy trust fabric of our societies, and for this aim variety of scenarios can be planned, including threats, fake incidents and other events which cause overreaction, or domino effects from overreaction (e.g. disruption of services caused by overreaction, rather than by incident itself).

"Threats of attack" is a well-known and widely used tool, which is handled by law enforcement (e.g. threats of explosion sent by email, etc.), and disruption caused by them is usually minimized.

THE CRITICAL THREAT

In this context we focus on fake-attacks, specifically tricking responsible parties to believe that hazard has occurred (by means of providing fake information, attacks on sensors, etc) which would trigger overreaction and further damaging consequences, may be used as powerful tool for hybrid attacks.

This falls clearly in the context of hybrid threats which organizations should be able to handle.

THE CRITICAL GAP

It is identified by practitioners, that risk assessment frameworks of organizations, incident handling preparations are focused on handling real incidents, while incidents fake attacks are not properly addressed and very often considered "false positives".

Thus, in case of it being hybrid attack, it may cause chain of reactions, but stay under the radar. If not properly researched, they may remain unnoticed lessons not drawn.

THE CRITICAL NEED

The need of practitioners is to strengthen ability of organizations to handle fake attacks:

- Risk assessment frameworks which include fake attacks (including impact assessment and management), practical guidelines for attribution of "false positives" to incidents
- Mitigation strategies of the fake attacks
- Awareness frameworks/tools which take into account capabilities recognition and handling of fake attacks
- Training strategies to handle fake attacks
- Check if projects of threat identification balance false negative with false positive identification (considering that false positive signals can be intentionally generated by adversaries)

RESEARCH AND OTHER RELEVANT OBSERVATIONS

Our research scan did not reveal research projects that would be specifically dedicated to the phenomena of fake attacks and their handling. It seems that it is considered still a practical discipline of the general preparedness framework, and decisions "real or fake" in the highly intense situation of limited awareness and time pressure is left to the experience and gut feeling of decision makers.

We thus collected EU funded projects which are not completed at the time of preparation of this deliverable, which deal with the hazard monitoring / mitigation, which should consider including in their scenarios early identification of false positives, considering that false positive signals can be intentionally generated by adversaries.

European System for Improved Radiological Hazard Detection and Identification, RADION

Start date 1 September 2020 - 29 February 2024

Web: https://cordis.europa.eu/project/id/883204

To better defend itself against chemical, biological, radiological, nuclear and explosive (CBRNE) attacks and threats, Europe needs a specialised, efficient and sustainable CBRNE protection scheme. The EU-funded EU-RADION project therefore aims to offer an innovative solution for some of the shortcomings that exist in CBRNE

protection. To this end, it will create an operational radiological threat detection and identification system consisting of several technological components. The components will include radiological threat dispersion modelling and analysis tools, test sensor platforms, including a swarm of mini unmanned ground vehicles, a tactical command tool, a network controller and a sensor integration unit. The project will play a role in improving European resilience against CBRNE attacks and threats.

Innovative Cluster for Radiological and Nuclear Emergencies, INCLUDING

Start date 1 August 2019 - 31 July 2024

Web: https://cordis.europa.eu/project/id/833573

Radiological and nuclear (RN) threats are more real than ever, and they know no borders. Safety in this field requires a wide collaboration of many actors. In Europe, the EU-funded INCLUDING project will build a dynamic cluster of 15 partners from 10 EU Member States acting in the INCLUDING Federation. An advanced web platform will shape a map of cooperation between governmental, security and medical institutions, industrial services and others. Partners will provide multidisciplinary knowledge, research, new technologies and infrastructure. Procedures will be formed for joint actions: field exercises, training and simulations. The project will be a base for a modern flexible network for better security in the RN field in Europe.

PReparedness against CBRNE threats through cOmmon Approaches between security praCTItioners and the VulnerablE civil society, PROACTIVE

Start date 1 May 2019 - 31 August 2023

Web: https://cordis.europa.eu/project/id/832981

Chemical, biological, radiological and nuclear (CBRN) risks represent a major concern for the EU. The role of professionals can be reinforced by preparation and civil society engagement. The EU-funded PROACTIVE project will evaluate the response of security professionals such as law enforcement agencies (LEAs) to the demands of civil society comprising vulnerable citizens. The estimation of the effectiveness of existing procedures will lead to innovative proposals for policymakers and security professionals and will support the EU Action Plan for CBRN threats. The project aims to create innovative tools, including an information platform for LEA use and a mobile app tailored to meet the needs of vulnerable groups.

4. INNOVATION AND RESEARCH PROJECTS MONITORING. CORE THEME: INFORMATION AND STRATEGIC COMMUNICATIONS

4.1 RESEARCH AREA: MEDIA CONUNDRUM

DEFINITION OF THE RESEARCH AREA

Whereas competition in general is considered conducive to promoting an increase in quality of provided services, the environment of increased competitiveness in which journalistic media is faced with today, is not to its advantage. Competition amongst media outlets in the form of click-bait practices with the intent of promoting their outlet over that of their competitors does not encourage quality journalism, as it other qualities rather than "quality journalism" prove to be main revenue drivers.

The social media environment has both positive and negative effects on the economic viability of investigative journalism. On the one hand, social media provides a platform for journalists to reach a wider audience and share their investigative work quickly. This increased visibility can attract more readers and potentially generate revenue through subscriptions or advertising.

However, the prevalence of free content on social media has also contributed to challenges for traditional media outlets. Advertisers often prefer targeted social media advertising over traditional outlets, impacting the revenue streams of investigative journalism. Additionally, the quick consumption of news on social media can undermine the in-depth nature of investigative reporting, potentially reducing the perceived value of such journalism.

Overall, while social media offers new opportunities for exposure, it poses economic challenges that news organizations must navigate to sustain quality investigative journalism.

THE CRITICAL THREAT

Countering disinformation, fact checking, as well as straightening up the debate and public discourse, all induce high costs. The added factor of having to compete for a market share with media outlets who rely mainly on click-bait practices consequently leads to the threat of depriving market shares from quality journalistic media. By quality journalistic media, what is meant is journalistic media with integrity, or else those outlets which actually place value upon opposing disinformation, ensuring fact checking, as well as straightening up the debate and providing a forum through which opinions and concerns regarding decisions and the decision-making process can be voiced.

If the threat of depriving market shares from quality journalistic media is not addressed, the resulting information domain hybrid threat of undermining and potentially influencing decision-making by not upholding the aforementioned journalistic values will continuously be present.

THE CRITICAL GAP

The identified gap therefore is the insufficient investment in (or funding of) true investigative journalism which, as mentioned in the threat, leads to a lack of true quality journalistic competitiveness (i.e. journalistic integrity), as opposed to competition in terms of which outlet will first transmit the story (i.e. speed of news coverage). It seems that readership charges alone are not able to sustain and reward quality journalism.

THE CRITICAL NEED

Successfully navigating models of quality journalism funding often requires a strategic approach and a deep understanding of the audience, market dynamics, and the specific challenges posed by the digital age and social media landscape.

In an everchanging environment, the need which arises therefore is the identification and sharing of best practices for economic sustainability of journalistic media.

A correct and accurate situational snapshot of the ways in which media can be sustained is required, to strengthen the economic model of journalism. Creating a register of good and best practices whereby media outlets have increased their economic viability without compromising content quality and journalistic investigations would therefore be beneficial, across the EU.

RESEARCH AND OTHER RELEVANT OBSERVATIONS

Several existing models which contribute to the economic viability of investigative journalism are the following:

- **Subscription Models:** Many news organizations are adopting subscription-based models, requiring readers to pay for access to high-quality investigative content. This helps generate direct revenue and reduces reliance on advertising.
- **Donations and Crowdfunding:** Some investigative journalism outlets rely on donations from individuals or crowdfunding campaigns to fund their work. This model fosters a sense of community support for independent and investigative reporting.
- **Collaborations and Partnerships:** News organizations may form collaborations or partnerships with other media outlets, NGOs, or even philanthropic organizations. Pooling resources can enhance the scale and impact of investigative projects.
- **Grants and Fellowships:** Investigative journalism organizations often seek grants from foundations, NGOs, or government agencies to fund specific projects. Fellowships may also be established to support journalists working on in-depth investigations.
- **Freemium Models:** Offering some content for free while requiring payment for premium or exclusive investigative pieces can strike a balance between accessibility and revenue generation.
- **Events and Conferences:** Hosting events, conferences, or workshops related to investigative journalism can serve as a revenue stream. Attendees may pay for tickets, and sponsors may be attracted to support such initiatives.
- **Syndication and Licensing:** Selling the rights to republish investigative content to other media outlets, both domestically and internationally, can be a source of income for news organizations.
- **Branded Content and Sponsorships:** Collaborating with brands or sponsors on investigative projects or producing sponsored content related to certain issues can provide financial support.
- **Digital Advertising:** While traditional advertising faces challenges, targeted digital advertising on news websites and social media platforms can still contribute to revenue.
- **Diversification of Revenue Streams:** Rather than relying on a single source of income, news organizations are increasingly diversifying their revenue streams to build resilience. This could include a combination of subscriptions, advertising, events, and grants.

None of them offers clear path for the media outlet to sustained funding of the quality journalism. Thus in this research we look into efforts to understand media market dynamics and develop knowledge of quality journalism funding.

RESEARCH AND OTHER RELEVANT OBSERVATIONS

Various EU projects were identified which are relevant to this topic and are involved overall with the sustainability of quality journalism, thus addressing also the gap and subsequent need of economic sustainability of journalistic media. A review of the available tools, concepts and methods also revealed various other European initiatives (relevant projects funded by European Union Member states, as well as European Union Agencies and Offices).

To identify relevant EU projects and initiatives that have been carried out to combat the threat mentioned above, the Cordis database was searched using the following keywords/terms (Projects; Domain of Application: Security/Society; Program: H2020): “sustainability of quality journalistic media” AND “viability of journalism” AND “economic sustainability of journalism”.

Harnessing Data and Technology for Journalism (JOLT), ID: 765140

From: 1 May 2018 to: 30 April 2022
Website: http://joltetn.eu/
Cordis: https://cordis.europa.eu/project/id/765140

JOLT aimed to deliver a world-class, multi-sectoral PhD research-training programme focused on harnessing digital and data technologies to advance economically sustainable and socially valuable journalism. Journalism is in profound crisis arising from declining advertising revenues, the dominance of US technology platforms, and the rise of online information-sharing including fake news. Journalism research has not kept pace with these changes. This is reflected in the lack of European, and indeed global, PhD programmes focussed on the intersections of journalism, data and technology. Europe lacks knowledge on the best-practice integration of data and digital technologies, strategies to overcome organization disruption, and on the political, social and ethical implications of digital journalism. JOLT addressed this lack by creating a multidisciplinary and multi-sectoral consortium of five leading European universities and twelve non-academic partners (four as beneficiaries) representing journalism NGOs, SMEs and large-scale media enterprises. JOLT’s training programme was grounded in the universities’ academic excellence and the complementarity of diverse non-academic partners. In addition to secondments with non-academic partners, all ESRs attended 3 industry workshops, 6 seminars on research and transferrable skills, and 3 summer schools, which drew on the cross-sectoral and multi-disciplinary expertise of all partners. JOLT’s key measurable outputs were much-needed open-source tools and technical protocols, 30 journal articles, 30 conference papers, 15 policy and best-practice guidelines, and extensive media outreach conducted in collaboration with JOLT’s media partners. JOLT acted as a pilot for the formalization of similar PhD programmes, creating a sustainable network of multi-disciplinary and cross-sectoral partners to advance research/innovation beyond the project, and support the renewal of a socially valuable and competitive European media sector.

MeDeMAP Mapping Media for Future Democracies, ID: 101094984

From: 1 March 2023 to: 28 February 2026
Website: https://www.medemap.eu/
Cordis: https://cordis.europa.eu/project/id/101094984

To set out future-proof pathways to strengthen democracy through improving accountability, transparency and effectiveness of media production and expanding active and inclusive citizenship, the project aims to clarify the extent to which certain media under which conditions perform which democratic functions for which audiences, thus making it apparent what is at stake for democratic media - and for democracy itself.

By applying an innovative multi-method design consisting of data science methods, large-scale quantitative analyses, in-depth qualitative approaches and participatory action research, the project will cover (1) perspectives of both representative and participatory notions of democracy as they exist in European societies, (2) the entire range of news media, regardless of distribution channel, mandate, ownership and source of

financing, (3) the legal and (self-)regulatory framework under which media houses and journalism operate and people use media, (4) the media's potential to promote and support political participation (supply side), and (5) the media use patterns, communication needs and democratic attitudes of the audiences (demand side) in all EU Member States.

Based on the research results, an interactive multi-layer map of European political information environments will be created, whose layers reflect the legal and regulatory framework and the democratically relevant features of media supply and demand. In addition, the obtained "real" map is to be confronted with a map of how European citizens envision the future media landscapes. By comparing these maps, conclusions can be drawn from congruencies and discrepancies between them, good practice examples can be identified and guidelines can be derived to support developments that promote democracy and counteract phenomena that may jeopardize democracy. These guidelines will be addressed to policymakers, regulators, self-regulation bodies, media houses, journalists, NGOs and citizens.

MeDeMAP could contribute to the identification and sharing of best practices for economic sustainability of journalistic media, even though it is mainly concerned with promoting democracy and counteracting phenomena that may jeopardize democracy. Since democracy in media and journalism is a crucial component of integrity and quality, the guidelines that will stem from the project will cover media use patterns and communication needs in all EU Member States, aside from the democratic attitudes, as mentioned in the project description. These media use patterns, but also communication needs, could provide invaluable insight into the steps required to lead to economic sustainability of journalistic media.

ReMeD RESILIENT MEDIA FOR DEMOCRACY IN THE DIGITAL AGE, ID: 101094742

From: 1 March 2023 **to:** 28 February 2026
Website: https://resilientmedia.eu/
Cordis: https://cordis.europa.eu/project/id/101094742

Resilient Media for Democracy in the Digital Age (ReMeD) responds to the European Commission's call HORIZON-CL2-2022-DEMOCRACY-01-06: "Media for democracy – democratic media" and will tackle existing challenges to a healthy relationship between media and democracy, by taking a bold approach to improve relations between citizens, media and digital technologies. With an interdisciplinary approach and an innovative methodology that combines qualitative and quantitative methods, ReMeD will gather, analyze, compare and contrast data on professional journalists, alternative media content producers and citizens operating in technologically mediated configurations, and on the media organizations, market structures and national and international regulations that underpin media production, circulation and consumption in the contemporary media landscape. ReMeD will work closely with all parties involved in order to co-produce high-impact knowledge and solutions that will contribute to the creation of resilient democratic media that reinvigorate, strengthen and uphold democracy, the rule of law and fundamental human rights. The project is particularly timely as ReMeD's results and policy recommendations will feed directly into the contemporary debates around the design and implementation of the Digital Services Act and Digital Markets Act.

ReMeD could contribute to the identification and sharing of best practices for economic sustainability of journalistic media, in the same way project MeDeMAP can.

By gathering, analysing, comparing and contrasting data regarding professional journalists, alternative media content producers and citizens which operate in technologically mediated configurations, as well as the media organizations, market structures and national and international regulations that underpin media production, circulation and consumption in the contemporary media landscape, ReMeD could, as a biproduct identify trends and qualitative indicators which could help better understand the demand of and thus the sustainability of quality journalistic media.

INJECT Innovative Journalism: Enhanced Creativity Tools, ID: 732278

From: 1 January 2017 **to:** 30 June 2018
Cordis: https://cordis.europa.eu/project/id/732278

INJECT's objective was to transfer new digital technologies to news organisations to improve the creativity and the productivity of journalists, to increase the competitiveness of European news and media organisations. To achieve this objective, INJECT extended and aggregated new digital services and tools already developed by consortium members to support journalist creativity and efficiency, and integrated the services and tools with current CMSs and journalist work tools in order to facilitate their uptake and use in newsrooms. The services undertook new forms of automated creative search on behalf of journalists, using public sources (e.g. social media) and private digital resources (e.g. digital libraries of political cartoons) to generate sources of inspiration for journalists who were seeking new angles on stories. The tools provide new interactive support for journalists to think creatively about new stories and reuse news content in new ways to increase productivity. To transfer the new services and tools to Europe's news and media organisations, INJECT established a new INJECT spin-off business, built up and expanded multiple vibrant ecosystems of providers and users of new digital technologies, and exploited its position at the heart of Europe's journalism industry to raise market awareness and take-up on the services and tools. With respect to Call ICT21, INJECT increased the competitiveness of one of Europe's most important creative industries – journalism - by stimulating ICT innovation in SMEs, by effectively building up and expanding vibrant EU technological ecosystems that met the emerging needs of Europe's new and existing news and media organisations.

RELEVANT EUROPEAN INITIATIVES

Media Pluralism Monitor (MPM): The MPM is an ongoing project that assesses risks to media pluralism in EU member states. It provides a comprehensive overview of the media landscape and highlights potential threats to media sustainability and diversity.
Website: https://cmpf.eui.eu/media-pluralism-monitor/

Media4EU: This initiative focuses on the sustainability of European media through research and policy recommendations. It aims to enhance media freedom, pluralism, and independence by fostering collaboration between media professionals, policymakers, and civil society.
Website: https://www.alda-europe.eu/progetto/media4eu/

Journalism Trust Initiative (JTI): While not an EU project, the JTI is an independent effort that has gained support from various European media organizations and stakeholders. It seeks to promote trustworthy journalism by establishing criteria for trustworthy media outlets, which can have implications for media sustainability.
Website: https://www.journalismtrustinitiative.org/

Creative Europe Program: The Creative Europe program, funded by the EU, includes initiatives that support the cultural and creative sectors, including media. It provides funding opportunities for media-related projects that contribute to cultural diversity and media sustainability.
Website: https://culture.ec.europa.eu/creative-europe

4.2 RESEARCH AREA: ANTAGONIZING VICTIMIZATION NARRATIVES IN THE INFORMATIONAL SPACE

DEFINITION OF THE RESEARCH AREA

In the age of information, narratives hold immense power. They shape our perceptions, influence our beliefs, and often dictate our actions.

Among the many narratives that have gained prominence in recent years, victimization narratives have been particularly pervasive. These narratives centre around the idea of individuals or groups portraying themselves as victims of injustice, discrimination, or oppression. While raising awareness about genuine issues is essential, the informational space has witnessed the antagonization of victimization narratives, where these narratives are weaponized, manipulated, or exploited for various purposes.

Victimization narratives have been an integral part of human storytelling for centuries. They serve a crucial role in highlighting societal injustices, fostering empathy, and driving positive change. When genuinely rooted in experiences of oppression or discrimination, they can lead to important social movements and legislative reforms. For example, the Civil Rights Movement in the United States was largely fuelled by the victimization narrative of African Americans who had suffered generations of systemic racism and segregation.

However, the rise of the digital age has transformed the way these narratives are constructed, disseminated, and consumed. The informational space, characterized by the proliferation of social media, online forums, and digital communication channels, has provided a platform for the rapid spread of victimization narratives. This newfound power of amplification has led to both positive and negative consequences.

Social media has empowered individuals who were previously ignored or silenced to share their stories and demand justice. The #MeToo movement, for instance, gained momentum through victimization narratives shared on platforms like Twitter and Facebook, leading to a global reckoning on issues of sexual harassment and assault.

However, the dark side of this amplification is the potential for victimization narratives to be manipulated or exploited. In the informational space, it has become all too common to witness the weaponization of victimhood.

THE CRITICAL THREAT

Threats can be realised in various forms:

Confirmation Bias and Echo Chambers: Social media algorithms often prioritize content that aligns with a user's existing beliefs and preferences. This can create echo chambers where victimization narratives are not subjected to critical scrutiny, leading to the reinforcement of biased views.

False or Exaggerated Narratives: In pursuit of attention or a particular agenda, some individuals or groups may fabricate or exaggerate victimization narratives. False claims can harm innocent parties and undermine genuine issues.

Political Manipulation: Victimization narratives are increasingly exploited for political gain. Politicians and interest groups may use these narratives to mobilize supporters, divert attention from other issues, or even scapegoat certain groups.

Cancel Culture: The online world has seen the rise of "cancel culture," where individuals are targeted and ostracized based on allegations or perceived wrongdoing. While this can hold those in power accountable, it can also lead to mob justice and the stifling of free speech.

THE CRITICAL GAP

The exploitation of victimization narratives can have far-reaching consequences, including the erosion of trust in media, increased polarization, and the suppression of constructive dialogue. It is essential to recognize the nuances surrounding these narratives and develop strategies to navigate the informational space more responsibly.

THE CRITICAL NEED

One strategy is to promote critical thinking and media literacy. Encouraging individuals to verify information, consider multiple perspectives, and question the validity of victimization narratives can help counteract the negative effects of confirmation bias and echo chambers. Schools and educational institutions play a crucial role in imparting these skills to young people.

Moreover, it is imperative for social media platforms to take responsibility for the content shared on their platforms. Algorithms that prioritize sensationalized or divisive content should be reevaluated, and mechanisms for fact-checking and content moderation should be improved to curb the spread of false narratives.

Additionally, media organizations and journalists have a responsibility to uphold ethical reporting standards. Fact-checking, thorough investigative journalism, and responsible reporting on victimization narratives can help maintain public trust and credibility.

Institutional accountability is another critical aspect of addressing the antagonization of victimization narratives. When individuals or groups exploit victimhood for personal gain or political agendas, they should be held accountable through legal channels. False accusations, defamation, and the incitement of hatred should not go unchecked.

Furthermore, it is essential to foster open and respectful dialogue. When confronted with conflicting victimization narratives, engaging in civil discourse rather than resorting to cancel culture can lead to a more productive exchange of ideas. Empathy and understanding should be the foundations of such conversations, as they can help bridge the gap between conflicting perspectives.

RESEARCH AND OTHER RELEVANT OBSERVATIONS

Understanding the Impact of Narratives and Perceptions of Europe on Migration and Providing Practices, Tools and Guides for Practitioners. PERCEPTIONS (HORIZON 2020 Grant agreement ID: 833870)

Narratives on a “better life” that can become reality elsewhere have always been shaping human migration. The image or idea of a “promised land”, however, might not be real, and newcomers are often faced with obstacles and challenges. Certain narratives and perceptions of Europe influence migration aspirations and false images can not only lead to problems when the image does not hold true, but it might also even lead to security threats, risks or radicalisation. It is, therefore, of the utmost importance to understand and investigate narratives about Europe, how these can lead to problems and threats, how they are distributed, and, in a next step, find ways to react and counteract on them. Perceptions on Europe are formed in the country of residence, and they are based on a multitude of sources. Social media and new communication networks, in addition, have increased the scope and the intensity of distribution of such narratives; and furthermore, so-called filter bubbles and echo chambers can lead to isolated misperceptions that are not corrected. Due to new communication technologies, false or incorrect claims become life on their own, raise expectations or disapproval. At the same time, however, these technologies and communication networks might also provide a channel to set an exaggerated image straight and to promote a more realistic narrative. It is, therefore, the aim of the PERCEPTIONS project to identify and understand the narratives and (mis-)perceptions of the EU abroad, assess potential issues related with the border and external security in order to allow better planning and

outline reactions and countermeasures. For that purpose, the project will conduct research on the narratives and the myths that are circulating about the EU in countries West- and Central Mediterranean area. Based on the research insights, the consortium will develop a PERCEPTIONS framework model including policy recommendations and action plans.

4.3 RESEARCH AREA: ATTACK ON INFORMATION

DEFINITION OF THE RESEARCH AREA

"AI model GPT-3 (dis)informs us better than humans "[37].

The term misinformation is not new; however, the research community has paid increasing attention since the recent development of so-called foundation models. A **foundation model** is a "paradigm for building AI systems" [38] in which a model trained on a large amount of unlabelled data can be adapted to many applications. Foundation models can contain trillions parameters. They are a form of generative AI[39]. The content produced by them, such as natural language texts, images, or videos, are challenging to distinguish from the one created by human. It has benefited many different industries and people in multiple ways.

THE CRITICAL THREAT

However, the potential of generative AI tools is increasingly being used for nefarious purposes by criminals, revealing the dark side of AI or foundation models to be more concrete. For example, several intriguing viewpoints were uncovered via a poll conducted in January 2023 among IT and cybersecurity decision-makers in businesses located in North America, the United Kingdom, and Australia. First, it was discovered that 53% of the respondents thought hackers might utilize ChatGPT to create phishing emails that were more convincing and official sounding. An additional 49% believed that the AI tool would be used for disseminating false information and for the purpose of helping less skilled hackers advance their technical expertise[40].

THE CRITICAL GAP

Diversity and outdatedness of systems and massive availability and transparency of personal data also support the dangers of AI while being taken advantage of. The attacker can use these data to generate malicious content with a foundation model with a technique called "prompt engineering."

Explainable AI has been a hot research topic for years, as it has tried to help people understand and interpret outputs made by AI models. However, it remains a very challenging problem. Now, with foundation models, this research topic is even more problematic. No algorithm can still detect the content generated by foundation models.

Foundation models are trained with billions of parameters, costing average organizations or institutions an enormous expense. Therefore, the research community has a massive problem while researching this topic.

[37] https://www.science.org/doi/10.1126/sciadv.adh1850

[38] https://crfm.stanford.edu

[39] https://aws.amazon.com/what-is/foundation-models/#:~:text=Foundation%20models%20are%20a%20form,%2C%20transformers%2C%20and%20variational%20encoders.

[40] https://www.statista.com/statistics/1378211/chatgpt-usage-cyber-crime-global/

THE CRITICAL NEED

Defining a code of practice for content moderation, protecting personal data, especially on social media platforms, are needed to counter the threat.

Furthermore, there is a need for counter tools, which can, for example, classify the content created by foundation models. Explainable foundation models could be another demand to make the model output more reliable. To do so, the governments need to support the research community with resources to do more research in foundation models.

RESEARCH AND OTHER RELEVANT OBSERVATIONS

NL4XAI - Interactive Natural Language Technology for Explainable Artificial Intelligence

Timeline: 01/10/2019 - 30/09/2024
Website: https://nl4xai.eu/

With the help of Explainable AI (XAI) systems, the project will address the problem of making AI self-explanatory and help transform knowledge into products and services for economic and social benefit. As a supplement to visualization tools, NL4XAI focuses on automatically creating interactive explanations in natural language (NL), as humans do naturally.

The project's output is interesting since it works directly with natural language. The foundation models, like GPT from OpenAI, LLaMA from Meta (Facebook), and PaLM from Google, are also large language models. Understanding them profoundly and constructing self-explanatory and reliable AI language models are needed to tackle the abovementioned threat.

TAILOR - AI systems made safe, transparent and reliable

Timeline: 01/09/2020 - 31/08/2024
Website: https://tailor-network.eu/

The goal of TAILOR is to establish a robust academic-public-industrial research network that can provide the scientific underpinnings for trustworthy artificial intelligence (AI) by leveraging and combining learning, optimization, and reasoning to create AI systems that incorporate safeguards that make them trustworthy, safe, transparent, and respectful of human agency and expectations.

This is another project considering the safety development of AI systems. The output can be later used for foundation models, more specifically. Within this project, the results of WP3 are highly relevant for the abovementioned threat-gap-need. The dimensions of the project - Explainability, Safety, Fairness, Accountability, Privacy, and Sustainability - are inextricably linked to the project's guiding principles through ongoing requirements and challenges to create approaches that balance value and legal protection. The question, which the WP3 addresses are:

- How can we guarantee user trust in AI systems through explanation?
- How to formulate explanations as Machine-Human conversation depending on context and user expertise?
- How to bridge the gap from safety engineering, formal methods, verification as well as validation to the way AI systems are built, used, and reinforced?
- How can we build algorithms that respect fairness constraints by design through understanding causal influences among variables for dealing with bias-related issues?
- How to uncover accountability gaps w.r.t. the attribution of AI-related harming of humans?
- Can we guarantee privacy while preserving the desired utility functions?

- Is there any chance to reduce energy consumption for a more sustainable AI and how can AI contribute to solving some of the big sustainability challenges that face humanity today (e.g. climate change)?
- How to deal with properties and tensions of the interaction among multiple dimensions? For instance, accuracy vs. fairness, privacy vs. transparency, convenience vs. dignity, personalization vs. solidarity, efficiency vs. safety and sustainability.

SHERPA - Shaping the Ethical Dimensions of Smart Information Systems

Timeline: 01/08/2018 - 31/10/2021
Website: https://www.project-sherpa.eu

HERPA project looked into, examined, and synthesized our knowledge of how ethics and human rights issues are affected by smart information systems (SIS; the fusion of artificial intelligence and big data analytics), working with a broad spectrum of stakeholders. The project:

- Described and represented the moral and human rights issues raised by intelligent information systems via case studies, scenarios, and creative representations.
- Collaborated with various stakeholders to determine their issues and ideal fixes (via stakeholder boards, Delphi studies, extensive internet surveys, and interviews).
- Created and published a workbook on the responsible development of smart information systems.
- Provided technical and regulatory options (such as a regulator's terms of reference).
- Used multi-stakeholder focus groups to validate and rank the proposals. Then, targeted dissemination and communication efforts to advocate for, promote, and implement the most promising solutions.

The project outputs are relevant to the addressed threat since they tackled the problem of protecting ethical aspects and human rights while developing smart information systems (AI and Big data). On their homepage, the two highly relevant guidelines are provided:

- Guidelines for the Ethical Use of AI and Big Data Systems[41]
- Guidelines for the Ethical Development of AI and Big Data Systems: An Ethics by Design approach[42]

[41] https://www.project-sherpa.eu/wp-content/uploads/2019/12/use-final.pdf
[42] https://www.project-sherpa.eu/wp-content/uploads/2019/12/development-final.pdf

5. INNOVATION AND RESEARCH PROJECTS MONITORING. CORE THEME: FUTURE TRENDS OF HYBRID THREATS

5.1 RESEARCH AREA: POLITICAL DEFICIENCY

DEFINITION OF THE RESEARCH AREA

EU's democratic processes, security and citizens are threatened through hybrid threats coming from various sources. Ever present disinformation, political cleavages, FIMI (Foreign Information Manipulation and Interference), not adequate level of media literacy among all age groups (depending on the country) – all these constitute a growing political and security challenge for the European Union. With local, national and upcoming European Parliament elections the threat is even bigger and hostile actions are intensifying. Both democratic and antidemocratic parties are, unfortunately, caught in this disinformation machine and very often use manipulative techniques in order to achieve their political goals.

THE CRITICAL THREAT

Within recent years we observed the terms 'disinformation' and 'fake news' to be more and more present in the public debate. On one hand it is positive as the emphasis is being put on media literacy and the message is clear: not everything we see or hear is in fact the truth. On the other hand those terms are overused and very often used inadequately to their meaning. It is being done so especially by politicians who brand 'fake news' every piece of information that does not support their political interests. Another thing is using fake, distorted, or unverified information in political campaigns against opposing party or candidate. Certain disinformation campaigns are created and disseminated by politicians. Others are being distributed by foreign sources and are picked up and publicized by politicians. Being done so, it leads to harmful distortion of reality and undermines democratic values. Voters are confronted with data which they are not able to or do not know how to verify. One thing that is becoming to be more and more visible is that some people do not mind fake news. When it fits their intentions, they are happy with fake news, they see it instrumentally.

THE CRITICAL GAP

The critical gap connected with the above is media literacy level and susceptibility of citizens to disinformation. It depends on different factors and is different in different countries but there are groups of vulnerable people that are extremely fragile and defenceless in the face of disinformation campaigns. They are attacked the most and these attacks are personalized in such a way to hurt them in an emotional way. These vulnerable groups may be for example elderly people, immigrants, unemployed, people with lower level of education or people with radical views. Whenever they are bombarded with news, opinions, political allegations or promises it hits them in an emotional way and, in addition to it, they are not able or do not want to verify it. Although there are numerous campaigns, actions, events, workshops etc. connected with countering disinformation, most of them tend to be focused on the overall society rather than being aimed at specific groups due to their disinformation vulnerability level.

THE CRITICAL NEED

Observing democratic values, using verified data and using promises that can be fulfilled, respecting one another including political opponents, promoting culture of listening and understanding is a much-needed step in political landscape. Until it is reached, we need to focus on prompting media literacy and critical thinking taking the approach of identifying especially those who are most vulnerable to disinformation and trying to reach them. Campaigns targeting the whole society are needed but not always effective. During political

elections, vulnerable groups can be identified and can be reached to make sure all citizens can make informed decisions.

RESEARCH AND OTHER RELEVANT OBSERVATIONS

Addressing the expressed Critical Need, we were looking for the projects addressing to most vulnerable citizens focusing on enhancing critical thinking and showing easy, practical ways of verifying information. Further, projects emphasizing national cohesion and European solidarity since many disinformation campaigns rely on anti EU slogans. Currently there are different projects focusing on media literacy also in political elections context. Some are very broad, addressing the public in a more general way, while others address highly targeted audiences.

Supporting vulnerable populations in combating disinformation and improving social participation, DesinfoEND

project duration: 1/02/2022-1/02/2024
web: https://desinfoend.eu/

The main purpose of this project is to promote the social inclusion of adults in a vulnerable situation through the acquisition of critical thinking and digital and media literacy skills.

The approach adopted by the project, which can be inspirational for other projects and actions connected with countering disinformation, is to define the groups of vulnerable individuals and boost critical thinking in those groups (Vulnerable populations defined in DesinfoEND: Unemployed adults, people with lower level of education, people aged 55+)

IMMUNE 2 INFODEMIC

project duration: 1/01/2023 – 31/12/2024
web: https://immune2infodemic.eu/

IMMUNE 2 INFODEMIC aims to immunise EU citizens against the disinformation and misinformation on selected themes by empowering and equipping them with several methods using eye-catching material and easy-to-use tools. The project consortium formulates and co-produces 3 instruments (vaccines): digital literacy, media literacy, critical thinking; and applies these instruments on 3 selected hot themes (boosters): elections, COVID-19 and migration.

The aspect that is especially interesting is the idea of being proactive (rather than reactive) and informing about disinformation action/campaign before it actually happens so that citizens are prepared before it starts.

5.2 RESEARCH AREA: NEW AGIT-PROP

DEFINITION OF THE RESEARCH AREA

Agit-prop refers to an intentional, vigorous promulgation of ideas. The term originated in the Soviet Union where it referred to popular media, such as literature, plays, pamphlets, films, and other art forms, with an explicitly political message in favour of communism[43]. In other words, "agit-prop" was related to propaganda and agitation techniques used to influence public opinion and promote specific political or social agendas. In contemporary times, the term "agit-prop" is still relevant and continues to evolve in response to new

[43] https://en.wikipedia.org/wiki/Agitprop

technologies, tools, strategies and communication methods to disseminate information and influence public sentiment.

THE CRITICAL THREAT

Agit-prop can involve the spread of false or misleading information to create confusion, manipulate public opinion, or discredit opponents. This can occur through fake news websites, bots, and viral disinformation campaigns. In today's world, representatives of anti-system movements and propagandists most often flatten the subject, finding conspiracy theories, foul deals and using populist messages, manipulate facts and spread false/incorrect information, hide the truth among a myriad of lies, and address topics that are already controversial, extreme left or right, thus polarizing society lowering public trust and this has a direct impact on the shape of future democracy.

THE CRITICAL GAP

Society as a whole is not prepared or appropriately informed by the media about emerging propaganda campaigns. Often journalists and the media are also unable to respond quickly and adequately to disinformation actions. Spreading propaganda and anti-system thinking among the public is often a long and arduous process, but unfortunately a feasible one, and the overall decrease in trust in the traditional media only exacerbates the problem. Globally, today's journalism faces several challenges, many of which, such as disinformation and propaganda, are the result of a rapidly changing media landscape, technological advances and evolving social dynamics. Moreover, the demand for real-time news on social media platforms has put pressure on journalists to report quickly, sometimes at the expense of thorough fact-checking and verification. Adapting to new technologies and platforms, can be not only challenging but overwhelming for media and journalists.

THE CRITICAL NEED

The digital age has made it easier for false information to spread quickly, and journalists must work diligently to verify facts and combat the spread of misinformation and disinformation. Trust in media has eroded with the public perceiving bias or political agendas in journalism therefore building and maintaining trust with audiences should be a constant challenge for journalists. Improving journalism and the media in the current environment requires a multifaceted approach that meets various challenges while maintaining the basic principles of ethical journalism. The long-term critical need is to restore democratic integrity through a sequence of initiatives focused on popularizing good practices among journalists and the media and equipping them with the necessary tools.

RESEARCH AND OTHER RELEVANT OBSERVATIONS

To identify relevant projects and initiatives undertaken to combat the aforementioned threat, the Cordis database was searched using a combination of the following keywords/terms: disinformation, propaganda, democracy, media literacy, journalists, media. We selected projects focusing strictly on current initiatives to counter disinformation and its negative effects on democracy, with a special emphasis on the importance of the media and journalists.

vera.ai / VERification Assisted by Artificial Intelligence, Grant agreement no: 101070093

Cordis: https://cordis.europa.eu/project/id/101070093
Project duration: 15 September 2022 - 14 September 2025

The main goal is to fighting online disinformation with trustworthy AI solutions. Online disinformation and fake media content has become a serious threat to democracy, the economy and society. Assessing the veracity/reliability of online content and uncovering highly complex disinformation campaigns is a huge challenge for researchers and media professionals. Vera.ai aims to build professional, trustworthy AI solutions against high-level disinformation technics, to be co-created with and for media experts and researchers, and to lay the groundwork for future research in AI counter disinformation. Key innovative features of artificial intelligence models will be fairness, transparency (including explainability), resistance to concept drift, continuous adaptation to the evolution of disinformation through a fact-checker-in-the-loop approach, and the ability to handle multimodal and multilingual sources. Recognizing the dangers of AI-generated content, the project will develop tools for deep detection of false information (audio, video, image, text). Artificial intelligence models will continuously collect fact-checking data collected from real-world content verified using the InVID-WeVerify plugin and the Truly Media/EDMO platform.

What is most interesting about vera.ai tool (Verification Plugin) is that social media and online content will be rapidly analysed and contextualised to reveal disinformation campaigns and measure their impact.

SMIDGE: Social Media narratives: addressing extremism in middle age, Grant agreement no. 101095290

Cordis: https://cordis.europa.eu/project/id/825469
Project duration: 1 March 2023 – 28 February 2026

Conspiracy theories, misinformation and extremism online having a direct impact on perceptions of democratic institutions, trust in science, and leads to calls for direct action to overthrow or disrupt democratically elected governments. Those in middle age (45-65) may be both susceptible to extremist narratives and also influential as decision-makers. SMIDGE will analyse the various forms of extremist discourses and narratives across Europe through social network analysis, textual and content analysis of extremist discourse, and will consider national and demographic specifics through survey, focus groups and interviews in 6 countries (UK, Italy, Belgium, Denmark, Kosovo, Cyprus). From this in-depth examination of the current state of the art, SMIDGE will:

- develop counter-narratives and educational resources to promote reflexivity and provide evidence-based tools and training for journalists and security professionals;
- provide guidelines & recommendations for policy and decision-makers based on the project findings, and present these findings to security professionals, policy makers, and journalists through roundtables and conference.

SMIDGE will provide effective and innovative countermeasures for policymakers with valuable insights and recommendations on how to tackle extremist narratives related to disinformation and conspiracy theories that affect the society (with special emphasies middle-aged adults).

FERMI: Fake nEws Risk MItigator, Grant agreement no: 101073980

Cordis: https://cordis.europa.eu/project/id/101073980
Project duration: 1 October 2022 – 30 September 2025

FERMI develops a framework to detect and monitor the way that disinformation spreads, both in terms of locations and within different segments of the society, and to put in place relevant security countermeasures. The main goal is to analyse and assess direct risks posed by disinformation to the offline environment and minimise the impact.

The FERMI project result will be relevant for European Police Authorities, other professionals and stakeholders, and EU citizens Facilitate the EU LEAs and (social) media organizations in the combat against disinformation by providing training and education material.

RECLAIM: Reclaiming Liberal Democracy in Europe, Grant agreement no: 101061330

Cordis: https://cordis.europa.eu/project/id/101061330
Project duration: 1 October 2022 – 30 September 2025

New tools to address post-truth politics in Europe. RECLAIM project will address the implications of post-truth phenomena in three distinct phases by generating a conceptual definition, operationalisation and empirical indicators to analyse post-truth/post-factual politics; analysing the current state of play as regards the various dimensions of post-truth politics in Europe; using its own empirical findings regarding the state of play of post-truth politics to develop policy recommendations, methods and toolkits to effectively address the various expressions of the phenomenon. One of the Work Package is dedicated to trust in and demand for quality journalism. Moreover, project will map and assess the demands and supply of quality news and journalistic standards in terms of impartiality and truth from the perspective of three key players in news production and dissemination: a) digital platform/social media providers; b) professional journalists and news media organizations; c) governments.

A key element of the RECLAIM project is to analyse disinformation in Europe and use the results to advise policy-making, education and action to respond to the negative impact of disinformation on democratic discourse and the basic structure of modern liberal democracy.

ReMeD: RESILIENT MEDIA FOR DEMOCRACY IN THE DIGITAL AGE, Grant agreement no: 101094742

Cordis: https://cordis.europa.eu/project/id/101094742
Project duration: 1 march 2023 – 28 February 2026

The project will address existing challenges to a healthy relationship between media and democracy by taking an approach to improving the relationship between citizens, media and digital technologies. Through an interdisciplinary approach and innovative methodology that combines qualitative and quantitative methods, ReMeD will collect, analyze, compare and contrast data on professional journalists, alternative media content producers and citizens operating in technologically mediated configurations, media organizations, market structures and national and international regulations that underpin media production, circulation and consumption in today's media landscape. This project's timing is especially pertinent, as the outcomes and policy suggestions from ReMeD will directly contribute to the ongoing discussions regarding the development and execution of the Digital Services Act and Digital Markets Act.

MeDeMAP: Mapping Media for Future Democracies, Grant agreement no: 101094984

Cordis: https://cordis.europa.eu/project/id/101094984
Project duration: 1 march 2023 – 28 February 2026

Project aims to establish forward-looking pathways to strengthen democracy by improving accountability, transparency and efficiency in media production and expanding active and inclusive citizenship. Based on the research results, an interactive multi-layer map of European political information environments will be created,

whose layers reflect the legal and regulatory framework and the democratically relevant features of media supply and demand. Moreover, the obtained map is to be compared with a map of how European citizens envision the future media landscapes. By comparing these maps, it is possible to learn from the compatibility and differences between them, identify good practices and develop guidelines to support development that promotes democracy and counteracts phenomena (disinformation) that may threaten it. These guidelines will be aimed at policymakers, regulators, self-regulatory bodies, media houses, journalists, NGOs and citizens.

5.3 RESEARCH AREA: EXTENDED REALITY AS THE OBJECT OF TECHNOLOGICAL MANIPULATION

DEFINITION OF THE RESEARCH AREA

Digital Twins (DT), Cyber-physical systems (CPS), and Extended Reality (XR) are essential supporting technologies of Industry 4.0. Making physical objects interact with their digital equivalents is the foundation of DT and CPS. In contrast, XR technologies emphasize enhancing the user experience by visualizing digital belongings, interacting with them, and operating them remotely or collaboratively[44]. Therefore, many companies are investing in Extended Reality as a promising solution for remote- monitoring, supporting, working, and remote communication.

THE CRITICAL THREAT

Besides these enormous advantages, the danger that extended reality can be used as the object of technological manipulation should be considered seriously as a hybrid threat. First, XR can collect and use (with or without consent) personal data with techniques such as eye tracking, emotion monitoring, behavior analytics, biofeedback, biometrics, and spatial analytics. The data can later be exploited for illegal purposes.

Second, Extended Reality can be operated as a cost-effective, rapid training solution, unfortunately not only by industry or the military but also by terrorists.

Finally, generative AI can be manipulated to generate manipulative content for XR to impact the human brain in unprecedented ways from endangerment of physical and mental wellbeing to inclusivity and ethical issues.

THE CRITICAL GAP

Unfortunately, data breaches are becoming more frequent, and even the platforms that appear to be the most secure might be vulnerable. In most cases, we cannot guarantee that personal data are only used for improving or optimizing user experience and are not stored anywhere. Lack of prevention and protection measurements against the massive availability and transparency of personal data could be determined as a central gap that can lead to the abovementioned threat.

Now, with the development of generative AI (foundation models such as GPT or BERT), manipulative, fake or malicious contents can be easily generated. It is even more dangerous since the attacker can use the personal data to make these content more reliable. They will genitively impact the human brain and behavior. Until now, there is still no technique, that can detect or classify these data.

THE CRITICAL NEED

XR development under a careful data protection and sharing principles design could minimize the abovementioned risks. Furthermore, creating easy-to-understand sensitization on social engineering risks is

[44] Cardenas-Robledo, L. A., Hernández-Uribe, Ó., Reta, C., & Cantoral-Ceballos, J. A. (2022). Extended reality applications in industry 4.0.-A systematic literature review. *Telematics and Informatics*, 101863.

needed to reduce the availability of sensitive data. Last, more reactive and incisive ethical reflection on immersive technologies is needed to enhance public awareness of developing or using Extended Reality and generative AI models.

RESEARCH AND OTHER RELEVANT OBSERVATIONS

Cordis scanning and analysis of projects revealed several relevant initiatives.

XRHuman: Establishing the European standards for extended reality

Timeline: 01/11/2022 - 31/10/2025
Project Website: https://xr4human.eu

The XR4Human project, financed by the EU, intends to create living standards for XR technology ethics and related legislative, regulatory, governance, and interoperability concerns within a European community of practice. The work on this project will prepare the path for a robust and competitive ecosystem, headed by European businesses, for the widespread deployment, use, and acceptance of XR technology[45].

The project addresses directly the need mentioned above by creating guidance documents and standards for XP development. The main outputs of the projects are:

- A European code of conduct for responsible XR technologies
- Test cases for demonstration and validation of XR development
- An Interoperability guidance document
- And a rating system and education sandbox for XR development.

GuestXR: A Machine Learning Agent for Social Harmony in eXtended Reality

Timeline: 01/01/2022 - 31/12/2025
Project Website: https://guestxr.eu/

GuestXR has been created to be a socially interactive multisensory platform system that leverages Extended Reality (virtual and augmented reality) as the medium to bring people together for immersive, real-time face-to-face engagement with valuable social outcomes. The crucial innovation is the involvement of artificial agents that assist online social gatherings in realizing their objectives through gradual learning. These agents use machine learning to figure out how to steer a meeting toward a particular goal [46].

The participants' individual and social behaviour will be analysed by a machine learning agent named "The Guest" using current theoretical frameworks from the perspectives of neuroscience and social psychology.

The results of GuestXR are highly relevant to the threat discussed above. We would like to see how the online social available information can be gathered and later used to train the agent and how the agent will influence human behaviour and human brain.

iv4XR - Intelligent Verification/Validation for Extended Reality Based Systems

[45] https://xr4human.eu
[46] https://guestxr.eu/

Timeline: 1/10/2019 - 31/12/2022
Project Website: https://iv4xr-project.eu/

iv4XR provides the XR developers with a novel AI-based content verification and validation environment. The developers will have a tool to test their developed virtual world automatically. Besides, to enable test agents to automatically evaluate the quality of the user experience and parameterize it by various demographic and socioeconomic kinds, such as male, female, young, and elderly, iv4XR also creates a socio-emotional AI[47].

The core idea and objectives of the project are interesting for the threat described above. The content of XR can be validated with AI agents. Besides improving user experience, we can extend the platform to validate the correctness of the virtual world or to experiment how the XR content can impact the human brain.

[47] https://iv4xr-project.eu/

6. OBSERVATIONS AND CONCLUSIONS

EU-HYBNET T3.3 “Ongoing Research Projects Initiatives Watch” in the scope of research project and innovation scan completed its third iteration which results are collected in this document (D3.9). In this iteration we continued to work on EU Funded projects scan.

We hope that our work will extend the understanding of the hybrid community about the investments EU is making in the research of phenomena, which has direct practical value for deeper understanding and mitigation of hybrid threats. At the same time such knowledge sharing should allow to leverage EU research project results wider purposes, that they were intended to.

We observe that Gaps and Needs defined by practitioners are very wide and represent significant interconnectedness of phenomena. So, the balance had to be found to define an area which can be meaningfully research, and but wide enough to represent practical significance for practitioners.

Some projects may appear in different research topics, again representing complexity and interconnectedness of subject areas. We tried to ensure, that project descriptions contain relevant take aways for particular research area.

Overall, we found that the exercise of reviewing subject area relevant for better understanding the state of play in the field, finding research groups working on subjects of common interests from other angles, rewarding. It does not only provide hybrid threats community with insight on progress in related fields but creates opportunities for collaboration. We hope that readers of this document will find value and ideas as well.

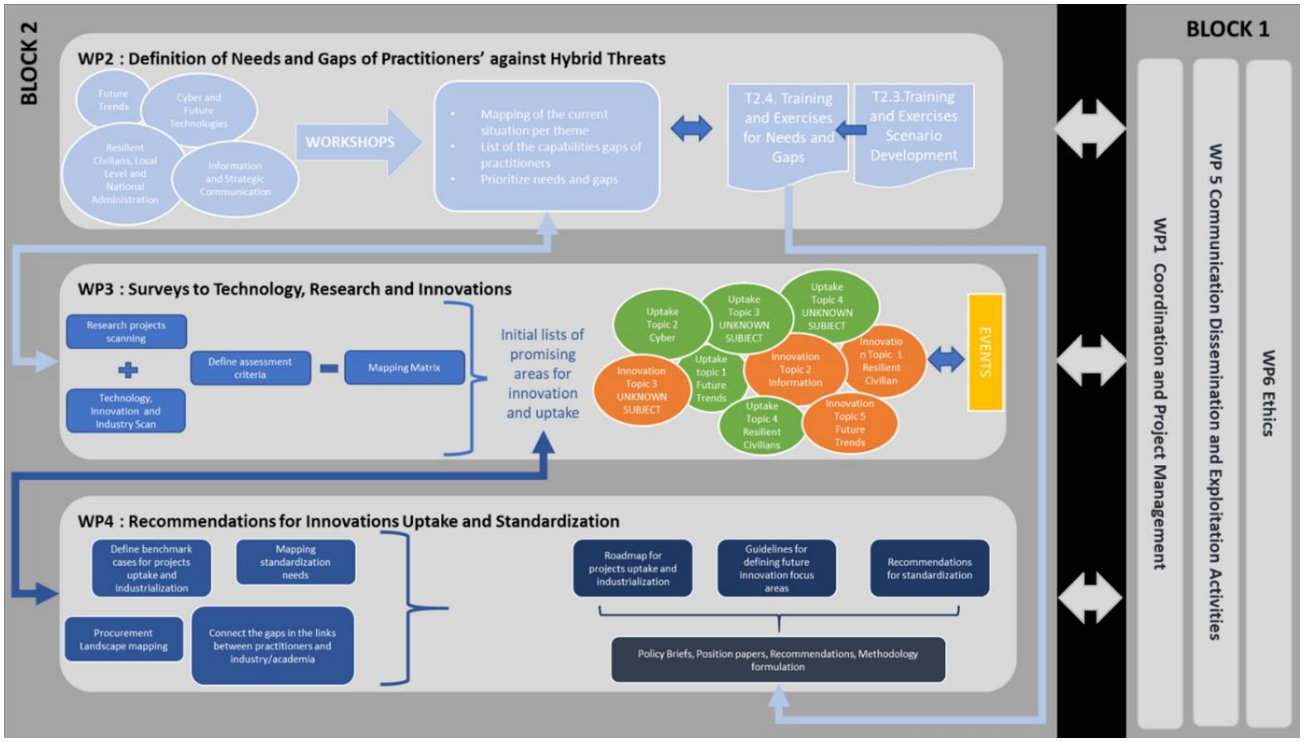
6.1 FUTURE WORK

The EU-HYBNET deliverable D3.9 "*Second Mid-Term Report on Innovation and Research Monitoring*" is a part of and Work Package WP3 "*Surveys to Technology, Research and Innovations*"/ Task T3.3 "*Ongoing Research Projects Initiatives Watch*".

Present document (D3.9) feeds information to T3.1 "*Definition of Target Areas for Improvements and Innovations"* and WP2 "*Gaps and Needs of European Actors against Hybrid Threats*"/ T2.3 "*Training and Exercises Scenario Development*" and T2.4 "*Training and Exercises for Needs and Gaps*".

D3.9 will deliver material for T3.1 to aggregate work of several scanning deliverables with the aim to analyse what could the most promising research directions and sound innovations addressing identified EU-HYBNET gaps and needs of pan-European practitioners.

Relationships between EU-HYBNET workpackages and tasks are highlighted in the project WP interdependency picture below:



D3.9 will be instrumental for EU-HYBNET and wider hybrid threats community to better understanding state of play of the fields identified by practitioners regarding the EU funded and thus readily available research. This, we hope will spur better collaboration between projects and exploitations of their results.

The D3.9 has also importance to deliver results to the EU-HYBNET project objective (OB) 3. and its goals and key performance indicators (KPI) as described in DoA Part B, chapter 1.1.

The objective OB.3 to which task T3.3 and deliverable D3.9 provides results is following:

OB3: To monitor developments in research and innovation activities as applied to hybrid threats		
Goal	**KPI description**	**KPI target value**

3.1	To monitor significant developments in research areas and activities in order to define and recommend solutions for European actors	Monitor research initiatives addressing EU actors gaps and needs in relation to knowledge/performance	At least 4 reports every 18 months will be delivered that outline findings from productive research efforts

ANNEX I. GLOSSARY AND ACRONYMS

Term	Definition / Description
AI	Artificial intelligence
APT	Advanced persistent threats
BRI	Belt and Road Initiative-countries
CCE	Common Configuration Enumeration
CEPS	Centre for European Policy Studies
CI	Critical infrastructure(s)
CIS	Centre for Internet Security
COMTESSA	Universitaet der Bundeswehr München
CPS	Cyber-Physical Systems
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
DoA	Description of Action of EU-HYBNET
EC	European Commission
EU	European Union
EU-HYBNET	A Pan-European Network to Counter Hybrid Threats project
FDI	foreign direct investment
FDI RRI	Foreign Direct Investment Regulatory Restrictiveness Index
FLOSS	Free and open-source software platform
GDPR	General Data Protection Regulation
IFCN	International Fact-Checking Network
IMMERSE	Integration of Migrants Matcher Service
JRC	Joint Research Center
KEMEA	Kentro Meleton Asfaleias
KPI	Key Performance Indicator
KRSC	Key Resources Supply Chains
L3CE	Lietuvos Kibenetiniu Nusikaltimu Kompetenciju ir Tyrimu Centras
LAUREA	Laurea-ammattikorkeakoulu Oy
MANET	Mobile Ad-Hoc Networks
ML	Machine Learning
MS	Milestone
NAAS	National Ecosystem for the Recognition and Analysis of the Information Effect Phenomena
NCSC	National Cyber Security Centrum
OECD	Organisation for Economic Co-operation and Development
PMT	Political Micro-Targeting
PPHS	Polish Platform for Homeland Security

Term	Definition / Description
PPP	Public Private Partnership
RISE	RISE Research Institutes of Sweden Ab
RTO	Research & Technology Organization
SCRM	Supply chain risk management
TNO	Nedelandse Organisatie voor Toegepast Natuuretenschappelijk Onderzoek TNO
Hybrid CoE	The European Centre of Excellence for Countering Hybrid Threats
WSN	Wireless Sensor Networks