ARTICLES AND PUBLICATIONS ON THEMES AND MEASURES

DELIVERABLE 2.16

Lead Author: Laurea, JRC
Contributors: Hybrid CoE, L3CE, URJC, UniBW, UiT
Deliverable classification: Public (PU)

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

D2.16 ARTICLES AND PUBLICATIONS ON THEMES AND MEASURES

Deliverable number	**2.16**	
Version:	**V1.0**	
Delivery date:	**30/04/2025**	
Dissemination level:	**Public (PU)**	
Classification level:	**Public**	
Status	**Ready**	
Nature:	**Report**	
Main authors:	Tiina Haapanen, Julien Theron	**Laurea, JRC**
Contributors:	Maxime Lebrun	Hybrid CoE
	Ruben Arcos	URJC
	Andrew Paskauskas	L3CE
	Gunhild Hoogensen-Gjorv	UiT
	Amirun Haqqim bin Eldeen Husaini	UniBW

DOCUMENT CONTROL

Version	Date	Authors	Changes
0.1	14/04/2025	Tiina Haapanen / Laurea	First draft
0.2	22/04/2025	Maxime Lebrun / Hybrid CoE	Content delivery
0.3	29/04/2025	Amirun Haqqim bin Eldeen Husaini / UniBW	Content delivery
0.4	29/04/2025	Tiina Haapanen / Laurea	Text editing
0.5	29/04/2025	Julien Theron / JRC	Text editing
0.6	30/04/2025	Gunhild Hoogesen-Gjorv, UiT	Content delivery
0.7	30/04/2025	Isto Mattila / Laurea	Review
1.0	30/04/205	Tiina Haapanen / Laurea	Final editing, deliverable submission to EC.

DISCLAIMER

TABLE OF CONTENT

TABLES

1. INTRODUCTION

1.1 OVERVIEW

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

The WP2 Objectives are the following:

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

The following report demonstrates that objectives 1, 2, 3, and 5 are met. In line with other 4th cycle WP2 deliverables (D2.4 4th Gaps and Needs Events" and D2.8 "Final Gaps and Needs Evaluation Report), the findings of D2.15 are reflected throughout the four core themes. The EU-HYBNET four core themes area:

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

The articles presented in this report reflect our initial results, after the 4th year of the project, pertaining to the above four core themes. The articles have been developed in relation to the project objectives, with the intent to increase European stakeholders' knowledge on hybrid threats through research on the main criticalities, previously identified, to counter hybrid threats (HT).

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

As during the project five years, Task (T) 2.2 has conducted research in multiple forms. EU-HYBNET served, indeed, as a platform for exchanges of ideas. It offered physical and online meetings where researchers, analysts and practitioners could exchange new data, concepts, ideas and approaches, making it a cradle for scientific exchanges. It also promoted at every event scientific cooperations, including through inter- and transdisciplinary approaches. The very braimstorming activities, at every

workshop, also worked as a ideas-generating incentive, offering innovative theoretical and applied research, as well as case studies from practitioners, industry or policy-makers. But the main activity related to T2.2 has been the scientific articles provided by core theme leaders and participants on a voluntary basis. These articles, focusing on the recent evolutions of hybrid threats, aimed at an advance understanding of the phenomenon, and how to tackle the threats. They don't only offer, therefore, a scientific investigation, but also a substantial benefit to practitioners, industry and policy-makers.

The authors of these papers have different professional belongings: some are academic scholars and others are analysts. They are also envolved in EU-HYBNET in different capacities, with EU-HYBNET consortium members in cooperation with interested EU-HYBNET Stakeholder Board members and extended network members. This diversity ensures works related to different domains, operated by different actors from multiple scientific fields. This also participates, therefore, to building ties between the project's participants. For this fifth and final year, the formula also aimed at complementing, in a new and future-oriented light, the articles published in previous years.

Task 2.2 has for aim to comprehend better how hybrid threats operate and to identify directly or indirectly measures to counter the threats. In the broader context of the project, this specific task brings therefore a substantial contribution to Horizon 2020 programme dedicated to "Secure Societies". The specificity of the programme indicates, in this respecm that "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 instructions to the fifth year's T2.2 participants have highlighted the importance to focus on important trends for the close future of hybrid threats. The aim of this incitation was to allow EU-HYBNET to conclude its scientific activities by projecting the investigation on future needs for adaptation. Every article submitted possesses indeed an anticipatory dimension, identifying very current issues that European societies still has to understand and counter. By doing so, the participants met the challenge to work on crucial trends. More generally, these articles kept the spirit of the whole project to bridge gaps, needs and solutions, providing valuable insights to policymaking on how better counter 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 European Commission - Joint Research Centre (JRC) and provide a sound window into supporting research and innovation activities in any of the hybrid threat domains considered by the project to be important and capable of delivering solutions during execution of the project cycles.

Each of the four project core themes embody visions that include the variety of challenges that European Union Member States (EU MS) may face when countering hybrid threats in targeted domains and interfaces with other domains. These visions are based on current European high-level research. The themes cover but are not limited to the following:

Future Trends of Hybrid Threats

To analyse trends has become even more vital than before due to the changed security environment. Hybrid Threats are by character difficult to detect. However, without detection countering becomes difficult and responses might always be two steps behind. Hybrid threats also have an ever-changing nature. Approach seldom repeats itself and combination of tools is tailor made for the target. For this reason, analysis relating to different security related trends will be essential to be able to have foresight and build early warning systems. Hybrid threat trend analysis needs to be multidisciplinary and multidimensional using also scenariobased thinking. The future trends of hybrid threats cover also the three other EU-HYBNET themes connecting them to wider security context. This will strengthen situational awareness and identify new and emerging capability needs for countering hybrid threats.

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

Cyber and Future Technologies

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

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

Resilient Civilians, Local Level and National Administration

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

for example. Law enforcement agencies might be in the frontline when it comes to detecting and countering hybrid threats. Many cases in the recent history have shown us that the local level can play a crucial role both in countering and enabling hybrid threats; Catalonia and Eastern Ukraine as best examples.

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

Information and Strategic Communication

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

Principal lead: University of Rey Juan Carlos (URJC)

1.3 GROUNDING AND STRUCTURE OF THE DELIVERABLE

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

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

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

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

- KPI description: Monitor existing innovations addressing gaps and needs; incl. areas of knowledge/performance.

- KPI target value: At least 4 reports every 18 months that address technological innovations that are able to fulfil European actors' gaps and needs.

The D2.16 deliverable provides elements for other WPs and Tasks. Indeed, it connects particularly to different WP achieved by the project:

- WP2: By investigating new issues, framing key questions, reviewing approaches or questioning phenomena, the articles all focus on gaps and needs in an innovative way. They connect, therefore, to other WP2 tasks that have been implemented, such as T2.1 "Needs and Gaps Analysis in Knowledge and Performance". They also have ties with T2.4 "Training and Exercises for Needs and Gaps", as they have relevant teachings in this area..
- WP3: the articles propose teachings to improve solutions to counter HT, including in terms of technology and innovation. They also propose new knowledge and paths that might lead to future studies in their pathway. For these two reasons, they also connect to WP3 "Surveys to Technology, Research and Innovations".
- WP4: the articles participated to propose new ways to understand specific issues that could lead to innovations uptakes and standardization of processes. In this respect, they connect to WP4 "Recommendations for Innovations Uptake and Standardization".

This document includes the following sections:

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

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: Breaking the system? Democratic Vulnerabilities to Foreign Interference

Journal: Open Research Europe (submitted)

Authors: Maxime Lebrun, Hybrid CoE

Focus: This essay sketches a landscape of democratic vulnerabilities to hybrid threat activities. It is the result of studies, consultations, and scenario-based forecasting with various experts in social sciences. This essays delves in particular onto contexts of democratic regression and democratic intimidation which are prone to foreign interference and dangerous for the strength of liberal democratic governance. Contemporary foreign hostile interference often exploits social media and their algorithmic content curation for engineering visibility at very individual levels. Techniques of micro-targeting and astroturfing are important levers in this respect. Foreign hostile interference campaigns can exploit emotional and psychological vulnerabilities at societal and individual levels in democracies. Those vulnerabilities have become exploitable to authoritarian states in weakening democracies from the inside. The narratives, emotions, and psychological needs that make citizens drift away liberal democracy need to be taken into account while fending off campaigns that exploit democratic vulnerabilities.

2.2 CORE THEME – CYBER AND FUTURE TECHNOLOGIES

Title: A Preliminary Ontology for 5G Network Security: Hybrid Threats, Risk Reduction, Compliance

Journal: Open research Europe

Article submitted to: 2025 5th International Conference on Computer Communication and Information Systems (CCCIS 2025),' February 28–March 2, 2025

Author: Andrew Paskauskas, L3CE

Focus: The increasing reliance on 5G networks as critical infrastructure across Europe, particularly along the EU's transport corridors, underscores the importance of securing these systems against hybrid threats. This paper presents a preliminary ontology for 5G network security, designed to model and mitigate hybrid threats while ensuring regulatory compliance with the European Commission's cybersecurity requirements. Grounded in the ENISA 5G Threat Landscape and ISO 27005 risk management standards, the ontology integrates critical concepts

such as assets, threats, risks, and mitigation strategies. It enables systematic risk reduction through iterative validation using SHACL constraints and logical reasoning via Protégé's HermiT reasoner. A detailed case scenario demonstrates the ontology's adaptability in addressing emerging risks, such as attacks on NGRAN, SDN, and cloud-based infrastructure, while supporting compliance with Connecting Europe Facility (CEF) mandates, including high-risk supplier management and data security. This work lays a foundation for deploying scalable, resilient, and adaptable 5G systems by bridging conceptual modelling with realworld compliance requirements. Future directions include testing the ontology in real-world testbeds to validate its robustness and applicability further.

Title: Quantifying Political Polarization on Social Media Platforms: A Systematic Review of Analytical Tools and Methodologies

Journal: Social Network Analysis and Mining (TBD)

Authors: Amirun Haqqim bin Eldeen Husaini, Stefan Pickl (UniBW), Son Pham (Le Quy Don Technical University)

Focus: Polarization has been linked to various outcomes that hinder effective political discourse, including reduced cooperation and compromise, entrenched policy positions, difficulties in forming coalitions, and a decline in trust toward governments, public institutions, and fellow citizens (Carothers & O'Donohue, 2019). In a polarized society, these challenges can make it difficult to collaboratively address critical issues, and can even exacerbate conflicts (van de Veen, 2023). Reflecting these concerns, political observers frequently identify political polarization as one of the most pressing political issues of our time, a view further reinforced by the surge in research efforts aimed at detecting, predicting and preventing its negative consequences.

The importance of addressing polarization is further underscored by its relevance to disinformation. This is defined as the deliberate, often coordinated spread of false information by actors within social media networks (Harris, 2024). Empirical research demonstrates that rising polarization is closely associated with the deliberate manipulation of public opinion and the spread of dis- and misinformation (Araźna, 2015; Mustonen-Ollila, Lehto, & Heikkonen, 2020; Turel, 2024). Furthermore, polarized group dynamics have been found to create fertile ground for the circulation and reinforcement of false or misleading information (Del Vicario et al., 2016; Törnberg, 2018; Zollo, 2019). Given the role of polarization in amplifying the spread of disinformation—particularly on social media—and its generally adverse effects on social cohesion and political discourse, research aimed at developing tools to detect and predict polarization is argued to be highly valuable (Alvarez-Galvez et al., 2023).

Objectives: This study seeks to address a critical gap in the literature by systematically examining the available methodologies and tools for detecting and predicting political polarization on social media platforms. It aims to (1) identify the extent of empirical research on this topic, (2) catalog the methodologies and tools employed, (3) analyze the types of polarization these methodologies target (e.g., ideological, affective, or misperceived), and (4) evaluate the methodologies in terms of computational complexity, accuracy, and robustness.

Methods: A systematic bibliometric review was conducted following PRISMA guidelines. Articles were sourced from Web of Science and Scopus between December 2024 and February 2025. A total of 400 initial articles were identified through keyword searches, complemented by an additional 200 articles retrieved via backward citation tracking. Following a screening process that excluded non-empirical studies and those not directly addressing polarization in social media contexts, 300 studies were selected for analysis. Data extraction included details on study chronology, geographic focus, the type

of polarization examined, and the primary methodological focus (measurement vs. prediction). Each methodology was then evaluated based on computational complexity, accuracy, and robustness.

2.3 CORE THEME – RESILIENT CIVILIANS, LOCAL LEVEL AND ADMINISTRATION

Title: Resilient Civilians and Hybrid Threats: The Eighth Baseline Requirement in Norwegian Total Defence

Journal: The Eighth Baseline Requirement: Resilient Civilians in Hybrid Threats and Warfare. Gunhild Hoogensen Gjørv, Sergii Glebov, Christopher Holshek, & Arsalan Bilal (eds). IOS/Sage Press. (Forthcoming)

Authors: Gunhild Hoogensen Gjørv, Jardar Gjørv, Ørjan Karlsson, Marte Aasen, Gjermund Forfang Rongved

Focus: This chapter contributes with a case study examining the degree to which the Norwegian total defence plans includes adequate understanding, facilitation and integration of a «resilient civilians» component. The chapter looks at the evolution of thinking in Norwegian defence planning as it pertains to the role of civilians and «individual security» and reviews recent white papers to show the ways in which the «eighth baseline requirement» is addressed or not. The chapter concludes with further recommendations.

2.4 CORE THEME – INFORMATION AND STRATEGIC COMMUNICATION

Title: Disinformation as an obstructionist strategy in climate change mitigation: a review of the scientific literature for a systemic understanding of the phenomenon

Journal: Open Research Europe (https://open-research-europe.ec.europa.eu/articles/4-169)

Authors: Manuel Gertrudix, Alejandro Carbonell-Alcocer, Rubén Arcos, Cristina M. Arribas, Valeri Codesido-Linares, Nerea Benítex-Aranda, Rey Juan Carlos University (URJC)

Focus: Background: This study examines the scientific misinformation about climate change, in particular obstructionist strategies. The study aims to understand their impact on public perception and climate policy and emphasises the need for a systemic understanding that includes the financial, economic and political roots.

Methods: A systematic literature review (SLR) was conducted using the PRISMA 2020 model. The sample consisted of 75 articles published between 2019 and 2023, sourced from Web of Science, Scopus and Google Scholar. Methodological triangulation was performed to improve the analysis.

Results: The results show that technological approaches to misinformation detection, such as immunisation and fact-checking, are widely used. However, few studies look in depth at the operational structures that support systematic disinformation.

Conclusions: The study emphasises the urgent need to expand and deepen research on climate disinformation and argues for more global, comparative and adequately funded studies. It emphasises the importance of addressing the systemic complexity of disinformation and integrating different theoretical and methodological approaches. This will help to develop effective measures against

hidden networks of influence and mitigate their disruptive effects. The research findings are relevant for policymakers, scientists, academics, the media and the public and will help to improve strategies to combat climate misinformation and promote science-based climate action.

3. CONCLUSION

3.1 SUMMARY

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

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

In sum, this document has provided the following:

- In Section 1 we have provided the descriptions of the core themes upon and for which each article was targeted. We also indicated which areas of the project description we have addressed in accordance with EU expectations.
- In Section 2 we provided descriptions of the five articles that have been written 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.

ANNEX I. GLOSSARY AND ACRONYMS

Table 1 Glossary and Acronyms

Term	Definition / Description
D	Deliverable
DoA	Description of Action
DOI	Digital object identifier
CEF	Connecting Europe Facility
EC	European Commission
ENISA	The European Union Agency for Cybersecurity
EU	European Union
EUAA	European Union Agency for Asylum
EU MS	European Union Member State
EU-HYBNET	Empowering a Pan-European Network to Counter Hybrid Threats project
GM	General Matters call
H2020	Horizon2020
HT	Hybrid Threats
Hybrid CoE	The European Centre for Excellence for Countering Hybrid Threats
ISO 27005	Information security, cybersecurity and privacy protection standard
JRC	Joint Research Centre
KPI	Key performance indicator
Laurea	Laurea University of Applied Sciences
L3CE	Lithuanian Cybercrime Centre of Excellence for Training, Research & Education
NGRAN	Next Generation Radio Access Network
OB.	Objective
PRISMA	Preferred Reporting Items for Systematic reviews and Meta-Analyses
PU	Public
SDN	Software-Defined Networking
SEC	Secure Societies Program
SHACL	Shapes Constraint Language
SLR	Systematic Literature Review
T	Task
UiT	University I Tromso/ Arctic University in Norway
UniBW	University of the Bundeswehr Munich
URJC	University of Rey Juan Carlos
WP	Work Package
5G	5th generation mobile network