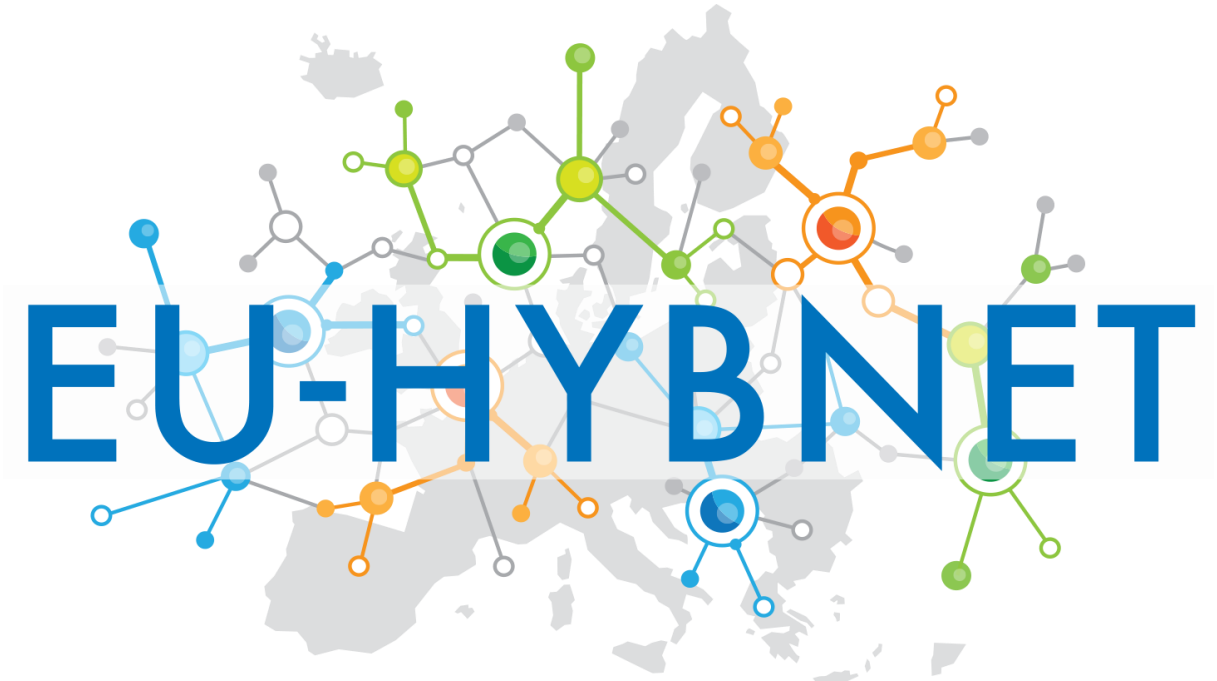
EUROPEAN POLICY BRIEF



Empowering a Pan-European Network to Counter Hybrid Threats

Build Societal Resilience – Share IMI* Information

* Information Manipulation and Interference

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

Introduction

The principal objective of the Empowering a Pan-European Response to Hybrid Threats (EU-HYBNET) project is to bring together pan-European security practitioners and stakeholders in the hybrid threat area to perform a joint in-depth analysis of gaps and needs and thereby identify, define and prioritize common requirements for countering hybrid threats. To this end, EU-HYBNET conducts research and highlights innovations and solutions that aim to close identified gaps and fulfil practitioners' needs. The considered innovations and solutions (technological and social) are assessed by practitioners, researchers and in gamified training events. For innovations and solutions that are assessed as promising, roadmaps for successful uptake, industrialisation and standardisation are developed.

This 3rd policy brief from the project presents some of the challenges in handling Information Manipulation and Interference (IMI) activities and campaigns together with actions that would help build increased societal resilience against such threats. Here IMI stand for any information manipulation and interference from any actor, i.e., it comprises both foreign and domestic information manipulation and interference.

Data and Methods Used

This policy brief is based EU-HYBNET Task4.2 "Strategy for Innovation uptake and industrialization" and its results presented in project deliverable 4.4 "1st Innovation uptake, industrialisation and research strategy" by Research Institutes in Sweden (RISE). The focus is on EU-HYBNET assessments of innovations targeting methods and procedures for how to counter IMI activities together with a review of ongoing EU activities in the field and in particular current European External Action Service (EEAS), Strategic Communication division initiatives. The research performed reveals that sharing, analysis and aggregation of IMI information between stakeholders is of outmost importance, especially for early/immediate and successful mitigation of the effects of IMI activities and campaigns. Having the means to produce joint near real-time situational awareness and a comprehensive overview of the threats in the mid and long term that are common to stakeholders within and between member states are key.

Main Findings

There are important actions that need to be taken to build and improve societal resilience against national and foreign IMI activities and campaigns. A solution for efficient cooperation between stakeholders would allow access to IMI information coming from concerned sources and would constitute a basis for early detection and joint actions to counter IMI activities. Cooperation must be based on trust between involved stakeholders and joint actions must rely on a common view of the situation at hand.

We first note that IMI activities and campaigns and the mitigation of their effects, affect and involve **a large number of stakeholders** on domestic, EU and international level. Important examples of stakeholders are the civil society in Member States, Member State and European institutions, research organisations, fact checking organizations, private industry, social media platforms, and other international partners like NATO and the G7.

Secondly, we note that **currently the sharing of IMI information is limited** by three factors: the first is that a commonly accepted and jointly used taxonomy for IMI and TTPs (Tactics, Techniques and Procedures) is missing which makes it difficult to ensure a common understanding of what described activities really mean. The second is that IMI information in many cases is deemed to be of national security interest and thus is

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

restricted with respect to sharing with other EU member states and stakeholders. The third is due to privacy concerns; what kind of information should a government be allowed to retrieve and store and within what kind of legal framework? It should also be noted that private companies might be hesitant or not at all willing to freely share IMI information, either because the IMI information has a business value like CTI (Cyber Threat Intelligence) or that the information may be business sensitive.

Our third observation is that **currently the main sharing of IMI information is in the form of reports presenting finalized analysis** of considered threats, incidents and procedures. This means that it is difficult to achieve near real-time awareness using such shared reports. Furthermore, aggregation of such information involves a lot of manual work. Today the Rapid Alert System on Disinformation (RAS) provides a platform for the EEAS to exchange information with other EU institutions, EU Member States, as well as a platform for cooperation with international partners, like the G7 Rapid Response Mechanism and NATO. The European Digital Media Observatory (EDMO) is another platform for information sharing. EDMO is an independent observatory bringing together fact-checkers and academic researchers with expertise in the field of online disinformation, social media platforms, journalist-driven media and media literacy practitioners. Established in 2020, it promotes scientific knowledge on online disinformation, advances on the development of fact-checking services, and supports media literacy programmes.

The fourth observation is that to achieve rapid and near real-time joint situation awareness more low-level **IMI information must be shared and distributed analysis solutions employed. The sharing and analysis must be supported by automatic and/or semi-automatic functions and services** to allow handling of the very large amount of IMI data involved and especially being capable of handling multi-lingual settings. The need for efficient tools supporting distribution and analysis of IMI information is of particular importance when immediate/early successful detection and mitigation of IMI activities is required.

Recommendations

Based on the findings described above, the EU-HYBNET project recommends that the following actions are implemented:

- **Develop an IMI taxonomy**, which comprises common definitions and required terminology to adequately and precisely describe the IMI threats and approaches.

- **Develop standards for IMI information exchange**. Such as standard could take the STIX standard (Standard Threat Information Expression) as a starting point and extend it to cover relevant but missing IMI aspects. STIX allows sharing of information about incidents including actors, vulnerabilities, TTPs etc., in a machine-readable format.

- **Develop a distributed networking solution for IMI information sharing and analysis**. The networking solution could take e.g., the European Maritime Security Authority (EMSA) Maritime CISE (Common Information Sharing Environment) networking solution format as a starting point and extend it with capabilities for joint automatic or semi-automatic analysis of IMI data. The networking solution must include functionality which gives the information owner control of which information that is shared with whom. It should also ensure that systems currently in use by different stakeholder for IMI situational awareness and analysis can be accommodated.

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

- **Initiate research and development in the area of automatic and / or semi-automatic IMI analysis tools**. Such tools will be required to cope with the increasing amount of information that has to be monitored, scanned and analysed for IMI activities and/or attacks. As sharing of information related to IMI may be sensitive and block sharing of IMI information, a remedy would be to base joint analysis efforts on federated machine learning methods. Furthermore, it should be considered to develop AI tools based on behaviour-based AI techniques as they may provide a more reliable solution which also is privacy and freedom-of-speech protecting.

- **Initiate an EU task force investigating how to build trust between private and public sector stakeholders** with the aim to make IMI information sharing available, i.e., analyse and propose solution for how to enable participation of private sector stakeholders in IMI information sharing and analysis networks. Issues at hand are how private ownership/control of assets should influence possibilities to participate, trust issues in general and barriers against sharing of secret or sensitive information, etc.

Conclusions and policy implications

The suggested activity is seen a way to enhance pan-European response to hybrid threats taking place in the information domain. Furthermore, the suggested actions could be a way to support the use of EU Member States' Rapid Alert System (RAS) and the implementation of the EU Democracy Action Plan, focus area "Counter disinformation, foreign interference and information influence operations". The suggested solution would also contribute to actions requested in the Security Union Strategy, focus: Hybrid Threats.

Research parameters

EU-HYBNET is a 5-year (2020 - 2025) 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 EC 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 security 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 pan-European security 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 No 883054

Project identity

Project name: Empowering a Pan-European Network to Counter Hybrid Threats (EU-HYBNET)
Coordinator: Laurea University of Applied Sciences, Finland
Editor for the Policy Brief: Rolf Blom, RISE

Consortium:

1. Arctic University in Norway (UiT), Norway
2. Bundeswehr University (COMTESSA), Germany
3. Central Office for Information Technology in the Security Sector (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 Platform 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. GA No. 883054
Duration: May 2020 – April 2025
Budget: 3 496 837,50€
Website: https://euhybnet.eu/

For more information: Laurea/ Coordinator Päivi Mattila paivi.mattila@laurea.fi

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