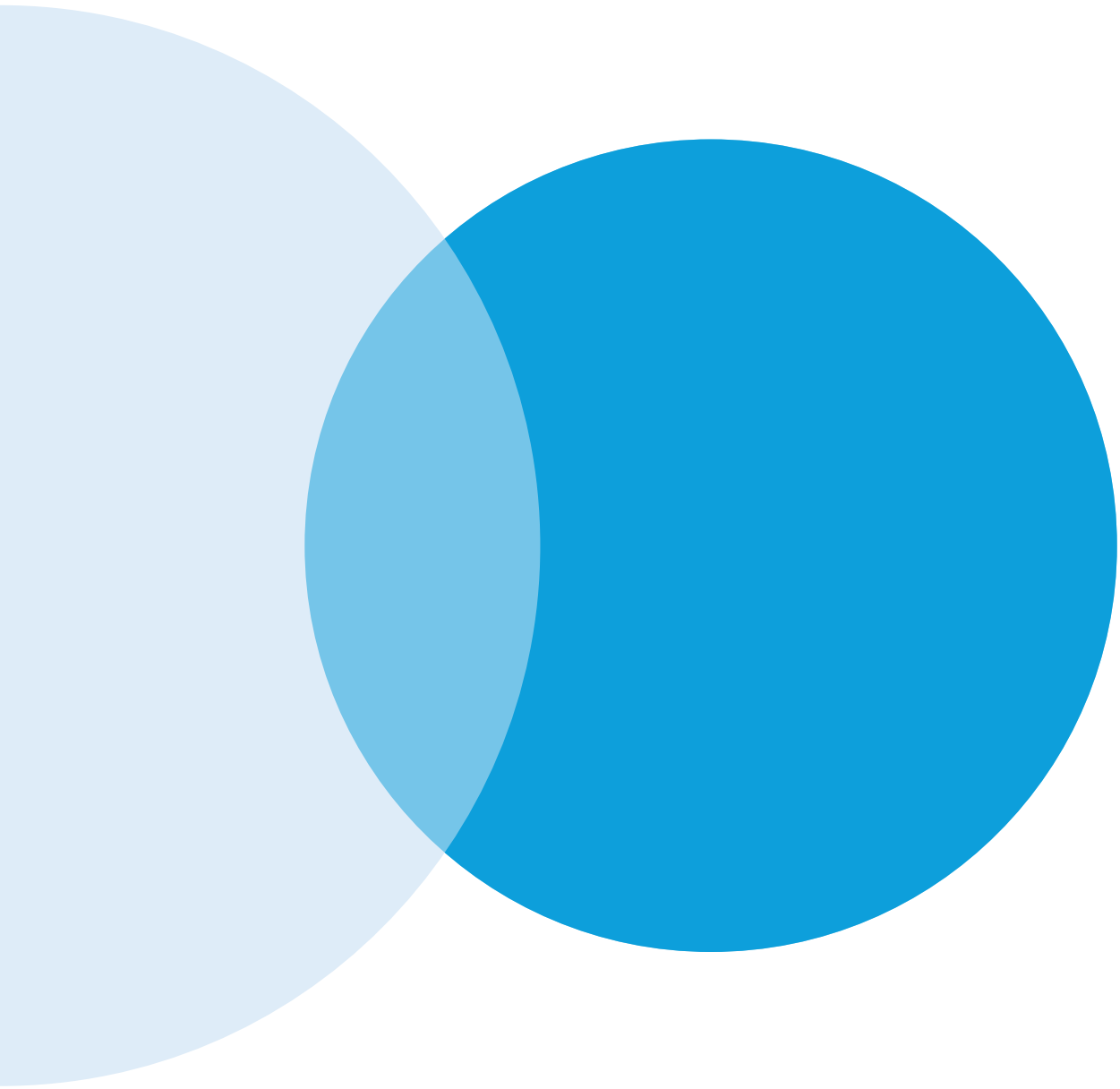
Hybrid CoE
key themes for 2024



Hybrid CoE

The European Centre of Excellence for Countering Hybrid Threats
tel. +358 400 253800 | www.hybridcoe.fi

Hybrid CoE's mission is to strengthen its Participating States' security by providing expertise and training for countering hybrid threats, and by enhancing EU-NATO cooperation in this respect. The Centre is an autonomous hub for practitioners and experts, located in Helsinki, Finland.

Hybrid CoE key themes for 2024

Introduction

The international situation remained very tense in 2023, with Russia's war against Ukraine causing instability and the risk of escalation in the Euro-Atlantic region. China continued to support Russia's official narrative on the origins of the war, which it also used in its own anti-Western information campaigns globally. Hybrid threat instruments were actively used to challenge the unity of the European Union and NATO, including their support for Ukraine.

Hybrid CoE finalized a number of large projects relevant from the point of view of the ongoing war. Among them was a major comparative report on the strategic cultures of Russia and China, as well as a report on hybrid threat trends in the Eastern Partnership region. Later in the summer, a wide-ranging report on economic security trends was published, identifying current and future security risks and vulnerabilities facing Western economies.

Given the urgency of the situation in Ukraine, and the common interests between Hybrid CoE and Ukraine in understanding the evolving nature of hybrid warfare, cooperation with Ukraine took the form of training, exercises, and information sharing. Hybrid CoE also closely studied Ukrainian practices in countering Russian disinformation.

Hybrid CoE broadened the selection of training and exercises provided for its Participating States. The basic Hybrid 101 course found its audiences among the Centre's stakeholders, together with election training and maritime hybrid threat scenario exercises, both of which were regularly offered to new groups.

Hybrid CoE's work plan for 2024 is firmly anchored in the work and fields of expertise developed during the previous year. New topics have been added based on demand, and changes in the hybrid threat landscape. The work plan first presents the key thematic fields for the Centre's work in analyzing, monitoring, and countering hybrid threats in 2024. It then outlines the Centre's main operational modes. The work plan concludes by outlining the detailed work plans for the Centre, its three Communities of Interest, and the Research & Analysis (R&A) and Training & Exercises (T&E) functions.

Hybrid CoE's key themes and approaches to countering hybrid threats in 2024

As defined in its constitutive document (Memorandum of Understanding), Hybrid CoE's key goal is "to serve as a hub of expertise supporting the Participants' individual and collective efforts to enhance their civil-military capabilities, resilience and preparedness to counter hybrid threats with a special focus on European security". The Centre fulfils this goal by providing a platform for its participants to come together, share best practices, build capability, test new ideas and practise defence against hybrid threats. As a hub of expertise, the Centre leads the discussion on countering hybrid threats through research and the sharing of best practices.

Hybrid CoE's assets are linked to its role as a network-based organization coordinating and supporting the expertise of its networks of practitioners, academics, and private sector

representatives. Enhancing both cross-governmental and public-private dialogue is an essential part of the Centre's work.

Thematically, the Centre's work plan for 2024 can be divided into three major fields of interest:

- Strengthening knowledge about **the particular characteristics of hybrid threats and their operational logic, and making proposals to counter them.**
- Strengthening knowledge about **hybrid threat actions as part of the strategies and policies of actors responsible for them, and generating ideas about how to cope with them.**
- Strengthening knowledge about the **key vulnerabilities of Western societies with respect to hybrid threats, and providing ideas about how to address them.**

In the following sections, the Centre's work plan will be presented by grouping the planned workstrands under these three main themes.

Strengthening knowledge about the particular characteristics of hybrid threats and their operational logic, and making proposals to counter them.

Hybrid threats differ from the traditional forms and instruments of power projection in international politics by virtue of their operational mode, instruments, and uses. They therefore have many specific characteristics, ranging from the use of various interfaces to the creation of confusion and ambiguity and the use of proxies, making it difficult to identify the actors responsible. All of these tactics are designed to prevent the target from responding effectively to the activity and protecting itself accordingly. As a consequence, hybrid threats usually occur in multiple domains simultaneously, and are designed to remain below the threshold of detection and attribution.

Hybrid CoE continues to work on studying the particularities of hybrid threat action both through conceptual work and by mapping the forms of ongoing hybrid threat activity.

One of the main efforts in this context takes place in the framework of the Deterring hybrid threats workstrand, which has been extended from its initial conceptual analysis phase to a module consisting of both training and exercise activities and various case studies in support of them. The goal is to increase understanding of how deterrence against hybrid threats can be built, what the various policy instruments are, and how the EU and NATO can best be involved in this activity. COI Hybrid Influence (HI) leads the project and will update its analysis on deterrence in 2024, providing new recommendations and a new exercise in support of its stakeholders' policies.

There are several workstrands planned for 2024 where the particularities of hybrid threat action will be analyzed by mapping their emergence within a specific geopolitical region or in a thematic context. The Research and Analysis (R&A) function will first focus on Russia's grand strategy in its war against Ukraine and how it influences the war efforts. The work on hybrid

threat potential in and towards the Arctic will be continued, aimed at investigating vulnerabilities, re-examining underlying assumptions, and seeking renewed situational awareness. Hybrid threats against Arctic infrastructures will be another focus area for this work. The Middle East and North Africa (MENA) region will be a third geopolitical focus area for R&A, with an earlier report on hybrid threat activities in the region set to be updated in 2024.

The Centre will also address hybrid threats in the Western Balkans with an exercise focusing on disinformation. The exercise will be provided for regional stakeholders and preceded by engagement with the Centre's expert pools, who will provide input, support and guidance for the exercise. This is a joint effort between the Centre's R&A and Training and Exercises (T&E) functions.

The Economic resilience workstrand (COI Vulnerabilities and Resilience, V&R) will continue focusing on potential means and effects of economic hybrid threats. To this end, it will continue studying the acquisition of strategic assets, shifting the focus to immaterial resources and knowledge security. These are essentially linked to Chinese forms of economic statecraft, which are also analyzed in R&A's workstrand on China's promotion of anti-Western narratives in Africa.

Another key effort to identify and map emerging hybrid threat activities takes the form of Hybrid CoE's internal open-source monitoring system, established in spring 2020 to monitor hybrid threat activities in the Covid-19 framework. Apart from enhancing situational awareness at the Centre, the system has produced bimonthly reports for the Centre's networks, focusing on actors and thematic fields of hybrid threat activity (Russia, China, the Arctic, disinformation, etc.). In 2024, the monitoring system will be expanded by distributing monthly reports to the Centre's networks and publishing an annual report mapping key trends of hybrid threat activities. The monitoring system is a Centre-wide project involving participants from all of the Centre's functions who monitor hybrid threat activity in their field of interest. It also serves as an important tool for the internal professional development of the Centre's staff.

Although there will not be a separate workstrand on instrumentalized migration (IM) in 2024, the topic will remain on Hybrid CoE's agenda. It will be addressed through various activities, including a publication on IM dealing with the EU's tools and policies in the field. The topic will also be covered by the Centre's internal open-source monitoring system, which distributes monthly reports on ongoing hybrid threat activities.

Hybrid warfare is one of the principal workstrands of COI Strategy and Defence (S&D), and in 2024 it will encompass several focal areas. First, the planning of wargames to practise command and control capabilities in a hybrid threat environment continues. The planned games will be used to train a variety of audiences. Ukrainian experts will form a very specific audience with regular training sessions on hybrid warfare to be continued in the framework of the EU Mission in Ukraine. The workstrand will continue to cover the use of military

exercises as a particular form of hybrid warfare, in order to collect experiences and practices and to learn to counter the use of this tool.

The Centre's work on enhancing knowledge about the particularities of hybrid threat action will continue in the thematic field of cyber and modern technologies. COI S&D will study the offensive potential of disruptive technologies and draw lessons from the application of these technologies in monitoring this potential. In addition, the work started in 2023 on the use of chemical, biological, radiological, and nuclear (CBRN) instruments in the context of hybrid threats and warfare will continue. The goal is to prepare a handbook in 2024 with recommendations for adapting existing training and exercises. Lastly, the cyber power project will continue to focus on the interlinkages between cyber power, the cyber domain, and hybrid threat action. Its results will be disseminated through the annual cyber power symposium and related training events and exercises.

Strengthening knowledge about hybrid threat actions as part of the strategies and policies of actors responsible for them, and generating ideas about how to cope with them.

Another key theme in Hybrid CoE's work plan deals with hybrid threat activities as part of the broader strategies and policies of actors responsible for them. This approach is designed to enhance knowledge about similarities and differences between various actors, as well as the more detailed political logic behind the selection of means used. The ultimate goal of the Centre's work in this respect is to provide ideas about how to cope with these forms of malign activity.

Two key workstrands planned for 2024 will shed light on different hybrid threat actors. The first is a project led by the R&A function that focuses on various forms of Chinese hybrid threat activity. This work will deal with China's narrative influence in a set of African countries on the one hand, and on China's efforts to create a global infrastructure network on the other. Chinese-Russian cooperation will be studied in the latter context. The aim is to enable the Centre's networks to understand not just what but why actors such as Russia and China make certain choices, facilitating efforts to anticipate and counter hybrid threats. The Chinese acquisition of immaterial assets will be addressed in COI V&R's Economic resilience workstrand.

The second workstrand dealing with hybrid threat actors is led by COI HI and will build on earlier work on non-state actors (NSAs) functioning as proxies in hybrid threat operations. Work planned for 2024 aims at gaining a greater appreciation of the facets and limitations of the operationalization of NSAs by hostile state sponsors, exploring how NSAs generate effects and developing indicators and warnings to help practitioners identify the employment of NSAs as a tool for hybrid influence. A new playbook will develop Participating States' capacity to take practical measures to address a wide range of hostile non-state actors. Another key publication will seek to enhance understanding of the Russian use of proxies by looking at the rise and fall of the Wagner Group.

Strengthening knowledge about the key vulnerabilities of Western societies with respect to hybrid threats, and providing ideas about how to address them.

The third key theme for Hybrid CoE's work in 2024 deals with identifying Western actors' vulnerabilities to hybrid threats and building resilience and response capabilities.

One of the key focus areas of this work deals with the broad democratic vulnerabilities of Western societies. The ongoing workstrand on Safeguarding democratic processes, led by COI HI, will be divided into two workstrands, one on 'Preventing election interference', and the other on 'Disinformation'. The first will capture and develop best practices from the 2024 election cycle. A practical guide will also be published for election authorities regarding the protection of the conduct of elections. The main aim of the Disinformation workstrand is to increase knowledge about disinformation and its mechanisms and to build the capacity to counter it in a comprehensive manner. A publication analyzing challenges for counter-disinformation actors, a Counter-Disinformation practitioners' workshop, and a tabletop exercise will be developed for the Participating States.

COI V&R will continue with the Maritime hybrid threats workstrand, focusing on legal vulnerabilities in the framework of international law at sea and the emerging and disruptive technologies shaping maritime hybrid threat activities. An updated handbook consisting of different legal scenarios will be offered to stakeholders along with training events based on those scenarios. Apart from the training events on multiple hybrid threat scenarios at sea, work in 2024 will focus on unmanned vessels as an emerging hybrid threat tool.

Another workstrand with the general goal of mapping important vulnerabilities is the COI V&R-led work on aviation and space, which will observe developments and increase awareness of hybrid threats leveraging the capabilities and vulnerabilities of space and aviation. In 2024, this workstrand will focus on China's developing space capabilities and their threat potential and how to build Euro-Atlantic actors' resilience in the space domain. The work on analyzing Sino-Russian space collaboration in global data-gathering as well as interconnections between space and the Arctic will be based on joint efforts between COI V&R and the R&A function. In addition, Hybrid CoE will continue building practitioner and expert networks for the Aviation and space workstrand due to its growing importance.

Hybrid CoE's cooperation with the European Commission's Joint Research Centre (JRC) will continue within COI V&R's Resilience and critical infrastructure workstrand. The joint work will build upon earlier efforts to conceptualize hybrid threats and resilience, with the aim of increasing Participating States', the EU's and NATO's resilience by detecting and preventing hybrid threat campaigns, or countering them in their initial phases.

The final theme in the context of the study of Western states' vulnerabilities to hybrid threats deals with existing forms of preparedness in the shape of governmental structures and legislation. Hybrid CoE plans to gradually extend the

work on mapping Participating States' policies, policy coordination and legislative efforts to counter hybrid threats. This work was already started in 2021 by COI S&D, focusing on the strategies and policies of Hybrid CoE's Participating States in countering hybrid threats. In 2023, the R&A function mapped governance structures and legislation put in place to counter hybrid threats in Nordic countries. This work will continue in R&A's Best practices in governance and resilience workstrand.

Hybrid CoE's operational modes for 2024

Hybrid CoE's Helsinki-based office currently hosts 41 members of staff representing 16 different nationalities and a wide variety of professional backgrounds. Secondees from the Participating States – currently 17 experts – play an important role in this context as the Centre leads and coordinates Hybrid CoE's multifaceted international activities.

Hybrid CoE's operational modes combine a wide range of activities to ensure that the Centre is a credible and relevant leader in promoting a greater understanding of hybrid threats, from small brainstorming sessions and sets of consecutive workshops to large-scale meetings and conferences. These are sustained by the Centre's own research activities, and by studies and reports commissioned from its academic and practitioner expert networks. Training, exercises and capacity-building for different target groups form an important part of the Centre's commitment to the work on countering hybrid threats.

Networks and partnerships

Hybrid CoE is a network-based organization, and hence its networks and partnerships will continue to play a key role, and will be strengthened in 2024. In 2020, the Centre's IR function started a comprehensive mapping of the expectations and interests of its Participating States vis-à-vis the Centre, and this work will continue annually. In 2024, Hybrid CoE will invite the Centre's national points of contact to a meeting in Helsinki for the second time to discuss common practices and expectations concerning the Centre's work, and to learn more about its activities. Continuous dialogue with the Centre's key stakeholders is a vital part of its activities and takes place regularly in the form of visits to Participating States, meetings, and visits to the Centre at various levels. Hybrid CoE will prioritize visitors from Participating States' government institutions as well as from the EU and NATO. The Centre continues to seek new ways to build networks and facilitate discussions between EU and NATO members.

Hybrid CoE will continue its close cooperation with the EU institutions (the Commission, including SG, DG DEFIS, DG HOME and the JRC, the Council and its bodies including the EEAS, the EDA and the ESDC, as well as the European Parliament, including its committees and secretariat). It will continue to support the incoming Council Presidencies in the Horizontal Working Party and other committees and events. Close cooperation will also continue with NATO, and Hybrid CoE's experts will present their work to its relevant political and military bodies (including the ESC and other relevant divisions, SHAPE,

ACT, JFC Brunssum and key NATO COEs). Hybrid CoE's annual High-Level Retreat will continue to provide an informal platform for discussions between the two organizations, bringing together leading EU and NATO officials.

The Centre will continue its work to deepen and structure its various partnerships in 2024. The partnership framework for non-EU and non-NATO countries has recently been refined to provide a concrete platform for third countries willing to deepen their cooperation with Hybrid CoE based on common interests. In 2023, an internal policy was established on cooperation with third countries, introducing the possibility of opening selected Centre activities and output to such countries. The Centre will build on this based on a case-by-case assessment. Cooperation with Ukraine – defined as an enhanced partnership – will be further developed based on the policy and discussions on a common framework document in 2024.

Development of the Centre's strategic partnerships with civil society actors such as think tanks, international and non-governmental organizations will also be further systematized. The aim is to contribute to a whole-of-society response and increase the Centre's visibility among the broader public.

The Research and Analysis function will continue to support the Centre's work by establishing networks with the transatlantic academic and research community. Its expert pools provide a tool for this. The format and composition of the expert pools was recently reviewed to ensure that they are fully representative of the Participating States. The EU-HYBNET project will provide the Centre with additional tools to create networks and partnerships with new actors.

Training and Exercises

Through the Training and Exercises function, Hybrid CoE's work is uniquely positioned to overcome obstacles to cross-societal, intra-governmental approaches aimed at reducing the effects of hybrid threats on Participating States' societies and institutions. The Training and Exercises function continues to support the Centre's work by developing original hybrid threat-related training and exercise programmes. In 2024, Training and Exercises will continue to provide expertise for both NATO and EU exercises, build Participating State capacity through hybrid training opportunities, and create original exercises inspired by the conceptualization of hybrid threats. Exercises will continue to be the best way to offer the network of practitioners an opportunity to apply tools to combat hybrid threats in order to strengthen knowledge and build institutional muscle memory to counter future hybrid threat effects.

Continuing to produce innovative ways to explore the spectrum of hybrid threats in a pragmatic way, Training and Exercises will again use wargaming simulations to provide a platform to strengthen democratic institutions, communicate with populations and develop a whole-of-society approach to recognize, respond to, and defend against threats such as disinformation. Based on continued interest from Participating States, Training and Exercises will continue the Countering Disinformation

Wargame (CDWG) series of events, which will allow participants to develop and employ their own strategies to counter disinformation using a virtual exercise platform. In 2024, the CDWG will test the EU's foreign information manipulation and interference (FIMI) toolbox and EU Rapid Alert system. With the assistance of the Research and Analysis function, the CDWG programme will more closely examine the manifestation of disinformation and other hybrid threat campaigns in the Western Balkans, culminating in a capstone event at the end of 2024. In addition, the Centre's Hybrid 101 training module and wargaming course will continue to be offered to the Participating States. Training courses and exercises available for the Centre's networks will continue to be presented in a training catalogue on the Centre's extranet.

Publications

Through its publications, the Centre will continue to deliver timely and tailored analysis, insights, and best practices on hybrid threat-related issues. In 2024, the Centre will adopt a new, more strategic publication philosophy, gearing its publications more clearly towards goals derived from the original Memorandum of Understanding and concentrating on key publications. The said goals will range from leading the discussion on hybrid threats to disseminating best practices and learning from prior experiences and examples related to hybrid threats. The Centre's publications continue to be divided into open access and limited circulation publications, where the former aim to reach a broader audience and the latter target Hybrid CoE's network of practitioners.

In response to feedback from its Participating States, in 2024 the Centre will also reorient its publications policy to help its Participating States and organizations maintain situational awareness and build foresight regarding hybrid threat developments. To this end, the Centre's hybrid threat monitoring and reporting system will be consolidated, and the monitoring reports developed.

Events and conferences

Events, training sessions, exercises, and courses of different sizes and forms constitute an integral part of Hybrid CoE's activities, engagement with its networks and dissemination of the knowledge and analysis acquired. In 2024, the Centre will organize major events on themes cutting across its work plan, including a large conference in the latter part of the year.

The Centre will also continue to organize events online as well as in a physical format, depending on the goal and scope of the activities at hand. In addition, hybrid events allowing for both physical and online participation will be organized where appropriate, to facilitate engagement with the Centre from a distance.

The Hybrid CoE Talks virtual event series, launched in 2023, will continue to provide regular moderated discussions and interviews in a virtual format, designed to foster dialogue and engage the audience. The purpose of the series is to highlight topical work carried out at the Centre, as well as to take up new emerging trends within the hybrid threat field.

In addition to inhouse-produced webinars, Hybrid CoE will act as a co-host or support

virtual events organized by distinguished think tanks, with a view to promoting the Centre's work and expertise, and contributing to the public discussion on hybrid threats.

Key plans for Hybrid CoE's administration for 2024

The security of Hybrid CoE's premises, including ICT security, is a key target for the development work of the Centre's administration. This work is aimed at ensuring a safe and secure working environment for the Centre and its staff and is being taken forward in cooperation with the Finnish Security and Intelligence Service (Supo). In 2024, the Centre will continue to implement the guidelines and recommendations regarding the Centre's ICT security based on the comprehensive ICT security audit conducted in 2023.

The Communications team will continue to support Hybrid CoE in achieving its objectives via timely and effective communications. In 2024, the Communications team will carry on promoting the use of the recently launched extranet among the Centre's Participating States and organizations, and increasing the Centre's visibility among its core stakeholders. In addition to developing the Centre's website and social media channels, the Communications team aims at obtaining relevant media visibility through proactive media work, carried out in cooperation with the Participating States' administrations when appropriate. The Centre's two newsletters, the publicly available *Hybrid CoE Newsletter* and the limited release *News for Networks*, will also be refined in 2024, with a particular focus on broadening the Centre's network of practitioners.

Impact assessment of Hybrid CoE's work

A mechanism for impact assessment has been developed for the Centre, based on the constant gathering of data and feedback for impact assessment purposes. The toolbox, which consists of both quantitative and qualitative indicators, has been fully operational since 2022, enabling the Centre to monitor the performance and effectiveness of its work and activities more systematically.

Hybrid CoE

The European Centre of Excellence
for Countering Hybrid Threats