EU-HYBNET 2nd Innovation and Standardisation Workshop (ISW)

8th November 2023, Valencia, Spain

Summary Report

Table of contents

Report developed by PPHS and Laurea University (EU-HYBNET Consortium Members)

Confidentiality status: Public available

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

1. General overview & Plenary Session

On the 8th of November 2023, the EU-HYBNET consortium successfully held its **2nd Innovation and Standardisation Workshop** in Valencia, Spain (at Valencia Local Police HQ). The workshop was attended by approximately 54 representatives of the EU-HYBNET consortium and network, as well as other stakeholders from industry, practitioner and policymaking organisations.

Building on the themes defined during the first iteration of this workshop, this edition allowed participants to discuss standardisation recommendations and case studies for countering hybrid threats in two thematic areas:

1. Foreign Information Manipulation and Interference (FIMI)
2. Protection of Critical Infrastructure.

Following a **Plenary session** featuring insightful keynote speeches on both topics, participants engaged in parallel breakout sessions, fostering interactive discussions, audience interventions, and the exchange of innovative ideas.

During morning Plenary session, **Kimini Delfos from the Dutch Ministry of Infrastructure and Water Management** presented the Dutch approach to security and critical infrastructure resilience. The Dutch methodology employs ***the polder model***, emphasising a whole-of-governance approach to counter hybrid threats and work towards resilience. Ms Delfos discussed the Dutch Security Strategy with the Ministry of Justice and Security coordinating national security and crisis management including government wide resilience measures. In the second part of the presentation, participants could hear about protection of North Sea infrastructure which is the responsibility of Ministry of Infrastructure and Water Management – it coordinates a **government**

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

wide strategic approach to protect the North Sea infrastructure. The main goal, discussed in detail by Kimini Delfos, is to protect the North Sea Infrastructure against state and non-state threats, in order to ensure the availability, continuity, confidentiality and integrity of the North Sea infrastructure, for the purpose of national safety.

Daniel Fritz, from the European External Action Service (EEAS) shared insights into the importance of standards and recommendations for innovation for sustainable, networked defence against Foreign Information Manipulation and Interference. He emphasized how important it is that innovations are adopted by as many stakeholders as possible and how important **networks (collaborations)** are in this process (such as EU-HYBNET). The larger the network, the cheaper the product. Mr Fritz emphasized that **innovations are essential** as we need to remember to be a step ahead and react before disinformation happens. Another topics which were brought into attention to the event participants were the important notion of market place of exchanging ideas as it makes knowledge transfer more effective. We should also remember about continuous work on **common standards and protocols**. Mr Fritz concluded his presentation by assuring that when it comes to networked defence against FIMI, every contribution is important and everyone has a role to play around a big table.

During the last speech of the plenary session, **Daniel Milo from Ministry of Interior of the Slovak Republic (Centre for Countering Hybrid Threats)** presented government approach to increasing Slovakia's resilience to hybrid threats **based on lessons learned** from Russia's invasion of Ukraine.

At the beginning of his presentation, Mr Milo showed a series of polls to show how Slovaks perceive such topics as: Russian invasion on Ukraine, NATO, USA vs. Russia, UE support for Ukraine. It was important to see this data in the light of the knowledge on how strongly Russian influence and disinformation is still present in Slovakia. In the second part of the presentation, participants could hear how Centre for Countering Hybrid Threats of Slovak Republic is working on increasing

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

Slovakia's resilience to hybrid threats. Some of the main achievements presented were: establishing inter-ministerial information exchange mechanism, coordinated Strategic communication and public awareness campaigns (including e-learning dedicated for public administration). Even though a lot has been done, there is still a lot to be done **in the short-term** and **long-term perspective**. As Daniel Milo emphasized, this is a continuous process and we need hybrid responses to hybrid threats.

2. Foreign Information Manipulation and Interference Session

Key takeaways for Foreign Information Manipulation and Interference Countering

Session dedicated to Foreign Information Manipulation and Interference (FIMI) enabled the gathered practitioners to have a lively discussion **on best practices**, **necessary standardisation** and **recommendations** that can efficiently deal with hybrid campaigns such as manipulation and interference by hostile actors. **Key finding from the discussions**:

- We must be step ahead of disinformation campaigns (inoculation)
- Countering FIMI and increasing resilience to hybrid threats is a continuous process
- Proactive defence rather than reactive policy
- Government and society level must connect (multisectoral cooperation)
- Common standards, protocols including standardised strategic communication approach, and constant work on innovations

Julien Théron from Join Research Centre (JRC) explained the **FIMI axiomatic approach** for better understanding of this threat, threshold of reaction, interdiction and deterrence. He stressed the three axioms: threshold of reaction, interdiction and deterrence. He referred to current worrying global trends of FIMI and concluded that they are nothing more than attacks on the foundation of democracy aimed at destabilising their various key elements such as civil rights and liberties or feeling of justice and equal treatment. He highlighted that hybrid campaigns are multi-domain, destabilising at multiple levels and the phenomenon is still increasing and while practitioners are now more aware of the risk, they **still need to identify effective and efficient ways** to deal with them.

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

Paula Rejkiewicz from Ministry of Foreign Affairs Republic of Poland (Strategic Communication and Countering Disinformation Unit) presented a pratical case study focused on antagonising Poles and Ukrainians through disinformation – main challenges and responses used to mitigate them. At the beginning Ms Rejkiewicz presented the most prominent false narratives circulating together with: TTPs used with them, their goals, target audiences and who stands behind those narratives. Thanks to the detailed presentation, ISW FIMI breakout group could find out how MFA StratCom conducted an analysis about **the potentially best way to respond** to the narratives, how the response is being formulated, in which countries those disinformation campaigns are debunked and what stratcom protocoles are initiated for such scenarios.

Esther Jacobs from TILT Insights presented a case study of online coordinated inauthentic campaigns from 'pro-Iranian' and 'pro-Palestinian' accounts on Twitter / X. Ms Jacobs showed how 172.242 inauthentic tweets have been used in 3 coordinated hashtags worldwide to spread pro-Palestina and anti-Semitic content and how these networks amplify anti-European content as well. The audience got familiar with TILT Insights, and how they proceed to: **analyze open social media platforms** (e.g. Twitter, Redit, Youtube, Open Telegram), **combine social science with tech science** and AI and how TILT Insights developed their own research platform METIS (we could see the demonstration of it). It was very interesting to hear how Tilt does multidisciplinary research and goes beyond simple tools such as BOT detection combining multiple features such as their AI similarity-model and hate-speech detection. Thanks to it they are able to detect coordinated campaigns on social media platforms, analyze the contribution and impact of coordinated accounts within a debate, provide early warnings on online manipulation or interference during important events, analyze the shared sources or URLs distributed by coordinated or inauthentic accounts and detect the most hateful or threatful messages spread by coordinated accounts.

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

David Arroyo from Spanish National Research Council (CSIC) talked about the core of a system he and his team designed for the early detection of FIMI by combining classical CTI (Cyber Intelligence) feeds and evidence gathered from ongoing advanced manipulation campaigns conducted through the clear and deep web. Mr Arroyo highlighted the increasing connection between APTs and APMs. This connection is determining a high complex scenario very challenging in terms of the characterization of the underlying hybrid threats. He went on to analyze this challenge in terms of the creation of European ISACs (Information Sharing and Analysis Centers) and **discussed how tools as MISP, openCTI (among others) could be applied to leverage STIX and DISARM** for the adequate annotation and exchange of FIMI events. This analysis involved three major aspects: strategic, tactical and operational.

3. Critical Infrastructure Session

Key takeaways for Critical Infrastructure Protection

During CI Working Group - **best practices** and view on existing or future **relevant standards** to critical infrastructure (CI) protection and **innovation development** to support pan-European security practitioners and other relevant actors to counter hybrid threats in the infrastructure domain were presented. The focus was on present, relevant directives, namely CER- and NIS-2 Directives demands to critical entities to ensure their preparedness, response and mitigation to risks and attacks, including hybrid threats, and how the directives may support the CI entities in their work. It was also under discussion if the CER- and NIS-2 Directives will lead and follow some standards and/or are there already some best practices to build on. Two case-studies, one from Poland and one from Italy, well highlighted importance of learning from real cases of hybrid attacks and to share views on current standards, needs and future possibilities for standardisation in the field of CI protection in light of the challenges deriving form hybrid threats.

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

Georgios Kolliarakis, from the German Council on Foreign Relations, noted that there is currently a multitude of regulatory instruments across jurisdictions focusing on critical infrastructure protection, but there appears to be a common understanding and a level of convergence. He emphasised that a **mix of instruments is necessary** as today's interconnected society is vulnerable to new types of threats. **Recommendation** was that regulations and directives are seen important because they demand and hence tricker change among CI entities to focus on security concerns and to update their measures to fast changing world and technology development. Without regulations and directives, not all critical entities may be aware of or keen to conduct changes in their operations that are central for securing themselves and in various of cases also other CI entities nationally and cross-border. The importance of CER and NIS-2 directives were highlighted and underlined that indeed directives and regulations are a necessity because they are "the start from necessary actions in paper to practice".

Karolina Wojtasik, from the Government Centre for Security (RCB) in Poland, explained the Polish approach for identifying critical infrastructure (CI) entities, pointing out that the criteria and results of this process are restricted – citizens are not aware of which infrastructures are considered critical. In addition, she pointed out that the amount of CI entities is in constant change due to new companies coming to market and existing facing changes. Therefore, sharing recommendations and information to CI entities e.g. on new directives, regulations and actions needed to secure their operations is, and needs to be, constantly on-going. Still, it is first and foremost CI operators responsibility to ensure their protection to attacks also related to hybrid threats. **Recommendation** is to increase knowledge of hybrid threats and malicious means related to them in infrastructure domain among CI entities, so that awareness of various forms used in hybrid threats to CI entities will increase alike preparedness to prevent the attacks. A Case study on hybrid threat attack against critical infrastructure operators, railway and airport traffic was given to learn on elements that CI operators may

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

face. Awareness of espionage, use of refugees for malicious actions and real violations to CI operators premises were central in the case. The case also underlined connection of the attack to Poland's political situation, international policy making with NATO and Poland's strong support to Ukraine in the war against Russia. Lesson learned and best practise was to keep CI entities aware how their security concerns and preparedness to attacks is not excluded from national or international political situation and hybrid threats.

Paola Tessari, from the Istituto Affari Internazionali, discussed hybrid threats against critical infrastructures with a focus on Italy's maritime interests, highlighting the importance of safeguarding critical assets, such as gas pipelines and sub-sea capable connections against malicious actions being part of hybrid threats. The importance of CER and NIS-2 directive was highlighted in the series of European measures during many decades to increase security of CI entities to novel threats and attacks alike nowadays hybrid threats. To counter the challenges **best practices** were shared from Italy on CI entities preparedness, mitigation and response to hybrid threats.

First of all, It was highlighted that Memorandum of Understanding signed in 2022 by the Italian Navy and Sparkle (the Italian company controlled by the TIM Group dealing with underwater cables) was done in order to improve the protection of subsea telecommunications infrastructure. This is a good example of civil-military cooperation in protecting vital CI entities operations. The agreement formalizes the desire to cooperate in a sector considered strategic for the socio-economic development of Italy with the creation of shared operating procedures and the possibility of carrying out joint activities for the recognition and monitoring of the submarine cables owned by Sparkle and the areas neighboring. Cartographic support from the Navy for the seabed of interest is also envisaged as well as assistance in emergency operational situations. The agreement will also allow the development of study and research activities deemed to be of common interest between the parties for the pursuit of their respective institutional tasks.

Secondly, in Italy the National Underwater Hub (Polo nazionale della dimensione subacquea – PNS) in La Spezia works as an active catalyst for technological research and development in respect of the underwater domain and hence support means to cover risk and challenges in the domain. In this way, it is intended to be a forum in which universities, research centres, start-up firms, SMEs, big companies, navy and the rest of the institutional stakeholders shall cooperate with respect to creating positive conditions for innovation, creation of expertise and development of technologies. In addition, EISAC Italian node of the European Infrastructure Simulation and Analysis Centre (EISAC)

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

between INGV (National Institute of Geophysics and Volcanology) and ENEA (New Technologies, Energy and Sustainable Economic Development) has established a Decision Support System (DSS) and interoperable platform for the operational 24/7 monitoring of CI and for the prediction of physical and functional impacts by natural and man-made events. This is a solid support for CI entities to have full scale awareness of emerging attacks and risks.

Furthermore, **some lessons learned** are that the assets in Italy are mostly owned and/or operated by private and civilian actors, but they are key for national security. Public-private partnership is needed to improve and ensure their resilience and protection. In the context of partnerships at the regional and international levels; renewed bilateral, north-south and NATO–EU cooperation will be all crucial in this regard. In addition, it was emphasized that thorough implementation of CER- and NIS-2 Directive against hybrid actions is needed - hybrid actions are not new, but the network of CIs that can be target are widely spread and that calls for an enhanced resilience and redundancy. Enhanced capabilities for early warning/threats identification and rapid reactions involving private actors, law enforcement agencies, MoDs and other relevant institutions ae much needed. Furthermore, interoperability and closer and timely dialogue among users and developers of technologies (dual use technologies) is seen central and synergies between civil, defence and space industries are called for.

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

The EU-HYBNET consortium received positive feedback on the organisation of the ISW and suggestions on how future workshops could be improved. Participants appreciated the selection of speakers and the topics of the parallel sessions. For further information on EU-HYBNET events, you can follow the project through X/Twitter and LinkedIn. If you are interested in participating in discussions on hybrid threats we encourage you to visit our website and explore the benefits of EU-HYBNET network.

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