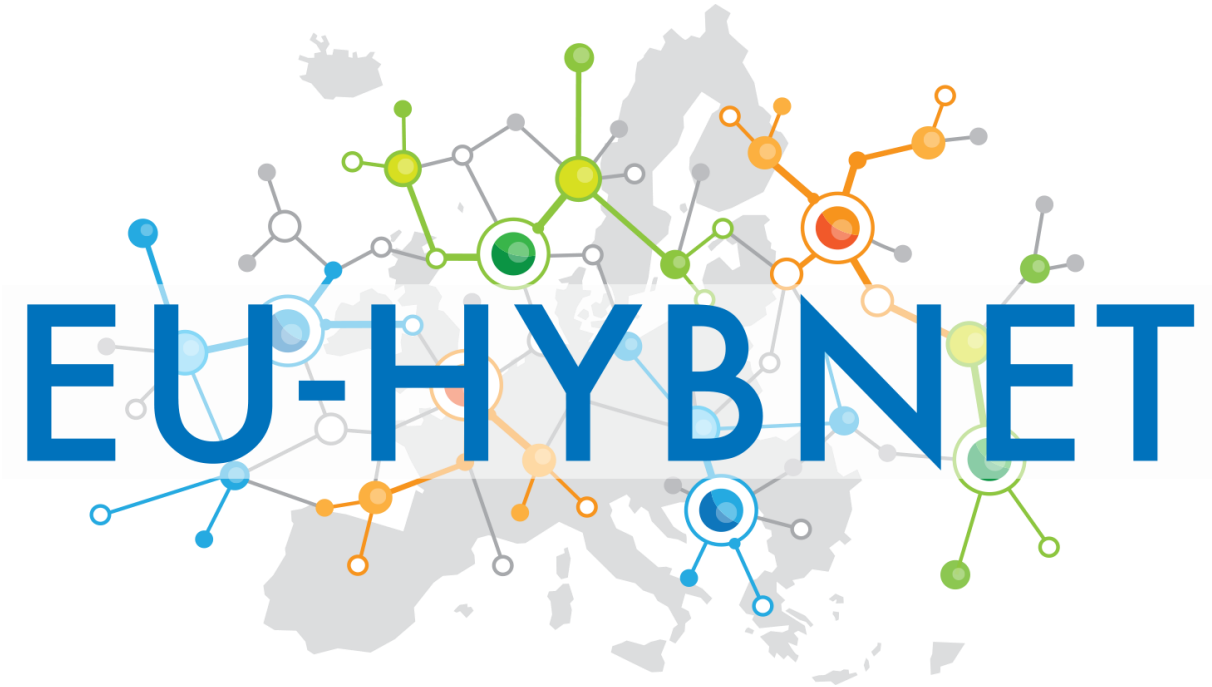

ARTICLES AND PUBLICATIONS ON THEMES AND MEASURES

DELIVERABLE 2.15

Lead Author: Laurea

Contributors: Hybrid CoE, L3CE, URJC, PPHS, JRC, UiT

Deliverable classification: Public (PU)

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

D2.15 ARTICLES AND PUBLICATIONS ON THEMES AND MEASURES

Deliverable number	**2.15**	
Version:	**V 1.0**	
Delivery date:	**05/06/2024**	
Dissemination level:	**Public (PU)**	
Classification level:	**Public**	
Status	**Ready**	
Nature:	**Report**	
Main authors:	Tiina Haapanen, Päivi Mattila	**Laurea**
Contributors:	Julien Théron	JRC
	Hanne Dumur-Laanila	Hybrid CoE
	Malgorzata Wollbach	PPHS
	Ruben Arcos	URJC
	Andrew Paskauska	L3CE
	Gunhild Hoogensen-Gjorv	UiT
	Sabina Magalini, Saverio Caruso	UCSC

DOCUMENT CONTROL

Version	Date	Authors	Changes
0.1	26/4/2024	Tiina Haapanen / Laurea	First draft
0.2	1/5/2024	Gunhild Hoogensen-Gjorv/Uit	Draft planning
0.3	13/5/2024	Andrew Paskauskas/ L3CE	Content delivery
0.4	13/5/2024	Ruben Arcos/ URJC	Content delivery
0.5	13/5/2024	Malgorzata Wollbach/ L3CE	Content delivery
0.6	14/5/2024	Julien Theron / JRC	Text editing
0.7	20/5/2024	Tiina Haapanen / Laurea	Text editing
0.8	22/5/2024	Hanne Dumur-Laanila / Hybrid CoE	Content delivery
0.9	23/5/2024	Tiina Haapanen/ Laurea	Text editing and delivery of the document for review
0.91	30/5/2024	Päivi Mattila / Laurea	Review and text editing
0.92	30/05/2024	Julien Theron/ JRC	Review
0.93	30/05/2024	Sabina Magalini, Saverio Caruso/ UCSC	Review
0.94	03/06/2024	Hanne Dumur-Laanila / Hybrid CoE	Content update
0.94	05/06/2024	Tiina Haapanen/ Laurea	Final editing and document ready for submission
1.0	05/06/2024	Päivi Matitla/ Laurea	Final review and submission of the document to the EC

DISCLAIMER

TABLE OF CONTENT

TABLES

1. INTRODUCTION

1.1 OVERVIEW

The Empowering a Pan-European Network to Counter Hybrid Threats (EU-HYBNET) project's description of Action (DoA) describes this deliverable as the "*Research to Support Increase of Knowledge and Performance*" (T2.2) and the importance to the project proceeding, conducted in EU-HYBNET Work Package (WP) 2 "*Definition of Needs and Gaps of Practitioners' against Hybrid Threats*".

The WP2 Objectives are the following:

1. To identify critical gaps and needs of practitioners, industry and academic actors in knowledge, performance and innovations in the measures against hybrid threats;
2. To increase European stakeholders' knowledge of the hybrid threats via research (focus on the four core project theme and their variations) and hence to enhance European actors' performance and measures against hybrid threats;
3. To facilitate knowledge transfer on present and future cases through dedicated training and exercises and lectures;
4. To test innovations that are seen likely to enhance European stakeholders' measures against hybrid threats and provide material that supports to consider their possible uptake;
5. To support the extension of actors in the European Network against hybrid threats via EU-HYBNET project four core themes' research activities and focus on new key actors in the network.

The following report demonstrates that objectives 1, 2, 3, and 5 are already met and will continue to be developed, while simultaneously feeding results to objective 4 to be tested. These results in turn will inform subsequent articles from the core themes.

In line with other 3rd cycle WP2 deliverables (D2.3 "3rd Gaps and Needs Events", D2.7 "Long list of defined gaps and needs" and D2.11 "Deeper analysis, delivery of short list of gaps and needs"), the findings of D2.15 are reflected throughout the four core themes. The EU-HYBNET four core themes area:

1) Future Trends of Hybrid Threats,
2) Cyber and Future Technologies,
3) Resilient Civilians, Local Level and National Administration,
4) Information and Strategic Communication.

The articles presented in this report reflect our initial results, after the third year of the project, pertaining to the above four core themes. The articles have been developed in relation to the project objectives, with the intent to increase European stakeholders' knowledge on hybrid threats through research on the main criticalities, previously identified, to counter hybrid threats (HT).

The core themes have been instrumental towards providing focal areas in which we can address the extensiveness of hybrid threat domains, but simultaneously to do a deeper dive or analysis that can give security practitioners, policy makers, and scholars alike more depth from which to understand and formulate innovation measures and solutions. Additionally the identification of four core themes allows partners to provide more explicit and concrete analyses of the interfaces that exist between them, and will ensure that the project delivers coherent results in relation to the model.
This deliverable involved collaboration with the core theme leaders and with EU-HYBNET partners' contributions, providing fruitful insights and sharing experience from different fields and points of view.

As during prevous project years, Task (T) 2.2 has conducted research in the form of brainstorming and information gathering in workshops with practitioners and scholars to identify the main gaps and needs targeted within WP2. We further investigated what could be done for a specific gap by each of the four project core theme leaders. The results are to been delivered at least in four articles (or publications) whose outcome produces initial and first-stage recommendations and guidelines for practitioners and policy makers and other EU-HYBNET stakeholders.

The research activity is conducted by the EU-HYBNET consortium members in cooperation with interested EU-HYBNET Stakeholder Board members and extended network members. This is to ensure a broad reach and participation into and by the Network, drawing from a broad and extensive information basis in Europe to contribute to these third and fourth project year research activities.

The overall goal in T2.2 therefore is to increase understanding regarding hybrid threats and support measures related to these threats by the EU. T2.2 contributes strongly to the the European Commission Horizon 2020/Secure Societies Programme/ General Matters (GM) 01-2019 call regarding long term impact that is "*Synergies with already established European, national and sub-national networks of practitioners, even if these networks are for the time being only dedicated to aspects of practitioners' work unrelated to research and innovation (in general, to the coordination of their operations)*".

The overall rationale is to analyse emerging trends of the hybrid threat security environment in order to foster improved anticipation, enable relevant policy formulation and efforts prioritization in responding to hybrid threats and to find innovations (technological and on-technological) that are seen as promising solutions to the gaps and needs. Furthermore, the goal of the EU-HYBNET is eventually to recommend innovation uptake and innovation standardization according to the results of the most promising innovations and hence answer to the needs of pan-European security practitioners and other relevant actors to counter Hybrid Threats. This is also to provide insights for the EC on new research and innovation development areas.

1.2 CORE THEMES

The four project core themes, together with the cycle approach, represent the leading multidisciplinary methodological principles of the project – the themes are 1) Future Trends of Hybrid Threats, 2) Cyber and Future Technologies, 3) Resilient Civilians, Local Level and National Administration, 4) Information and Strategic Communication. These themes link and interface with other hybrid threat domains identified and defined by the European Commission - Joint Research Centre (JRC) and provide a sound window into supporting research and innovation activities in any of the hybrid threat domains considered by the project to be important and capable of delivering solutions during execution of the project cycles.
Each of the four project core themes embody visions that include the variety of challenges that European Union Member States (EU MS) may face when countering hybrid threats in targeted domains and interfaces with other domains. These visions are based on current European high-level research. The themes cover but are not limited to the following:

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

essential to be able to have foresight and build early warning systems. Hybrid threat trend analysis needs to be multidisciplinary and multidimensional using also scenariobased thinking. The future trends of hybrid threats cover also the three other EU_HYBNET themes connecting them to wider security context. This will strengthen situational awareness and identify new and emerging capability needs for countering hybrid threats.

Principal lead: The European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE)

Cyber and Future Technologies

At present, Cyber is treated as a domain of activity or knowledge where there are no rules. As regards hybrid threats specifically, Cyber and future technologies are key components through which new developments produce not only new kinds of hybrid threats, but also act as powerful countering measures in the fight against such threats. Todays' technological upheavals and those of the future suggest that the portfolio of tools used in the realm of hybrid threats will continue to expand rapidly. Computers are ubiquitous, and getting smaller, while processing power is increasing at enormous rates. Other fundamental breakthroughs include robotics, nano- and bio-technologies, artificial intelligence, sensor and 5G technologies. Taken together, these technologies connect symbiotically with people; and they structure society in all spheres – from the interpersonal to the social, and to the military. To be sure, communication technologies are driving these developments. There is still a great deal to learn about how an adversary can make use of these new tools and technologies, how cyber is connecting areas previously not connected to realm of security, like hospitals, and of how we can in fact use these same tools to detect and counter hybrid threats.

Principal lead: Lithuanian Cybercrime Centre of Excellence for Training, Research & Education (L3CE).

Resilient Civilians, Local Level and National Administration

Civilians are central as targets and as actors seeking human and societal security. Too much focus has been placed on the state/government level when it comes to hybrid threats. There is still too little research on how this play out in hybrid threat security environment. Having a better understanding of where the potential vulnerabilities lie within possible target societies enables these same societies – and the diverse civilians within them - to develop measures that can build trust and solidarity within them, making them less vulnerable to such manipulations. This understanding will also help in resilience building that is important for all the EU member states. Civilians are not passive recipients of information or governmental guidance, and trust levels between the governed and government need re-examination. In a democratic society, political decision-making and the opinions of residents are influenced. Various methods are also combined in order to reach the objective of influencing more effectively. This is a normal, deliberative political activity. Just as there is social or communicative influence that cannot be classified as a threat, there is also governmental influence, i.e. diplomacy. However, outside interference and influence may sometimes be a threat. Classifying something as a threat constitutes normative classification: a threat is something unwanted, i.e. something that is deemed to be wrong or evil. Threats can often easily be classified in the legal sense: in many cases, they are a criminal activity. A considerable proportion of the political decisions that affect people's everyday lives are made by municipal boards and councils, and municipalities are in charge of social services, health care and education for example. Law enforcement agencies might be in the frontline when it comes to detecting and countering hybrid threats. Many cases in the recent history have shown us that the local level can play a crucial role both in countering and enabling hybrid threats; Catalonia and Eastern Ukraine as best examples.

Principal lead: The Arctic University of Norway, Tromsø (UiT)

Information and Strategic Communication
Information, strategic communication and propaganda are among the areas that, together with cyber, have been linked to hybrid threats most often. The range of hostile and covert influence activities employed in the past include falsely attributed or non-attributed press materials, leaks, the development and control of media assets, overt propaganda, unattributed and black propaganda, forgeries, disinformation, the spread of false rumors, and clandestinely supported organisations, among others. These activities are recognised to be part of the hybrid playbook. Internet and social media channels have changed the game board for covert influence actions, providing a fertile context for the massive dissemination of overt and covert propaganda by hostile States and non-governmental groups: anyone can produce and disseminate content; connections, funders and identities are blurred; information flows are huge; the speed of information dissemination is breathtaking. AI-generated audiovisual forgeries and the likely future improvements in deep fakes technology appear on the horizon as an insidious threat for democracies that will require developing analytic capabilities to detect and counter them. All these require a sound understanding of communication processes and information flows, developing analytic capabilities and skills for assessing open sources and content, raising strong disinformation awareness, critical thinking, and media literacy, and building positive narratives instead of being on the defensive. While social media networks provide an unprecedented dimension for adversely impacting the potential exposure of target audiences, gathering empirical evidence on disinformation content is required for a full understanding of the effects of influencing campaigns, and thus developing effective strategies and tactics to counter influence. Principal lead: University of Rey Juan Carlos (URJC)

1.3 GROUNDING AND STRUCTURE OF THE DELIVERABLE

This report is grounded in the requirements stipulated by the European Commission Horizon 2020 Secure Societies Programme General Matters (GM) No.1 call that EU-HYBNET follows as funded GM-01 project (DoA Part B/Chapter 1.2) and is also in line with the project Objectives and Key Performance Indicators (KPIs) (DoA Part B/ Chapter 1.1), especially Objective (OB.) 3. "*To monitor developments in research and innovation activities as applied to hybrid threats*" and its Goals and KPIs:

Goal 3.1: To monitor significant developments in research areas and activities in order to define and recommend solutions for European actors.

- KPI description: Monitor research initiatives addressing EU actors gaps and needs in relation to knowledge/performance.
- KPI target value: At least 4 reports every 18 months will be delivered that outline findings from productive research efforts.

Goal 3.2: To monitor significant developments in technology that will lead to recommending solutions for European actors' gaps and needs.

- KPI description: Monitor existing innovations addressing gaps and needs; incl. areas of knowledge/performance.
- KPI target value: At least 4 reports every 18 months that address technological innovations that are able to fulfil European actors' gaps and needs.

The D2.15 deliverable feeds to other WPs, Tasks and forthcoming project cycles. In particular, it refers to:

- WP2 T2.1 “Needs and Gaps Analysis in Knowledge and Performance”: the articles provide the framework upon which new gaps and needs can be addressed in the forthcoming T2.1 Gaps and Needs event. T2.1 will conduct assessment of the critical gaps and needs in knowledge and performance and innovations of practitioners, industry and academic actors focusing on measures against hybrid threats. WP2 T2.4 “Training and Exercises for Needs and Gaps”: the articles tackle relevant contents and means to counter HT which can be used as an additional training material in the EU-HYBNET trainings arranged in T2.4.
- WP3 “Surveys to Technology, Research and Innovations”: the articles include recommendations and reference material to address new innovations or innovation needs which can be benefitted in WP3 activities. WP3 will draw from WP2 a longlist and shortlist of current (and if possible, also future) gaps and needs as identified by the practitioners and the WP 2 team. WP 3 will then use this as input to scan and monitor potential research and innovations that can cover the gaps, needs and requirements. This can range from existing and available research and innovations to future research and innovations.
- WP4 “Recommendations for Innovations Uptake and Standardization”: the articles include recommendations for innovation and uptake of research results which can be benefitted in WP4 activities. In addition, the research articles may provide information to policy papers and briefs delivered in T4.4. “Policy Briefs, Position Paper, Recommendations on Uptake of Innovations and Knowledge”.

This document includes the following sections:

- Section 1 – Introduction to the document
- Section 2 - Research articles’ focus: In this section each research article will be described, including how and why the particular focus of these initial articles were selected, and why the focus was seen especially important to additional research. Moreover, the chapter will clarify how each of the four core themes identified new gaps for their investigations. Furthermore, the articles publishing arena and submission dates are provided, along with the rationale for the selected publishing arena.
- Section 3 - Conclusion: In this section a summary of the research focus and findings are presented as well as the importance of the articles for future work of the EU-HYBNET project.

2. RESEARCH ARTICLES' FOCUS

In what follows, each research article will be described, including how and why the particular focus of these initial articles were selected, and why the focus was seen especially important to additional research. Moreover, the chapter will clarify how each of the four core themes identified new gaps for their investigations and what kind of solutions may be delivered for the gaps. Furthermore, the articles publishing arena and submission dates are provided, along with the rationale for the selected publishing arena.

2.1 CORE THEME – FUTURE TRENDS OF HYBRID THREATS

Title: Employment of uncrewed systems (US) in attacks on critical infrastructure: hybrid threat perspective. Challenges related to recent developments in US technology

Journal: Open Research Europe

Authors: Malgorzata Wolbach, Polish Platform for Homeland Security, Magda Okuniewska, PPHS, Michał Piekarski, University of Wrocław

Focus: The uncrewed systems, known colloquially as drones are nowadays widely used in various roles, including strictly civilian, law enforcement and military. The pace of technological development is high and includes use of modern technologies, like artificial intelligence. Due to the growing threat to critical infrastructure that includes physical attacks, a fundamental question arises: how the development of uncrewed systems shapes the threat to critical infrastructure. Therefore, the article is divided into several parts. The first one describes a legal definition of critical infrastructure. The second one describes the development of uncrewed systems. Finally, scenarios of possible attacks are described. The assessment of influence of modern technology (especially Artificial Intelligence on those scenarios) is provided.

2.2 CORE THEME – CYBER AND FUTURE TECHNOLOGIES

Title: Countering Hybrid Threats: Towards an Ontology for Securing 5G Networks

Journal: Conference Proceedings by SPRINGER Nature under Open Access programme

Article submitted to: 'Computer and Communication Engineering, Third International Conference,' CCCE 2024 in Oslo, May 24-26, 2024, and subsequently published in the Conference Proceedings by SPRINGER Nature under Open Access programme

Author: Andrew Paskauskas, L3CE

Focus: The key findings, or research outcomes and results, can be summarized as follows:

- 5G Threat Taxonomy: Within the framework of the ENISA 5G taxonomy of threats, which classifies the major categories posing threats to 5G infrastructure, critical assets under threat, such as SDN, NFV, MANO, RAN, MEC, CLOUD, and others, are identified, reflecting key components of the 5G architecture.
- 5G Vulnerabilities: An extensive analysis of vulnerabilities within the 5G framework is provided. This covers the 5G Core Network, Network Slicing, RAN, NFV, SDN, MEC, and security

and physical architecture considerations. Specific vulnerabilities in these areas are highlighted, offering insights into potential weaknesses and areas for improvement in 5G security.

- Development of a Basic 5G Ontology: The paper presents an initial ontology for 5G based on ENISA's recommendations from its 5G Threat Landscape Report. This ontology is grounded in the ISO 27005 standard and defines relationships between risks, owners, threats, vulnerabilities, assets, control measures, countermeasures, and attack vectors. This ontology is aligned with the overall design and architecture of the ENISA framework and forms the foundation for securing 5G infrastructure, particularly in support of the 5G Action Plan for Europe and the TEN-T transport corridors.
- Management of Hybrid Threats in 5G ROUTES Project: The paper discusses the management of hybrid threats, which often combine conventional and unconventional methods across different domains. The proposed ontological framework integrates specific risk management strategies to protect and defend against hybrid threats in the 5G ROUTES project. This includes identifying hybrid threat scenarios, assessing their impact on 5G infrastructure, and implementing tailored countermeasures such as enhanced network security protocols and revised operational guidelines.
- Applicability to TEN-T and 5G Action Plan for Europe: The ontological approach is deemed beneficial for the 5G ROUTES trials integral to the functioning of TEN-T corridors. The ontology enables comprehensive risk assessment and management, addressing the complex interactions between different 5G components. It offers a robust framework for managing hybrid threats and aligns with the objectives of the 5G Action Plan for Europe, ensuring the protection and resilience of critical 5G infrastructure within the EU's transport corridors. These findings reflect a comprehensive and multidimensional approach to understanding and securing 5G networks against hybrid threats. They demonstrate the importance of a holistic and integrated framework that considers the complex interplay of various elements within the 5G ecosystem.

2.3 CORE THEME – RESILIENT CIVILIANS, LOCAL LEVEL AND ADMINISTRATION

Title: Weaponized humanitarian migration and potential EU-wide responses to it /TBC

Journal: Open Research Europe

Authors: Maxime Lebrun, Hanne Dumur-Laanila (Hybrid CoE), Annabel Miller, Beth James (Ridgeway BV), Marek Świerczek (ABV), Gordan Akrap (Hybrid Warfare Research Institute) /TBC

Focus: The article addresses the European Union capabilities (tools) to support Member States (MS) facing disproportionate and engineered border pressures from humanitarian migration fluxes. This article only deals with weaponized international humanitarian migration in the form of asylum-seekers being forcibly displaced towards an EU border. It also addresses the strategies of buffer states and non-state actors in terms of extracting revenue from the EU for curbing migration fluxes while obtaining strategic advantages from the EU Member states by encouraging migration towards the EU. EU MS tend to have divergent national interests or priorities while the distribution of asylum-seekers, legal and policy gaps, additionally strain the European asylum system. Further, migration is highly politized issue, as witnessed recently in Finland, Latvia and Estonia. The article unpacks the kind of threat that weaponized migration actually poses to the EU. It should consider and list the feasible options for an EU member state to call for help in facing disproportionate pressure with full respect to human rights standards, especially the role of FRONTEX and the EUAA. The article sheds light on what are the key enablers and barriers and how EU could support more effectively its Member States.

2.4 CORE THEME – INFORMATION AND STRATEGIC COMMUNICATION

Title: Rethinking education and training to counter AI-enhanced disinformation and information manipulations: a Delphi study

Journal: *European Security.*
The article final draft (preprint) will be published at Zenodo with a DOI number on 19 May and submitted simultaneously for consideration to the journal European Security (note that publication times depend on the journals and the review process and not on authors).

Authors: Cristina Arribas-Mato, Manuel Gertrudix, Rubén Arcos Martín, Rey Juan Carlos University (URJC),

Focus: The increasing power and capacity of techniques and technologies associated with the development of Artificial Intelligence have opened a new scenario for the spread of disinformation and propaganda, offering enhanced capabilities for future activities of foreign information manipulation and interference (FIMI). The potential instrumentalization of synthetic content through the presentation of AI-generated audiovisual objects as documentary evidence of events or statements by malicious actors for political aims or economic purposes has been assessed to represent a security threat. However, even if the recognition of the problem and the understanding of the threat are necessary, addressing the phenomenon ultimately requires capabilities and competences from both government authorities and practitioners, but also from a set of stakeholders within civil society. This research article framed under the EU-HYBNET project aims to examine the needs and existing competence gaps for dealing with advanced disinformation as part of hybrid threats and FIMI. Methodology: A Delphi study was conducted during 2023 as part of the research activities of the EU-HYBNET project and through different rounds of online questionaries with experts (n=12) from the EU-HYBNET consortium organizations, the EU-HYBNET network and other experts identified through the project. Existing European competence frameworks were also considered for the research design and its core competences constitute some of the bases for interrogating the experts on present status and potential competence gaps and needs. After processing the data generated from experts and once a sufficient degree of consensus among experts was assessed to exist, we analyze the findings from study. Findings: The results from the Delphy study indicate that AI-based disinformation activities not only constitute already a key challenge for societies, but experts believe that advanced forms of disinformation/FIMI through the use of generative AI and other technologies will be widespread and dominant and will require a proficient level of competence by practitioners. Among other relevant results, the study indicates agreement of the experts (92% with a confidence level of 85%) in that the current Digital Competence Framework (DigComp) for citizens should be expanded with additional areas of competence aimed at practitioners, for providing contextual knowledge on disinformation/FIMI (e.g. threat actors, geopolitical conflicts, historical revisionism) and other additional skills (e.g. detection and analytic techniques, argument-checking). Discussion and conclusion: This suggest that addressing future forms of disinformation and FIMI from an anticipatory and strategic perspective, rather than reactively, would require adapting existing frameworks today and plan education and training approaches to provide competences at a fast pace. For the case of practitioners, this may involve building a formal system of micro-credentials with a practical focus (how-to approach, rather than a what-is approach) and technology-oriented in addition to utilize and augment the existing DigComp framework with additional competences relevant to countering disinformation and FIMI.

3. CONCLUSION

3.1 SUMMARY

In this document we have described research articles' focus, how they were developed, the investigation they are based on, and which are the ways forward to increase understanding on the hybrid threat phenomenon across European practitioners and other relevant actors.

The research activity carried out in each article provided an important initial gathering of information and relevant current literature to strengthen our initial gaps and needs workshops (T2.1) and research, demonstrating further that the gaps and needs that were identified were on track, but further providing initial inputs on hybrid-related vulnerabilities. This work has strengthened our (and readers') knowledge about the current state of the art, but has pushed already beyond this state of the art through novel theoretical and conceptual thinking that will support project proceedings further.

In sum, this document has provided the following:

- In Section 1 we have provided the descriptions of the core themes upon and for which each article was targeted. We also indicated which areas of the project description we have addressed in accordance with EU expectations.
- In Section 2 we provided descriptions of the five articles that have been submitted by the four core theme lead authors and by additional consortium partners, addressing how the focus of each article was selected and why, and what relevance these articles will have to future research.
- In Section 3 the findings of all five research articles are to address. They now contribute to the initial findings established after the third year of the EU-HYBNET project. These results are also linked to potential recommendations and guidelines for practitioners and policy-makers and other stakeholders.

3.2 FUTURE WORK

According to research findings, state-of-the-art analyses and monitoring of developments in research and innovation activities, this document will support increase European stakeholders' knowledge on hybrid threats and performance of implemented measures based on scientific literature, empirical experiences and real-case studies. The findings that have been produced by the articles, will undergo a process of analysis as a basis of work for the next, 4th project cycle in T2.2. It pertains to vulnerabilities, gaps and needs, requirements relevant to each of the four core themes, flagged under 13 hybrid threat domains identified in European Commission's "The Landscape of Hybrid Threats: A Conceptual Model" written by JRC and Hybrid CoE 2020 and further developed in "The comprehensive resilience ecosystem (CORE) model" by JRC and Hybrid CoE in 2023.[1]

Each project cycle will acknowledge findings of earlier research results while also provide new focus areas for research. Each cycle will initiate, continue and stimulate the overall work process, supporting increase of capacity and knowledge and producing in-depth analysis and progressive selection of research focus areas within each project core theme.

[1] Conceptual Model: https://publications.jrc.ec.europa.eu/repository/handle/JRC123305 . CORE Model: https://joint-research-centre.ec.europa.eu/jrc-news-and-updates/new-method-help-policymakers-defend-democracy-against-hybrid-threats-2023-04-20_en

ANNEX I. GLOSSARY AND ACRONYMS

Table 1 Glossary and Acronyms

Term	Definition / Description
D	Deliverable
DoA	Description of Action
EC	European Commission
PU	Public
EU	European Union
EU MS	European Union Member State
EU-HYBNET	Empowering a Pan-European Network to Counter Hybrid Threats project
H2020	Horizon2020
SEC	Secure Societies Program
GM	General Matters call
WP	Work Package
T	Task
OB.	Objective
KPI	Key Performance Indicator
HT	Hybrid Threats
UiT	University I Tromso/ Ar´ctic University in Norway
JRC	Joint Research Centre
Hybrid CoE	The European Centre for Excellence for Countering Hybrid Threats
URJC	University of Rey Juan Carlos
L3CE	Lithuanian Cybercrime Centre of Excellence for Training, Research & Education
Laurea	Laurea University of Applied Sciences
UCSC	Universita Cattolica Sacro Cuore
ABW	The Internal Security Agency (Agencja Bezpieczeństwa Wewnętrznego), Poland
FRONTEX	European Border and Coast Guard Agency
EUAA	European Union Agency for Asylum
5G	5th generation mobile network
DOI	Digital object identifier
ZENODO	General-purpose repository for research data hosted by CERN
FIMI	Foreign Information Manipulation and Interference
SDN	Software Defined Networking
NFV	Network functions virtualization
MANO	Network functions virtualization management and orchestration
RAN	Radio Access Network
MEC	Multi-Access Edge Computing
5G-ROUTE	5th Generation connected and automated mobility cross-border EU trials project
ISO 27005	Information security, cybersecurity and privacy protection standard
TEN-T	The Trans-European Transport Network
ENISA	The European Union Agency for Cybersecurity

ANNEX II. REFERENCES

European Commission Decision C (2014)4995 of 22 July 2014.

Communicating EU Research & Innovation (A guide for project participants), European Commission, Directorate-General for Research and Innovation, Directorate A, Unit A.1 — External & Internal Communication, 2012, ISBN 978-92-79-25639-4, doi:10.2777/7985.