EUROPEAN POLICY BRIEF

EU-HYBNET

Empowering a Pan-European Network to Counter Hybrid Threats

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883054

EU-HYBNET Policy Brief No2. – Countering Hybrid Threats: Areas for Improvement and Developing Innovations – December 2021

- Currently identified solutions and innovations focus on enhancing resilience and defensive capabilities. Offensive capabilities to deter or counteract hybrid threats remain a sensitive topic in democracies. However, it might be interesting to also look into this direction in order to broaden the counter hybrid capability portfolio.
- Citizen trust in government is an essential baseline upon which to improve resilience against hybrid threats. In absence of such trust, the effectiveness of solutions and innovations that involve citizen participation will be low.
- Policymakers play a vital role in creating and monitoring the frameworks through which possible solutions are developed and implemented, such as frameworks that define legal conditions, privacy regulations and standards for international cooperation.

Introduction

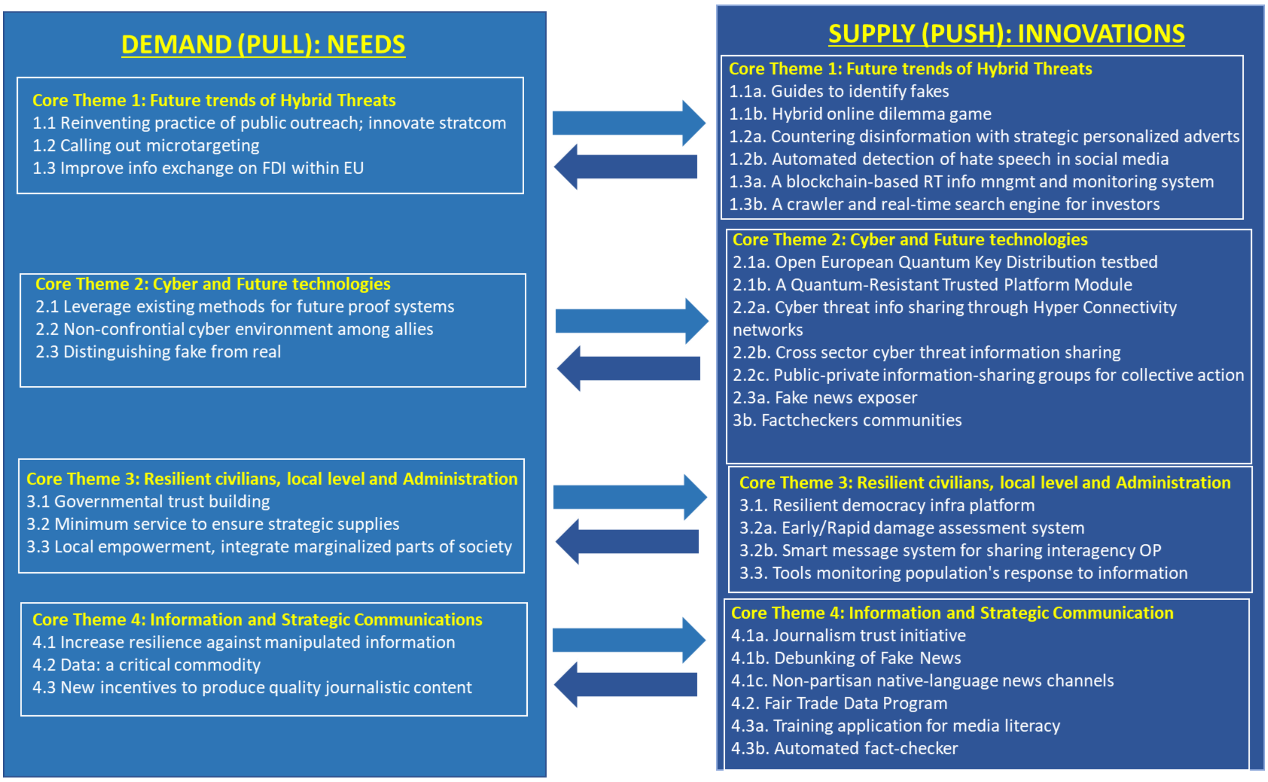
EU-HYBNET project's principal objective is to bring together practitioners and stakeholders to identify and define their common requirements for countering hybrid threats by undertaking an in-depth analysis and prioritisation of gaps and needs. The project conducts research and highlights innovation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

This second Policy Brief presents some clear recommendations for policymakers to improve EU resilience and options to counter Hybrid Threats, based on the project findings that have identified areas for improvement and clusters of innovation that require further Research and Development to such ends.

Data and methods used

The project has identified 12 gaps and needs that need to be filled, to help improve countering hybrid threats. Based on these gaps and needs, 27 technical and non-technical innovations and solutions were identified that could help fill these gaps and needs. In order to assess which innovations and solutions could be useful to help bridge specific gaps and needs, the project has created a mapping of the innovations and solutions onto the gaps and needs. The clustering of the gaps and needs has followed the project's Core Themes, which form the backbone of the EU-HYBNET project.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883054



DEMAND (PULL): NEEDS

Core Theme 1: Future trends of Hybrid Threats
1.1 Reinventing practice of public outreach; innovate stratcom
1.2 Calling out microtargeting
1.3 Improve info exchange on FDI within EU

Core Theme 2: Cyber and Future technologies
2.1 Leverage existing methods for future proof systems
2.2 Non-confrontial cyber environment among allies
2.3 Distinguishing fake from real

Core Theme 3: Resilient civilians, local level and Administration
3.1 Governmental trust building
3.2 Minimum service to ensure strategic supplies
3.3 Local empowerment, integrate marginalized parts of society

Core Theme 4: Information and Strategic Communications
4.1 Increase resilience against manipulated information
4.2 Data: a critical commodity
4.3 New incentives to produce quality journalistic content

SUPPLY (PUSH): INNOVATIONS

Core Theme 1: Future trends of Hybrid Threats
1.1a. Guides to identify fakes
1.1b. Hybrid online dilemma game
1.2a. Countering disinformation with strategic personalized adverts
1.2b. Automated detection of hate speech in social media
1.3a. A blockchain-based RT info mngmt and monitoring system
1.3b. A crawler and real-time search engine for investors

Core Theme 2: Cyber and Future technologies
2.1a. Open European Quantum Key Distribution testbed
2.1b. A Quantum-Resistant Trusted Platform Module
2.2a. Cyber threat info sharing through Hyper Connectivity networks
2.2b. Cross sector cyber threat information sharing
2.2c. Public-private information-sharing groups for collective action
2.3a. Fake news exposer
3b. Factcheckers communities

Core Theme 3: Resilient civilians, local level and Administration
3.1. Resilient democracy infra platform
3.2a. Early/Rapid damage assessment system
3.2b. Smart message system for sharing interagency OP
3.3. Tools monitoring population's response to information

Core Theme 4: Information and Strategic Communication
4.1a. Journalism trust initiative
4.1b. Debunking of Fake News
4.1c. Non-partisan native-language news channels
4.2. Fair Trade Data Program
4.3a. Training application for media literacy
4.3b. Automated fact-checker

Figure 1: Mapping of the 1st cycle's Gaps and Needs onto the Innovations (D3.1).

The clustering of the gaps and needs has followed the project's Core Themes, which form the backbone of the EU-HYBNET project. Following the mapping of the solutions and innovations onto the gaps and needs, the project assessed the individual innovations by using the EII (Excellence, Impact, and Implementation) assessment framework, which has led to the selection of 6 most promising innovations that should be considered for further uptake into the innovation roadmap.

The six best assessed innovations

Four (4) of the six (6) best assessed innovations are deemed to be useful in filling gaps and needs related to the disinformation area, whilst the other two (2) best assessed innovations are related to cyber and quantum security. The relatively high scores on these innovations are partly motivated by a high sense of urgency, high maturity of Technology Readiness Levels (TRL), high cost-effectiveness, and a clearly defined gap/need that is addressed by the identified solution.

The 6 best assessed innovations are the following:

- **Fake news exposer:** A software tool that helps to follow, analyse, and report on what is happening with public content on social media posts and assists users to identify fake news and disinformation. Such tooling uses both content and metadata to evaluate the articles in question.
- **Guides to identifying fakes:** Public guides to inform the citizens about the possibilities in the verification of visual materials. This includes a guidance as well as a list of several public tools that can support the user identifying fakes by providing e.g. an online analysis of suspicious objects.
- **Debunking of fake news:** The previous two tools to help identify and debunk disinformation should be integrated into a platform that is accessible and usable by users from the public and private spheres, as well as individual citizens. This solution aims at creating such a digital platform in the form of an independent crowdsourced analytical centre.

- **Countering disinformation with strategic personalized advertising:** By personalized adverting, the attention for the correct information on a topic can be given to the user, including the trustworthiness of the source. The user will then not look for other, less trustworthy sources, which helps weakening the spread of disinformation.
- **Cross sector cyber-threat information sharing:** Cyber-threat information sharing remains rare, due to a lack of willingness to share and a lack of trust between potentially collaborative partners. This is an issue on national, international, and European levels. Cross-sector cyber-threat information sharing envisions better forms of collaboration to share cyber-threat information across sectors.
- **Public-private information sharing groups developing collaborative investigations and collective action:** A similar lack of information sharing occurs between public and private entities. Especially when relating to cyber-threats, both public institutions and private companies remain reluctant to share vulnerabilities and cyber incidents with each other which enhances these vulnerabilities across society. Public-private information sharing groups should help drive willingness to collaborate on cyber-threat investigations and collective action.

Some key observations

- **All solutions are directed to increasing resilience and defence against hybrid threats:** The project's first cycle (May 2020 – September 2021) was limited to innovations and solutions that enhance resilience and improve defensive capabilities against hybrid threats. Offensive innovations and solutions, aimed at targeting a hybrid actor in order to prevent or mitigate hybrid threats, were not identified in the first cycle of the project. Western ethical and legal restrictions are a limiting factor to the identification of such solutions and innovations. Policymakers should evaluate such limitations and consider the pros and cons of such limitations in light of increased tensions and hybrid threats proliferation.
- **Information collection and information sharing opportunities:** Information is collected by many different entities, including governments, NGO's, private business, and citizens. Yet the willingness to share information cross sectors remains inadequate. To counter hybrid threats, where a hostile campaign might only be observable by linking together a myriad of weak signals across various sectors and countries, it is essential that information sharing is enhanced. This ranges from establishing and expanding specialized cross-sector cyber threat information sharing platforms, early damage assessment platforms, public-private information sharing groups civilian emotional detection tools, and foreign direct investment monitoring platforms, to a more holistic society-wide resilience-improving network in the form of resilient democracy infrastructure platforms.
- **There are structural challenges to the upscaling of national initiatives to EU level:** All EU member states work on various hybrid threats and appropriate tools to counteract these challenges. Whilst it is commendable that all member states are taking hybrid threats seriously and engaging to look for solutions, it remains a challenge to share best practices and to scale-up effective solutions from a national level to the EU level. Such challenges include diverging conceptualisations of hybrid threats, different prioritizations of hybrid threats, and a lack of awareness of clear benefits from such sharing.
- **Blowback risk due to low societal acceptance:** Innovations related to improving civilian resilience and enhancing governmental strategic communications to citizens are highly dependent on citizens' acceptance of tooling that interacts with, informs, and influences the citizenry. Such tools can only be implemented in settings where a certain threshold of societal acceptance of these tools has been

reached. In absence of such community support, tools that are intended to improve citizen resilience and expand accessible and understandable information could have the counter-productive effect of further citizen distrust towards the government, which in turn could further polarize societies. Policymakers have an essential role in understanding the constraints of citizen-focused solutions, and should consider roadmaps of implementation for such solutions.

- **Lacklustre addressing of legal and ethical challenges:** Hybrid threats and its constituent elements remain a topic that is not adequately known nor understood amongst policymakers. Given the novelty of the field of research, the evolving nature of hybrid threats, a lacklustre anticipatory approach towards legal and ethical challenges is not surprising, but nonetheless a hindrance to developing and implementing solutions. Legal and ethical challenges should be addressed throughout the entire process of identifying, developing, and implementing solutions. Policymakers have a vital role in setting up and monitoring adherence to legal and ethical for possible solutions. Without these structures that dictate how innovations would fit within the legal and ethical frameworks of practitioners, innovations might remain unusable upon development.
- **Improve post-quantum cyber security position:** Whilst quantum computing-enhanced cyber-attacks are not yet an imminent and urgent threat, this will drastically change the playing field once such capabilities become operational. As such, it is essential to invest in cyber security against future quantum computing-enhanced cyber-attacks. The quantum key distribution testbed could help improve societal resilience against such quantum computing-enhanced cyber-attacks for Business-to-Business and Business-to-Consumer collaborations, as well as for crisis-time emergency communications. Research into quantum technology and its implications is not yet well regulated. Such regulations could help ensure that critical applications that are being built today, are quantum-safe or quantum-upgrade-ready.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883054

Research parameters

EU-HYBNET is a 5-year EU funded project aiming to build a sustainable Pan European network of security stakeholders, especially security practitioners, 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.

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 Norwar (UiT), Norway
2. Bundeswehr University (COMTESSA), Germany
3. Central Office for Information Technology in the Security Sphare (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 Soceties Programme, General Matters-01-2029 call

Duration:

May 2020 – April 2025

Budget:

3 496 837,50€

Website:

https://euhybnet.eu/

For more information:

The Netherlands Organisation for Applied Scientific Research/ Rick Meessen and Okke Lucassen rick.meessen@tno.nl okke.lucassen@tno.nl

The European Center of Excellence for Countering Hybrid threats/ Mr. Maxime Lebrun maxime.lebrun@hybridcoe.fi

Laurea/ Coordinator Päivi Mattila paivi.mattila@laurea.fi

Recommended reading

- EU-HYBNET First report on improvement and innovations, D3.3. Sofou, S. et al. (2020).
- EU-HYBNET First report on innovation and research project monitoring, D3.7. Zylius, R. et al. (2020).
- EU-HYNBET First interim report mapped on gaps and needs, D3.1. Meessen, R., Lucassen, O.G., et al. (under review, draft available upon request).