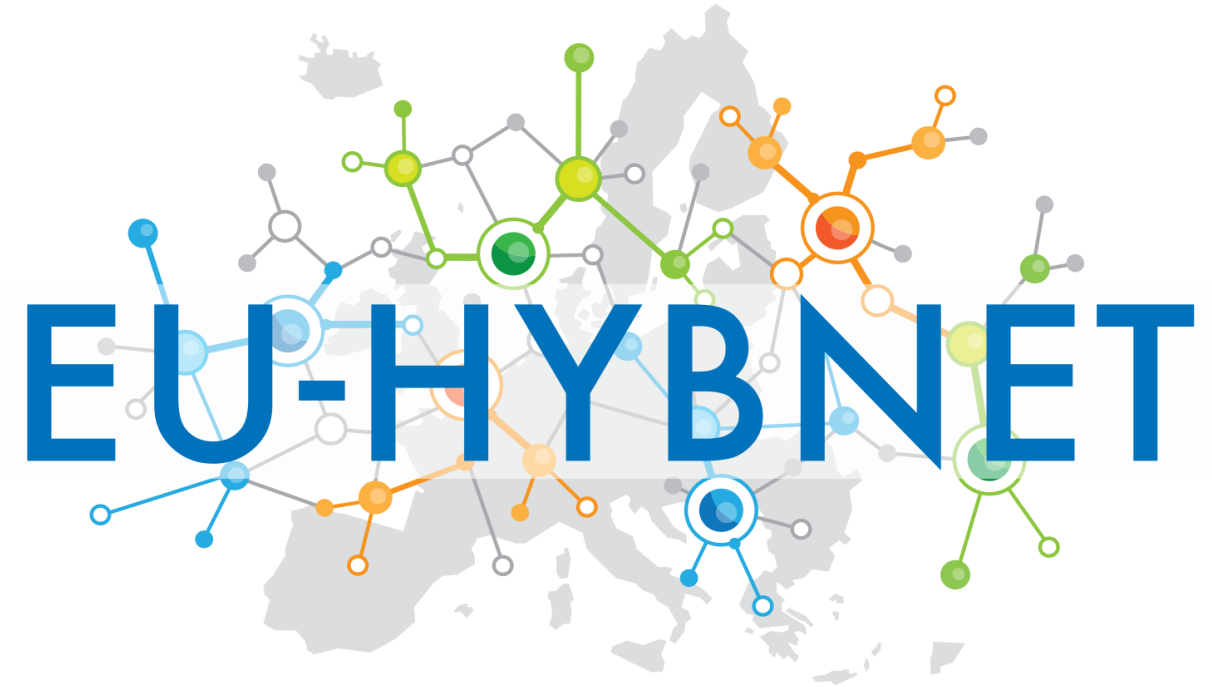

ARTICLES AND PUBLICATIONS ON THEMES AND MEASURES

DELIVERABLE 2.12

Lead Author: UiT

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

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

D2.12 ARTICLES AND PUBLICATIONS ON THEMES AND MEASURES

Deliverable number	**2.12**	
Version:	**V1.0**	
Delivery date:	**03/5/2021**	
Dissemination level:	**Public (PU)**	
Classification level:	**Public**	
Status	**Ready**	
Nature:	**Report**	
Main authors:	**Gunhild Hoogensen Gjørv and Isabel Dineen**	**UiT**
Contributors:	**Ruben Arcos** **Maxime Lebrun** **Evaldas Bruze** **M. Cardarilli, Rainer Jungwirth, Georgios Giannopoulos** **Stefan Pickl, Son Pham** **Päivi Mattila**	**URJC** **Hybrid CoE** **L3CE** **JRC** **COMTESSA** **Laurea**

DOCUMENT CONTROL

Version	Date	Authors	Changes
0.1	10/3/2021	UiT/ G. Hoogensen Gjørv, I. Dineen	First draft
0.2	16/4/2021	Hybrid CoE/M. Lebrun	Contribution to text
0.3	26/4/2021	URJC/ R. Arcos	Contribution to Text
0.4	20/4/2021	UiT/ G. Hoogensen Gjørv and I. Dineen	Text editing
0.5	28/4/2021	L3CE/ E. Bruze	Contribution to Text
0.6	28/4/2021	COMTESSA/ S. Pickl, S. Pham	Review
0.7	30/4/2021	JRC/ M. Cardarilli, R. Jungwirth, G. Giannopoulus	Review
0.8	30/4/21	UiT/G. Hoogensen Gjørv and I. Dineen	Text editing and final draft
0.9	3/5/2021	Laurea/ P. Mattila	Review
1.0	3/5/2021	Laurea/ P. Mattila	Final version for submission

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 previous WP2 deliverables (D2.1 "1st Gaps and Needs Events", D2.2 "Long list of defined gaps and needs" and D2.9 "Deeper analysis, delivery of short list of gaps and needs"), the findings of D2.12 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 first 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 D2.2 and D2.9.

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 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.

Task (T) 2.2 conducted research in the form of brainstorming and information gathering 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 have been delivered 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 was conducted by the EU-HYBNET consortium members in cooperation with interested EU-HYBNET Stakeholder Board members and extended network members. This ensured a broad reach and participation into and by the Network, drawing from a broad and extensive information basis in Europe to contribute to these first 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.

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 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 D2.12 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”.

All the aforementioned aspects are depicted in the image below:

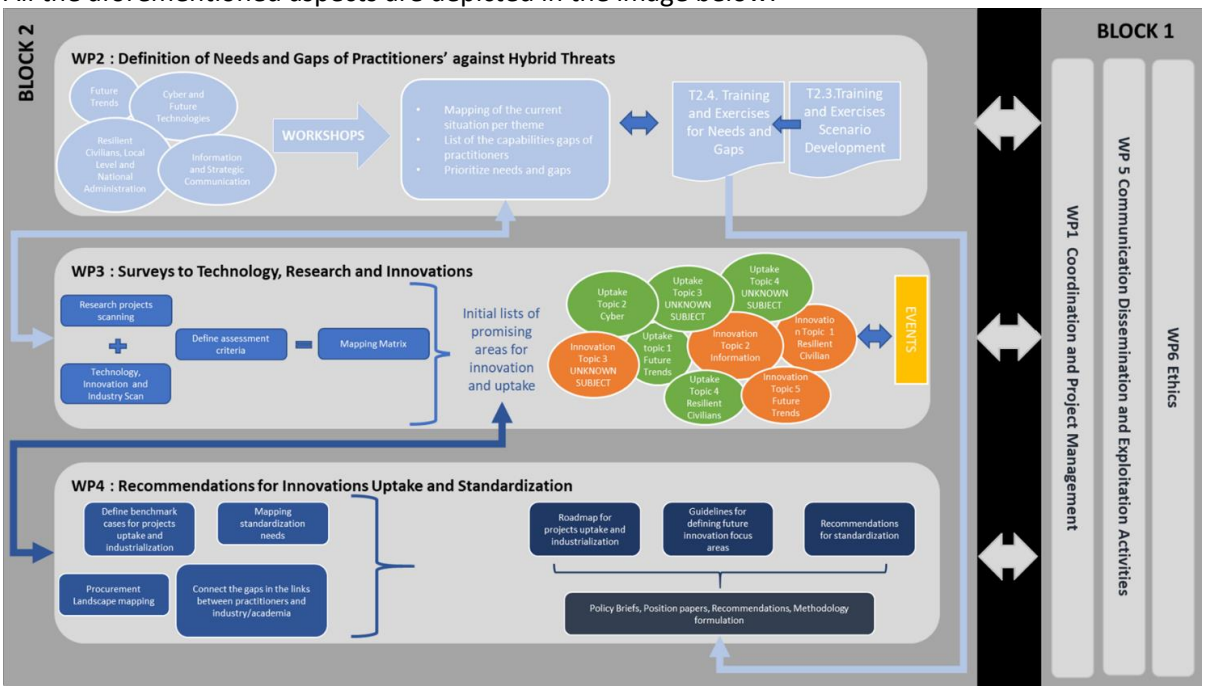

Figure 1 EU-HYBNET Structure of Work Packages and Main Activities

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.

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. 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: **"Intelligence and information – the challenge of hybrid threats"**
Journal: *Journal of Intelligence and Counterintelligence*
Authors: Hanna Smith, Ruben Arcos, Maxime Lebrun

The article frames the issue of the manipulation of information and how it relates to the processes of intelligence analysis in liberal, democratic states in a hybrid threats security environment. The focus on intelligence, information environment and decision making were selected because it contributes to filling a gap in knowledge and awareness in this domain and remains a question not substantially explore in academia. The article rests on a thorough analysis of academic literature in intelligence studies as well as on a series of qualitative interviews with intelligence practitioners at operational and strategic levels. Building on literature review and empirical observations, the article sets a frame to conceptualize the effects of intelligence analysis on decision-making. It traces back the difficulties in intelligence analysis that stemmed from the past two decades' focus on counter and anti-terrorism as well as what it shows as "institutional stress". In order to locate the issue of the manipulation of information in a hybrid threats security context, the article analyses the ends, ways and means employed by actors from authoritarian strategic cultures in the manipulation of information in order to assess their margin of maneuver in influencing the processes of intelligence analysis. Finally, the article analyses the essential characteristics of the contemporary public digital spaces as the networks of interaction within social media. New gaps identified consist in how to apprehend the different strategies of authoritarian strategic cultures in utilizing information (antagonization and relativization); how the structure of information circulation on social media and public digital spaces constitute a horizontal, transparent and very scalable series of opportunities for leveraging individual signals, traces, desires and expectations online and in the physical world.

2.2 CORE THEME – CYBER AND FUTURE TECHNOLOGIES

Title: **Quantum as a disruptive technology in hybrid threats**
Journal: *JRC Publications Repository*
Authors: Evaldas Bruze, Monica Cardarilli

Hybrid Threats and hybrid operations are very commonly combination of activities leading towards consolidated impacts involving two or more domains and leveraging the conventional and nonconventional means of attacks and/or instruments. It leverages lawful and criminal activities in the way, that planned effects would appear slowly and silently in covert manner, that highly disrupts our societal status qua, natural cycles of democratic processes, influence people perception and natural decision-making process path. In some way it can be seen as societal and system hacking while using backdoors into our societies, governance processes and daily life. If to borrow the term from e-commerce domain, hybrid operations exploit, so called "dark patterns" heavily and in all possible ways. Quite often it is backed by supremacy position, so that we cannot fightback, even though we have discovered it. Naturally it has own cycle of continuous innovation and improvement, as known dark

techniques and patterns are being learned to recognize, facilitating emergence of resistance barrier, continuous innovation and improvement cycle on dark techniques and dark patterns side, continuously searching for new instruments to be adopted for new disruptive areas and new disruptive effects. In our days, the major battlefield is on technologies side or to be more precise on ICT side. It builds new level of importance, even though it was already highly important decade ago. At the same time, landscape is very different and almost infinite from adoptions and applications perspective. It is challenge, to summarize and consolidate it into one commonly recognized list and even more challenging to agree on common priorities. We recognized that it is impossible in our scope of work and tried to look at it from another perspective, while asking THE questions: "what are the topics we do not talk about", "what we know, that we do not know", "what are the blind spots we can identify". And even though, over last few years ICT and cyber developments, especially in security related areas, have got high attention and closed some major gaps, there are few more to work on. At the same time we have been looking into highest plausible and possible disruptor in near future in the context of hybrid threats and hybrid operations. Running though several rounds of experts' workshops, it was recognized that one of top priority Quantum Technologies (QT) and Quantum Computing.
Initial scan showed that Quantum Technologies and Quantum Computing are under intensive research however, additional scan showed, that security related aspects are in very early stage and potentially lack of strategic attention. While analyzing and considering that not all new technologies evolve into major disruptor led to common understanding, that QT have the perspective to become the one. It has the potential to break existing status quo, the order and if combined with Internet of Things (IoT) and Artificial Intelligence (AI) developments, make major shift in nations power positions.

2.3 CORE THEME – RESILIENT CIVILIANS, LOCAL LEVEL AND ADMINISTRATION

Title: **The role of the "ordinary civilian" in hybrid threats.**
Journal: *Defence Strategic Communications* journal: https://stratcomcoe.org/projects/academic-journal
Authors: Gunhild Hoogensen Gjørv, Ørjan Karlsson, Rachele Brancaleoni, Isabel Dineen, Jardar Gjørv, Sabina Chiara Magalini, Marco Di Liddo, Mihaela Teodor, Marte Foyn Aasen.

This article addresses a gap in the literature, focusing on the role that civilians play in the development, escalation, and/or mitigation of hybrid threats and warfare and providing a theoretical and conceptual strategy for addressing civilian roles. One of the most central gaps in hybrid threats and warfare literature has been a focus on civilians or general populations, and how they are a central feature of the conflict landscape. Frequently civilians are characterised as passive or victims, rather than actors, in conflict scenarios. The NATO baseline requirements for civil defence and preparedness provide a good example of this type of approach, whereby management and mitigation of conflict is only acknowledged from a state or authority level. People play a role as those who are managed or need to be controlled (ie: with regard to uncontrolled movement of people during conflict).
In this article we argue for a comprehensive security approach to understanding and working against hybrid threats, that acknowledges the role of both different levels of security as well as different actors, from state to civilian. We begin with detailing the threat landscape as it is currently articulated, drawing from a variety of sources including NATO, EU, US Intelligence community, and other security organisations, to provide an overall picture of what are considered to be central global threats today. Many of these threats emanate or draw their strength from the civilian or general population domain. We then examine what we know about hybrid threats and warfare, and provide a brief overview of some of the key literature in this area. We argue in favour of using the recent JRC conceptual baseline report produced in cooperation with the Hybrid CoE, which provide illuminating details about the processes of priming, destabilisation and coercion along the hybrid threat and warfare spectrum. In particular we focus on the role of disinformation and how it affects the civilian domain, exacerbating marginalisation, polarisation, and "under threshold" violence.

Both the threat assessments, as well as the conceptual descriptions of hybrid threats and warfare, make very clear the degree to which the civilian domain plays a role. We then discuss what we mean by comprehensive security (describing and discussing the connections between state, societal and human security), and further move into three supporting concepts for comprehensive security: "civilian agency", which captures how we can understand "what people do" in conflict; "resilience" how civilians and other actors (various state authorities for example) can respond to potential hybrid attacks and mitigate destabilisation and potential conflict; and "societal trust" which plays a central role in the ability for both states and their civilians to resist hybrid threats and warfare.
This is followed by a brief examination of the corona crisis in the European context, and how these concepts and a perception of comprehensive security has been important to how crisis has been handled, and in particular, the role of disinformation in potentially exacerbating fragmentation and vulnerability in societies.

2.4 CORE THEME – INFORMATION AND STRATEGIC COMMUNICATION

Title: **Responses to digital disinformation: an evidence-based analysis on the effects of disinformation and the effectiveness of fact-checking/debunking**
Journal: *El Profesional de la Information* (The Information Professional): http://www.profesionaldelainformacion.com
Authors: Rubén Arcos, Manuel Gértrudix, Cristina Arribas and Monica Cardarilli

The dissemination of purposely deceitful or misleading content to target audiences for political aims or economic purposes constitute an insidious threat for democratic societies and institutions, being recognized as a major security threat, and particularly after evidence and allegations of hostile foreign interference in several countries during the last five years. Disinformation can also be part of hybrid threat activities. This research paper examines findings on disinformation effects and addresses the question of how effective are being counter digital disinformation strategies with the aim of assessing the impact of responses such as the exposure and disproof of disinformation content and conspiracy theories. The paper objective is to synthetize the main scientific findings on disinformation effects and on the effectiveness of debunking, inoculation, and forewarning strategies against digital disinformation. A mixed methodology is used, combining qualitative interpretive analysis and structured technique for evaluating scientific literature such as SLR, following the PRISMA framework. The research article starting point is the gap "Addressing the mass of manipulated information in social media" and "Increase resilience against manipulated information," identified during previous research work conducted in the framework of EU-HYBNET. An important element when addressing counter responses to online disinformation and hostile activities in the information domain by hybrid threat actors is starting with a thorough understanding of disinformation effects in targeted individuals and societies. Similarly, assessing the effectiveness of fact-checking and debunking practices bases on evidence-based analysis is important for acquiring lessons learned and honing those practices for optimizing results. The paper is premised on the assumption that providing an evidence-based analysis from scientific research (communication sciences, social psychology, decision sciences, another relevant fields and disciplines) on the effects of disinformation and of counter measures against manipulated information through practices such as inoculation (and resistance to inoculation), forewarning on incoming persuasive messages, debunking, should provide a good foundation for posterior research in the project under the core theme and provide a solid base from which to develop positive strategic communication responses to disinformation and to hostile information influencing.

3. MAIN FINDINGS PRESENTED 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.

3.1 CORE THEME – FUTURE TRENDS OF HYBRID THREATS

The guiding idea of the article is to frame the information environment and how intelligence analysis should apprehend its main determinants. The article thus discusses the opportunity for intelligence agencies to implement academic reach policies as well as attempts to connect to a wider network of professionals in open source in order to make sense of increasingly complex adaptive systems. No specific recommendations or guidelines have been created in the framework of this article but if fills useful gaps in knowledge and awareness. The reader's interpretation of the argumentation of the article may suggest recommendations stemming from the reader's reception and own professional or interest background.

3.2 CORE THEME – CYBER AND FUTURE TECHNOLOGIES

In the future Quantum Technology (QT) advanced technologies will evolve with extended capability for quantum enabled sensing, gravitational and magnetic anomalies detection, Positioning, Navigation and Timing (PNT) systems, greatly reducing external references and providing ultra-precise measurements, development of Quantum-enhanced remote sensing as well Magnetic and Gravity Sensing with distant location and surveillance capabilities of underground and underwater, that will enable thousands of times higher precision comparing to current capability levels.
In parallel new quantum optimized algorithms are under the development, already illustrating that in various sectors their quantum implementation can drastically improve complex calculation processes, especially related to advanced statistics or similar.
Quantum cryptography and communications have challenged current cybersecurity implementations illustrating how protection instruments, thought before as unbreakable can be broken or overcome in matter of few minutes. It is already known issue strongly addressed by leading security practitioners and should solve the problem for critical infrastructures, however there is no solutions yet how to upgrade large scale public and private infrastructures to solve so called Post Quantum Security related issues.
A number of nations are currently investing heavily in quantum research in order to derive economic and military benefits, learning from USA, China, Russia strategies and focus, it can be concluded that they do recognize QT potential to rebuild power balance in technological supremacy perspective.
We conclude, that among different application domains, quantum enablement will create new game arenas for hybrid operations while combining new remote intelligence and remote-control possibilities in defense and security sectors, ultra-fast and ultra-precise algorithms enabling near real-time micro targeting, as well challenging current technological supremacy positions for major global markets.
If weaponized QT will become new generation warfare, however another large application area is general society and new interference and influence capabilities targeted on societies and individuals.
We conclude that QT enabled hybrid operations is least at the moment researched and investigated area, that requires special focus in order to ensure EU societies security in near future.
The main impact areas of hybrid threats that are discussed in the publication are:

- Technological supremacy,
- Post Quantum Security risks,
- Real time micro targeting,

- Economical dependencies.

While leaving all the technological challenges and other technical aspects for technology engineers and cybersecurity community, the list provided, gives guidance for hybrid threats community on topicalities for further research and investigation. Those impact and intersection points should serve as a bridge between different communities working on different aspects of QT application and talking different languages.

3.3 CORE THEME – RESILIENT CIVILIANS, LOCAL LEVEL AND ADMINISTRATION

This article provides the crucial ground work for the work focusing on the role of civilians in conflict, in particular hybrid threats and warfare. This is the article that looks methodically at the nature of threats and warfare today, and demonstrates that the role of civilians is both crucial, but under examined. This article provides the arguments for conceptual and theoretical tools that can be applied in further work. Thus the Resilient Civilians (RC) core theme can move more in-depth into empirical cases using the theoretical and conceptual tools provided in this first, foundational article. Subsequent articles indeed can draw from the other core theme articles in this reporting period, looking at linkages between the civilian domain and disinformation, quantum technologies, and intelligence, among others. The article can also be useful for practitioners and policy makers in that it makes explicit and clear why state-based approaches to preparedness and conflict and crisis management are insufficient, and that only a broader understanding of security enables analysts and policy-makers alike to understand what societal vulnerabilities are being targeted, how, and by whom.

3.4 CORE THEME – INFORMATION AND STRATEGIC COMMUNICATION

Disinformation produces effects on audiences, although those effects will depend on several factors and pre-existing attitudes and beliefs play a very important role on the acceptance of disinformation content by individuals.

Studies show that correcting dis- and misinformation through fact-checking is not necessarily effective for all subjects and that when corrections come from friends and a mutual relationship tend to be more effective.

Holders of partisan positions are not only more vulnerable to disinformation attacks consistent with their views, but also will likely be more resistant to debunking unless the debunking message is consistent with their initial positions.

Existing experiments on the effects of Deepfakes combined with micro-targeting suggest that there is a potential amplification effect of micro-targeting but still prior attitudes and beliefs will mediate on the effects.

Inoculation can be a successful strategy although disinformation actors can develop meta-inoculation practices and reduce the effectiveness of inoculation.

Assessing the reach and impact of disinformation requires to count with reliable data on audiences and their exposure to disinformation messages for full understanding of its impact.

Need for introducing the time perspective when assessing disinformation effects as part of hybrid threats; some activities in the information domain might be part of the priming phase before posterior full effects can become visible.

The long-term impact of disinformation, “wicked media content” and influence operations by foreign state actors in societies is difficult to know unless regular public opinion studies, are conducted.

The effects component of disinformation studies is an important subfield of research that is receiving increasing attention and producing relevant scholarship that provides evidence-based findings on the

dynamics of online mis- and disinformation and on the effectiveness of fact-checking/debunking practices, what practices work better and the challenges derived from psychological factors, social factors, and the structure of the current media system of our digital age.

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 four articles that have been submitted by the four core theme lead authors, addressing how the focus of each article was selected and why, and what relevance these articles will have to future research.

In Section 3 we presented the findings of all four research articles, which now contribute to the initial findings established after the first year of the EU-HYBNET project. These results have also been 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.

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 project cycles within and beyond 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.

Analytical elements, facts and experiences on the field, will proceed and extrapolate from project partners' contributions and other relevant EU-HYBNET stakeholders in relation to the urgency of gaps and needs, determining the direction of proceedings within project's Tasks and WPs.

In particular, this deliverable will provide the necessary elements to EU-HYBNET WP2, 3 and 4 to design training activities and exercises as well as future innovations and actions to counter hybrid threats.

Moreover, this document will orient the scanning and monitoring of potential research and innovations destined to fill the respective capability gaps and needs identified in previous tasks and project cycles, channelling into policy briefs, priorities and guidelines for practitioners and decision-makers to counter hybrid threats. The research outcomes will ensure that the project can express the most promising innovations to be recommended for innovation uptake, in order to empower practitioners' future performance.

Each cycle will build upon the findings of earlier research results while also provide new focus areas for research. Together with network extension, this cyclical approach will ensure vitality of proceedings and diversity of views in order to increase the overall quality and output of the project where project's partners will be asked for feedback in order to develop the research further. Each cycle will initiate, continue and stimulate the overall work process to support increase of capacity and knowledge for an in-depth analysis and selection of research focus areas within each project core theme in order to define requirements and prioritisation for the most urgent research and innovations.

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
US	United States
NATO	North Atlantic Treaty Organization
ICT	Information and Communications Technology
QT	Quantum Technology
PNT	Positioning, Navigation and Timing
AI	Artificial Intelligence
IoT	Internet of Things
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
COMTESSA	Bundeswher University
Laurea	Laurea University of Applied Sciences

ANNEX II. REFERENCES

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

[2] 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.