FINAL 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

D3.10 FINAL REPORT ON INNOVATION AND RESEARCH MONITORING

Task number	T3.3	
Deliverable number	D3.10	
Version:	1.0	
Delivery date:	03/03/2025	
Dissemination level:	Public (PU)	
Classification level:	Public	
Status	FINAL	
Nature:	Report	
Main authors:	Rimantas Zylius	L3CE
Contributors:	Petteri Partanen, Tiina Haapanen	LAU
	Malgorzata Wolbach, Magda Okuniewska	PPHS
	Rolf Blom	RISE
	Athanasios Kosmopoulos	KEMEA
	Stefan Pickl	COMTESSA
	Edmundas Piesarskas	L3CE
	Souzanna Sofou	Satways

DOCUMENT CONTROL

Version	Date	Authors	Changes
0	07-1-2025	L3CE/ Rimantas Zylius	Table of Contents, structure of the document, table of contents, contextual texts
0.1	04-02-2025	All partners	Consolidated contributions of partners
0.2	07-02-2025	L3CE/ Rimantas Zylius	Initial draft prepared, all partners' contributions structured
0.3	11-02-2025	L3CE/ Rimantas Zylius	Internal review of contributors
0.4	13-02-2025	L3CE/ Rimantas Zylius	All contributions incorporated, submitted for EU-HYBNET review
0.5	25-02-2025	LAU/Isto Mattila, TNO/Okke Lucassen	Review
0.6	28-02-2025	L3CE/ Rimantas Zylius	Incorporated comments from the EU-HYBNET peer review. Final review. Document prepared for submission to EC.
1.0	03-03-3035	LAUREA/Tiina Haapanen	Final text editing and submission to EC

DISCLAIMER

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

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

CONTENTS

1. INTRODUCTION

T3.3 "Ongoing Research Projects Initiatives Watch", as defined in the Description of Action, was planned to be implemented in four cycles.

The first three cycles, 18 month each, took as input the Gaps & Needs defined in each relevant cycle in WP2 and performed the activity of Research Projects Initiative scanning.

The fourth cycle, which has significantly smaller time and resources assigned, "<…>will collect results from each of three previous cycles, draw conclusions, and make suitable recommendations". Further DoA describes that "<…> a last mini-cycle will also take into account the outcomes arising from each of the previous cycles for recommendations regarding future research, innovation and training".

1.1 OVERVIEW

OBJECTIVES OF THE DELIVERABLE

EU-HYBNET's Task (T) 3.3 "*Ongoing Research Projects Initiatives Watch*" deliverable "Final Report on Innovation and Research project Monitoring" (D3.10) is focused on reflecting the work done during the three previous cycles of T3.3, reflecting on the practical application of used method, and consolidating final recommendations relevant beyond the end of the project (April 2025).

STRUCTURE OF THE DELIVERABLE

This document is structured in the following 7 sections, with a focus on the scan results in each of the 4 core themes:

- Section 1: Introduction to the deliverable and work conducted, methodology review
- Section 2: Core Theme: Future Trends of Hybrid Threats
- Section 3: Core Theme: Cyber and Future Technologies
- Section 4: Core Theme: Resilient Civilians, Local Level and Administration
- Section 5: Core Theme: Information and Strategic Communications
- Section 6: Observations and discussion
- Section 7: Conclusions

1.2 METHODOLOGY REVIEW

In the same ways as the whole EU-HYBNET project, Deliverable D3.10 is structured around Core Themes:

- Resilient Civilians, Local Level and Administration
- Cyber and Future Technologies
- Information And Strategic Communications
- Future Trends of Hybrid Threats

Analysing the Core Themes, all 3 deliverables (of three cycles) and D2.8 "Final evaluation of Gaps and Needs" will be reviewed in consolidating manner. Within this deliverable we avoid chronological review but rather take all three iterations material as a consolidated body of knowledge. Still, observations about how similar topics iterated over cycles may be important to emphasize.

There was a notable difference in the research scanning process used in D3.7, the first iteration of the task T3.3 "Ongoing Research Projects Initiatives Watch", and the subsequent two deliverables D3.8 and D3.9. Every deliverable in detail describes the process used, here we aim to highlight key differences.

As initial step all iterations started their work from analysis of T2.1, "Needs and Gaps Analysis in Knowledge and Performance" and its relevant Deliverable iteration. In this task practitioners of hybrid threats identified relevant hybrid threat areas, defined the gaps which expose countries to the threats, and pointed to needs which have to be filled in order to mitigate risks.

EU-HYBNET was structured through the 4 core themes, so T3.3 deliverables consistently stuck to this structure.

In all three iterations T3.3 operationalized these findings. Gaps and Needs were redefined from broadly framed phenomena to rather more focused areas with strong hybrid threats dimension.

In the D3.7 the team targeted their scanning to the overall research arena. The deliverable aimed to define and discuss selected topics from the point of view of hybrid threats. The scanning team analyzed the scientific research landscape for the gaps and needs identified by practitioners in the field of hybrid threats. The deliverable contributed to deeper understanding of the hybrid threats community of the state of play of the research on the phenomena of interest, and what outcomes could be expected from the scientific research field. Not less importantly, document identified areas, which apparently lack research of the phenomena, which is deeply important for mitigation of hybrid threats.

D3.8 and D3.9 focused on EU funded research projects. The team was reviewing EU funded projects that are relevant to topics identified by practitioners. In the deliverables projects were analysed from the perspective of hybrid threats, what specific aspects of the project may be of interest to community and what can be expected as an outcome of this project.

In three iterations T3.3 reviewed over 70 EU funded projects. Some of the projects were reviewed from the different angles, as the same project might have been relevant in several core themes.

Overall the evolution of the method of research scan allowed to better respond to the needs of hybrid threats community, improve understanding about the EU funded projects which are relevant and to facilitate communication and collaboration between projects.

In this deliverable contributors:

- Describe most relevant researched topics, based on material of the deliverables D3.7, D3.8, D3.9 and D2.8. Recurring topics should be consolidated to avoid repeating. It is important to emphasize recurring nature and relevance to hybrid threats of such topics and discuss how they evolved.
- Provide observations, discussion and recommendations

2. CORE THEME: FUTURE TRENDS AOF HYBRID THREATS

In this To the core theme we there is three ongoing and future threats with multifaceted hybrid threats. Stemming from the previous project work the recognized following three trends are: increasing dependency of critical services, populism and instrumentalized immigration.

2.1. RESEARCH AREA: INCREASING STRATEGIC DEPENDENCY OF CRITICAL SERVICES

Foreign direct investment (FDI) discussed in D3.7. In EU states there is a need for FDI screening to follow the situation because of earlier and still continuing privatization of State-owned companies and infrastructure facilities. For example, China's global foreign direct investment was at its peak in 2016. In Europe, Germany was the main recipient of Chinese investment. Since 2016 the FDI trend has been downward. The reason behind is claimed to be deglobalization and protectionism.

FDI pattern has a close connection to hybrid threats. In D3.7 it is stated that potential national security threats from foreign ownership affects at least in three categories:

- the transfer of (military) sensitive technology
- the denial or manipulation of access to a critical input by a foreign controlled supplier and
- the infiltration, surveillance or sabotage of production systems

D3.7 observes that there are no clear tools that support the ongoing analysis of the risks associated with FDI.

Donald Trump's return back to office in USA (2025) brings new uncertainties to the global markets affecting also the FDI situation. This is why the research and follow-up of this trend is needed.

- The core phenomenon underpinning the increasing strategic dependency of critical services, as highlighted across the EU-HYBNET deliverables, is the growing vulnerability of nations due to **reliance on complex and interconnected critical infrastructures and supply chains**, particularly in the context of globalization and evolving geopolitical landscapes. Deliverable D3.7 explicitly addresses "Increasing Strategic Dependency of Critical Services" within the "Future Trends of Hybrid Threats" core theme, emphasizing the role of Foreign Direct Investment (FDI) as a key factor. This dependency creates a significant vulnerability to hybrid threats, as disruptions to these essential services can have cascading effects across society, impacting economic stability, public safety, and national security. The deliverables collectively underscore that modern societies' reliance on energy, transportation, healthcare, digital communications, and other critical sectors creates potential leverage points for malicious actors seeking to exert influence or cause disruption.
- A crucial aspect of this phenomenon is the **geopolitical dimension of FDI**, particularly concerning investments from state-controlled or influenced entities in strategic sectors. D3.7 highlights China's FDI trends and the growing concerns about the transfer of sensitive technologies, manipulation of access to critical inputs, and potential for infiltration or sabotage of production systems through foreign ownership. While **D3.7** notes the lack of specific tools for ongoing FDI risk analysis, the broader discussion within D2.8 and D3.8 underscores the heightened threat landscape facing these strategically vital services. The potential return of geopolitical uncertainties, as mentioned in D3.7 regarding the US political landscape, further amplifies the need for vigilance and proactive measures to secure critical service dependencies.
- Furthermore, the **economic and political context of globalization and deglobalization** plays a significant role in shaping this dependency. D3.7 suggests that the downward trend in FDI since 2016, attributed to deglobalization and protectionism, may paradoxically *increase* strategic dependency by concentrating control of critical assets in fewer hands, potentially making them more vulnerable to targeted hybrid threats. This complex interplay of economic trends, geopolitical shifts, and technological vulnerabilities necessitates a holistic and adaptable approach to critical service resilience.

- The phenomenon of "Increasing Strategic Dependency of Critical Services" is a complex interplay of economic, geopolitical, and technological factors that creates significant vulnerabilities to hybrid threats. Addressing this issue requires a multi-faceted approach encompassing robust FDI screening mechanisms, enhanced cybersecurity measures, proactive risk management strategies, and a deeper understanding of the evolving global landscape to safeguard the resilience of critical services essential for modern societies. The documents emphasize the urgency of research and the development of practical tools and frameworks to navigate this increasingly complex and strategically important domain.

2.2. RESEARCH AREA: RISE OF THE POPULISM

Populism was discussed in D3.8. Populism is difficult to define. Populism as many other concepts should be defined and interpreted in its relevant context.

In this context populism can be interpreted as a divisionary political stance confronting popular sentiment against “elite” or “experts” fueled by the popular feeling that a large part of the population is not represented, their needs are not understood, and they are marginalized. The claim is that there is systematic effort to suppress and exploit this part of society.

The changes in global politics, private owned platforms, uncontrolled algorithms and AI of the social media and increasing number and gravity of the groups which feel to be dropped out from the western democratic societies, all these together feed the rise of populism enabling hybrid influencing combined with poor level of literacy. Lack of transparency and filtered news has a remarkable influence to the views and emotions of the population.

In D3.8 suggests that there is a need to openly discuss philosophy, logic, and consequences of news filtering/personalization.

- All deliverables (D2.8, D3.7, D3.8, and D3.9) discuss growing societal division and erosion of trust in established institutions and expertise, fueled by a complex interplay of technological and socio-political factors. Deliverable D3.8 directly addresses **"Rise of Populism"** as a critical need, recognizing its multifaceted nature and the difficulty of defining it precisely, emphasizing the importance of context-specific interpretation. The documents converge on the understanding of populism as a divisionary political stance that exploits a perceived disconnect between "the people" and "elites" or "experts," tapping into a widespread feeling of marginalization and lack of representation within segments of society.
- Several interconnected factors are identified across the deliverables as contributing to this rise in populism and its susceptibility to hybrid influence. These include **global political changes and anxieties**, creating fertile ground for populist narratives that offer simplistic solutions to complex problems. The **dominance of privately-owned social media platforms and their uncontrolled algorithms and AI-driven curation** are also crucial elements. As highlighted in D3.9 under "Media Conundrum" and "Online Manipulation attacking democracy," these platforms, while offering benefits, can also amplify misinformation, create filter bubbles, and personalize news in ways that contribute to polarization and distrust.
- The consequences of this rise in populism, as detailed in the deliverables, are significant for hybrid threats. D3.8 notes the "Rise of Populism" as a "Critical Need" in Core Theme 5: Future Trends, linking it to the increased potential for hybrid influencing due to a poor level of media literacy within segments of the population. The lack of transparency and filtered news, as highlighted in D3.8's call for open discussion of "news filtering/personalization," further exacerbate the problem by creating information environments where misinformation and emotionally charged content can thrive, reinforcing populist narratives and undermining trust in factual reporting and expert knowledge. Projects like **PersoNews** (D3.9), investigating the impact of algorithmic news recommenders, and **AI4Dignity** (D3.9), exploring AI's role in hate speech

detection, are relevant to understanding the technological dimensions of this challenge. In essence, the rise of populism, fueled by technological and societal shifts, creates a more vulnerable and polarized environment, making societies more susceptible to hybrid threats that exploit these divisions and undermine democratic discourse.

2.3. RESEARCH AREA: INSTRUMENTALIZED IMMIGRATION

Instrumentalized immigration combined with irregular immigration in general feeds the xenophobia and on the other hand creates informal (ethnic) societies which does not respect the state borders in the EU. Immigrants are or are (in danger to drop) outside the official societies, networks, social support etc. and on the other hand the xenophobic populist groups are fueled with information against immigration. All this creates can be leveraged by hybrid threat actors and is one another possible avenue for shattering to undermine the democratic states. The media literacy of these groups may be poor. The multinational nature of the immigrant movements needs the EU level approach and action.

See Frontex Strategic Risk Analysis Report 2024, especially chapter 6 “Hybrid Threats” which highlights the instrumentalized migration as a hybrid threat and its implications to European societies.

The response to the irregular and especially the instrumentalized immigration need more research and common tools as well as shared situational awareness. The phenomenon is strengthened by the evolving crisis nearby Europe and climate change which both are the push factor for the immigration.

- The core phenomenon underpinning "Instrumentalized Immigration" as a future trend of hybrid threats is the strategic exploitation of migration flows by malign actors to create societal division, fuel xenophobia, and destabilize democratic states. This phenomenon leverages the vulnerabilities inherent in irregular and instrumentalized immigration, turning migration itself into a tool of hybrid warfare. Deliverables highlight how this instrumentalization manipulates public sentiment, exacerbates existing societal fractures, and undermines the foundations of democratic societies.
- The marginalization and vulnerability of immigrant populations themselves are central to this phenomenon. Deliverables observe that immigrants are often at risk of falling being dropped outside official societies, networks, and social support systems, creating a sense of disenfranchisement and alienation. This vulnerability is then exploited by malign actors who can manipulate and instrumentalize these marginalized communities for their own purposes. While the documents do not explicitly detail projects directly focused on instrumentalized migration as a hybrid threat *tactic*, projects addressing migrant integration and social cohesion, such as **MIICT** and **IMMERSE** (D3.7, D3.9), become highly relevant in mitigating the broader societal vulnerabilities that instrumentalized immigration exploits. These projects, focused on improving migrant access to services and fostering integration, can be seen as crucial for building resilience against this specific hybrid threat vector by strengthening social cohesion and reducing marginalization.
- Finally, deliverables find the need for an EU-level approach and enhanced situational awareness to address instrumentalized immigration. The multinational nature of migration flows necessitates coordinated action across EU member states. The Frontex Strategic Risk Analysis Report 2024, referenced in the text, explicitly highlights instrumentalized migration as a hybrid threat, underscoring the urgency and strategic importance of this issue for European security. The push factors of evolving crises near Europe and climate change, emphasize the long-term and complex nature of this challenge, requiring sustained research, policy development, and international cooperation.

3. CORE THEME: CYBER AND FUTURE TECHNOLOGIES

Thise Core Theme during EU-HYBNET project focused naturally on the protection of digital infrastructure, private data and growing technological capacities use for personalized targeting of individuals and emergence of disruptive technologies and related threats.

3.1 RESEARCH AREA: EMERGING CAPABILITIES AND EMERGING THREATS: ACCESS TO SPACE, QUANTUM AND OTHER DISRUPTIVE TECHNOLOGIES

Intense development of technologies reveal gaps in international regulations, thus posing new kinds of threats, including hybrid threats.

Space exploration and usage, critical to many civilian and military uses, was possible only by major countries. Currently it is increasingly commercially viable, and space commercialization poses, and congestion poses new kinds of risks.

Quantum developments were explored as an example of highly disruptive technologies, which will create a significant window of opportunities for massive hybrid and non-hybrid attacks on communication and overall infrastructure.

SPACE INTERFERENCE

The world is increasingly dependent on space systems for economic and military security. Commercial space has opened markets and enabled entirely new industries worldwide. Moreover, the global economy depends on weather data, communications, navigation, timing, remote sensing, and other space systems.

Due to the strategic importance of space, some nations are developing weapons that can target and destroy space systems, which can destroy space systems and threaten the availability of such systems to other regions. However, the strategic importance of space has also inspired new efforts to mitigate conflict and protect the region for peaceful purposes. International agreements and tools are needed to ensure the safety of outer space.

To address the challenges of space interference, some experts in space security have called for more robust norms of behavior in outer space. A report published by Jessica West et al. “Space Dossier 7 – Norms for Outer Space: A Small Step or a Giant Leap for Policymaking?” explored the role of norms as a tool for outer space governance and their challenges and limitations. This becomes crucial, as many countries take steps to militarize outer space. But essentially the ongoing changeover in European space policy has to be recognized that significantly affects how we envision a “united Europe in space”, that outer space moves from ”security” area of governance to ”defense”.

DISRUPTIVE TECHNOLOGIES

Two iterations touched upon the same disruptive technologies subject. Innovations became a very important driver of economic and military power, reflecting this most of the countries fund research and development effort as well as innovation uptake. In most cases innovations became a leverage factor of continuous improvement. This is an effort where country must invest in order “not to lose”.

From the power perspective, disruptive technologies have a potential for significant advancement of interest of country – for the first mover disruptive technologies give an asymmetrical advantage against others.

While research in quantum, artificial intelligence or other high potential disruptive technologies are abundant, JRC technical report “Quantum as a disruptive technology in Hybrid Threats” published in 2021 is a rare example of trying to illuminate hybrid threat aspects in such a technology -heavy area. The report finds it necessary to

discuss how countries should be prepared for the negative outcome of the race. In the report authors discuss the aftermath of adversary country succeeding to develop usable quantum computer first (example of disruptive technology). It states, that “there may be significant benefits to be attained by an adversarial country, which would provide the greatest opportunities for increased attacks based on innovative technologies, even though these could only be sustained for a brief period. In the future, we should expect that a post-quantum equilibrium will be reached, as the quantum secure technologies are developed and deployed. Thus, the motivation to leverage this opportunity for the adversary in such a limited time span could be very tempting.”

Though we found no research in this subject, it seems there is a compelling case for the conceptualization of hybrid threats landscape and response in case of losing disruptive technology race. Quantum computing is important, but nonetheless only one of examples of such disruptive technologies.

- **Space Security and Weaponization (D2.8, D3.8, D3.9)** emphasize the increasing strategic importance of space and the emerging threats related to its weaponization and interference. **D3.8** under "Space Interference and Counterspace Weapons" highlighting projects like PROGRESS and 7SHIELD aimed at protecting space infrastructure. **D2.8** lists "New Space" as a priority area, noting challenges related to contested access to space and the reliance of the EU on commercial space capabilities.

- **Quantum Computing as a Disruptive Technology (D3.7, D3.8, D3.9):** Quantum computing is consistently presented as a prime example of a disruptive technology with significant security implications. Reference to the JRC technical report "Quantum as a disruptive technology in Hybrid Threats" defines tendencies while projects like INSPIRE-5Gplus and ISOCRYPT exploring post-quantum cryptography discuss research efforts.

- **Disruptive Technologies and Asymmetric Advantages (D3.7, D3.8, D3.9):** The documents emphasize the potential of disruptive technologies, beyond just quantum, to create asymmetric advantages and alter the balance of power. **D3.7** specifically notes the lack of attention to the "hybrid threat dimension of disruptive technologies" in EU project funding and calls for "conceptualization and practical preparation."

3.2. RESEARCH AREA: DIGITIZATION OF PRIVATE LIVES, MASSIVE AVAILABILITY OF PERSONAL DATA AND TECHNOLOGIES FOR PERSONALIZING MESSAGES

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. This information is shown to be suitable for profiling of individuals and adjusting the messaging for them.

Social media now becomes an ever- more important vehicle for cheap delivery of personalized information to individuals on a very large scale. As social media fails to control identities of users, with the proliferation of bots and manipulation of algorithms, it was demonstrated on multiple occasions that social media can be used effectively to deliver messages and influence citizens. by foreign powers.

The problem manipulative potential of social media is further augmented as deep-fake content became so sophisticated that technologies are becoming very hard to recognize differentiate, and cheap to produce.

THE INDIVIDUAL AS A DIGITAL ENTITY

Deepfakes may result either from modifications and transformations of existing media content or from entirely synthetic generation. Accordingly, we identify three distinct problem areas:

- Detection: Determining whether media content has been modified, transformed, or produced synthetically.

- Relationship Identification: Linking non-synthetic deepfake content to its corresponding original media.
- Attribution: Verifying that the original media content is correctly associated with its authentic source.

In conclusion, while the detection of deepfakes remains an active area of research—with current methodologies applied in practice PRACTICE, the rapid evolution of deepfake technologies necessitates continuous advancements in detection techniques. Although operational methods exist, there are no established standards or universally applicable services.

The challenge of linking deepfakes to their original media has been less extensively explored, possibly due to its diminished relevance in contexts such as fake news, where credibility is immediately compromised upon disclosure of tampering.

Conversely, the issue of content attribution is critically important in the realm of fake news, as it enables the verification of the claimed origin of media content. This domain is likely to attract significant attention from online content-sharing service providers, spurring the development of innovative media search solutions and robust attribution schemes, methodologies and processes. It is imperative that these solutions be designed and implemented in a manner that fosters public trust and widespread adoption. It has to be recognized, that in the widespread mistrust environment, even brilliant technical solutions if implemented without sensitivity to the public perception, might be considered as “effort to control the discourse and free speech”, so can counterproductive.

STEALING DATA ATTACKING INDIVIDUALS

The most important need is the implementation of up-to-date industrial standards for cybersecurity in all IT systems and for those handling personal and sensitive information. The required knowledge to do this already exists. What is missing is awareness, resources and willingness. On the positive side, , and the significant progress and investment is observed in the area from business and governments.

On the other hand, awareness to the population about the risks on the internet and of voluntary sharing of sensitive information on social media and other platforms still a significant problem. While anonymization and data protection technologies receive very significant attention, both in research and in industrial developments, the voluntary sharing of information is overlooked. Social media and other companies invest significant funds to ensure that data sharing is facilitated and incentivized.

- **Personalized Messaging and Micro-Targeting (D2.8, D3.7, D3.9):** Research recognizes that readily available personal data and technologies enable highly personalized messaging and micro-targeting. **D2.8** lists "Massive availability of societal data aggregates and algorithmic computation" and "Foreign interference in democratic politics making full use of algorithmic and mass data affordances" as priority areas, directly connecting data availability to political manipulation. **D3.7** under "Trend; Big data as a new power source" and **D3.9** under "Online Manipulation attacking democracy" and "Research Area: Political deficiency" further explore the techniques and implications of micro-targeting and personalized messaging, particularly in political contexts.

- **Deepfakes and Synthetic Media (D3.7, D3.9):** The documents highlight deepfake technologies as a significant augmenting factor in information manipulation. **D3.7** and **D3.9** under "The Individual as a Digital Entity" directly address deepfakes, discussing the challenges of detection, attribution, and the increasing sophistication and affordability of their production. Projects like **DIGGER and WeVerify (D3.9)** serve as examples of technological efforts to combat deepfakes and misinformation.

- **Erosion of Trust and Increased Susceptibility to Manipulation (D2.8, D3.9):** Research indicates that the combination of personalized messaging, disinformation, and deepfakes erodes trust in information sources and increases susceptibility to manipulation. **D2.8** and **D3.9** across various sections consistently

emphasize the erosion of trust in democratic institutions and media, directly linked to the proliferation of misinformation and manipulative content.

- **Cybersecurity and Data Protection Gaps (D3.9):** The documents point to gaps in cybersecurity and data protection as critical vulnerabilities in the context of massive data availability. The deliverable emphasizes the ongoing efforts in the EU to improve data protection through GDPR and other initiatives. Projects like **FLUTE, SECURED, HARPOCRATES, PAROMA-MED, and ENCRYPT (D3.9)** are examples of research focusing on Privacy Enhancing Technologies (PETs) and secure data processing, reflecting the efforts to address these gaps.

- **Awareness Gap Regarding Online Risks and Data Sharing (D3.9):** The documents identify a significant awareness gap among the population regarding online risks and the implications of voluntary data sharing. **D3.9** under "Stealing Data Attacking Individuals" explicitly directs that awareness to the population about the risks on the internet and of voluntary sharing of sensitive information on social media and other platforms is a significant problem. Projects like **Open Your Eyes: Fake News for Dummies (D3.9)** try to improve digital literacy and awareness.

3.3 RESEARCH AREA: CYBERATTACKS, ELECTRONIC INTERFERENCE ON CRITICAL INFRASTRUCTURE AND SUPPORTING TECHNOLOGIES (E.G. GPS SPOOFING) AS MANIFESTATSION OF ORCHESTRATED MULTIMODAL ATTACKS

HYPER CONNECTIVITY AS AN IMPACT MULTIPLIER OF CYBER

Software nowadays is embedded almost everywhere: in smartphones, cars, offices, and even homes. This fact in addition to hyperconnectivity reveals that most of these software products are exposed to vulnerabilities. It has been estimated that the average software program has at least 14 separate points of vulnerability. Estimates vary, but it is consistently found that majority of the codebases have vulnerabilities and the trend is worsening[1].. Each of those vulnerabilities can allow an attacker to compromise the integrity of the program and exploit it for personal gain. Hence, software vulnerabilities and their timely patching have become a crucial concern for everyone. Security vulnerabilities in software are one of the fundamental reasons for security breaches; and a critical challenge from knowledge management perspective is to establish an efficient method for the knowledge disclosure of those vulnerabilities. In an ENISA research from 2016, it is clearly demonstrated that it is urgent to bring different stakeholders together to discuss the challenges associated with vulnerability disclosure and the ways such challenges can be addressed[2]. The development of a core set of principles upon which different stakeholders can agree, and to which they can adhere, can go a long way towards reconciling the existence of distinct and at times conflicting interests. Thus, it can be characterized as a crucial requirement in future research, to identify the key cyber security vulnerabilities, targeted/victimized applications, mitigation techniques and infrastructures, so that researchers and practitioners could get a better insight into it.

It was observed that the development of a European framework for EU cross country cooperation in the case of cybersecurity crisis is a work in progress. The NIS Directive does not address this. Current EU's abilities to act at the operational and political level in large-scale cybersecurity crisis has been characterized as "limited" .

While networks and information systems are designed to be protected cyber-attacks, some kinds of attacks require active response capabilities. Offensive Cyber Capability (OCC) combines human, technical, and organizational attributes to support offensive cyber operations: the adversarial manipulation of digital services

[1] Synopsys Report Finds 74% of Codebases Contained High-Risk Open Source Vulnerabilities, Surging 54% Since Last Year, https://www.blackduck.com/resources/analyst-reports/open-source-security-risk-analysis.html

[2] https://www.enisa.europa.eu/publications/vulnerability-disclosure

or networks. The OCC focuses primarily on its (de-escalation) potential in terms of diplomatic tension, instability, or power.

Tools are needed to share the knowledge between different members of the EU to improve and faster develop the offensive cyber capabilities to handle the new challenges. Limited EU funded research explored the development and use of offensive cyber capabilities (OCC) by western powers, namely France, Israel, and the United States. The research discussed the cultural, socio-political, historical, and ideological factors involved. Overall offensive cyber capabilities seem to be lacking attention in EU funded research.

- **Vulnerabilities due to Hyperconnectivity and Software Embedding (D3.7, D3.9)** discusses increased attack surface and vulnerability stemming from the pervasive embedding of software in all aspects of modern life and the hyperconnected nature of systems. **D3.7** "Hyper connectivity as an impact multiplier of cyber" directly addresses this, noting the estimated average of 14 vulnerabilities per software program and the resulting exposure.

- **Multimodal and Orchestrated Attacks (D3.8):** Research recognizes that modern attacks are increasingly multimodal and orchestrated, combining cyber and physical elements, requiring comprehensive and integrated defense strategies. **D3.8** under "Exploitation of Critical Infrastructure Weaknesses" describes how " complex attack strategies are employed – they combine multistage action, combine information and cyber-attacks. The PRAETORIAN project, discussed in **D3.8** aims to address advanced combined cyber and physical threats.

3.4. RESEARCH AREA: THE PERCEIVED RELIABILITY OF INFRASTRUCTURES

Security of critical infrastructures is an 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 actors, disruption of one or another infrastructure or service may not be an aim in itself, but only an 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 a specific reaction, to an 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.

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 still considered 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.

- **Overreaction and Societal Impact:** the context of CBRNE, the potential for panic and societal disruption from a perceived radiological or nuclear threat, even if it's fake or exaggerated, is immense. Therefore, robust detection and verification capabilities, like those INCLUDING and RADION in **D3.9** aims to improve detection capability and management of incidents. Though deliverable observes, that there is a need to counter the effectiveness of "fake attack" scenarios designed to cause chaos and erode trust.

- **Multimodal and Orchestrated Attacks (D3.8):** Research recognizes that modern attacks are increasingly multimodal and orchestrated, combining cyber and physical elements, requiring comprehensive and integrated defense strategies. The PRAETORIAN project in **D3.8**, aims to address advanced combined cyber and physical threats.

- **Gaps in Cross-Border Cooperation and Crisis Response (D3.7):** The documents highlight limitations in EU-level cross-border cooperation for responding to large-scale cybersecurity crises.

- **Lack of Standardization and Knowledge Sharing (D2.8, D3.8):** Research underscores the need for improved standardization, knowledge sharing, and information exchange within the EU to enhance cyber resilience. **D2.8** under "Operationalizing European responses to hybrid threats" points to the need for clear and common definitions, situational awareness, solidarity, and counter measures at European level.

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

Core Theme Resilient Civilians, Local Level and Administration turns around the subject of resilience of democratic countries, with a focus on mechanisms of foreign influence on democratic processes and harm to basic state functions. This core theme emphasizes preservation of trust and solidarity within societies to make them less vulnerable to manipulation.

4.1 RESEARCH AREA: NORMALIZATION OF VIOLENCE

This area encompasses the multifaceted ways in which public confidence in democratic institutions is intentionally undermined by autocratic adversaries. Hybrid threats frequently target the very foundations of social cohesion by exploiting existing societal divisions and political fractures. These divisions can be based on a range of factors such as political ideology, socio-economic status, ethnicity, religion, or geographic location.

By amplifying these divisions through disinformation campaigns and propaganda, malign actors seek to create a climate of mistrust and suspicion. A critical element of this erosion is the creation of a sense of cynicism, where people no longer believe that their political systems are capable of addressing their needs, or that political actors can be trusted to act in their best interest. This can manifest as a loss of faith in political decision-making, which can lead to widespread apathy, disengagement from civic participation, or even active opposition to the established order.

A further consequence of this erosion of trust is that it makes societies more susceptible to manipulation. When citizens no longer trust their governments, they are more likely to believe false or misleading information, especially if it confirms their existing biases. This creates fertile ground for propaganda and the spread of disinformation. The goal here is to weaken the social fabric of democratic societies, by undermining the shared values and beliefs that hold communities together. This weakens the collective ability to respond to external threats and creates an environment that is conducive to the spread of extremism and violence.

Another key aspect of the erosion of trust is the normalization of violence. When political discourse becomes excessively polarized and hostile, it creates a climate where excessive actions, and even violence, is perceived as an acceptable means of expressing disagreement or achieving political aims. This can be seen in both online spaces, where extremist groups can use social media to promote violent ideologies, and in the real world, where political rallies can quickly descend into clashes between rival groups. The use of social media platforms and online networks can exacerbate this trend, enabling the rapid and widespread dissemination of inflammatory rhetoric and the mobilization of extremist groups, while making it easier to promote and plan violent activities.

- **Exploitation of Political Cleavages (D2.8, D3.8, D3.9):** Research recognizes that hybrid threats exploit existing societal divisions (political, social, cultural) to sow discord and undermine trust. Projects like **WeVerify, SOCIALTRUTH, and Co-Inform (D3.8)**, while focused on disinformation detection, address the broader issue of information manipulation that fuels these cleavages. **D2.8** emphasizes "The spread and demand of conspiracy theories weaken democratic politics" and "Emotions and victimhood in social relations as a lever of hybrid threat activity" as priority areas, directly linking to the polarization and societal division aspects.

- **Information Manipulation and Disinformation (D2.8, D3.8, D3.9):** Numerous deliverables emphasize the role of disinformation in eroding trust and normalizing harmful narratives. Projects like **IMEDMC, DIGGER, and WeVerify (D3.8, D3.9)** explore mechanisms of information manipulation, fake news detection, and tools to increase citizens' resilience to misinformation.

- **Weakening of Democratic Politics (D2.8, D3.9):** Research identifies the acceptance and mainstreaming of violence in political discourse and the spread of conspiracy theories as factors that weaken

democratic processes. **D2.8** directs "The growing acceptance and mainstreaming of violence weaken democratic politics" and "The spread and demand of conspiracy theories weaken democratic politics" as priority areas. **D3.9** under "Spreading Violence" research area discusses how violence becomes normalized in political expression and the erosion of social contracts.

- **Social Media and Online Spaces as Amplifiers (D2.8, D3.8, D3.9):** Deliverables observe that social media platforms are key channels for the dissemination of disinformation, extremist content and inflammatory rhetoric, contributing to the normalization of violence. Projects like **COMPROP, RUSINFORM (D3.8, D3.9)** explore the use of algorithms and bots in computational propaganda and foreign influence operations within social media contexts. **D2.8** highlights “Adapting the news media landscape to new and evolving consumption patterns” and “The problem of foreign and private ownership of social media platforms that impact the European landscape” as priority areas.

4.2. RESEARCH AREA: CRITICAL INFRASTRUCTURE AND SERVICE RESILIENCE

This topic is focused on the vulnerabilities stemming from a reliance on essential services and technological systems, such as the supply of energy, transportation, healthcare, and digital communications. Modern societies depend on these systems for basic needs, and any disruption to their operations can have severe consequences, both for the public and the state. Hybrid threats often target critical infrastructure to disrupt essential services, causing chaos and eroding public confidence in the government's ability to protect them. This can be achieved through a variety of means, such as cyberattacks, physical sabotage, or disinformation campaigns designed to sow uncertainty about the reliability of these essential services and goods.

A notable vulnerability of our highly interconnected societies is their increasing reliance on digital infrastructure. Functioning of services relies on internal ICT infrastructure, while more and more services and functions move online, these digital systems become attractive targets for malicious actors. Cyberattacks can cripple networks, leading to widespread disruption and loss of essential services. Similarly, physical attacks on critical infrastructure, such as power grids or transportation networks, can have devastating consequences, with serious cascading effects on other systems and infrastructure. The very nature of cyber-attacks means that they can be carried out from great distances and may come from multiple actors working together to create a coordinated attack.

A fundamental aspect around which this research area revolves is the inadequacy of resources and capacities, especially at the local level. Local authorities are typically the first responders in a crisis and therefore must have adequate resources and the necessary expertise to secure these vital services. This involves addressing supply chain vulnerabilities, improving decision-making processes related to infrastructure management, and building stronger partnerships with the communities they serve.

It should be observed that reaction of institutions was underwhelming during recent disruptions of the services (e.g. damaged power and communication cables, fires in strategic enterprises in EU and attempts to disrupt). Most notably, more interaction of policy makers with the hybrid threat community is necessary to shape the response policies and algorithms to such incidents.

- **Cyberattacks on Critical Infrastructure (D2.8, D3.8, D3.9):** Deliverables repeatedly emphasize cyberattacks as a primary threat to critical infrastructure. **D2.8** priority area "Hacktivism, sabotage, and electronic warfare targeting critical infrastructure in the EU" reflect it directly, projects like **PROGRESS and 7SHIELD (D3.8)** focus on protecting ground-based infrastructure and ground segments from cyber and physical threats. **D3.9** under "Offensive Cyber Capabilities" highlights the increasing cooperation in cyber defense and the need for knowledge sharing in this domain.

- **Interdependencies and Cascading Effects (D3.8):** Research recognizes the complex interdependencies within critical infrastructure systems, making them vulnerable to cascading failures. **D3.8** describes the **PRAETORIAN** project, aiming to create a toolset to understand and manage these multidimensional risks and combine physical and cyber situational awareness.

- **Situational Awareness for Critical Infrastructure Protection (D2.8, D3.8):** The need for comprehensive situational awareness, extending beyond just cybersecurity, is a key iterating theme. **D3.8** highlights the **SPARTA** project (T-Shark) which aims to develop a "Comprehensive Full-Spectrum Cybersecurity Threat Intelligence" framework to improve situational awareness and orchestration across stakeholders. **D2.8** notes "Operationalizing European responses to hybrid threats" as a priority area, which includes situational awareness at the European level.

- **Supply Chain Vulnerabilities (D2.8, D3.8):** The documents acknowledge the vulnerability of supply chains, particularly in hardware and components production (D3.8 under "Targeting the psychological reliability of digital infrastructures"). While not a central theme for specific projects, **D3.8** observes "Dependency on hardware and components production global supply chains" as a gap in Cyber and Future Technologies. **D2.8** touches upon this through "The perceived reliability of digital infrastructures," as supply chain issues can impact perceived reliability.

4.3. RESEARCH AREA: INSTITUTIONAL INTEGRITY AND INTERNAL ORGANISATION

INTERNAL STRUCTURES OF GOVERNMENTAL BODIES AND OTHER KEY ORGANISATIONS

This area focuses on the vulnerabilities that exist within the internal structures of governmental bodies and other key organizations.

Hybrid threats are not only external attacks; they also target the inner workings of institutions, aiming to weaken their ability to respond effectively to crises. This can include a variety of tactics such as cyberattacks on internal systems, the spread of disinformation within the organization, or attempts to manipulate internal decision-making processes. The goal is to compromise the integrity of the institution and to disrupt its effective operations.

A critical vulnerability in many institutions is the lack of a system-wide approach. Organizations often fail to establish a coherent framework for identifying and addressing vulnerabilities across all of their departments and functions. This means there is a failure to consider the multiple dimensions of hybrid threats, which can lead to a fragmented and ineffective response. When institutions do not approach security in an integrated way, they are significantly less resilient and more likely to be successfully targeted. This means that there must be a strong central authority within the organization capable of understanding and coordinating a response.

Another key vulnerability is the lack of understanding on the part of leadership as to what constitutes political interference and manipulation. This primarily stems from the evasive nature of the hybrid threats phenomena, and as a consequence a failure to recognize when an organization has become compromised by malign actors. When there is a failure of leadership, it can significantly undermine the ability of an organization to respond effectively and ethically to a crisis.

Building institutional integrity and internal organization requires a focus on improving security, with specific focus on cybers security as a fast-developing discipline, and strong internal policies, procedures, and communications protocols. This requires a clear understanding of the risks that an organization faces, and an approach that prioritizes preventative measures and planning for potential crises. There must be a focus on developing a more integrated approach to security, which includes all levels of the organization, and which also recognizes that hybrid threats can simultaneously target multiple dimensions of an organization. This should

include regular training programs for all staff members, designed to increase awareness of the potential threats and to empower them to respond effectively.

- **Internal Vulnerabilities to Hybrid Threats (D3.9):** Research observes that hybrid threats target not solely external but also internal organizational structures.

- **Lack of System-Wide Approach (D3.9)** identify a lack of a holistic, system-wide approach to security within institutions as a key vulnerability. D3.9 under "Creating institutional stress for authorities" discusses layers of policy and hierarchy a hindrance to passing timely legislation and formulation of policy, etc.

- **Leadership Awareness and Understanding of Political Interference (D2.8, D3.9)** research points to a gap in leadership's understanding of political interference and manipulation as a critical vulnerability. D2.8 lists "Authorities under institutional stress" as a priority area, highlighting that authorities may lack situational awareness and that short term and ushered decision-making hampers public authorities' abilities to see situations clearly and act wisely.

- Destructive **Culture of Secrecy and Inefficient Processes (D3.9)** in institutions and institutional cooperation can be exploited by malign actors. **Need for Enhanced Cooperation and Information Sharing (D3.9)** research underscores the importance of improved cooperation and information sharing, both internally within organizations and externally between different institutions. D3.9 highlights projects like EUCISE2020, ANDROMEDA, and CONNECTOR, which focus on developing "Common Information Sharing Environments" to improve interoperability and collaboration between various security authorities.

- **Training and Capacity Building (D3.9)**: The documents suggest that training and capacity building are crucial for improving institutional resilience. D3.9 discusses the NOTIONES project, which aims to build a pan-European ecosystem of security and intelligence practitioners for knowledge exchange and capacity building.

5. CORE THEME: INFORMATION AND STRATEGIC COMMUNICATIONS

The modern information landscape has undergone a seismic shift, with social media emerging as a dominant platform for public discourse, overtaking traditional media. This transformation has democratized content creation and dissemination, empowering individuals to share their stories and opinions. However, this has also led to the proliferation of misinformation and disinformation, creating challenges for traditional media outlets and strategic communication channels. The rise of social media has also led to filter bubbles and echo chambers, where individuals are primarily exposed to information confirming their existing beliefs, which can reinforce misperceptions and distrust

Compounding these challenges is the fact that social media platforms are primarily owned and operated by private companies. The regulation of these platforms is still in its nascent stages, and platform owners have, at times, demonstrated a willingness to take strong positions and leverage their platforms to promote specific views, sometimes bordering with election interference. This raises concerns about potential bias and the need for greater transparency and accountability in content moderation practices.

Simultaneously, the reliability and trustworthiness of traditional strategic communication channels are decreasing, making it more difficult for authorities to effectively communicate with the public and maintain public trust.

5.1. RESEARCH AREA: MEDIA CONUNDRUM

MEDIA CONUNDRUM

This area delves into the complex challenges facing contemporary journalistic media in a rapidly evolving information landscape. The core issue revolves around the increasing competitiveness within the media industry, which has led to a surge in practices such as click-bait journalism. This hyper-competitive environment often prioritizes sensationalism and speed of delivery over accuracy and in-depth reporting, creating a situation where quality journalism is at a disadvantage. This not only impacts on the standard of information available to the public but also erodes public trust in established news sources. The problem is further compounded by the rise of social media as a primary source of news for many, where algorithmic curation and the spread of misinformation can easily overshadow responsible reporting. There is also the problem of how to maintain journalistic standards in the context of the pressures to deliver more content, faster, and with fewer resources.

The discussion also extends to the ethical dilemmas that media professionals face, particularly regarding content moderation and data protection. The collection and use of personal data by media platforms raises serious privacy concerns, while the need to moderate harmful content presents challenges related to freedom of speech and censorship. This has led to a call for a clearly defined code of practice for content moderation, especially on social media platforms, and for robust mechanisms to protect personal data. In addition to that, there is a highlighted need to restore the democratic integrity of the media by promoting good practices among journalists and providing them with necessary tools to maintain their standards. This includes improving media literacy to allow the general public to make a difference between true and false information. No less important, that we must recognize, that media is a “business”, so profitable business models is a must for sustaining the ecosystem. The challenge is to balance accuracy and fairness, privacy and transparency, and convenience and dignity in a digital world.

The analysis of this research area includes the understanding that this is not just a technological problem but primarily a societal one, where the values and practices of journalism are questioned, and the solutions should be a mix of sustainable business models, technical and societal means. It is recognized that the media is not only a mirror of society but also a powerful tool that shapes public opinion and therefore, there is a need to ensure

that this tool is used responsibly and ethically. The role of the media as the fourth estate, and its impact on democratic societies, is central to this area of focus. There is also recognition of the need for greater collaboration among different stakeholders, including media organizations, tech companies, governments, and the general public to collectively address the challenges related to media quality and data protection.

- **Economic Viability of Quality Journalism (D3.7, D3.9)** discusses the economic pressures on traditional media and the struggle for sustainable business models for quality journalism. **D3.9** under "Media conundrum" and **D3.7** under "Primary Context No.3: Deterioration of the Quality of Content" directly address this, highlighting the shift towards click-bait journalism and the decline in revenue for quality outlets. **D3.7** points to various alternative business models being explored (subscription, donations, grants, etc.) suggesting a research and testing is needed finding viable economic solutions.

- **Deterioration of Content Quality and Journalistic Standards (D3.7, D3.9)** acknowledges a decline in the quality of journalistic content, driven by economic pressures and the speed-driven nature of online news.

- **Erosion of Public Trust in Media (D3.7, D3.9):** The documents consistently emphasize the erosion of public trust in traditional media sources, also noting that while trust in journalistic content is still present, it is generally decreasing.

- **Rise of Social Media and Algorithmic Curation (D2.8, D3.9):** Research recognizes the transformative role of social media as a primary news source and the challenges posed by algorithmic curation and filter bubbles. **D2.8** priority area "Adapting the news media landscape to new and evolving consumption patterns" directly addresses this shift. **D3.9** under "Media conundrum" highlights how social media can overshadow responsible reporting and contribute to the spread of misinformation. The **PersoNews** project in **D3.9** directly tackles the impact of recommender systems and algorithms on news consumption.

- **Information Manipulation and Disinformation in the Media Landscape (D2.8, D3.7, D3.9):** The documents link the "Media Conundrum" to the broader issue of information manipulation and disinformation. **D2.8** priority areas like "Anticipating cases of foreign information manipulation and interference (FIMI)" and "Understanding the systemic effects of disinformation, misinformation, propaganda" are directly relevant. **D3.7** and **D3.9** under "Going Viral" explore the mechanisms and impact of manipulated information, including fake news, hoaxes, and propaganda, within the media ecosystem.

- **Ethical and Regulatory Challenges (D2.8, D3.9):** Research acknowledges the ethical dilemmas related to content moderation, data protection, and freedom of speech within the evolving media landscape.

- The projects identified, like **PersoNews**, **JOLT**, **MeDeMAP**, and **ReMeD**, exemplify efforts to explore these complex issues and develop solutions for a more resilient and trustworthy media ecosystem.

5.2 RESEARCH AREA: SOCIAL MEDIA AND INFORMATION MANIPULATION

INFORMATION MANIPULATION WITH THE AIM OF DESTABILIZATION

Information manipulation, as detailed across several of the provided documents, has become a primary tool for those seeking to destabilize societies and undermine democratic institutions. The sources underscore the multi-faceted nature of this threat, encompassing not just the deliberate spread of false information (disinformation) but also the unintentional dissemination of inaccurate content (misinformation). This manipulation extends beyond simple fabrication and involves the strategic use of techniques designed to mislead, confuse, and polarize

public opinion. The increasing sophistication of these techniques, particularly with the advent of AI-powered tools, poses a significant challenge for both individuals and institutions.

The development of deep fakes, as highlighted in many research areas, represents a particularly insidious form of information manipulation. The public was already used to the fact, that the “text” is easy to fake, so the audio and video were the primary means to gather the truthful citation. But proliferation of deep fakes, particularly high-quality video and audio, changes the dynamics. These convincingly fabricated videos, audio recordings can be used to damage reputations, incite violence, or sow distrust in political leaders. The ability to convincingly mimic individuals makes it exceedingly difficult to discern what is real, and the increasing capacity of AI models to generate highly convincing but false content raises the stakes even higher. The sheer volume of content being created and disseminated online makes it all but impossible for human fact-checkers to keep up, and that volume also means that these false and manipulated information can spread rapidly and widely on social media platforms. The "filter bubbles" and "echo chambers" created by social media algorithms further exacerbate these problems by reinforcing users’ existing beliefs and creating conditions where misinformation can flourish uncorrected.

The intentional spread of disinformation is often coordinated by state-sponsored actors and other malign groups, who seek to influence public opinion in support of their objectives. This can include foreign interference in elections, attempts to destabilize governments, or efforts to sow discord among different groups within society. EU-HYBNET Research Scan deliverables highlight the critical need to develop robust fact-checking and verification systems that can quickly and accurately identify false information.

However, fact-checking alone is not enough. It is also necessary to understand the motives behind the spread of disinformation, and the sources, and who is likely to be impacted by it, which also includes the psychological and emotional vulnerabilities of different populations. The sources also stress that attribution of this manipulation is essential to hold those responsible to account. This is not always easy, as the digital information space allows malign actors to conceal their identities and operations, which is part of the hybrid nature of this threat.

GOING VIRAL

This area focuses on the rapid spread of information, particularly in the digital era, and its implications for hybrid threat scenarios. The core issue is that the speed at which information can propagate online can be used as a powerful tool for both good and ill. The rapid transmission of data can amplify the impact of any piece of information, regardless of its veracity. This area acknowledges the potential of this capability for spreading positive and beneficial content but also the capacity to spread disinformation and propaganda very quickly to a large number of people, which is the area of focus for this discussion. The rapid spread of misinformation makes it more difficult to control or correct. The focus is to understand how this viral dynamic can be exploited and what solutions can be implemented to mitigate the negative effects.

Research in this area is primarily concerned with defining the scope of the problem, identifying the potential causes and impacts of virality, and proposing solutions to limit the harmful aspects, while utilizing the beneficial ones. The sources note that there is a general lack of a unified approach to reduce the spread of manipulated information, which also acknowledges that there are not universally applicable approaches because of the different context the spread occurs in. There is a fundamental question about the kind of news ecosystem we should be building, one that values and promotes the truth. This includes the need to look at different types of information, whether they are textual or multimedia and how they contribute to the spread. Also, the impact of manipulated information on individual and collective behaviors needs to be examined. There is also a recognition that, the negative impacts are currently assumed but research is needed to more clearly examine the specific effects of misinformation on different segments of society. The discussions highlight that there is a need for international cooperation to find solutions to this problem.

The goal is not just to counteract the spread of manipulated information after it has already gone viral but also to work on the infrastructure and culture that prevents this kind of information to spread in the first place. The sources also acknowledge that simply reacting to viral content is not enough and there is also a need to be proactive in creating an ecosystem that supports the distribution of reliable information. There is a need to find an economically viable business model that supports quality media, which labels their content accordingly to enable the users to make informed choices. The main take away is that the problem is not only technology but also the culture and values, so all these different aspects should be taken into account to create the best possible solutions.

- The research underpinning the "**Normalization of Violence**" highlights phenomena related to the erosion of trust in democratic institutions and the manipulation of public discourse, particularly in the context of hybrid threats. A key research area is the Exploitation of Political Cleavages, where hybrid threats leverage existing societal divisions to sow discord. This is connected to the broader issue of Information Manipulation and Disinformation, with research recognizing its role in eroding trust and normalizing harmful narratives. While projects like **WeVerify**, **SOCIALTRUTH**, and **Co-Inform** (D3.8) are primarily focused on disinformation detection, their work is relevant to understanding the information manipulation that fuels these cleavages. The weakening of Democratic Politics is also examined, where politics and election periods witness increased violence and intimidation. Finally, Social Media and Online Spaces as Amplifiers are considered, as these platforms become key channels for disseminating disinformation and extremist content, with projects like **COMPROP** and **RUSINFORM** (D3.8, D3.9) exploring computational propaganda and foreign influence operations on social media.

- The research underpinning the "Digitization of Private Lives, Massive Availability of Personal Data and Technologies for Personalizing Messages" focuses on phenomena related to the implications of readily available personal data and advanced technologies for manipulation and privacy. Massive Availability of Personal Data and Transparency is a foundational element, leading to concerns about Personalized Messaging and Micro-Targeting and their potential for manipulation, though specific projects for these broader phenomena aren't named directly. Deepfakes and Synthetic Media are highlighted as a significant manipulation technique, with projects like **DIGGER** and **WeVerify** (D3.9) developing detection tools. These factors contribute to the Erosion of Trust and Increased Susceptibility to Manipulation. To counter these threats, research focuses on Cybersecurity and Data Protection Gaps, with projects like **FLUTE**, **SECURED**, **HARPOCRATES**, **PAROMA-MED**, and **ENCRYPT** (D3.9) exploring Privacy Enhancing Technologies (PETs). Finally, addressing the Awareness Gap Regarding Online Risks and Data Sharing is seen as crucial, with projects like **Open Your Eyes: Fake News for Dummies** (D3.9) aiming to improve digital literacy.

5.3 RESEARCH AREA: SHIFTING DYNAMICS OF STRATEGIC COMMUNICATION

OFFICIAL STRATEGIC COMMUNICATION LOSING POWER

This area explores the declining effectiveness of traditional, official strategic communication methods in the current information environment. The core issue is that public trust in official sources is eroding, leading to a situation where the messages conveyed by governments and institutions are increasingly viewed with skepticism and disbelief. This trend poses a significant challenge to the ability of authorities to inform and engage with the public effectively, especially in times of crisis or when it is necessary to explain complex and difficult matters. This is caused by the increasing amount of information coming from various unofficial sources, which are not controlled by official bodies, the perceived bias of official sources, and also the different narratives that are prevalent in the information environment. This loss of trust impacts the ability of authorities to manage crises,

counter misinformation, and promote public good. There is a growing tendency to distrust any kind of official information. This shift requires rethinking of how official communication should be approached in the future.

A critical aspect is the observed lack of scientific research that guides the process of official communication in today's information environment. The sources specifically mention the absence of research on how to communicate uncertainty and bad news without causing panic or further eroding public trust. This lack of a scientific framework leads to an advisory approach, with little empirical base, making it difficult for authorities to develop communication strategies that can effectively counter misinformation and strengthen public engagement. This area of research focus explores how transparency and efficiency of decision-making can be used as a tool for better communication, and how to best involve the public in the process of policy making. It is recognized that transparency can be a means to build trust between the authorities and the citizens. The area also acknowledges that information overload has become a major factor that makes it hard for people to pay attention to official information. The key is to find ways to communicate the information in a clear, concise, and compelling way that can penetrate through the information clutter.

There is a recognition that this problem is not only about techniques of communication but also about the fundamental relationship between the government and the governed. This involves building a culture of open dialogue, where citizens feel that their concerns are heard and addressed, and where communication is not a top-down process but one that is based on collaboration and mutual respect. It also involves recognition that trust needs to be earned and maintained, and that any communication from official bodies must be based on factual information and integrity. There is an underlying discussion about what constitutes a trustworthy source in the modern information landscape and how such sources can be effectively promoted. The main takeaway is the need to move away from traditional, one-way communication approaches and move towards a more dynamic and inclusive model of communication that builds trust.

In summary, the shifting information dynamics present a significant challenge to established communication models. Addressing this involves a multifaceted approach, requiring stronger media literacy, rebuilding trust in credible sources, developing new communication strategies, and tackling systemic issues that contribute to the spread of disinformation. It's also vital to encourage transparency and to support quality journalism, all while adapting to the ever-evolving technological landscape.

- **Erosion of Trust and Societal Cohesion:** A fundamental phenomenon across all research areas is the deliberate and unintentional erosion of trust in democratic institutions, societal structures, and reliable information sources (throughout D2.8, D3.7, D3.9, particularly in topics like "Normalization of Violence," "Institutional Integrity," and "Media Conundrum"). This erosion is fueled by information manipulation and disinformation campaigns, as explored in projects like **COMPROP, RUSINFORM, and IMEDMC (D3.8, D3.9)**, and is exacerbated by the rise of social media and algorithmic curation, as investigated by **PersoNews (D3.9)**. This loss of trust weakens societal cohesion, making populations more vulnerable to polarization, extremism, and manipulation, as highlighted in **D2.8** under "Weakening of Democratic Politics" and research on the "Landscape of Hybrid Threats."
- **Weaponization of Information and Perception:** Information and perception are increasingly weaponized as key instruments in hybrid threats. This is observed in the deliberate spread of disinformation, deepfakes (addressed by projects like **DIGGER and WeVerify (D3.9)** in D3.7 and D3.9 under "The Individual as a Digital Entity"), and manipulated narratives aimed at destabilizing societies and undermining democratic processes (as seen in D2.8's priority areas related to FIMI and disinformation effects, and in D3.9's "Media Conundrum").
- **Gaps in Preparedness, Resilience, and Governance:** Across all domains, the documents highlight gaps in preparedness, resilience, and governance frameworks to effectively counter these complex and evolving hybrid threats. This includes inadequacies in institutional capacities (D2.8 and D3.9 under "Institutional Integrity"), limitations in cross-border cooperation (D3.7 under "Hyperconnectivity"), and a lack of comprehensive regulations and norms to govern emerging technologies and the digital

information space (D2.8 and D3.8 under "Emerging Capabilities" and "Regulation"). While projects like **SPARTA, PRAETORIAN, RADION, and INCLUDING (D3.8, D3.9)** are developing tools and frameworks to improve resilience and situational awareness, the scale and complexity of the challenges require ongoing and intensified efforts. Furthermore, a lack of public awareness and media literacy (addressed by projects like **Open Your Eyes: Fake News for Dummies (D3.9)** and initiatives mentioned in D3.7 and D3.9 under "Media Conundrum") remain significant obstacles to building societal resilience against information manipulation and hybrid threats.

6. OBSERVATIONS AND DISCUSSION

MATURATION OF HYBRID THREATS KNOWLEDGE IS NEEDED

Hybrid threats knowledge areas are still in the maturation stage, and EU-HYBNET no doubt is a very impactful initiative of EC in this maturation path. It helps to expand the hybrid threat community, deepen and spread the knowledge of hybrid threats, as well as build a common vocabulary and understanding.

This maturation path is not easy. Hybrid threats is a very complex and interrelated research area, where management, regulation, and technical aspects of social media and their algorithms, cybersecurity, etc. are very important. But the hybrid threats community still must find its distinct and very clear voice to show what is hybrid in cybersecurity? What is hybrid in space technology?

Task T3.3 "Ongoing Research Projects Initiatives Watch" had its mission look for the hybrid angle in the social and technical phenomena selected as research areas.

This work is ongoing and by no means completed, thus must be continuously done to shape the efforts of hybrid threat community in a most productive manner. We strongly believe, that the efforts like EU-HUBNET is important for consolidating awareness on hybrid threats, developing community and integrating this knowledge area in all aspects of the functioning of society.

NECESSITY OF EVIDENCE BASED REGULATION

One of the frequent proposed solutions in various research areas is regulatory. That international, EU or member state level some aspects of the phenomena (be it space or social media).

While regulations are obviously an extremely important instrument of risk mitigation and encouragement of positive outcomes, two aspects should be stressed in this regard.

First of all, it is important to engage in education of policymakers on hybrid threats, as well as hybrid communicty to actively participate in shaping such regulation, bringing depth of understanding of the phenomena.

Secondly, hybrid threats related phenomena (e.g. social media) are based on human thought process, motivation and behavior, and in broader perspective – politics. So further extensive research is needed to understand fake news related phenomena – how much people are actually susceptible to propaganda? Are they immune to known false information, when it supports their beliefs? How much does it influence their actual behavior?

It is obvious, that even in the very short time EU-HYBNET project lasted, the fact checking necessities were researched in sevaral iterations and highligthed importance of tools and mechanisms there, while after US President D. J. Trump election there was high profile questioning of the concept and cancellation of several initiatives in this area.

Thus recognizing the necessities of regulation, it is important to highlight that extensive research of the human sciences is needed on how information shapes human behavior. .

STRONG EFFORT TO INTEGRATE HYBRID THREATS TO VARIOUS RESEARCH DOMAINS AND MULTIFACET FUNCTIONING OF SOCIETY

Research and efforts in areas relevant to countering hybrid threats are usually fragmented and lack coordination. We consider it a widespread issue.

The ongoing Research Projects Initiatives Watch task revealed, that even EU funded research which works in the areas directly related to the hybrid threats (e.g. chemical and radioactive incidents), hybrid threats are not recognized and consequently defined as the relevant areas in their projects.

EU-HYBNET demonstrated necessity to integrate hybrid threats understanding across the board, as this is a cross disciplinary area. Insufficient understanding and awareness of hybrid threats will result in omitted signals, delays in reaction, failure to act which can have huge cascading effects to countries. Thus it seems of high importance that hybrid threats become an integral part of disciplines.

HYBRID THREATS MITIGATION NEED TO EMBRACE MORE SOCIETAL MECHANISMS, NOT TO RELY SOLELY ON TECHNICAL CAPABILITIES

Both in discussion of Gaps & Needs, and the scanning of research of solutions mitigating hybrid threats, there is a visible tendency of eroding capacity of traditional strategic communication to deliver impactful messages to the population. At the same time social media with popularized alternative views further challenges institutional information.

There are two directions of research. The prevailing line of thought sees strengthening of the resilience against hybrid threats in new regulations, technologies, institutional capacities, etc.

Not so expressed but also visible tendency is to look for up-to-date concepts, methods, and tools, with clear guidance for constructive social dialogue between government and the public. Societal resilience, built on social trust, legitimate governance, and effective institutions, is key to preventing governance breakdown and violent conflict and must be constantly reinvented.

HYBRID THREATS SHOULD BECOME A PAN-EUROPEAN DISCIPLINE

In the research there is an expressed need of better data sharing in strategic and tactical level, as well as common action in the European level.

This stems from the essential feature of hybrid threats – adversaries try to act under the radar, without triggering warning signals in the attacked country.

So there is a very clear case for the better cooperation and coordination among the EU members. Common strategies, sharing signals and information about incidents, sharing competence, can significantly improve situational awareness, identify planned hybrid attacks beyond separate incidents, and improve attribution as well as reaction capacities.

HYBRID THREATS RESEARCH AND PRACTICAL IMPLEMENTATION EFFORTS SHOULD BE SUSTAINED, ESPECIALLY IN THE TURBULENT TIMES OF GLOBAL POLITICS

The overarching common denominator of many observed trends we can identify as “commercialization”, increasingly private ownership of critical Infrastructures, communication platforms, etc. connected with complex and hidden ownership. Their regulation becomes increasingly complex, as one usually has to deal with the very large companies with the complex corporate structure across geographies, significant technological complexities and extremely wide supply chains.

At the beginning of the EU-HYBNET project Russia’s full-fledged war against Ukraine started, which changed very significantly landscape of the hybrid threats.

The hybrid threat subject does not lose dynamism further. With the re-election of D.J. Trump, and his somewhat unpredictable and very active second term, will bring significant changes in the global politics, as well as will reshape transatlantic partnerships.

There is still very clear case to follow the situation and continue research from the point of view of the Hybrid Threats in ever changing global politics landscape.

7. CONCLUSIONS

This deliverable concludes the work done in EU-HYBNET project T3.3 “Ongoing Research Projects Initiatives Watch”.

This deliverable reviews major iterating areas of research, concisely introducing to them in the timeframe of EU-HYBNET project. For more detailed material on specific topics or EU funded projects reader is directed to the deliverables D3.7, D3.8, D3.9.

This deliverable highlights essential evolution of the method used and the results of the scanning.

Lastly, the deliverable offers “Observations and discussion”, which in a concise manner discusses observations in the field of hybrid threats related research and projects.

We believe, that work of T3.3 extends 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 facilitates leverage of EU research project results for wider purposes, than they were intended to.

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	Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek TNO
Hybrid CoE	The European Centre of Excellence for Countering Hybrid Threats
WSN	Wireless Sensor Networks