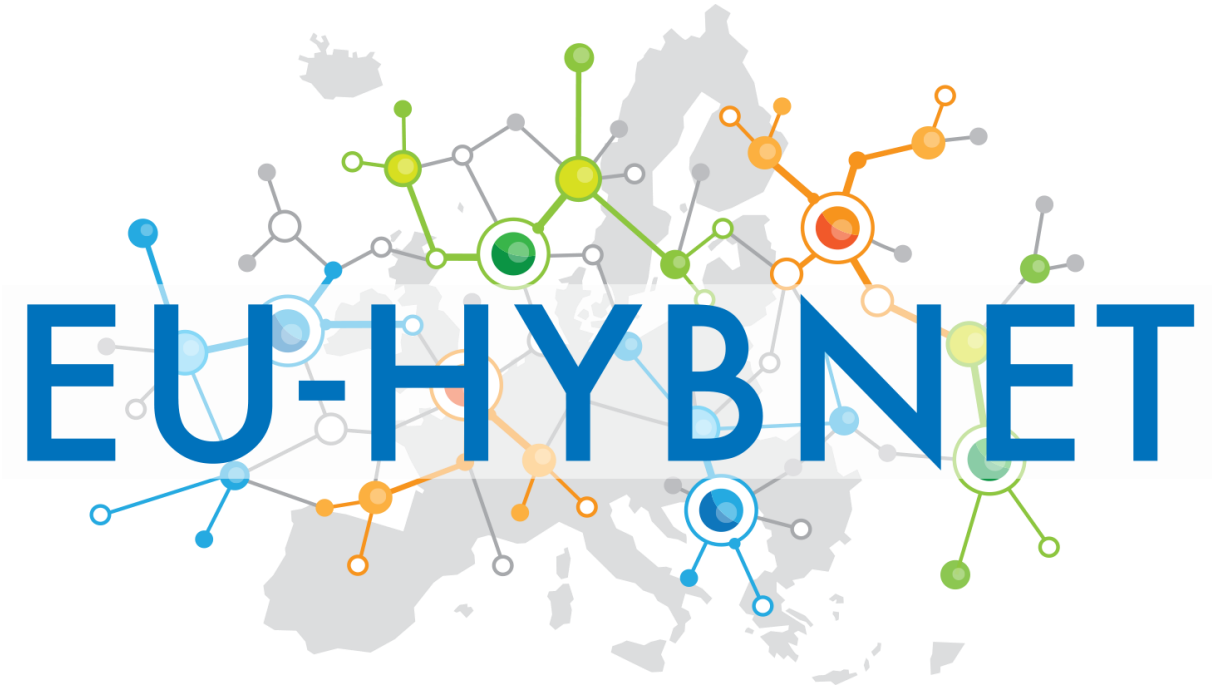


ARTICLES AND PUBLICATIONS ON THEMES AND MEASURES

DELIVERABLE 2.13

Lead Author: UiT

Contributors: Hybrid CoE, L3CE, URJC, Laurea, DSB, MTES, JRC, Maldita

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

D2.13 ARTICLES AND PUBLICATIONS ON THEMES AND MEASURES

Deliverable number	**2.13**	
Version:	**V1.2**	
Delivery date:	**29/4/2022, 29/12/2022**	
Dissemination level:	**Public (PU)**	
Classification level:	**Public**	
Status	**Ready**	
Nature:	**Report**	
Main authors:	**Gunhild Hoogensen Gjørv, Isabel Dineen**	**UiT**
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
	Teodor Mihaela, Elena Novăcescu, Ileana Surdu, Valentin Stoian	MVNIA
	Isto Mattila, Päivi Mattila	Laurea
	Antoine-Tristan Mocilnikar	MTES
	Orjan Karlsson	DSB
	Pablo Hernández-Escayola, Antonio García-Jiménez	Maldita
	Monica Cardarilli	JRC

DOCUMENT CONTROL

Version	Date	Authors	Changes
0.1	11/4/2022	Gunhild Hoogensen-Gjorv/UiT	First draft
0.2	13/4/2022	Monica Cardarilla/JRC	Review and comments
0.3	14/4/2022	Maxime Lebrun/ Hybrid CoE	Description of the article
0.4	14/4/2022	Arsalan Bilal/ UiT	Description of the article
0.5	15/4/2022	Evaldas Bruze/ L3CE	Description of the article
0.6	15/4/2022	Isto Mattila, Päivi Mattila/ Laurea	Description of the article
0.7	15/4/2022	Ruben Arcos/URJC	Description of the article
0.8	27/4/2022	Pablo Hernández-Escayola, Antonio García-Jiménez/ Maldita	Review
0.9	28/4/2022	Päivi Mattila/ Laurea	Review and text editing. Comments for final text editing
1.0	29/4/2022	Päivi Mattila/ Laurea	Final review and submission of the document to the EC
1.1	29/12/2022	Gunhild Hoogensen-Gjorv/UiT	Final review, text editing
1.2	29/12/2022	Tiina Haapanen, Päivi Mattila / Laurea	Final review and submission of the document 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 previous WP2 deliverables (D2.5 "2nd Gaps and Needs Events", D2.6 "Long list of defined gaps and needs" and D2.10 "Deeper analysis, delivery of short list of gaps and needs"), the findings of D2.13 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 second 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 D2.6 and D2.10.

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.

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 second 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 D2.13 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.

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: *Populism and tyranny, a threat to democratic security*
Journal: Hybrid CoE Publication series
Lead Author: Maxime Lebrun

Focus: This article explores why hybrid threat actors could exploit populistic politics, movements, and leaders to destabilize and discredit democratic regimes. One purpose of democracy is to make tyranny impossible by limiting abuses of power. Tyranny aims to concentrate and maximise power in the hands of a tyrant. Power in democracy is limited by design because it belongs to all citizens and the system impeaches abuses of power. This article characterizes the challenge that democracies can face if hybrid threat actors would leverage populist movements and use them against the safeguards of democracy. This article contributes to refining the dichotomy between democracies and authoritarian systems by identifying the ways in which democratic systems can erode towards tyranny.

2.2 CORE THEME – CYBER AND FUTURE TECHNOLOGIES

Title: *5G Generic Networks in the scope of Hybrid Threats*
Journal: JRC Publications Repository
Lead Authors: Andrew Paskauskas and Evaldas Bruze
Contributors: Edmundas Piersarskas, Egidija Versinskiene, Rimantas Zylius, Sigute Stankeviciute, Ruta Ziberkiene

Focus: 5G as well as other advanced new technologies carries high disruptive potential to the ecosystem. In many technical advancements we can observe incremental evolution of trends, however some – radically different or new technologies can result in so called quantum leap, that forms new mega trends, disrupts societies, forms new centers of gravity in economical and geopolitical means. 5G technology provides new capabilities those increase mobile data throughput from 10's to 100's of times, enabling on-device complex systems deployment, next level video processing and new levels of communication interactions organization. At the same time it brings set of new risks, vulnerabilities, open new perimeters of security and enables new means of weaponization by adversarial actors. In combination with information domain negative trends, - mis-/disinformation, fake news, massive brainwashing it forms new area of hybrid threats, those are subject of this analysis paper. Paper studies EU response to 5G related threats from multi-discipline perspective including policy, core technology, application (IoT, AI, Social Media, ICT), governance, hybrid threats, addresses major experiments how 5G technologies can be applied to maintain or even sometimes strengthen EU security while safeguarding EU values, citizens, their privacy, freedom, democracy and finally culminates with disruptive points still to be addressed in order to secure EU strategic security, autonomy and maintain power equilibrium in economical, geopolitical and democracy means.

2.3 CORE THEME – RESILIENT CIVILIANS, LOCAL LEVEL AND ADMINISTRATION

Title: *Comprehensive Security During the Covid-19 Pandemic: Impacts of Mis/Disinformation In the Age of Populism*
Journal: To be determined
Lead Authors: Arsalan Bilal and Gunhild Hoogensen Gjørv
Contributors: Caleb Aluola, Christin Horrigmoe Hagen, Daniele Gui, Jardar Gjørv, Justyna Karolina Kielar, Marc Lanteigne, Rachele Brancaleoni, and Sabina Magalini

Focus: The Covid-19 pandemic has presented 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, which combined provide a comprehensive security picture. Drawing on both security theory and policy, the report addresses how Covid-19 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 examines 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.

Title: *Critical Infrastructure Protection and Hybrid Threats*
Journal: JRC Publications Repository
Authors: Isto Mattila, Antoine-Tristan Moncilnikar, Orjan Karlsson, Päivi Mattila

Focus: Existing critical infrastructure protection has led to the situation where increased interdependencies and related risks of cascading effects across sectors are not sufficiently taken into account in EU level. The existing EU legislative framework does not provide sufficient mechanism necessary for Member States to assess and to manage all infrastructure related threats/risks in a systematic way. Today, these risk management approaches are sector and country specific, which does not allow forming a coherent risk awareness between sectors or countries. New Directive proposal on the resilience of critical entities (Brussels, 16.12.2020 COM(2020) 829, final) will enhance MS level capacity to answer these evolving risks. However, it does not give clear answers and means to do so, especially in situation, where hybrid risks play significant role. This article will introduce a methodology for identifying weak signals and their possible connections of different hybrid attacks to critical infrastructures (CI) in different CI domains identifying signature of an attacker. Objective is to improve existing vulnerability between variety of sectors in modern highly sophisticated interconnected and globalized Critical Infrastructure (CI) environment. Hybrid attacks are serious threats and they can

effect to CI interdependences, which might generate harmful multinational or -sectoral cascading effects to our society. This initiative supports EU's desire to strengthen its strategic autonomy.
Most probably, today many CI operators are not even able to recognize the hybrid character of the attacks in their own business environment. This article will introduce the power of the information sharing and its benefits for critical infrastructure operators. Our socio-economic CI system can benefit from operators' better awareness and recognition of hybrid attacks. It is acknowledged that when citizens feel safe with the critical infrastructure this builds trust to whole society. This may eventually enhance the critical infrastructure resilience itself and make the society more resilient to other types of hybrid threats and attacks. This article is linked to the discussion of CER and NIS-2 directive proposals and their possible implementation measures in EU Member States (EU MS) and in pan-European wide.

2.4 CORE THEME – INFORMATION AND STRATEGIC COMMUNICATION

Title: *Information Manipulation and Historical Revisionism*
Journal: Open Research Europe
Authors: Cristina Arribas, Rubén Arcos, Manuel Gertrudix, Kamil Mikulski, Pablo Hernández-Escayola, Teodor Mihaela, Elena Novăcescu, Ileana Surdu, Valentin Stoian, Antonio García-Jiménez

Focus: The research explores and discusses hostile narratives against the EU that make use of historical revisionism as a specific tool of hybrid threats. Based on the new geopolitical framework set by Russia's invasion of Ukraine in February 2022, an analysis is made on the use of historical revisionism and hostile narratives based on manipulated history employed by the Kremlin to legitimize its imperialist foreign policy agenda, and specifically on the "Near Abroad" and "Ruskii Mir Concepts" and Alexander Dugin's approaches to the creation of a Eurasian space as a counter-concept to the West.
The main objective of the article is to deepen in the knowledge on the actors that are involved in the dissemination of these malicious campaigns, channels, goals and intentions as well as the historic events that are exploited in the narratives. It employs a mixed methodology of desk research, systematic literature review, and the analysis of databases of mis- and disinformation from European institutions, think tanks, and fact-checking organizations.
Thus, it analyses information campaigns based on historical revisionism as a tool of manipulation employed by Russia´s structure of propaganda but also European political parties and governments that since the last decade have built nearby positions to the Kremlin. Finally, the article discusses the implications of its use as a manipulative tool from an educational and countermeasures perspective, and how to build resilience.

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

Title: *Populism and tyranny, a threat to democratic security*
Populism pushes radicalisation and extremism in democracies while it promotes an ultimately tyrannical mode of governance by depleting the added value of democracy. The logic of populism can reduce the space for deliberation and compromise, crippling democratic decision making and undermining the idea of democratic representation. Digital social networks can exacerbate polarization within the people. Echo chambers and filter bubbles on social media, combining with stronger identities based on victimhood and resentment can lock individuals and groups in opposing worldviews. It can contribute to the formation of transnational political movements, connecting audiences and narratives around the dynamic of populism. Facts-based discussion could give way to confronting "alternative facts". Because it renders the people's expression ultimately trivial, the logic of populism points to a concentration of powers, in the name of the People.

3.2 CORE THEME – CYBER AND FUTURE TECHNOLOGIES

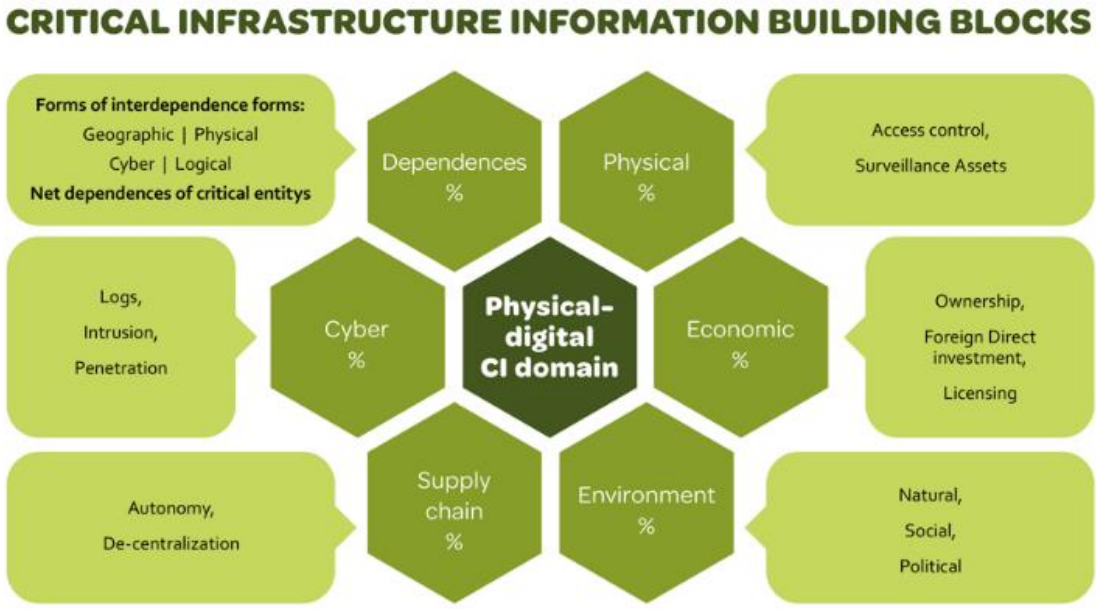
Title: *5G Generic Networks in the scope of Hybrid Threats*
5G technological supremacy and dominance is already driven by two major markets: China and USA with very high Chinese dominance. EU have high dependency on external technology providers. At the same time it is impossible scenario to suspend or slow down technology rollout that can cause losses in techno-societal leadership positions cross all domains. Therefore, balanced approach – combining security and EU technical advancement, must be deployed. Extremely important roles plays common EU 5G policy development related activities. They will enable tools, instruments, prioritized and targeted EU driven technological R&I&D developments those can balance back dependency from external technology providers and prepare us for new generation of cyber and hybrid threats. We will not avoid new threats, but we can be better prepared, autonomous and highly resistant.

3.3 CORE THEME – RESILIENT CIVILIANS, LOCAL LEVEL AND ADMINISTRATION

Title: *Comprehensive Security During the Covid-19 Pandemic: Impacts of Mis/Disinformation In the Age of Populism*
The Covid-19 pandemic has had far-reaching implications for the world as it undercut comprehensive security – that is security on the state, societal, and individual levels. Apart from health, political, and economic implications, it had significant consequences for the functional capacity of the state, potentially weakening societal cohesion necessary for well-being, equality, and peaceful existence. Moreover, the pandemic particularly exacerbated the vulnerabilities of non-dominant groups, that is certain racial and ethnic minority communities, which were often pitted against a sense of articulated marginalisation, insecurity and non-representation within the state amongst dominant groups. Although present well prior to the pandemic, the continued expressed senses of insecurity and fear of dominant groups that they were losing power and representation to non-dominant (minorities etc) groups became heightened during the pandemic. Right-wing populism, which provided a safe haven for the articulation of many of these fears, combined with mis- and disinformation (or the infodemic), added to this socio-political polarisation. Mis-/disinformation has impacted trust and social cohesion, often negatively, in different ways. It has disproportionately reduced trust among some minority

groups and made them more susceptible to contracting the virus. Mis/disinformation has also been used to exacerbate narratives about minority groups as a threatening "other" resulting in increased discrimination and prejudice by dominant groups as well as government authorities. On a more general level, mis- and disinformation translated into overall declining public trust in governments and leaders, not only turning compliance into a challenge, but also pitting the people against their own authorities in certain countries. Mis- and disinformation around Covid-19 dovetailed with populist and exclusionary discourses and narratives. Also, external powers—particularly Russia and China—amplified this to the detriment of democratic polities. States and societies, working with media, must strengthen measures to ensure that factual information reaches the public. It is additionally important to rebuild (where necessary) and strengthen trust between people and their representatives within the state. More work needs to be done to fuse democratic norms, principles, and processes with good governance to enhance trust and pluralism at the societal level. Without this, modern-day challenges like mis- and disinformation are likely to have a significant effect on comprehensive security, especially in times of crisis.

Title: *Critical Infrastructure Protection and Hybrid Threats*
Most probably, today many critical infrastructure(CI) operators are not even able to recognize the hybrid character of the attacks in their own business environment. This approach suggest in the article "Critical Infrastructure protection and Hybrid Threats" introduces the power of the information sharing and its benefits for critical infrastructure operators. Main finding is that an unified data model will reach to a unified representation (block chain) for most of the data sources and data cases from the point of view of prediction of future developments and trend analysis. The basic problem is that different processes within the use cases have different organization and causality structure. We can identify the common structures like trends, and trend thresholds if certain data sharing is agreed by CI owners. This has not yet been done in such a wide context. Concerning data management, data can be divided into 6 different risk areas where data is collected from each particular risk category into the whole risk landscape of critical infrastructure domain where similar signatures of attacker can be recognised.



3.4 CORE THEME – INFORMATION AND STRATEGIC COMMUNICATION

Title: *Information Manipulation and Historical Revisionism*

Historical revisionism has gained momentum in the last years, linked to the rising of Far-Right parties within Europe and Russia's expansionist foreign policy. The main narratives employed in influence and propaganda campaigns are focused on historic events situated in the Second War World, the Peace Treaties that led to the end of the First World War, the Communist Past of the CEE and more recently the processes of independence that took place in the post-Soviet space.

The Trianon Treaty (1920) is a major issue in recent Hungarian history and has been the object of revisionism since the arrival of Fidesz to the government. This event is instrumentalized by Orban's government on a dual level, directed both domestic and foreign interests, serving to reinforce patriotism and nationalism presented itself as a national trauma, and erode institutional support between Magyar minorities in Romania, Slovakia and Ukraine.

The Great Patriot War has been used in Russian propaganda since the Soviet period as a fundamental axis to construct its state identity, presenting the defeat of Nazism at the hands of the Soviet Union as an element of union for all the Soviet people. This narrative continues today, and is overlapped with antiliberalism and antifascist narratives that situate the West, especially the US, as a like-fascism continuum. At this point, NATO is presented together with EU as the enemy.

The accusation of historical manipulation by the West and countries of the former USSR, especially the Baltic States, is another of the narratives encouraged by Moscow, being a common topic in Kremlin outlets -RT and Sputnik so much in German, Czech, Greek, Polish or French. These attempts to re-write history usually put their attention on Second War World, encouraging the idea of a supposed campaign that seeks to harm the perception of the USSR and Russia.

The Molotov-Ribbentrop Pact (1940) is another key theme revisited by the Kremlin with repercussion in countries that were objected of repartition between Germany and the Soviet Union within the Secret Protocol. This issue embraces with anti-Western narrative, as it assumes that in the Pact, Communism and Fascism were understood as movements on the same level.

The information manipulation techniques employed are the distortion of the historical truth. The accusations that some countries (Ukraine, Poland, and Baltic States) associate themselves with Hitler; the framing of Russia and its actions positively; framing Russia as a victim of the West.

In the analysis of EU vs. Disinfo historical revisionism cases, there were identified 6 principal themes:

1. The WEST aggressive intentions against Russia, the EU with the focus on France and Germany relation; and EU-NATO relations.
2. Moscow reclaiming its “zone of influence” by denying the Soviet occupation in the neighborhood or accusing the former Soviet states, especially the Baltic States (Lithuania, Latvia and Estonia), of *historical revisionism, Russophobia and violation of human rights*.
3. Denying Ukraine Nation and Statehood and using the historical revisionism to justify Crimea, the Eastern occupation and the war.
4. Disinformation cases about WWII and Molotov-Ribbentrop Pact.
5. Poland as the central of the narratives about WWII and Molotov-Ribbentrop Pact: the underestimation of responsibility of the USSR over the political developments in the Polish People’s Republic.
6. Denying the crimes of Soviet Army and Soviet occupation in Central and Eastern Europe by promoting USSR/ Russia as a peacemaker and liberator, as a victim of Russophobia, as a victim of violations of the international law, as a victim of propaganda.
7. Three lines of disinformation have been employed by the Russian media concerning the case of the 1999 bombing of Yugoslavia. The number of victims of the air raids is disputed, the intentions of NATO are questioned and the legality of the interventions in discussed. While the last remains debatable, the first two are intentionally deliberately misrepresented.

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 and 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 we presented the findings of all four research articles, which now contribute to the initial findings established after the second 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 also in the perspective of innovations mapping to the gaps and needs and eventually most promising innovations uptake and standardization recommendations.

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 project 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
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
CER	Proposal for a Directive on the resilience of critical entities (revision of the Critical Infrastructure Directive)
NIS-2	Proposal for a revised Network and Information Systems Directive
COMM	EC Communication
NATO	North Atlantic Treaty Organization

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.