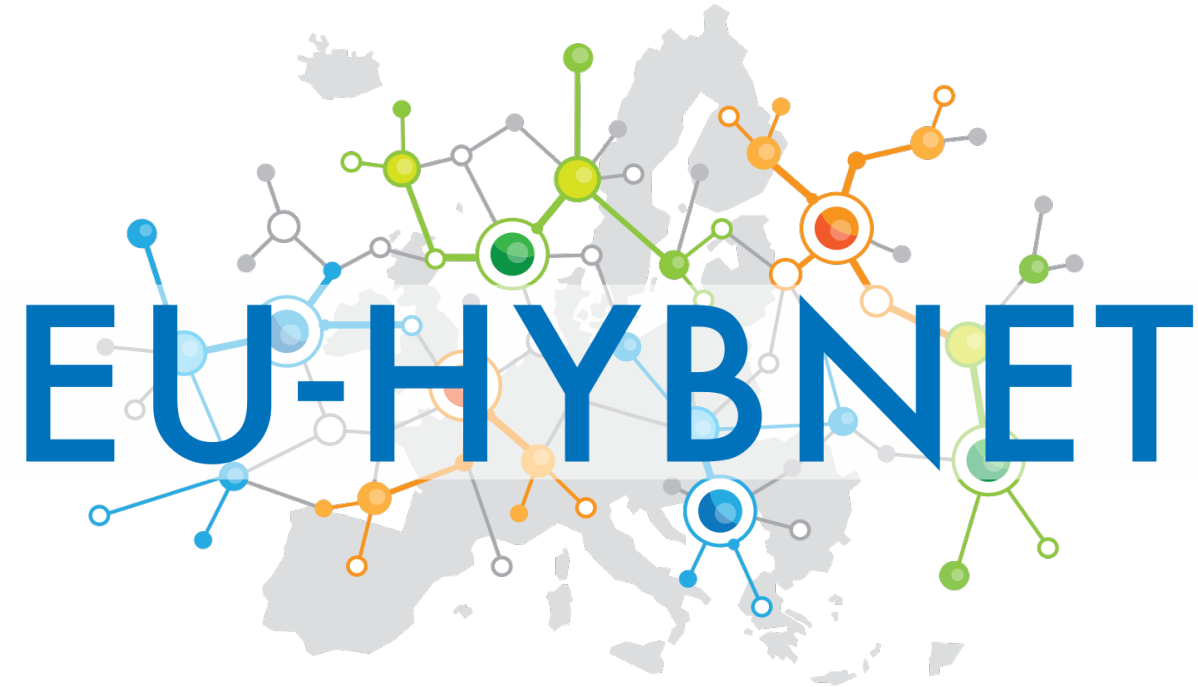
EUROPEAN POLICY BRIEF



Empowering a Pan-European Network to Counter Hybrid Threats

On Information Sharing between Critical Entities for early and efficient detection and mitigation of Hybrid Threats

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

Summary

Hybrid threats are complex challenges that exploit societal weaknesses and undermine democratic societies. These threats combine traditional, unconventional, and cyber tactics, often causing cascading effects across different domains. Current protection strategies focus on asset protection, neglecting interdependencies and risks. This policy brief, based on the WINS methodology, proposes enhancing resilience through effective information sharing. The European Union's Critical Entities Resilience (CER) Directive emphasizes the need for comprehensive risk assessments and measures to ensure uninterrupted essential services.

To manage hybrid threats, early detection and information sharing between critical entities is crucial. The brief recommends identifying essential information, termed Indicators of Hybrid Threats (IoHT), and using privacy-preserving technologies for secure data sharing and analysis. These steps will enable rapid detection and mitigation of hybrid threats, fostering resilience across various sectors and domains.

Introduction

Hybrid threats[1] are complex and evolving challenges that undermine the functioning of our democratic societies and the acceptance of their foundational principles. These threats aim to exploit societal weaknesses, foster distrust in institutions, divide groups, and ultimately weaken a society's operational and decision-making capacities.

Hybrid threats often combine traditional, unconventional, and cyber tactics with economic pressure and other coercive methods, making attacks difficult to predict and counteract. Furthermore, hybrid threats involve parallel and/or sequential attacks across different domains and may be used to generate cascading effects. For example, an attack on a power system can cause problems and malfunctions in other essential services like water supply or heating. Therefore, to uphold the social contract that underpins our democratic societies, it is imperative to ensure the continuous and reliable operation of critical entities and their essential services.

At present, protection of critical entities is mainly based on asset protection, which has led to a situation where increased interdependencies and related risks of cascading effects are not sufficiently considered. Current risk management approaches are mostly domain and country-specific, which does not allow for coherent risk awareness between domains or countries.

This policy brief **presents two promising avenues for detecting hybrid threats and enhancing the resilience of critical entities**. Both avenues aim to enable effective sharing of essential information between critical entities as sharing is essential for developing robust platforms that enable early detection of hybrid threats across various critical sectors and domains. The basic idea originates from WINS[2], an innovative approach that provides a methodology for determining which information needs to be shared to enhance resilience and counter hybrid threats.

[1] EU-HYBNET project use the term hybrid threats as defined in the EU documents The landscape of Hybrid Threats: A Conceptual Model (Public Version) and the so called CORE model described in Hybrid threats: A comprehensive resilience ecosystem. Hybrid threats refer to when, state or non-state, actors seek to exploit the vulnerabilities of the EU to their own advantage by using in a coordinated way a mixture of measures (i.e. diplomatic, military, economic, technological) while remaining below the threshold of formal warfare.

[2] The WINS solution emanates from the EU-HYBNET ("Empowering a Pan-European Response to Hybrid Threats") project's research described with details in deliverable D4.5 "2nd Innovation uptake, industrialisation and research strategy".

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

EU Guidance

The need for greater attention from European Union (EU) Member States as well as owners and operators of critical entities has been clearly stated in the new *Critical Entities Resilience (CER) Directive*[3] and the plan of action for strengthening the EU's security and defence policy, the *Strategic Compass for Security and Defence*[4].

The CER Directive mandates EU Member States to implement specific measures to ensure the uninterrupted provision of essential services vital for societal functions and economic activities within the internal market. To comprehensively address these issues, the Directive establishes a framework which addresses the resilience of critical entities against all hazards, whether natural or human-caused, accidental, or intentional.

Critical entities are required to have a thorough understanding of the relevant risks they face, and they must analyse these risks including, but not limited to, cross-sectoral and cross-border threats, accidents, natural disasters, public health emergencies, hybrid threats, and terrorist offences. Risk assessments must be tailored to the specific circumstances at hand, any interdependencies between sectors, and the evolving nature of these risks. Relevant elements of these risk assessments must be shared with the identified critical entities to help them conduct their own assessments and enhance their resilience.

The CER Directive only talks about the sharing of risk assessment elements, which indicates that cross-sectoral, cross-border and interdependent threats are of great concern, which in turn implies that fast and reliable sharing of hybrid threat information is key for efficient and rapid detection and mitigation of hybrid threats. In the memo *What If the EU Did Not Share Data to Protect Its Critical Infrastructure?*[5] what could happen if the EU fails to establish an information exchange environment among its critical infrastructure entities is discussed, and it is noted that the importance of sharing relevant information between critical entities.

What to share and how

Understanding and managing hybrid threats and their associated risks require both technical and strategic measures. Early warnings and detection are essential for the successful implementation of mitigating actions. Since hybrid threats span multiple domains, information sharing between critical entities is crucial for detection. A critical entity cannot see a single attack as a hybrid attack, and only a combination of attacks with the overarching intent of influencing societal operational and decision-making capacities can be defined as hybrid attack. Only sharing of information will enable creation of the necessary awareness of where, when, and how to protect critical entities and their essential services, enabling identification, protection, and mitigation of risks.

An efficient information-sharing solution would also enable rapid analysis using various AI methods, allowing for near-real-time detection of hybrid threats, and facilitating early mitigation actions.

However, sharing information in relation to hybrid threats between different critical entities—whether they provide the same, similar, or different essential services—is often restricted due to security and business reasons. This limitation significantly hinders early detection and the initiation of counteractions. Currently, the CER directive only requires, under sanctions, that “critical entities of particular European significance”

[3] https://eur-lex.europa.eu/eli/dir/2022/2557/oj
[4] https://www.eeas.europa.eu/eeas/strategic-compass-security-and-defence-1_en
[5] #WHAT IF DGAP MEMO No 41: What If the EU Did Not Share Data to Protect Its Critical Infrastructure?

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

share information on severe incidents. Furthermore, current risk management approaches are typically domain- and country-specific, preventing coherent risk awareness across different domains and countries.

To alleviate the barriers posed by mandatory as well as business related information sharing restrictions, we recommend two primary actions. First, identify and define the essential information that must be shared, ensuring that only necessary and sufficient data is exchanged to maintain efficiency and security. Second, explore the implementation of privacy-preserving techniques to facilitate the secure sharing and analysis of sensitive information.

The essential information that must be shared to detect hybrid threats is termed Indicators of Hybrid Threats (IoHT). **The first step in developing a sharing solution is then to determine what constitutes an IoHT**. One way to do this is by applying a hierarchical attack tree approach: first, cover a single critical entity; then, include attack vectors from and to other critical entities; and finally, incorporate more generic threat vectors from open-source intelligence.

In parallel, investigations using adapted versions of the MITRE ATT&CK[6] and Cyber Kill Chain[7] frameworks should be conducted. These actions aim to identify prototypes of hybrid threats, which can be used to determine the necessary information, the required IoHT, for their detection and potential generalizations of the attacks.

The second action to increase the willingness and possibilities to share IoHT is to use privacy-enhancing technologies for data sharing and analysis. Today, there are a few different techniques proposed for use in other applications, such as sharing private and sensitive personal health-related data. Examples of techniques used are homomorphic encryption[8], secure multi-party computation[9], and hybrid approaches that combine advanced cryptography with the framework of differential privacy to limit information leakage. They all have different advantages and drawbacks when it comes to performing computations and their influence on the reliability of the computational results. Thus, the selection of the technique(s) used should be based on the requirements of the analysis procedures and the required reliability of the results.

Policy implications

This policy brief, based on WINS, advocates for a collaborative effort **to facilitate the sharing of essential IoHT information necessary to identify, assess, and analyse hybrid threats against critical entities and their essential services.** The first step in adopting this proposal should be entrusted to the research community for **determining and validating the specific methods for sharing IoHT information to be used and the results that can be achieved.** The subsequent steps would **involve developing an efficient sharing platform and introducing it across EU Member States and critical entities.**

---

[6] MITRE ATT&CK is a globally accessible knowledge base of adversary tactics and techniques based on real-world observations. MITRE ATT&CK®.

[7] The *Cyber Kill Chain* framework is part of the *Intelligence Driven Defense* model for identification and prevention of cyber intrusions activity. This model identifies what the adversaries must complete in order to achieve their objective. Cyber Kill Chain® | Lockheed Martin.

[8] *Homomorphic encryption* is a method to make your data confidential or secret and once encrypted, the data can be worked with. Homomorphic Encryption: How It Works | Splunk.

[9] Secure multi-party computation (SMPC) is a cryptographic method that enables multiple parties to compute a function using private inputs and view a public output without revealing their inputs to the other parties. Secure Multi-Party Computation - Chainlink.

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

The primary impact of this proposal's implementation would be the enhanced capability for cross-domain and cross-border event and anomaly information (IoHT) exchange. This would bolster resilience against external threats, identify systemic risks, and increase detection of hybrid threats across various domains. It would also foster comprehensive awareness that supports decision-making at domain-specific, national, and EU levels, in alignment with the NIS-2[10] and CER Directive requirements.

Recommendations

The gap in information sharing between critical entities makes the proposed solution crucial for their protection in the coming years. Digital surveillance in a cross-sectoral, critical entities environment necessitates information sharing and analysis to enhance societal resilience. At the EU level, measures for protected information sharing and situational analysis provide national entities with better awareness of the current state of hybrid threats. We strongly support research and development actions in this field and recommend that:

- The European Commission **extends the CER Directive to include the near-real-time cross-domain sharing of IoHT.**
- The European research community is asked to:
    - **Propose sets of sufficient and needed IoHT** and **validate that sharing this information would allow for the detection of hybrid threats** with required performance measures.
    - **Propose an architecture and tools for near-real-time analysis** of the shared IoHT to detect hybrid threats, propose mitigating actions, and predict possible next step attacks.
    - **Propose efficient privacy-enhancing technology for data sharing and analysis of the IoHT.**

- **The European Commission procures the implementation of a first live test and demonstration solution.**

Research parameters

EU-HYBNET is a five-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 to counter hybrid threats on a European level. EU-HYBNET conducts research and highlights innovations and solutions that aim to close the identified gaps and fulfil practitioners' needs. The considered innovations and solutions, both technological and social, are assessed by practitioners, researchers, and in gamified training events. For innovations and solutions that are assessed to be promising, roadmaps for successful uptake, industrialisation, and standardisation are developed.

To achieve its goal, the project is organised in four Core Themes: 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 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 European Commission's (EC) "The landscape of Hybrid Threats: A Conceptual Model"[11]. In this context, practitioners were invited to express their needs in countering hybrid threats, which were later analysed and prioritised.

[10] NIS 2 Directive (Directive (EU) 2022/2555)
[11] JRC Publications Repository - The landscape of Hybrid Threats: A Conceptual Model (Public Version) (europa.eu)

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

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.

Project identity

Project name: Empowering a Pan-European Network to Counter Hybrid Threats (EU-HYBNET)
Coordinator: Laurea University of Applied Sciences, Finland
Editors of this Policy Brief: Päivi Mattila/Laurea and 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 Isto Mattila isto.mattila@laurea.fi

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