European Policy Brief

Framing the information domain vulnerabilities

EU-HYBNET Policy Brief No1.– Information and strategic communications -June 2021

- Exposing disinformation requires a thorough work on definition of what constitutes harmful content and a solid categorization of manipulative practices in information circulation. The use of algorithms to help identify disinformation in real time requires a thorough ethical approach and standards.
- Debunking and fact checking must rely on scale and networks constituted from pools of experts. Fact checking should be decentralized to take advantage of and connect expertise, while retaining a margin of manoeuvre for proactive approaches.
- The horizon of debunking fake news is necessarily reactive, resource consuming and can give unintended audience to fake content and their producers. An anticipatory approach should be privileged instead, whereby target groups could be warned of their being potentially subject to information manipulations.

Introduction

EU-HYBNET project's principal objective is to bring together practitioners and stakeholders to identify and define their common requirements for countering hybrid threats by undertaking an in-depth analysis and prioritisation of gaps and needs. The project conducts research and highlights innovation initiatives, including arranging training and exercise events to test the most promising innovations (technical and social) which will lead to creation of a roadmap for success and solid recommendations for uptake, industrialisation and standardisation.

This first Policy Brief of the project presents some of the challenges that the security environment of hybrid threats poses to the information and cognitive domain.

Data and methods used

This policy brief collects a series of preliminary findings and ongoing work of the EU-HYBNET project, in light of EU policy and regulatory developments in the field of digital platforms, information and cyber security. The project highlighted that the massive circulation of manipulated information on social media is a serious vulnerability as it related to hybrid threat actions because it coincides with a general decrease of trust in authority and expertise. The decreasing integrity and reliability of image, video and identity in the virtual world are additional threat surfaces. EU-HYBNET has also identified micro-targeting practices as a crucial lever in the landscape of hybrid threats. The status and role of individual data in this context is a focal point. The project will explore avenues to avoid the most disruptive effects of data aggregation for destabilisation. EU-HYBNET addresses the social demand for disinformation as well as some of its main supply channels.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No883054

Main Findings

The gradual development of a different kind of information circulation unsettled the dynamics of information and cognitive security. The circuits and flows of information on social media form digital public spaces. Those represent the network of interactions, conversation and content circulation patterns that underpin the digital information landscape. Current Information circulation patterns are conversation-based, both connecting and empowering users. Digital public spaces have a horizontal structure which contests and undermines sources hierarchies.

- **The weakening of the business model of journalism undermines democratic barriers to manipulated information**. Information circulation patterns in digital public spaces blur the separation between the steps of reception and conversation. The model of journalism implies that information descends first to the reader. Only in a second step readers engage with each other in conversation about information. Social media gives conversation a visible, public and potentially superseding character by comparison, to the content of the information itself. This is an important factor to assess the margin of manoeuvre opened to information manipulators in public digital spaces: the stages of reception and conversation in the circulation of information have merged and levelled. The diffusion of information on social media is unhinged, viral and undergoes little to no control mechanism. The Facebook model has extrapolated to the majority of social media and it has created entirely alternate systems of discussion, building echo chambers with selective exposure to content.

- **The social demand for disinformation, misinformation and manipulated information must be understood better.** EU-HYBNET has identified social exclusion as a core vulnerability because the circulation of content associated with disinformation cannot solely be explained by irrationality or media illiteracy. Individual actors are empowered to offer and promote their opinion online. The market of disinformation has an audience base for which sharing fake news or disinformation can be a social or political identity marker. Individuals tend to believe less in the information itself than to adhere to a worldview that corresponds to it. Beyond being a vector of political expression, the marketplace of disinformation gives tools to individuals with a self-declared duty to provide “alternative” viewpoints to “mainstream” media. The circulation of conspiracy theories offers a key example of the social and political character of disinformation.

- **EU-HYBNET underlines the destabilizing and disproportionate effects of hyper personalized targeting**. Individual behaviours became computable and predictable through the use of algorithms exploiting massive amounts of personal data, traces and signals online. This led to a significant possibility to anticipate, entice or discourage individual behaviour. The conjunction of advanced algorithms, computational power and massive amounts of data allows for the interpretation of the social world starting from individual levels. ***The project points to private individual data being the product of a market from which consumers are largely excluded***. EU-HYBNET therefore reflects upon the opportunity to further regulate a specific status to individual data online in order to avoid the most unsettling effects of its trade. This should further the logic of the General Data Protection Regulation (GDPR). The European Democracy Action Plan in particular

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No883054

identifies the need to counter disinformation, promote media pluralism and the sustainability of and promoting of free and fair elections. Those pillars resonate especially with the EU-HYBNET findings and the concerns of the network members.

Conclusion, policy implications and recommendations

The findings of EU-HYBNET correspond with current legislative and policy developments under **the European Democracy Action Plan in particular**: the effects of hyper personalised targeting correspond with the challenges to free and fair elections; the difficulties that EU-HYBNET identified as to the business model of journalism match the imperative to strengthen media freedom and pluralism; and finally the regime of individual data aggregates points to the question of obligations and accountability of very large platforms in improving the EU's response to foreign interference.

EU-HYBNET has especially found that exposing disinformation requires defining categories thoroughly: what constitutes harmful content and a solid categorization of manipulative practices of information circulation. The use of algorithms to help counter disinformation in real time requires a thorough ethical approach and standards. ***Practices centred on debunking "fake news" must be based on scale and the constitution of networks and pools of experts. Decentralizing fact checking should be favoured in order to take advantage of and connect expertise, while retaining a margin of manoeuvre for proactive approaches***. The horizon of debunking fake news is necessarily reactive, resource consuming and can give unintended audience to fake content and their producers. ***An anticipatory approach should be privileged instead, whereby target groups could be warned of their being potentially subject to information manipulations.***

Research parameters

EU-HYBNET is a 5-year EU funded project aiming to build a sustainable Pan European network of security stakeholders to collaborate with each other in order to increase the capacity on a European level to counter hybrid threats. In order to achieve its goal, the project is organised in four Core Themes, namely 1) Future Trends of Hybrid Threats, 2) Cyber and Future Technologies, 3) Resilient Civilians, Local Level and National Administration, and 4) Information and Strategic Communication. These Core themes will provide an opportunity to focus on all hybrid threat domains, especially interfaces between the domains, ensuring that the project delivers coherent results in relation to the conceptual framework model countering hybrid threats. In this context, practitioners are invited to express their needs in countering hybrid threats, which were later prioritised as the most urgent and crucial ones. Following the above, the project identifies the most promising technologies and innovations that could address the needs of the end users and develops a roadmap for their uptake and industrialisation, providing standardisation recommendations.

Research outputs from the project will be presented in a series of policy briefs, position papers and recommendations. The formulation of these outcomes will take place in close collaboration with stakeholders, who are included in the project activities from its outset, thereby maximizing its intended impact.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No883054

Project identity

Project name: Empowering a Pan-European Network to Counter Hybrid Threats (EU-HYBNET)

Coordinator: Laurea University of Applied Sciences, Finland

Consortium:

1. Arctic University in Norway (UiT), Norway
2. Bundeswehr University (COMTESSA), Germany
3. Central Office for Information Technology in the Security Sphere (ZITiS), Germany
4. Espoo City and Region (Espoo), Finland
5. Estonian Information Systems Authority (RIA), Estonia
6. The European Centre of Excellence for countering Hybrid Threats (Hybrid CoE), Finland
7. European Organization for Security (EOS), Belgium
8. France Ministry for an Ecological and Solidary Transition (MTES), France
9. International Centre for Defence and Security (ICDS), Estonia
10. Joint Research Centre EC (JRC), Italy
11. KEMEA, Greece
12. Laurea University of Applied Sciences (Laurea), Finland
13. Lithuanian Cyber Crime Centre of Excellence for Training, Research and Education (L3CE), Lithuania
14. Maldita, Spain
15. The Mihai Viteazul National Intelligence Academy (MVNIA), Romania
16. The Netherlands Ministry of Defence (MoD), Netherlands
17. Norwegian Directorate for Civil Protection (DSB), Norway
18. Polish Platfrom for Homeland Security (PPHS), Poland
19. Polish Internal Security Agency (ABW), Poland
20. Research Institutes in Sweden (RISE), Sweden
21. SATWAYS, Greece
22. TNO, Netherlands
23. Universita Cattolica Sacro Cuore (UCSC), Italy
24. University of Rey Juan Carlos (URJC), Spain
25. Valencia Local Police (PLV), Spain

Funding scheme: Horizon2020 Secure Societies Programme, General Matters-01-2029 call

Duration: May 2020 – April 2025

Budget: 3 496 837,50€

Website: https://euhybnet.eu/

For more information:

The European Center of Excellence for Countering Hybrid threats/ Mr. Maxime Lebrun maxime.lebrun@hybridcoe.fi; Laurea/ Coordinator Päivi Mattila paivi.mattila@laurea.fi

Further reading:

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

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No883054

- Article **Quantum as a disruptive technology in hybrid threats** in journal: *JRC Publications Repository.* Authors: Evaldas Bruze, Monica Cardarilli
- Article **The role of the "ordinary civilian" in hybrid threats** in 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.
- Article **Responses to digital disinformation: an evidence-based analysis on the effects of disinformation and the effectiveness of fact-checking/debunking** in journal: *El Profesional de la Information* (The Information Professional): http://www.profesionaldelainformacion.com Authors: Rubén Arcos, Manuel Gértrudix, Cristina Arribas and Monica Cardarilli

PROJECT

Partners

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No883054