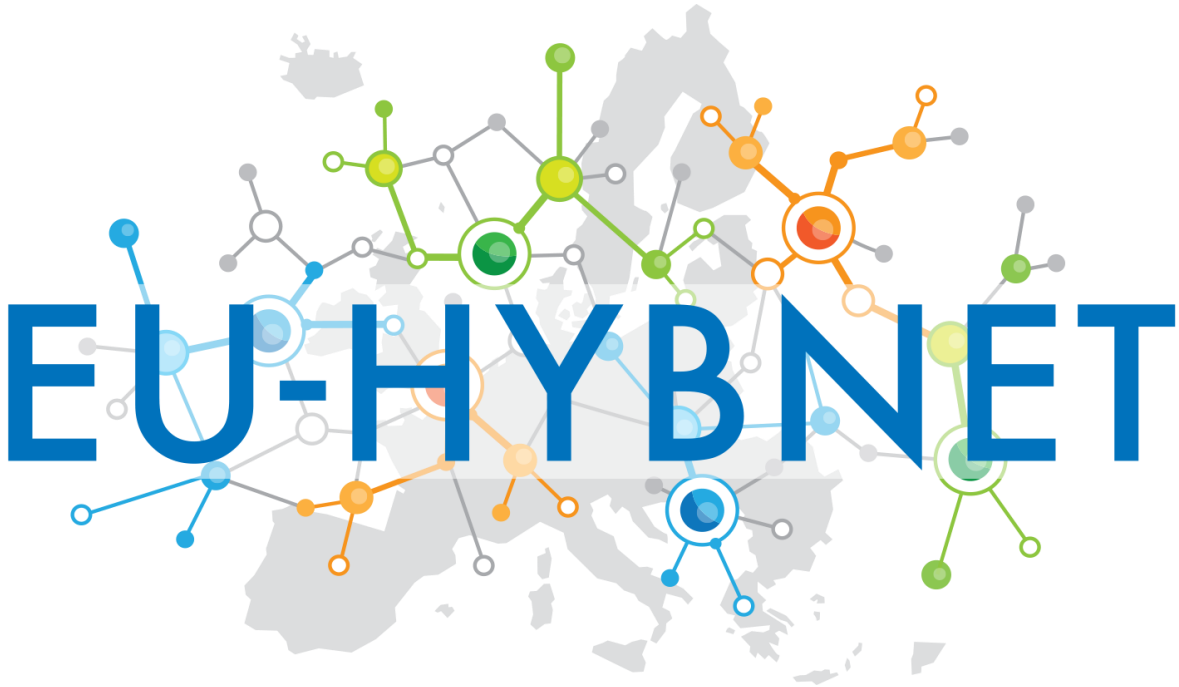

ARTICLES AND PUBLICATIONS ON THEMES AND MEASURES

DELIVERABLE 2.14

Lead Author: UiT

Contributors: Hybrid CoE, L3CE, URJC, Laurea, JRC, Espoo

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

D2.14 ARTICLES AND PUBLICATIONS ON THEMES AND MEASURES

Deliverable number	**2.14**	
Version:	**V 1.2**	
Delivery date:	**26/05/2023 and re-submission 12/1/2024**	
Dissemination level:	**Public (PU)**	
Classification level:	**Public**	
Status	**Ready**	
Nature:	**Report**	
Main authors:	**Gunhild Hoogensen Gjørv, Isabel Dineen, Re-submission/ Julien Théron**	**UiT JRC**
Contributors:	Maxime Lebrun	Hybrid CoE
	Andrew Paskauskas, Evaldas Bruze, Edmundas Piersarskas, Egidija Versinskiene, Rimantas Zylius, Sigute Stankeviciute, Ruta Ziberkiene	L3CE
	Cristina Arribas, Rubén Arcos, Manuel Gertrudix, Kamil Mikulski	URJC
	Satu Laukkanen, Petri Häkkinen	Espoo
	Monica Cardarilli	JRC
	Päivi Mattila, Tiina Haapanen	Laurea

DOCUMENT CONTROL

Version	Date	Authors	Changes
0.1	10/4/2023	Gunhild Hoogensen Gjørv, Isabel Dineen/UiT	First draft
0.21	12/4/2023	Maxime Lebrun/ Hybrid CoE	Text contribution
0.22	12/4/2023	Cristina Arribas, Rubén Arcos, Manuel Gertrudix, Kamil Mikulski/ URJC	Text contribution
0.23	12/4/2023	Andrew Paskauskas, Evaldas Bruze, Edmundas Piersarskas, Egidija Versinskiene, Rimantas Zylius, Sigute Stankeviciute, Ruta Ziberkiene/ L3CE	Text contribution
0.3		Gunhild Hoogensen Gjørv, Isabel Dineen/UiT	Editing
0.4	5/5/2023	Päivi Mattila/ Laurea	Review
0.51	5/5/2023	Monica Cardarilli/ JRC	Text editing
0.52	10/5/2023	Monica Cardarilli/ JRC	Text contribution
0.6	10/5/2023	Andrew Paskauskas/ L3CE	Addtional text
0.7	10/5/2023	Rubén Arcos/ URJC	Additional text
0.8	15/5/2023	Satu Laukkanen, Petri Häkkinen/ Espoo	Review
0.91	24/5/2023	Gunhild Hoogensen Gjørv/UiT	Text editing
0.92	25/5/2023	Päivi Mattila/ Laurea	Final review and text editing.
0.93	26/5/2023	Gunhild Hoogensen Gjørv/UiT	Final Review
1.0	26/5/2023	Päivi Mattila/ Laurea	Document submission to the EC
1.1	11/1/2024	Julien Théron/ JRC	Document updates and text editing
1.2	12/1/2024	Päivi Mattila/ Laurea	Final review. Document re-submission to the EC.

DISCLAIMER

TABLE OF CONTENT

TABLES

FIGURES

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 D2.14 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 themes of the articles are deriving from the 3rd Gaps and Needs Event held in Rome on 28 March 2023.

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 (HCoE)

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 D2.14 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 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 - Main findings in research articles: In this section a short summary of each of the research articles' research findings is described. In addition, it is explained how the research outcomes has produced recommendations and guidelines for practitioners and policy makers and other EU-HYBNET stakeholders.
- Section 4 - 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.

Lastly the document addresses the Requested Improvements from the 2nd EC Project Review. In short, in the 2nd EC Project Review the following improvements to the EU-HYBNET article and research delivery were requested:

- The project team should evaluate the quality of their academic output, and that it is highly recommended that the project team attempt to publish academic work through journals with a more robust peer-review process.
- Achieve more coherence across the 13 domains and 4 core themes. One of the findings from the EC Project Review was that *the project is unable to identify the exact defining patterns and traits of hybrid threats.*

- If the project partners can publish work in peer-reviewed journals with open access, then this would be ideal.

Based on these recommendations, the following improvements are planned for article delivery:

1. Broader communication and dissemination of project publications will be done to ensure better public outreach and exploitation of project findings and products. This could be done by presenting project outcomes in more international conferences and special workshop sessions (following the example of CRITIS 2022). An additional way could consist in creating a EU-HYBNET group on LinkedIn where sharing of research articles, project initiatives and periodic newsletters could be fostered, enhancing project visibility and awareness of stakeholders at the same time. This would be discussed and done in collaboration with the project communication office.
2. Despite EU-HYBNET Description of Action (DoA) does not require peer-review process for project publications, in the next cycle the authors of the research articles will be encouraged to consider peer-review publication process. Targeted journals are mentioned next to each article described in this document.
3. During the present 3rd cycle the analytical work will enhance coherence across the 13 domains, involving more inter-disciplinary knowledge and cross-cutting expertise of consortium partners as well as through the engagement of new network members for a more comprehensive outcome within the respective competences of the 4 core themes. This approach aims also to strengthen network partners' collaboration so as to identify and incorporate further perspectives and inputs into the project's present 3rd and forthcoming 4th cycle deliverables.

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: Conspiracy beliefs and the platforms: circulation, impact, and the crux of regulation
Journal: Open Research Europe
Open Research Europe was chosen because it offers an easy and good-quality publishing platform to share EU-funded project research findings openly. Other journals are considered as well.

Articule submitted to: *Open Research Europe*

Lead Author: Maxime Lebrun

Other authors: Hanne Dumur-Laanila, Pablo Hernández Escayola, Gwenda Nielen

Focus: This article addresses the patterns of circulation of conspiracy beliefs and their attractiveness on social media and online platforms. It proposes a qualitative analysis of their impact, their virality patterns as well as the systemic risks it carries. The circulation and mainstreaming of conspiracy beliefs is a key leverage for hybrid threat activity against the integrity and soundness of liberal democratic governance. This article addresses the current regulatory landscape in the EU as concerns very large online platforms in light of the DSA and DMA. It further wonders the type of relevant regulatory needs or breakthrough in order to address the political risk created by the ease and virality of conspiracy beliefs circulation and especially how it undercuts growing and essential parts of liberal democratic governance.

2.2 CORE THEME – CYBER AND FUTURE TECHNOLOGIES

Title: An Ontological Approach to Understanding and Managing Hybrid Threats in 5G Networks

Journal: *Open Research Europe*

Article submitted to: *Open Research Europe*

Part 1 of this EU-HYBNET research effort was published by ORE earlier this year: 'ENISA: 5G design and architecture of global mobile networks; threats, risks, vulnerabilities; cybersecurity considerations' [version 3; peer review: 3 approved] - https://open-research-europe.ec.europa.eu/articles/2-125

In the Summary statement of this publication a commitment was made to continue the work in a follow-up paper. In effect, the 'Decoding 5G security...' effort represents the results of this commitment. However, this is not say that this is the only reason why a decision was made to publish

in ORE's platform. Indeed, publishing in Open Research Europe (ORE), the European Commission's affiliated platform, instead of a traditional journal, has several strategic advantages and implications: ORE is an open-access platform, ensuring that the research is freely available to a wider audience without any paywall barriers. Publishing on ORE, an EC initiative, aligns the research with the EC's objectives and strategies, ensuring it directly reaches key decision-makers and influencers in the European context. ORE caters to a diverse, interdisciplinary audience. Given the multifaceted nature of 5G security, which intersects technology, policy, and societal impacts, the platform is well-suited to reach a broad range of disciplines that traditional journals may not. ORE provides faster publication times compared to traditional journals. Given the rapid evolution of 5G technology and its associated threats, timely publication is crucial to ensure the research is relevant and can promptly inform policies and practices. The open peer-review process of ORE fosters transparency and constructive feedback, potentially leading to collaborations and engagements with other experts in the field. This interactive review process can enrich the research and its applicability. Publishing in ORE adheres to the principles of open science, promoting accessibility, transparency, and reproducibility in research. This aligns with contemporary movements towards more open and collaborative scientific inquiry. Open-access articles are generally more accessible and have a higher likelihood of being cited, increasing the impact of the research. This is particularly beneficial for research with significant societal implications, like 5G security. Choosing ORE demonstrates a commitment to the democratization of knowledge and supports the EC's initiatives to make scientific knowledge openly accessible, benefiting the wider European research community.

Author: Andrew Paskauskas

Focus: This paper presents an ontological approach to understanding and managing hybrid threats in 5G networks. The concept of hybrid threats is explored, with a focus on their principal targets and the actors perpetrating the most serious threats. The study utilizes an analytical framework and taxonomy that interconnects all relevant elements of the techno-socio-politico ecosystem to facilitate a comprehensive understanding of hybrid threats in relation to 5G infrastructures, as well as unwanted cyber attacks. Most of the ideas regarding structure, analytical framework, domains, and phases are influenced by JRC's study on "The Landscape of Hybrid Threats: A Conceptual model". It is found that all phases have a strong psychological component and may involve strategies of interference, influence, operational campaigns, or at times involve escalation or even de-escalation. The paper also highlights the best-in-class 5G security measures to counter hybrid threat onslaughts. In conclusion, this ontological approach provides a more comprehensive understanding of the complex nature of hybrid threats in 5G networks and can help organizations and policymakers develop effective countermeasures to safeguard against potential threats.

2.3 CORE THEME – RESILIENT CIVILIANS, LOCAL LEVEL AND ADMINISTRATION

A particular effort has been made in this Core Theme in order to catch back the project's year 1 and 2, to deliver to year 3 and to plan a delivery for year 4. The three first years' articles have been completed and are in the submitting process. The article which had been proposed in the earlier version of this report has been

- **Year 1 (submitted to the publisher by 3 february):**

Title: The merging of people, states, and fear: the role of civilians in hybrid threats

Published in: *Targeting the core of state security: Resilient Civilians in Hybrid Threats and Warfare*. Gunhild Hoogensen Gjørv, Sergii Glebov and Christopher Holshek, eds: Sage/IOS Press

Authors: Gunhild Hoogensen Gjørv and Sergii Glebov

Focus: To be provided. Funded by EU HYBNET and NATO SPS Programme.

- **Year 2 (submitted to the publisher by 3 february):**

Title: Fearing Identities: Gender and Intersectional Analyses of Hybrid threats

Published in: *Targeting the core of state security: Resilient Civilians in Hybrid Threats and Warfare*. Gunhild Hoogensen Gjørv, Sergii Glebov and Christopher Holshek, eds: Sage/IOS Press

Authors: Gunhild Hoogensen Gjørv, Jane Freedman, Velomahanina Razakamaharavo, Outi Jalonen

Focus: To be provided. Funded by EU HYBNET and NATO SPS Programme

- **Year 3 (November 2023):**

Title: Comprehensive security, disinformation, and COVID-19: An analysis of the impacts of mis- and disinformation and populist narratives during the pandemic

Published in: *Open Research Europe*

Main reason for publishing in Open Research Europe: Open Access. This publication venue has been used by other EU-HYBNET authors, and seemed like a good venue also for this paper.

Authors: Arsalan Bilal, Gunhild Hoogensen Gjørv, Marc Lanteigne, Rachele Brancaleoni, Jardar Gjørv, Daniele Gui, Justyna Karolina Kielar, Caleb Aluola, Sabina Magalini

Focus: The Covid-19 pandemic has generated many fundamental and challenging implications regarding security, for both states and people. This report addresses the pandemic as a security threat, whereby societal and human dimensions of security are intertwined with the narrower (so-called traditional) state dimensions, culminating in comprehensive security. Drawing on both security theory and policy, the report examines how the Covid-19 pandemic jeopardised security on multiple levels. First, the state's capacity to effectively act and deliver in the domestic sphere waned. Second, the social contract between the state and its citizens eroded as public trust dissipated. This report argues however that the most pervasive threat to security during the pandemic pertains to the exploitation of the information domain in relation to the state, society, and people. The report interogates how mis- and disinformation about the pandemic compounded and exacerbated the security challenges it posed, often relying on existing narratives within right-wing populism movements to increase mistrust and discontent. These largely right-wing populist narratives contributed to broadening the gap between states and people, weakening public compliance with state health security measures. The nature of populism and the narratives of particularly right-wing populism contributed to increases in fragmentation, polarisation, and discrimination impacting societal trust. The report concludes with recommendations to mitigate the impact of mis- and disinformation, including reinvigorating the relationship between state institutions and the people to strengthen comprehensive security. Funded by EU-HYBNET and Norwegian Research Council (FAKENEWS project).

- **Year 4 (Submission target date April 2024):**

Title: Populism, everyday security, and the threat of disinformation

Journal: *Journal of Human Security*

Lead Author: Gunhild Hoogensen Gjørv and select authors (tbd).

Focus: This paper explores the interaction and integration of technology into human life, which in turn facilitates or amplifies perceptions of security and insecurity. People's lives, expression of values, and their "everyday security" are more integrated with the digital world than ever before, to the extent that it is no longer a question of being online, but being in our "onlife". Technological developments from mechanical to digital capabilities have not only made many people's lives easier (eg reduced task time, quicker communication, etc), but have been platforms for, and amplifiers of, average person's essential values and thus their perceptions of in/security. Populism—a concept that depending on its content, fosters a political trajectory that pits "the pure people" or "us" against a manipulative or even evil "elite" has resurged as we have become more digitally dependent.

Technology itself is not the threat, but a potential threat emanates from the human relationship to technology. Thanks to algorithms that curate people's values and choices on the basis of what their interests appear to be, individuals find themselves echo chambers and down rabbit holes where the information received becomes ever-more targeted toward certain narratives reflecting concentrated back at us. This customized information confirms and reconfirms our values and beliefs, often framing these as facts. There is already ample evidence that algorithmic information feeds are easily susceptible to disinformation because the constant tailoring of information to fuel engagement almost inevitably gravitates to that which is increasingly shocking and provokes anger, disgust, fear, or a combination of these. People are susceptible to certain types of disinformation because of our preexisting beliefs, values, and opinions that reflect a distrust of others (particularized distrust) or society (general distrust). This generates reactions like fear, anger, shame and disgust often filtered through assumptions and prejudices rooted in gender, race, class, age, ethnicity, and sexual orientation. Some forms of populist rhetoric take advantage and benefit from these reactions, to polarize debates on the basis of feelings of fear, hate and disgust. Drawing on theories of human security, civilian agency, (general and particularised) trust, and cognitive security, and combined with intersectional methods, this paper introduces a method of everyday security that attempts to better understand perceptions of security as products of targeted by populist-informed disinformation. Funded by EU-HYBNET and Norwegian Research Council (FAKENEWS project).

2.4 CORE THEME – INFORMATION AND STRATEGIC COMMUNICATION

This CORE theme has been the object of particularly intense research. The authors are scholars and performed strong qualitative investigations in order to build robust research. The URJC team started in this respect to draft the article and elaborated a first online questionnaire to be sent to security experts already in August 2023. They aimed to reach at least 20 experts with a balanced representation of practitioners/experts (i.e.: HCoE, EEAS, Europol, NATO Stratcom CoE, intel/sec organizations, fact-checking/debunking orgs, academia/research centers and from business orgs). As the contacts and meetings revealed, the received answers were not strong enough to build solid results, and instead of building a weak piece, the authors preferred to elaborate a subsequent questionnaire more integrated to EU-HYBNET consortium and organizations. The questionnaire have been sent in the beginning of the fall, and time was missing to analyse the productive data. It has been therefore proposed and agreed to the team to continue and achieve their work, but to transfer the deliverable in the framework of year 4 of the project.

Title: Rethinking education and training to counter AI-enhanced disinformation and information manipulations: integrated awareness, professional competences, and technologies

Journal: Potential OA journals we are considering :

- *New Media and Society*
- *Learning, Media and Technology*
- *European Security*
- *El Profesional de la Información*
- *Open Research Europe*

Authors: Rubén Arcos and Manuel Gértrudix

Focus: This article explores existing knowledge and competences gaps for addressing technology enhanced FIMI and disinformation as part of hybrid threats. As such, the article aims to building a competence-based education and training model, analyzing cases illustrating knowledge and skills gaps (i.e., synthetic content, immersive communication, virtual reality, and others) as well as analyzing expected impact against hybrid threats and in cognitive warfare.

The article explores existing knowledge and competences gaps for addressing technology enhanced FIMI and disinformation as part of hybrid threas. The aim of the article is to build a competence-based education and training model. The article will analyze cases illustrating knowledge and skills gaps (i.e., synthetic content, immersive communication, virtual reality, and others), and analyze expected impact against hybrid threats and cognitive warfare.

2.5 ADDITIONAL ARTICLES BY PROJECT PARTNERS

No additional articles have been submitted by the partners.

3. MAIN FINDINGS PRESENTED IN RESEARCH ARTICLES

In this section a short summary of each of the research articles' research findings will be added when the articles have been submitted to review. This will be early autumn 2023.

3.1 CORE THEME – FUTURE TRENDS OF HYBRID THREATS

Title: Conspiracy beliefs and the platforms: circulation, impact, and the crux of regulation

The way social media companies work is relevant to tame the potential for hybrid threat activity. Disinformation, misinformation, conspiracy belief circulation, brutalisation, and polarization of societies are phenomena deeply detrimental to civic discourse and more broadly to the soundness of liberal democratic governance. The business model of social media – capitalizing on human attention encourages the phenomena structurally. The circulation of conspiracy beliefs runs wide on various social media platforms, with the notable examples of Telegram and X under Elon Musk. The article advances that social media exploit a legal loophole that makes them non responsible publishers since they are historically and durably shielded by a blanket immunity provided by the US legislation. This legal loophole must be fixed considering that the platforms may produce their own content via the message their suggestion algorithms deliver to their users. The legal loophole is also wide in terms of responsibility since social media platforms also clearly work beyond publication of content: they also sustain real-world networks of affinities. For this series of reasons as outlined in the article, countering hybrid threats implies taming the circulation of conspiracy beliefs on social media by getting the platforms to become responsible of the contents that go through their services. This would place an appropriate business incentive for regulation and would likely preserve the profitability of social media companies as businesses.

3.2 CORE THEME – CYBER AND FUTURE TECHNOLOGIES

Title: An Ontological Approach to Understanding and Managing Hybrid Threats in 5G Networks

ENISA's 5G Threat Taxonomy provides a comprehensive framework for classifying threats. Starting with this taxonomy the research has uncovered the route towards the formulation of a prototype ontology for 5G security in relation to the challenge of countering hybrid threats. The research has produced the means to take into account ENISA'S use of ISO 27005 to reveal the critical relationships between the various classes of risks, owners, threats, vulnerabilities, assets, controls, countermeasures and attack vectors, and their respective sub-classes and attributes, and construct an ontology that makes use of RDF/OWL coding techniques to effectively connect the ontology to the relevant categories of JRC's Cybersecurity Taxonomy. In uncovering this path, the principal outcome of the research demonstrated how to align the specific EC cybersecurity requirements demanded of European R&D consortia seeking funding for EU 5G infrastructure projects.

3.3 CORE THEME – RESILIENT CIVILIANS, LOCAL LEVEL AND ADMINISTRATION

Title (Year 1): The merging of people, states, and fear: the role of civilians in hybrid threats

To be provided.

Title (Year 2): Fearing Identities: Gender and Intersectional Analyses of Hybrid threats

To be provided.

Title (Year 3): Comprehensive security, disinformation, and COVID-19: An analysis of the impacts of mis- and disinformation and populist narratives during the pandemic

The Covid-19 pandemic impacted security on different levels, such as state, society, and people: economic and sociopolitical instability, derailed social contract between the state and its citizens, unrest, citizen's physical survival, livelihood, and dignity, and data exploitation. The Covid-19 pandemic questioned how freedom of expression could be used to erode society's and state's security. This paper addresses many importante issues, such as the nature of the threat, the source of the threats, how freedom is looked for, the security level (individual, group, nation, state, multi-level), security opmtima for the concerned actors. This article dives into questioning, in the light of Covid-19 exceptional situation and through a comprehensive approach, the state of security and threats beyond traditional realist paradigm. Using critical security studies, it embraces a multi-actor and multi-sector approach.

Title (Year 4): Populism, everyday security, and the threat of disinformation

The rate and extent of disinformation is increasing rapidly, where incidences of tampering of news, images and videos are multiplying well beyond our capacity to track each incidence and its impact. This form of hybrid threat activity is often defined as a tool that targets existing vulnerabilities in society, spreading information that is distorted in some way or another - from making small alterations to a truth to a full distortion or false claim – for the purpose of fomenting distrust and doubt between people and authorities, or between groups of people themselves. Often these disinformation events are characterized as being unattributable, that is, that it is not easy or at all possible to track where the disinformation originated. Mitigation measures have included media literacy, encouraging people to check the legitimacy of sources of information, particularly that which is provocative or engenders strong emotional reactions. The goal is to increase awareness within society, which is the target of disinformation, of how to identify disinformation material when it can be linked to suspicious, obscure sources. But what happens when the source is open, and one that you trust?

An increasing challenge is emerging as disinformation has been shared by people in "positions of trust", that is, are leaders in a community that make claims that repeat and/or perpetuate disinfo in the public space. These include media, political, and academic actors. Core values are challenged, pitting academic freedom and freedom of speech or expression against today's potential to exacerbate and inflame existing vulnerabilities and conflict lines in society, that can threaten the stability of society. The potential for contributing to polarizing debates is heightened when problematic, disinformation-laden narratives are shared openly by people who the general public usual respect or look to for their information about potential threats to their own (human or individual security, including economic, identity/community, health, etc security) and the security of society and the state.

3.4 CORE THEME – INFORMATION AND STRATEGIC COMMUNICATION

Title: Rethinking education and training to counter AI-enhanced disinformation and information manipulations: integrated awareness, professional competences, and technologies

As indicated in "2.4 CORE THEME – INFORMATION AND STRATEGIC COMMUNICATION", the main findings of the article will be presented in the year 4.

3.5 ADDITIONAL ARTICLES BY PROJECT PARTNERS

No additional articles have been submitted by the partners.

4. CONCLUSION

4.1 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.

Finally, it is worthy highlighting an indirect, but equally (if not more) important result; the synergies that become clear between the priorities of the core themes. Each core theme has provided a solid product that highlights in fact similar or related concerns, but from importantly different angles. These articles provide the substantive departure point the core themes need to now find overlapping research interests and questions that can be pursued as we move forward, in addition to building on research within each core theme.

CORE Theme – Future Trends Of Hybrid Threats

The article topic transcends all core themes by addressing the challenges on how social media companies' activities poses a systemic risk to the democratic resilience. The legal loophole in which the social media companies operate, offers a gateway to spread harmful and illegal content and a space for malicious interference, which all are in the core of hybrid threats.

CORE Theme – Cyber And Future Technologies

Contribution to Project Coherence. The article contributes to the coherence of the EU-HYBNET project, particularly aligning with the first two core themes: 1. Future Trends of Hybrid Threats and 2. Cyber and Future Technologies. The research findings and developed ontology provide a nuanced understanding of the complex interplay of 5G related cyber risks, offering insights crucial for addressing challenges in several of the project's domains.
Theme 1: The paper directly addresses future trends in hybrid threats by outlining a structured taxonomy and ontology of emerging and existing cyber threats in 5G networks. This approach not only

identifies current vulnerabilities but also anticipates future challenges, enhancing the resilience of critical infrastructures and digital systems against sophisticated hybrid threats.
Theme 2: By focusing on the cybersecurity challenges posed by 5G technologies, the article contributes to a deeper understanding of the cyber domain. It highlights the intricacies of network-based, device-related, application-level, and virtualization threats, which are paramount in safeguarding digital infrastructure and maintaining the integrity of the digital economy.

Relevance to Specific Domains; 6/13. The article reinforces the interconnectivity of the 13 domains by demonstrating how advancements in 5G technologies and their associated cybersecurity challenges influence various aspects of modern society. By providing a comprehensive framework for understanding and countering 5G related hybrid threats, the research outcomes offer valuable guidance for practitioners, policymakers, and stakeholders across multiple domains, ensuring a cohesive and informed approach to countering hybrid threats in an increasingly interconnected world. Six of the thirteen domains are of special relevance in the present context. These are:

- Infrastructure: The paper's insights into network-based threats are vital for protecting critical infrastructure like energy and transportation systems, especially as they increasingly rely on 5G technologies.
- Cyber: The comprehensive categorization of cyber threats provides a framework for understanding and mitigating diverse cyber risks, from malware attacks to data breaches.
- Space: The research indirectly supports the space domain by highlighting the significance of secure communication networks, which are fundamental for satellite operations and GPS services.
- Economy: By addressing cybersecurity risks, the article indirectly contributes to the economic domain, where digital security is crucial for financial stability and trust in trade networks.
- Military/Defence: Insights into emerging 5G threats have implications for military and defense strategies, particularly in the context of hybrid warfare and information security.
- Information: The research underscores the importance of protecting information integrity, aligning with efforts to counter disinformation and misinformation in the information domain.

CORE Theme – Resilient Civilians, Local Level And Administration

The four articles are centred on the core theme Resilient Civilians – they are products of the project that informs EU-HYBNET. As for the domains – the work done in the Resilient Civilians core theme – whether at EU-HYBNET or in other related projects I have going, address virtually all the themes because they are almost all within the civilian domain! (see another paper I have coming out with Hybrid CoE – but they did not want that shared with EU-HYBNET The results of these two projects are logically connected, as they are also connected to further funded projects I have from the Norwegian Research Council and the Norwegian Defence Dept.

4.2 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.

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.

ANNEX I. GLOSSARY AND ACRONYMS

Table 1 Glossary and Acronyms

Term	Definition / Description
D	Deliverable
DoA	Description of Action
EC	European Commission
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
RC	Resilient Civilians
UiT	University I Tromso/ Artic University in Norway
JRC	Joint Research Centre
Hybrid CoE/HCOE	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, Finland
DSB	Norwegian Directorate for Civil Protection
MTES	Ministry of Ecological Transition, France
Maldita	Maldita, a fact checker organization, Spain
MVNIA	The “Mihael Viteazul” National Intelligence Academy, Romania
CI	Critical Infrastructure
COMM	EC Communication

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.