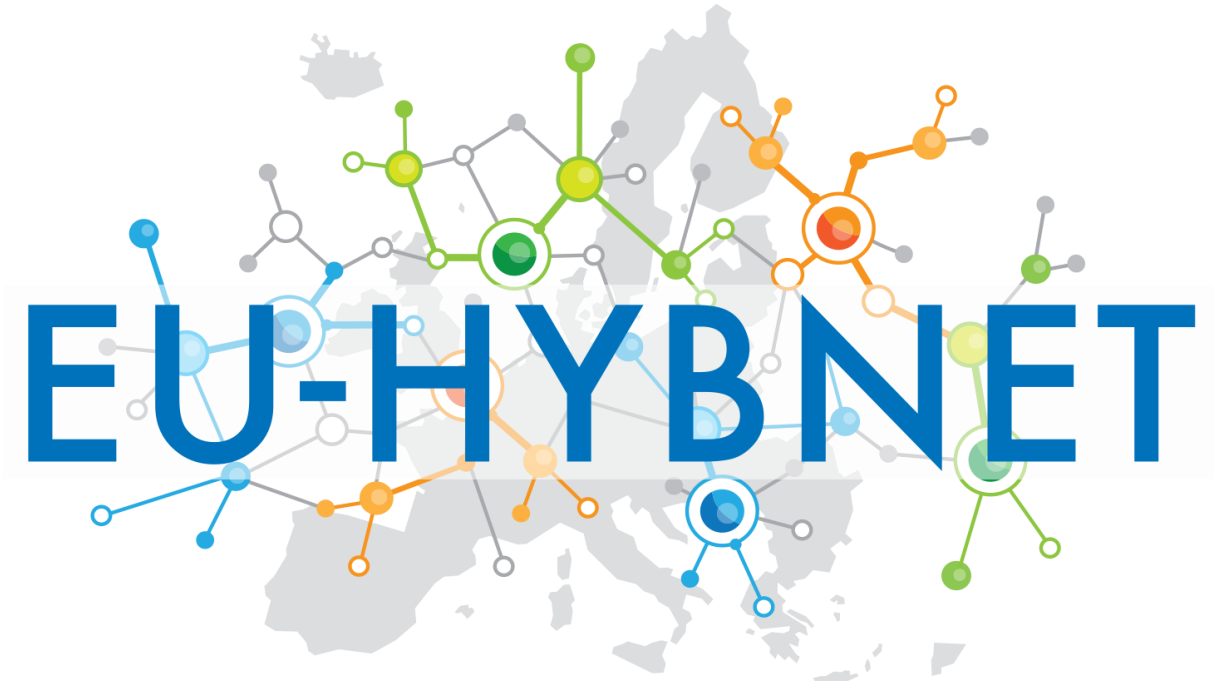
EU-HYBNET REPORT No 2



Empowering a Pan-European Network to Counter Hybrid Threats

MIMI: An EU-HYBNET Innovation

Boost Sharing of IMI* Information

Create MIMI, a Marketplace

* 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 report from the project presents **an innovation for stimulating and supporting increased sharing of Information Manipulation and Interference (IMI) Information (IMII).**

IMI in the information domain describes a mostly non-illegal pattern of behaviour that threatens or has the potential to negatively impact values, procedures and political processes. Such activity is manipulative in character, conducted in an intentional and coordinated manner, often in relation to other hybrid activities. IMI actors can be state or non-state actors, including their proxies inside and outside of their own territory. [i]

This conceptual definition of IMI reflects into an analytical sector that follows a specific approach to understanding, detecting, cataloguing and addressing the techniques used by various threat actors to influence and manipulate the information space. Subsequently, the solution proposed in here addresses the need of using analytical insights to ensure informed, timely and effective counter actions, as well as prevention and deterrence, which would lead to increased societal resilience against IMI activities and campaigns, as well as an economic incentive for those working on analysing/countering IMI. This proposal for actions covers both foreign and domestic IMI. It also is strongly related to the 3rd EU-HYBNET Policy Brief *Build Societal Resilience – Share IMI Information*[ii] in which the need and means for IMII sharing is established. What is suggested is to establish **a Market place for Information Manipulation and Interference information sharing called MIMI**.

Data and Methods Used

This report is based EU-HYBNET Task4.2 "Strategy for Innovation uptake and industrialization" and its results presented in project deliverable 4.5 "Second 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, alongside a review of ongoing EU (European Union) activities in the field and, in particular, the current approach promoted by the European External Action Service, Strategic Communication (EEAS StratCom) division[iii].

The research performed reveals that prompt sharing, aggregation and analysis of IMI information is of utmost importance, especially for early and successful mitigation of the effects of IMI activities. In this case, as in many other solutions requiring situational awareness, the more information available the greater the possibilities for early and correct detection of relevant events and activities. However, information availability alone is not sufficient, if there is no way to efficiently aggregate it and combine it to fully understand its complexity. Obstacles with respect to sharing of IMII exist and need to be overcome, in order to set up the required flow of information between providers, analysts and end users. The proposed way forward to eliminate/relieve these obstacles, is to create MIMI an open and free market for IMII sharing.

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

Setting the scene

Within the European Union, several policy documents present different strategies, actions and regulations with respect to how to handle IMI activities and campaigns (of which disinformation is just one dimension). In 2020 the *European Democracy Action Plan*[iv] *(EDAP)* was published and now a new initiative "Defence of Democracy Package"[v] is under preparations. In the context of this report, the following actions listed in the EDAP are deemed relevant to counter disinformation and IMI:

- Put in place a new protocol to **strengthen existing cooperation structures** to fight disinformation, both in the EU and internationally
- Develop a common framework and methodology for **collecting systematic evidence** on foreign interference and a structural **dialogue with civil society, private industry actors and other relevant stakeholders** to regularly review the threat situation.
- Increase support for **capacity-building** of national authorities, independent media and civil society in third countries **to detect and respond to disinformation and foreign influence operations**.

In 2022 *A Strategic Compass for Security and Defence*[vi] was published, which together with its annex *Foreign Information Manipulation and Interference (FIMI) Toolbox* highlights the necessity of developing a European Hybrid Toolbox. The annex underlines a set of preventive and counter measures to be applied at EU level in order to counter FIMI, including a FIMI Data space built on a common analytical framework and methodology to collect systematic evidence of FIMI incidents.

The MIMI innovation, inspired from the structure of the FIMI Data Space, can practically support this initiative as a concrete tool to connect information providers and requesters from different fields across the society, thereby enhancing the societal responsiveness to IMI.

This report presents **MIMI**, a recommendation that will contribute to the implementation of the referenced policy actions, and suggest a solution for the toolbox, thereby building on ongoing research regarding the development of a common framework and methodology for collecting systematic evidence on IMI activities. The aim is to strengthen and widen cooperation structures in the fight against IMI and enhance the ability of national authorities, independent media and civil society to detect and respond to IMI operations.

Main findings

We first note that the analysis of IMI activities 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 States and European institutions, research organisations, fact checking organizations, private industry, social media platforms, and international partners like NATO and the G7.

Furthermore, **today, sharing of IMII is limited**. IMI does not know borders, therefore fostering the active sharing of IMII among all concerned stakeholders, nationally as well as internationally, remains a priority in this field. Reluctance to share, depends on many factors and is a severely limiting factor in current work to improve the quality and timeliness of possible mitigating actions. Increased sharing of base information as well as analysed data must thus be encouraged, and this would need supporting activities to establish standardised sharing means and procedures.

We note that **there are some initiatives within the EU to share IMII information** retrieved by authorities in the MS. This is of course of great value in the work to improve the situational awareness when it comes to how society can handle IMI activities and campaigns. A more open environment for sharing of IMII would

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

open up also for a more general availability of business and end-user adapted IMII. It would at the same time also improve the situation for national authorities and international organisations as it would give access to more IMII and most likely also lead to cost savings in the process.

Today most **IMII collection, analysis and end-use is performed in silos**, in fact, as underlined in the 3rd EU-HYBNET Policy Brief *Build Societal Resilience – Share IMI Information*[vii], the sector still lacks commonly adopted and interoperable taxonomy frameworks to describe the different constitutive parts of IMI. For comparison, a similar situation is prevalent when it comes to CTI (Cyber Threat Intelligence). More often than not, this means that when a situational awareness solution is needed, it is built from scratch based on its own collection of evidence through OSINT[viii] (Open-Source Intelligence). The aim here is to achieve a horizontal distribution of actors in an open market and to avoid duplication of efforts across the sector. A MIMI would need to lay its foundation on commonly agreed taxonomies for IMI and compatible data formats that allow for systems' interoperability when sharing IMI data among stakeholders.

MIMI, a marketplace for IMII would stimulate the establishment of multiple actors that specialize and compete in different segments of the supply chain. There may be actors that mine the Internet, others monitor media outlets, domains, social media or the darknet, searching for relevant data and content, and in this way produce baseline IMII. Others may specialize in analysis of such baseline IMII data to detect certain aspects of IMI, like identifying specific tactics, techniques and procedures (TTPs) used by threat actors, in diverse cultural regions and languages. Still others, may base their work on already analysed IMII data in order to get an overarching situational awareness or to base decisions on where and how to intervene. If such a marketplace is established, it would lead to a situation with highly competent and specialized competing actors, and in the end, this would provide high quality results and end products.

An IMII sharing environment and supply chain can be depicted in a value chain. At least five categories of stakeholders can be envisioned in an IMII sharing value chain:

1. **Data providers** that do different types of monitoring and generate data for IMI incidents and related information.
2. **Aggregators** that collect descriptions from different data providers and sort and relate them.
3. **Analysts** that perform analysis of incidents on IMI activities, campaigns and mitigating actions.
4. **Distributors** that collect analysts results and make them available for interested end-users.
5. **End-users** that based on distributors' reports perform mitigating actions.

Already now, **numerous companies and organizations work in the field of IMII analysis.** On a commercial basis they sell their results to different types of end-users. Oftentimes, these results take the form of written reports presenting finalised analysis and therefore their usability remains limited in time. The possibility to obtain IMI data and reuse it, thereby aggregating different types of knowledge obtained from different providers, is currently a service that few actors in the market are able to offer, but which remains in high demand. Furthermore, **IMII often has a direct business value** (similar to CTI[ix]) and may also be business sensitive giving, for example, clues about ongoing market events. The willingness to share IMII without compensation may thus be limited in private business ventures. Hence there is a need for the establishment of **an open commercial IMII marketplace (MIMI)** in which the value of IMII is recognized.

Basic requirements for the establishment of an IMII marketplace **(MIMI)** would be:

1) **Standardized taxonomies, procedures and protocols** for descriptions, interpretation of and distribution of IMII. The development of the **MIMI** should build on ongoing standardization activities around IMII sharing, in particular the ongoing work at the EU-level by the EEAS to establish what is called the FIMI (Foreign Information Manipulation and Interference) Dataspace. This work includes a commonly

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

accepted and used taxonomy for IMII and TTPs (Tactics, Techniques and Procedures), the extension of STIX[x] and TAXII[xi] to cover IMII sharing needs and the use of the DISARM framework[xii] as TTPs categorization methods. The work is presented in the *1st EEAS Report on Foreign Information Manipulation and Interference Threats*[xiii]. The EEAS currently uses OpenCTI[xiv] as knowledge management and sharing platform, but other possibilities, like MISP[xv] platforms exist. The EEAS's framework for establishing a standardized IMII sharing environment has been agreed with the US[xvi] and will be a joint development effort. Likewise, some EU Member States are on their path to establish services that apply said methodologies in their analytical work.

2) **Sharing platforms that are secure and trusted by stakeholders** which means that stringent security guarantees must be incorporated in the specifications of utilized implementations and platforms. In some cases, IMII is considered to be a security threat and thus is restricted with respect to sharing. Thus, there is a need to ensure that the process of sharing IMII can be trusted by all the users of MIMI and that sharing can be securely controlled with respect to how and with whom the information is shared and how the aggregated and analysis results are shared. The set-up of MIMI must implement safeguards against malicious actors becoming part of the market place.
3) **A business model for IMII sharing** which is accepted by all stakeholders needs to be developed. There can be different options for access and sharing like subscriptions or "pay-per-view". The relevance of the options partly depends on the distribution mechanism used. Anyhow, there should be standardized procedures and interfaces for ordering, specifying and paying for IMII. These procedures and interfaces should be integrated into the sharing platform and follow standard procedures for business agreements, contracts and payments.

Recommendations

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

- **Convene IMII sharing stakeholders to discuss and agree baseline requirements for the establishment of an IMII marketplace (MIMI)**. The baseline requirements should at least cover a business model, access methods and controls, service level agreements, payment and charging solutions, and stakeholder mutual trust establishment.
- **The stakeholders should also agree policies for the use of the IMII,** this to ensure that its use doesn't lead to political censorship but allows freedom and speech and legitimate political expressions.
- **Drive the development and adoption of common data sharing standards and taxonomies based on open and interoperable standards like STIX or TAXII** to achieve wide adoption and interoperability of IMII sharing solutions. IMII sharing standards should be based on standardized, collaborative and open frameworks, taxonomies, and data standards, enabling users to build upon shared threat models and information. It should also strive for interoperability with other information sharing solutions in other communities e.g., cybersecurity, OSINT, etc, to provide access to as much (relevant) information as possible.
- **Standardize required security solutions for trusted and controlled sharing of IMII.** The authenticity and integrity of the IMII must be verifiable as well as its origin so that contaminated information will be detected and not entered into the sharing environment. Furthermore, sharing must be controlled so that IMII items only are shared with intended recipients and not forwarded/leaked to "external agents" and unauthorized parties
- **Develop and integrate the required interfaces and APIs (Application Programming Interfaces) for support of the IMII marketplace in the sharing and analysis framework.**
- **Review if there are any EU or national rules and regulations that would be hindering IMII sharing.**

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

- **Create demand for services that provide IMII in accordance with common frameworks.**

Conclusions and policy implications

The suggested activities are seen as a way to enhance the possibilities for a pan-European response to hybrid threats taking place in the information domain. Furthermore, the suggested actions would be a way to support the implementation of the EU Democracy Action Plan, focus area "Counter disinformation, foreign interference and information influence operations" and be a support to the toolbox proposed in the EU Strategic Compass for Security and Defence. The suggested solution would also contribute to actions requested in the Security Union Strategy, focus: Hybrid Threats alike forthcoming new policy initiative "Defence of Democracy Package". Depending on the outcome of the review about if there are EU or national rules and regulations that would be hindering IMII sharing, updates and revisions of MIMI and/or the regulations might be necessary.

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 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 (European Commission) 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 reports, 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.

Project identity

Project name: Empowering a Pan-European Network to Counter Hybrid Threats (EU-HYBNET)
Coordinator: Laurea University of Applied Sciences, Finland
Editor for this report: 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

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

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

---

[i] From the FIMI definition in https://www.eeas.europa.eu/eeas/tackling-disinformation-foreign-information-manipulation-interference_en
[ii] https://euhybnet.eu/wp-content/uploads/2022/02/EU-HYBNET_Policy-Brief_-Information-Manipulation-and-Interference_Feb-2022.pdf
[iii] https://www.eeas.europa.eu/eeas/1st-eeas-report-foreign-information-manipulation-and-interference-threats_en
[iv] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0790
[v] Commission Work Program 2023, p. 14.
[vi] https://www.eeas.europa.eu/eeas/strategic-compass-security-and-defence-1_en
[vii] https://euhybnet.eu/wp-content/uploads/2022/02/EU-HYBNET_Policy-Brief_-Information-Manipulation-and-Interference_Feb-2022.pdf
[viii] OSINT (Open-Source Intelligence) is defined as intelligence produced by collecting, evaluating and analyzing publicly available information with the purpose of answering a specific intelligence question.
[ix] CTI (Cyber Threat Intelligence) is a branch of cybersecurity that deals with the collection, analysis, and dissemination of information about current and potential cyberattacks that pose a threat to an organization's assets.
[x] STIX (Structured Threat Information Expression) is a structured language for describing cyber threat information and how it can be shared, stored, and analysed in a consistent manner. http://stixproject.github.io/about/
[xi] TAXII (Trusted Automated eXchange of Intelligence Information) defines how cyber threat information (e.g., in STIX) can be shared via services and message exchanges. https://oasis-open.github.io/cti-documentation/taxii/intro.html
[xii] DISARM is the open-source, master *framework* for categorizing Tactics techniques and Procedures of information manipulation, as well as related counter-actionshttps://www.disarm.foundation/framework
[xiii] https://www.eeas.europa.eu/eeas/1st-eeas-report-foreign-information-manipulation-and-interference-threats_en
[xiv] OpenCTI, an open source platform for managing cyber threat intelligence knowledge and observables. It structures, stores, organizes and visualizes technical and non-technical information about cyber threats. https://github.com/OpenCTI-Platform/opencti#readme
[xv] MISP, an open source software solution for collecting, storing, distributing and sharing cyber security indicators and threats about cyber security. https://www.misp-project.org/

[xvi] Joint Statement EU-US Trade and Technology Council of 31 May 2023 in Lulea, Sweden (section "Foreign information manipulation and interference (FIMI) in third countries") and the technical annex.

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