EU-HYBNET: EMPOWERING A PAN-EUROPEAN NETWORK TO COUNTER HYBRID THREATS

Stručni rad
DOI: https://doi.org/10.37458/nstf.23.1.6

José L. Diego, Iván L. Martínez*

Chapter 1: Joining efforts to counter Hybrid threats

EU-HYBNET is a Pan-European network of security practitioners, stakeholders, academics, industry players, and SME actors across EU collaborating with each other in ever increasing numbers to counter hybrid threats. EUHYBNET aims to build an empowered, sustainable network beyond the scope of the project through its on-going association with a key partner, The European Centre of Excellence for Countering Hybrid Threats, and it will: define common requirements that can fill knowledge gaps, deal with performance needs, and enhance capabilities of innovation endeavours; monitor significant developments in research and innovation; deliver recommendations for uptake and industrialisation of the most promising innovations that address the needs of practitioners, and determine associated priorities for

* José L. Diego and Iván L. Martínez are members of Valencia (Spain) Local Police

standardisation; establish conditions for enhanced interaction among its members; and persistently strive to increase its membership and continually build network capacity through knowledge exchange incl. exercises. EU-HYBNET's principal objectives align with the H2020 SEC-SU-GM01-2019 call and are of crucial relevance to it. A technology and innovations watch, facilitated by scientific research, will ensure smooth execution of searching, monitoring, identifying and assessing innovations both under development or already proven, including the level of technology readiness for uptake or industrialisation. EU-HYBNET will bring together practitioners and stakeholders to identify and define their most urgent requirements for countering hybrid threats by undertaking an in-depth analysis of gaps and needs and prioritising those that are crucial to address through effective research and innovation initiatives, including arranging training and exercise events to test the most promising innovations (technical and social) which will lead to creation of a roadmap for success and solid recommendations for uptake, industrialisation and standarisation across the European Union.

"Hybrid threats aim to exploit a country's vulnerabilities and often seek to undermine fundamental democratic values and liberties." To be sure, hybrid threats can be characterised as a coordinated and synchronised action that deliberately targets democratic vulnerabilities of states and institutions through a wide range of means. The aim is to influence different forms of decision making at institutional, local, regional and state levels to favour and/or achieve strategic goals while undermining and/or hurting the target. To effectively respond to hybrid threats, improvements in information exchange, along with breakthroughs in relevant research, and promotion of intelligence-sharing across sectors, and between the EU and its MS and partners, are crucial. Presently, the EU counter-hybrid toolbox is impressive, and a significant number of legislative proposals have been adopted to underpin efforts at national and EU levels, as seen below.

Figure 1(JRC): EU current activities and policies.

In support of attempts to deal with hybrid threats a new unit was established in 2017 within the EU Intelligence and Situation Centre (EU INTCEN), the EU Hybrid Fusion Cell (HFC). It continues to raise situational awareness, and provides strategic analysis to EU decision-makers by operating closely with MS networks and intelligence personnel. Moreover, a Council working group for countering hybrid threats, also established in 2017, was charged with assessing the capability gaps of Member States and developing indicators for hybrid activity.

More significantly, however, Finland's Presidency of the Council of the European Union, on 11 July 2019, made the following announcement, regarding the establishment of a "Horizontal Working Party on Enhancing Resilience and Countering Hybrid Threats," which by implication positions the Finnish led EU-HYBNET project and its network partners, especially The European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE, HCOE), also headquartered in Finland, in the forefront of consequential hybrid threat initiatives. The following excerpt from the announcement highlights the significance of this:

> "... The mission of the working party is to improve the resilience of the EU and its member states against hybrid threats and to support action to strengthen the crisis resilience of societies. The working party will also facilitate coordination within the Council and foster cooperation with the other EU institutions, services and agencies.
>
> The EU member states and institutions continue to face multidimensional hybrid threats which are difficult to detect and define. This is why Finland's Presidency aims to improve the capacity of the EU and its member states to identify hybrid threats and step up cooperation to counter them, with the aim of increasing the safety and security of EU citizens in a comprehensive manner. The member states have intensified their cooperation considerably over the past few years because of the cross-border nature of hybrid threats."

What is more, within the European Commission, an Inter-Service Coordination Group (ISG) functions as a vehicle for countering hybrid threats. The main goal of this group is to coordinate activities between different DGs, including not only preparations of the Parallel and Coordinated Exercise (PACE) initiative to test different EU response mechanisms and their ability to interact efficiently with each other, but also to determine how the EU's response to hybrid threats interacted with the North Atlantic Treaty Organisation's action. Significantly, in 2017.

PACE provided an arena for a detailed testing of the EU's response capacities to a large-scale hybrid crisis. Unprecedented in terms of scope, it put to test not only the "EU Hybrid Playbook," i.e. the different EU response mechanisms and their ability to interact efficiently with each other, but also how the EU's response to hybrid threats interacted with NATO's response in 2017. If the application of such tests continue in the future, EU-HYBNET will support the execution of such exercises to exploit the capabilities of Member States to reinforce their hybrid crisis response capacities, and the project's outputs in general will align themselves with such initiatives.

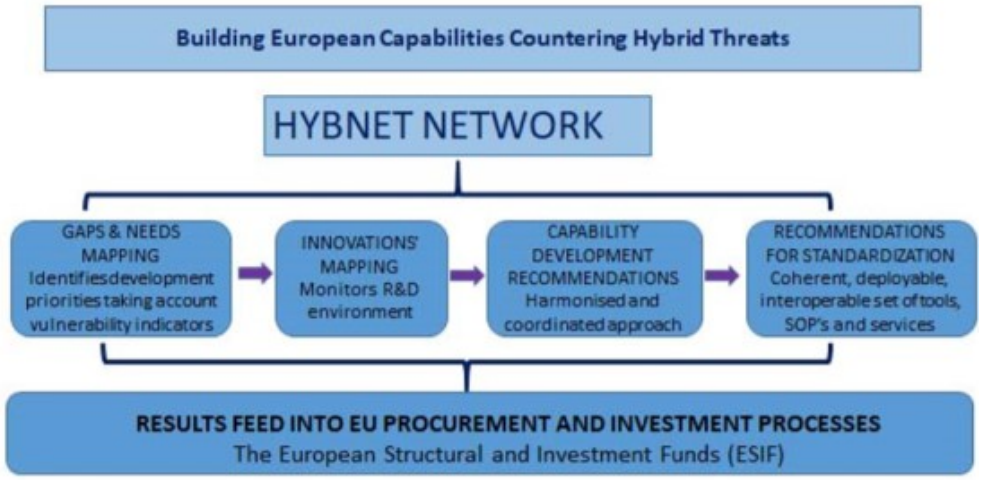
The European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE, HCOE) was established in April of 2017, and its cross-governmental, cross-sectoral networks consist of an extensive array of practitioners and experts working in hybrid threat related areas with MS, and with NATO. Since 2016, NATO and EU have identified countering hybrid threats as a priority for cooperation and Hybrid CoE plays a unique role in facilitating this. Hybrid CoE is also the main international hub for practitioners and experts building capabilities of MSs to counter hybrid threats, sharing best practices, testing new ideas, and providing training and exercises for MS and NATO allies.

Significantly, Hybrid CoE and the Joint Research Centre (JRC) are leading partners of our EU-HYBNET project proposal. They have developed a conceptual model to characterise hybrid threats. This conceptual model integrates all relevant parameters, such as actors, tools, domains and timeline, with a view to furnishing an extensive landscape of hybrid threats and thereby helping experts to adequately assess crisis incidents and to design counter-measures. This model will be the basis for understanding hybrid threats in the contemporary security environment. Indeed, it is the conceptual cornerstone of the EU-HYBNET project, which demonstrates a strong commitment to operate in accordance and in support of the EC JOIN (2016) and SWD (2019) communications.2 In this context, the EUHYBNET project will 1) monitor strategic research and innovation (technical and social); 2) express common requirements as regards innovations that could fill capability and other gaps, and improve future performance of European practitioners; 3) designate priorities in relation to areas requiring more standardisation; and 4) empower a Pan-European network to counter hybrid threats. All of this will positively influence public procurement processes involving projects funded by the European Structural and Investment Funds (ESIF).

In this manner, the project will enhance EU's resilience to hybrid threats by creating a state-of-the-art network (EUHYBNET/ Pan-European Network to Counter Hybrid Threats) that will ensure synergies with other European,

subnational and national networks, and especially with security practitioners, academia, and industry. This will allow existing resources to connect gaps and dots coherently in the innovation solutions and research landscape and therefore to increase EU awareness and capabilities established to detect hybrid threats. Accordingly, Hybrid CoE will continue to coordinate its network operations after the conclusion of the EU-BYBNET project; and hence, we anticipate that this proposal will have a strong and lasting impact over the long term.

Figure 2: HYBNET network



Furthermore, the EU-HYBNET proposal aims to empower its network to fight against hybrid threats by proliferating knowledge and facilitating cooperation between industry, practitioners and academia, and by providing advanced solutions for network collaboration and delivering recommendations for training, standardization and industrialization of cutting-edge innovations.

EU-HYBNET will address four core themes to ensure coherence in the project's results: 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 themes will afford 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.

EU-HYBNET will also encompass future innovations and solutions in the domain of technical and social research, and deliver results on e.g. cognitive/informational aspects (message exposure, understanding, and retention), attitude manipulation (attitude creation, modification, and reinforcement), and behavioural effects (creation, change, and reinforcement) of overt and covert disinformation and propaganda campaigns. This will ensure that the conceptual framework model against hybrid threats is brought forward and implemented in an efficient and sustained manner and that the EU-HYBNET proposal will therefore fully support the existing EU policy framework, especially JOIN(2016) and SWD(2019), as mentioned previously.

Although there are numerous networks in Europe that are currently dealing with different aspects of hybrid threats, these networks do not integrate practitioners, academics and industry in the form of an eco-system, as EU-HYBNET aims to do; nor do these explicitly focus on employing outcomes of research and innovation, as a means for countering hybrid threats, as EU-HYBNET clearly intends to do in a coherent manner; and the existing networks do not sufficiently pay attention to the changing nature of hybrid threats over time, but EU-HYBNET will by focusing strongly on its first core theme: Future Trends of Hybrid Threats. Further, these networks do not integrate industry into the process of discovering solutions. But EU-HYBNET will embrace cooperation with the private sector concentrating on threats to critical infrastructure and supply chains, and will seek solutions from best practices that have been established in bilateral interactions between the potential target and solution provider.

Finally, these existing networks do not sufficiently embrace EU's focus on the political level, especially the process of supporting policy dialogues that could enhance overall resilience of a country or EU more generally. Significantly, EU-HYBNET will build a network eco-

system starting from the grass roots level and include the practical experience of practitioners in the field of security and civil protection at local levels across the EU by paying strict attention to signals below the threshold of crisis, and focusing on day-to-day events, thereby further shaping a Secure Union that protects freedoms and privacy of EU citizens.

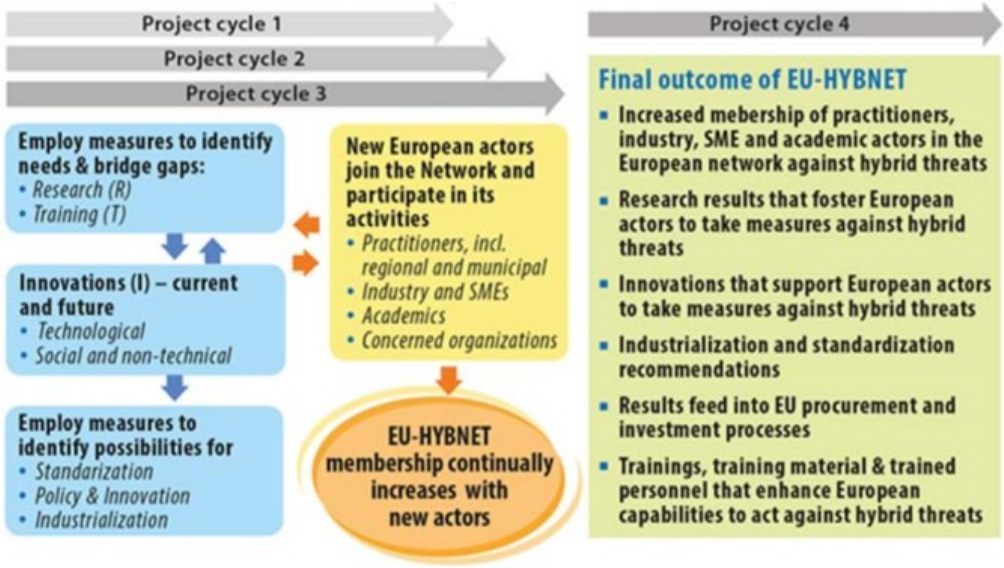
Chapter 2: Concept

To achieve the objectives of the project, we will apply an iterative approach, consisting of three full scale project cycles in three core activity areas: i) research (incl. training), ii) innovation monitoring, and iii) recommendations for standardisation and innovation uptake (including industrialisation). Additionally, in a concluding fourth cycle, the project will collect results from each of the previous three cycles, draw conclusions, and make suitable recommendations. The figure below depicts the structure of the principal activities of EU-HYBNET. Each cycle will employ measures of high quality that will allow for agile responses to the proliferation of hybrid threats by continually increasing the network's membership with professionals that will be trained to deal with hybrid threats and have the potential to enhance European capabilities along the same lines.

Project cycle approach for needs and gaps – Each of the three project cycles will begin with an event organised for all European actors associated with the project with the aim of determining the most important gaps and timely needs in the fight against hybrid threats. During the event topical challenges facing the project will be dealt with and appropriate measures identified that can bridge existing gaps and provide answers to the most essential needs. This approach will be undertaken in an iterative manner to ensure that the project will be able to deliver the most critical solutions for countering hybrid threats over a five-year period. Accordingly, a last mini-cycle will also take into account the outcomes arising from each of the previous cycles for recommendations regarding future research, innovation and training. Finally, the project recognises that a manual of "the European Hybrid threats vulnerability indicators" will provide a solid

basis for selecting the most important gaps and needs to focus on in each of the project cycles in relation to research and innovation monitoring as well as innovation uptake recommendation (incl. standardisation) activities.

Figure 3: EU- HYBNET process and content



A coherent approach focusing on the domains of hybrid threats – It is important to note that hybrid threats can arise in any of 13 different domains, according to the HCoE/JRC model. This means also a new approach to find countering solutions. EU-HYBNET will address four core themes to ensure coherence in the project's results: i) Future Trends of Hybrid Threats, ii) Cyber and Future Technologies, iii) Resilient Civilians, Local Level and National Administration, iv) Information and Strategic Communication. These four core themes will create an opportunity to focus on all hybrid threat domains, including interfaces between the domains, and will ensure that the project delivers coherent results in relation to the model.

The four core themes of EU-HYBNET are identified in EC's latest 'Report on the implementation of the 2016 Joint Framework on countering hybrid threats (SWD

(2019) 200 final).' Regarding future trends and situational awareness, EU-HYBNET will not attempt to compete with security agencies, however, the crowdsourcing of information gathering will provide sectoral granularity and supplement centralized activities and strategic threat assessments. EU-HYBNET will bring these activities to the attention of Network members and build on respective national initiatives. Moreover, recent EU publications pay a lot of attention to analyzing the trends in cyber issues and strategic communications, which could be characterized as frontline fields of concern for any hybrid activity – indeed, various combinations of these two areas, are most often utilised by adversaries and it is therefore most pertinent to address these seriously in all aspects. The core theme related to resilient civilians, serves as a framework to assess whether EU level activities really do reach the grass roots level. Due to subsidiary considerations, EU policies will trickle down through a long chain of transformations on national, regional and local levels. Through our gaps and needs analysis, practitioners will be able to assess the effectiveness of policies, and whether the recent steps taken have actually addressed the most critical issues in a practical manner.

Research and innovation monitoring – The four core themes of the project together with the determination of gaps and needs in relation to the measures employed to counter hybrid threats in each of the project cycles will provide a solid foundation for European actors to carry out EU-HYBNET project activities. In addition to 1) research and innovation monitoring, these activities include: 2) defining new measures for countering hybrid threats (e.g. guidelines for cities as to how to detect hybrid influencing); 3) expressing common requirements as regards innovations that could enhance capabilities, bridge gaps and improve future performance; an 4) identifying priorities in areas requiring increased standardisation. The project will also arrange a set of events and workshops to precisely unveil and define innovations (technical and social, non-technical innovations) that can effectively address gaps and needs essentials, and that will ensure greater involvement from public procurement bodies upstream in the innovation cycle. The soundness

of the novel solutions will eventually be tested during planned project training events where results from activities associated with the four project core themes will provide European actors with new sets of skills and enriched knowledge in the fight against hybrid threats. The strong interplay between these activities will offer greater insights into how best to prioritise applicable innovations and skills necessary to answer European needs, position these in the foreground, and allow EU-HYBNET to make meaningful recommendations for uptake.

.

Chapter 3: Approach/ Methodology

The project's understanding and definition of hybrid threats is based on the European Commission characterization provided by the HCoE and the JRC. Because both of these organisations, HCoE and JRC, are partners in the EU-HYBNET consortium, this ensures that the characterization of hybrid threats will be adhered to throughout the project's duration and its activities aligned accordingly.

The EU-HYBNET project consists of three project cycles of 1,5 years duration, with a fourth cycle of one-half year. The cycle approach has been included as part of the methodology in order to assure that European actors' gaps and needs in countering hybrid threats are always current. This will ensure that the project is able to deliver up-to-date research and innovation based solutions and recommendations for their uptake and for standardisation in relation to ever evolving hybrid threats.

Today's world is experiencing many changes relating to renegotiation of the world order, technological revolution, the media landscape, the nature of war, conflict and peace, as well as generational changes that result in reinterpretations of history, and even challenges to democratic state systems. Hybrid threats are a product of this time and age. They occur in many domains and for this reason four project core themes have been selected to serve as focal points over the course of the whole project in order to ensure a coherent approach to achieve-

ment of project results and to enhance European capabilities in countering hybrid threats. The four project core themes, together with the cycle approach, represent the leading multidisciplinary methodological principles of the project – the themes are

1) Future Trends of Hybrid Threats,

2) Cyber and Future Technologies,

3) Resilient Civilians, Local Level and National Administration,

4) Information and Strategic Communication.

These themes link and interface with other hybrid threat domains identified and defined by the Commission/JRC and provide a sound window into supporting research and innovation activities in any of the hybrid threat domains considered by the project to be important and capable of delivering solutions during execution of the project cycles. In short, the project relies on a fixed but flexible approach in its focus on hybrid threat challenges and provides a comprehensive multidisciplinary methodological approach in delivering needed solutions and recommendations concerning innovations and their uptake, including standardisation. The domains and interfaces of hybrid threats in relation to the four project core themes are in line with the Commission's characterization of hybrid threat domains as depicted in the figure below (figure: conceptual model and main hybrid threat domains – as visualized by the European Commission, JRC and HCoE).

Each of the four project core themes have a vision that encompasses the variety of challenges that EU MSs may face when countering hybrid threats in targeted domains and interfaces with other domains. These visions are based on current European high-level research. In the EUHYBNET project the research activities related to the themes are led by a named consortium partner whose professional background complements the theme. These themes will incorporate European actors' (practitioners, industry, SME and academic actors, NGOs) concerns regarding gaps and needs can be re-

garded as starting points. The themes cover but are not limited to the following:

Figure 4: EU- HYBNET – challenges

Future Trends of Hybrid Threats: To analyse trends has become even more vital than before due to the changed security environment. Hybrid Threats are by character difficult to detect. However, without detection countering becomes difficult and responses might always be two steps behind. Hybrid threats also have an ever-changing nature. Approach seldom repeats itself and combination of tools is tailor made for the target. For this reason, analysis relating to different security related trends will be essential to be able to have foresight and build early warning systems. Hybrid threat trend analysis needs to be multidisciplinary and multidimensional using also scenario based thinking. The future trends of hybrid threats cover also the three other EU_HYBNET themes connecting them to wider security context. This will strengthen situational awareness and identify new and

emerging capability needs for countering hybrid threats. Principal lead: The European Centre of Excellence for Countering Hybrid Threats (HCoE):

Cyber and Future Technologies: At present, Cyber is treated as a domain of activity or knowledge where there are no rules. As regards hybrid threats specifically, Cyber and future technologies are key components through which new developments produce not only new kinds of hybrid threats, but also act as powerful countering measures in the fight against such threats. Todays' technological upheavals and those of the future suggest that the portfolio of tools used in the realm of hybrid threats will continue to expand rapidly. Computers are ubiquitous, and getting smaller, while processing power is increasing at enormous rates. Other fundamental breakthroughs include robotics, nano- and biotechnologies, artificial intelligence, sensor and 5G technologies. Taken together, these technologies connect symbiotically with people; and they structure society in all spheres – from the interpersonal to the social, and to the military. To be sure, communication technologies are driving these developments. There is still a great deal to learn about how an adversary can make use of these new tools and technologies, how cyber is connecting areas previously not connected to realm of security, like hospitals, and of how we can in fact use these same tools to detect and counter hybrid threats. Principal lead: Lithuanian Cybercrime Centre of Excellence for Training, Research & Education (L3CE).

Resilient Civilians, Local Level and National Administration: Civilians are central as targets and as actors seeking human and societal security. Too much focus has been placed on the state/government level when it comes to hybrid threats. There is still too little research on how this play out in hybrid threat security environment. Having a better understanding of where the potential vulnerabilities lie within possible target societies enables these same societies – and the diverse civilians within them - to develop measures that can build trust and solidarity within them, making them less vulnerable to such manipulations. This understanding will also help in resilience building that is important for all the EU

member states. Civilians are not passive recipients of information or governmental guidance, and trust levels between the governed and government need re-examination. In a democratic society, political decision-making and the opinions of residents are influenced. Various methods are also combined in order to reach the objective of influencing more effectively. This is a normal, deliberative political activity. Just as there is social or communicative influence that cannot be classified as a threat, there is also governmental influence, i.e. diplomacy. However, outside interference and influence may sometimes be a threat.

Classifying something as a threat constitutes normative classification: a threat is something unwanted, i.e. something that is deemed to be wrong or evil. Threats can often easily be classified in the legal sense: in many cases, they are a criminal activity. A considerable proportion of the political decisions that affect people's everyday lives are made by municipal boards and councils, and municipalities are in charge of social services, health care and education for example. Law enforcement agencies might be in the frontline when it comes to detecting and countering hybrid threats. Many cases in the recent history have shown us that the local level can play a crucial role both in countering and enabling hybrid threats; Catalonia and Eastern Ukraine as best examples. Principal lead: the Arctic University of Norway Tromså (UiT)

Information and Strategic Communication: Information, strategic communication and propaganda are among the areas that, together with cyber, have been linked to hybrid threats most often. The range of hostile and covert influence activities employed in the past include falsely attributed or non-attributed press materials, leaks, the development and control of media assets, overt propaganda, unattributed and black propaganda, forgeries, disinformation, the spread of false rumors, and clandestinely supported organisations, among others. These activities are recognised to be part of the hybrid playbook. Internet and social media channels have changed the game board for covert influence actions, providing a fertile context for the massive dissemination of overt and

covert propaganda by hostile States and non-governmental groups: anyone can produce and disseminate content; connections, funders and identities are blurred; information flows are huge; the speed of information dissemination is breathtaking. AI-generated audiovisual forgeries and the likely future improvements in deep fakes technology appear on the horizon as an insidious threat for democracies that will require developing analytic capabilities to detect and counter them.

All these require a sound understanding of communication processes and information flows, developing analytic capabilities and skills for assessing open sources and content, raising strong disinformation awareness, critical thinking, and media literacy, and building positive narratives instead of being on the defensive. While social media networks provide an unprecedented dimension for adversely impacting the potential exposure of target audiences, gathering empirical evidence on disinformation content is required for a full understanding of the effects of influencing campaigns, and thus developing effective strategies and tactics to counter influence. Principal lead: University of Rey Juan Carlos (URJC).

The four project core themes create windows for EU-HYBNET to focus on European actors' awareness, gaps in both understanding and countering and needs for capacity building to strengthen resilience and counter hybrid threats as well to deliver tailor made solutions. Each of the four project core themes identified starts with mapping event to see what is missing and what is needed. The whole process is facilitated by the use of innovative collaboration platforms.

Knowledge Exchange Events, Future Trends workshops, and Annual workshops where recommendations on the testing of existing and future innovations will specifically be asserted in the project training event. The innovation testing and resulting practitioners' views on the most promising innovations will give rise to further analysis and expression of common requirements as regards innovations that could fill capability and other gaps and improve future performance. This will be supported by analyzing the European procurement landscape and measures to be taken in the innovation uptake process.

Furthermore, EU-HYBNET will build a taxonomy for research and innovations monitoring in order to uncover and analyse existing and future research and innovation initiatives that answer to the defined gaps and needs. In addition the EU-HYBNET project will deliver a mapping matrix that includes various in-depth levels and various perspectives to identified gaps and needs addressing the four project core themes and their most important interfaces to other hybrid threat domains. The matrix will ensure that potential current and future solutions will be mapped from innovations and research findings to the gaps and needs.

Conclusion:

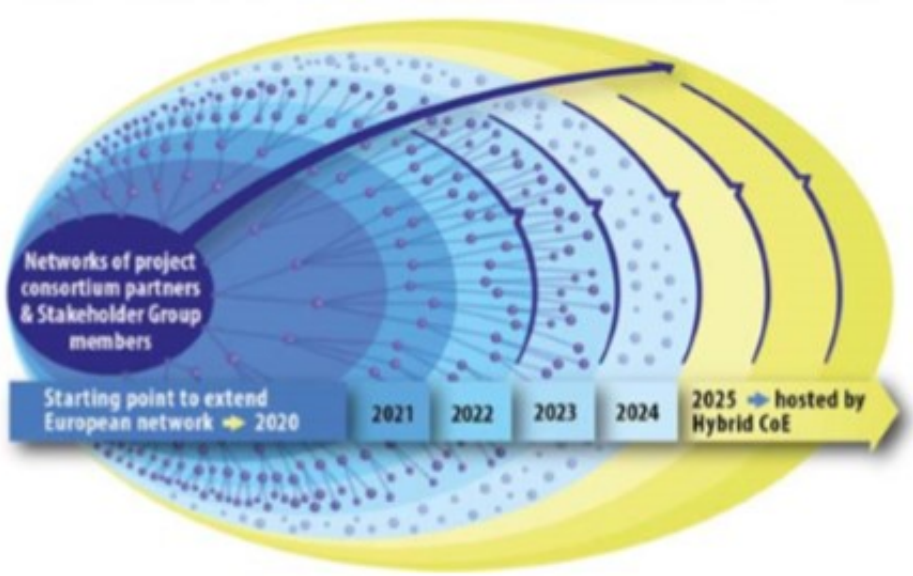
Conclusions of 6th Zagreb Security Forum clearly stated that strategic planning, foresight mechanisms and international cooperation at global level are key factors (and thus performance indicators) in the fight against hybrid threats.

In this sense, as a conclusion and linked to the above article, the extension of the network and its sustainable existence is grounded in the fact that after the project's completion HCoE will continue to host the Network and make use of its various platforms, which will ensure that network activities will be able to sustain a long lasting impact.

The extension of the European Network against hybrid threats and its sustainability (visualized below), and the project's gaps and needs related research activities in each of the four core themes, will be conducted jointly with the project consortium partners and new or potential members of the extended EU-HYBNET Network in order to share expertise in the named research field. This also represents a methodological measure of the project to expand the scope of activities and increase the number of participating actors, thereby empowering the European network in the fight against hybrid threats. All project activities will be planned and conducted in a manner that supports ways of finding and attracting new and potentially valuable European actors (practitioners, industry,

SMEs and academic actors, NGOs) to the European Network against hybrid threats. A principal feature of the methodology is to provide the means for empowering the network and for facilitating activities of project consortium partners and stakeholder board members in identifying potential new key actors. In addition, the project dissemination and communication measures will ensure that new actors may become aware of the network's activities and by their own initiative may request to become members. The project administration board will eventually select new members on a yearly basis which will allow for cooperation and information sharing with other network members in forthcoming years.

Figure 5: EU- HYBNET network extension from 2020



Literature:

1. *EU-HYBNET DoA: LAUREA-AMMATTIKORKEAKOULU OY (LAUREA) (2020).*
2. *Hybrid threats – Local perspective: Diego, José L. & Martínez, Iván L. (2020) – Valencia Local Police.*