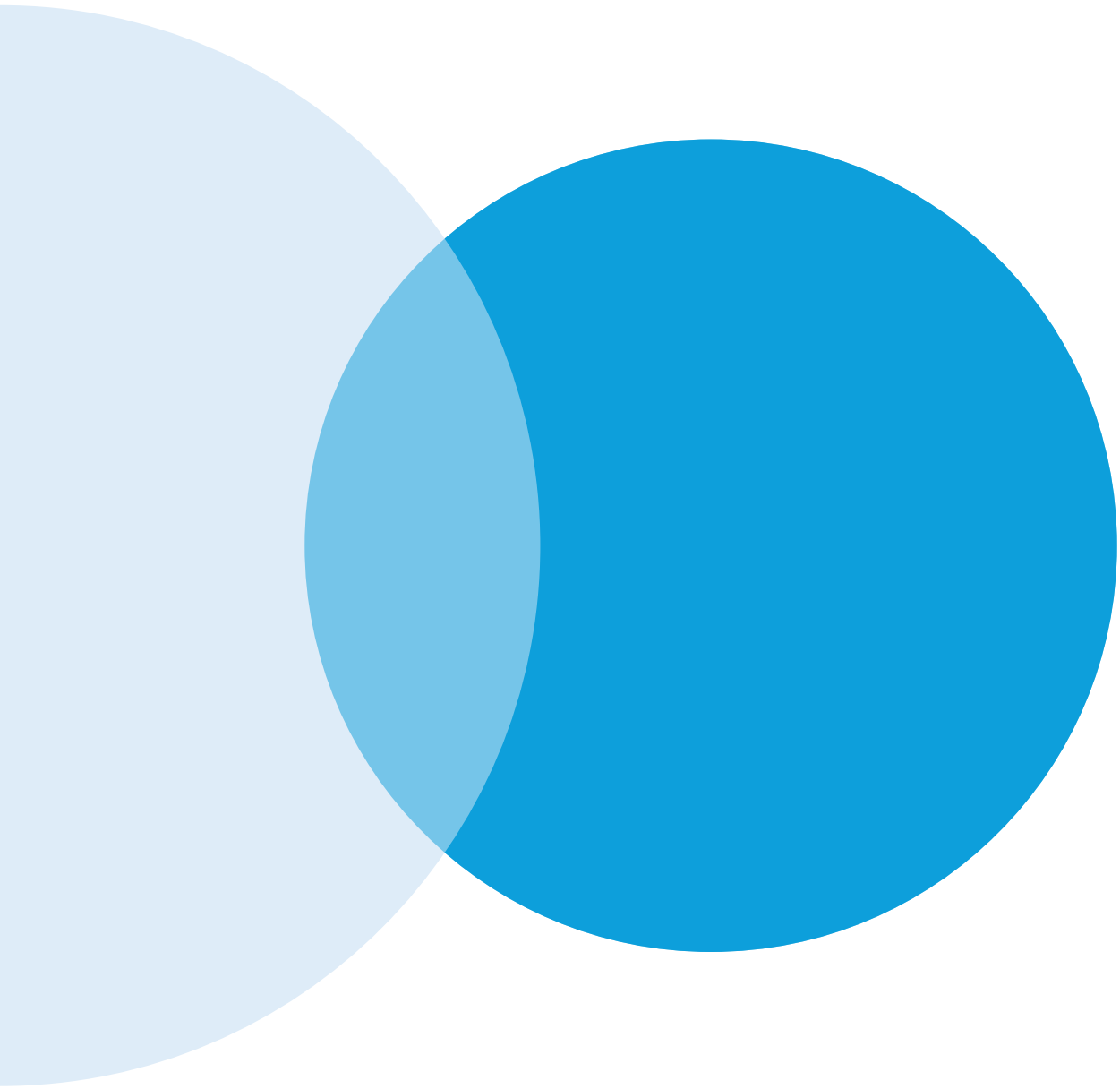
Hybrid CoE
key themes for 2025



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 2025

Introduction

Apart from Russia's ongoing war against Ukraine and the associated geopolitical risks, democratic vulnerabilities in the Euro-Atlantic region dominated the discourse on hybrid threats in 2024. Concerns about election interference peaked during a year marked by multiple elections with significant implications for foreign policy and Western unity. In this context, the role of new technologies, particularly AI, as a tool for hybrid threat operations was strongly brought to the fore. A wave of diverse malign operations targeting Western critical infrastructure accelerated the debate on the need for proactive countermeasure policies against hostile actors.

Hybrid CoE finalized a number of important projects focusing on both the characteristics of hybrid threat operations as well as the tools to counter them. A comprehensive analysis of Russian hybrid threat operations against Moldova (Hybrid CoE Working Paper 28) exemplifies the first approach. Research on Ukrainian countermeasures to Russian disinformation operations (Hybrid CoE Research Report 11), as well as a report comparing the governmental and legislative practices of the five Nordic countries in countering hybrid threats (Hybrid CoE Working Paper 31), illustrate the latter approach.

The wide range of training and exercises offered to the Centre's key stakeholders continued to expand in 2024. Scenario-based exercises on critical infrastructure protection and countering maritime threats were offered to multiple audiences, while training on countering election interference and the basic Hybrid 101 training course continued on a regular basis. In addition to these, several major national and regional exercises took place, the largest of which was a regional exercise on the Western Balkans, organized in Vienna in October 2024.

Hybrid CoE's work plan for 2025 is firmly anchored in the work and fields of expertise developed during previous years. As the Centre expands and now includes all 36 EU and NATO member states, 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 2025. 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 2025

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, civil society organizations, private sector representatives and the media. Enhancing both cross-governmental and public-private dialogue is an essential part of the Centre's work.

Thematically, the Centre's work plan for 2025 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 perpetrating 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 actions, both through conceptual work as well as 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 aims 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 be adequately involved in this activity. COI Hybrid Influence (HI) leads the project and will update its Playbook on Deterrence in 2025 and continue to provide an exercise in support of its stakeholders' policies. A number of new analyses will be conducted to broaden understanding of the prerequisites for an efficient deterrence policy.

Several workstrands are planned for 2025, where the particularities of hybrid threat actions will be analyzed by mapping their emergence within a specific geopolitical region or in a thematic context. A strengthened focus on

the Western Balkans will take the form of an updated trend report on hybrid threats, and a series of conferences focused on building expertise and sharing best practices to counter foreign information operations in the region. This work, led by COI HI, will be supported by other functions and is partly funded by a grant from the Global Engagement Center at the US State Department. Work will continue on the hybrid threat potential in and towards the Arctic, aimed in 2025 at enhancing knowledge about how new technologies and the development of infrastructure will affect the future of the hybrid threat landscape in the Arctic. The Middle East and North Africa (MENA) region will be another geopolitical focus area for R&A, with an earlier report on hybrid threat activities in the region set to be updated. This work will be finalized in 2025.

The Economic Resilience workstrand (COI Vulnerabilities and Resilience, V&R) will continue focusing on the potential means and effects of economic hybrid threats. To this end, it will study forms of economic and critical infrastructure cooperation between Russia and China in Africa. This work is linked to China's Multidomain Influence, which is a workstrand led by the R&A function. It analyzes various forms of Chinese hybrid threat activities as well as the development of a global data- gathering infrastructure by China and Russia.

Another key effort is to identify and map emerging hybrid threat activities via Hybrid CoE's internal open-source monitoring system, established in spring 2020 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 was expanded based on positive feedback from stakeholders to include monthly reports and an annual Hybrid Threat Trend Outlook. The hybrid threat monitoring system is a Centre-wide project involving participants across 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.

Hybrid Warfare is one of the principal workstrands of COI Strategy and Defence (S&D), and in 2025, it will encompass several focal areas, including the continued offering of wargames to practise command and control capabilities in a hybrid threat environment. The planned games will be used to train a variety of audiences. The workstrand will also focus on the use of military exercises as a particular form of hybrid warfare, aiming to collect experiences and practices in an effort to learn how to counter such threats.

In 2025, 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, particularly AI and biotechnology, and draw lessons from the application of these technologies. Work will also continue on the use of chemical, biological, radiological, and nuclear (CBRN) instruments in the context of hybrid threats and warfare. The plan for 2025 is to

provide training on the challenges of detecting and responding to CBRN threats in the context of hybrid conflict. Lastly, the Cyber Power in Hybrid Warfare project will continue to focus on the interlinkages between cyber power, the cyber domain, and hybrid threat activities, with a particular emphasis on cognitive warfare and superiority. The findings will be disseminated through the annual Cyber Power Symposium, related training events and exercises. Additionally, Hybrid CoE will also contribute to a four-year EU-funded EU-INSPIRE project aimed at building a higher educational ecosystem within cybersecurity.

Finally, the COI V&R-led workstrand on Instrumentalized Migration will be re-established in 2025 due to the topicality of the issue, with the aim of sharing experiences and best practices in countering this form of hybrid threat activity. The work will be carried out in the form of closed-door workshops available to interested stakeholders.

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

Another key theme in Hybrid CoE's work plan deals with the broader strategies and policies that generate hybrid threat activities as well as the actors responsible for them. This approach is designed to enhance knowledge about similarities and differences between various actors, including 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 on how to cope with these forms of malign activity.

Three key workstrands planned for 2025 will shed light on different hybrid threat actors. The first is an R&A-led project focusing on different forms of Russia's multidomain influence. This workstrand builds on work conducted during previous years on Russian hybrid threat activities against Ukraine, Moldova and the Eastern partnership countries more broadly. In 2025, the project will focus on the objectives, mechanisms and operating models behind Russia's multidomain malign activities against EU and NATO countries.

In addition to addressing forms of Chinese economic statecraft, the above-mentioned workstrand on China's multidomain influence continues to focus on China's role in Africa by identifying and analyzing country-specific vulnerabilities to malign Chinese activities in sub-Saharan Africa. The aim of the two workstrands is to enable the Centre's networks to understand not just how, but also why actors such as Russia and China make certain choices. This understanding will facilitate efforts to anticipate and counter hybrid threats.

The third workstrand dealing with hybrid threat actors is led by COI HI and will build on earlier work on non-state actors (NSAs) as a tool of hybrid threat operations. The work planned for 2025 aims to gain a greater appreciation of the operationalization of various NSAs serving as proxies or surrogates for hostile states, and for Russia in particular, and to develop

countermeasures against them. Both analytical work and the sharing of best practices will be used to achieve the objectives.

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 2025 deals with identifying Western actors' vulnerabilities to hybrid threats, as well as building resilience and response capabilities.

One of the key focus areas of this work is the broad democratic vulnerabilities of Western societies. The earlier workstrand on Safeguarding Democratic Processes, led by COI HI, will now be re-established and will consist of OSINT and election interference prevention training. Related to the latter topic, a Practitioner Workshop will be organized to identify new trends and share best practices. The conclusions of the corresponding event organized in 2024 will be shared as a conference report and discussed in this framework.

The Disinformation workstrand will be strengthened with a specific focus on the role of AI. It will continue with the established forms of activity: the Counter-Disinformation Practitioner Workshop and a report based on it, with a new training course on countering disinformation. The AI component will be progressively integrated into the work to improve understanding of the use of this tool in disinformation operations.

A new workstrand on Cognitive Strategies and Cultural Resilience has been established in COI S&D, focusing on the instrumentalization of identity and other societal cleavages as a tool for hybrid threat activities and disinformation operations in particular. Training will be developed to improve the skills and strategies of government officials when it comes to recognizing and countering values-based disinformation.

The Economic Resilience workstrand will continue to be covered by COI V&R, aiming to boost Participating States' capacities to enhance economic resilience by providing stress tests and timely information about malign actors. The other part of the workstrand will focus on economic and critical infrastructure cooperation between Russia and China in Africa.

COI V&R will continue with the Maritime Hybrid Threats workstrand, focusing on legal vulnerabilities within the framework of international law at sea, and the emerging and disruptive technologies shaping maritime hybrid threat activities. The previously published Handbook on Maritime Hybrid Threats will be complemented with new scenarios and training based on the handbook, and will continue to be made available to stakeholders. In addition to these activities, the analytical work will be extended with a publication on maritime hybrid threats to choke points and their economic implications for shipping.

Another workstrand with the goal of mapping critical vulnerabilities in Aviation and Space is the COI V&R-led work on these topics, which will monitor and increase awareness of hybrid threats in this rapidly developing area. In 2025, this workstrand will focus both on conceptual work, by elaborating on the notion of space

resilience, and on formulating a set of space-related hybrid threat scenarios. Discussions based on the scenarios will aim to increase understanding of cross-domain considerations in threat analysis and resilience development. In addition, Hybrid CoE will continue to build practitioner and expert networks for the Aviation and Space workstrand, given 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 the resilience of Participating States, the EU and NATO by introducing a broad policy-making response to countering hybrid threats. A comprehensive report on the topic will be published in 2025 and introduced to a broad audience.

The final theme in the context of the study of the vulnerability of Western states to hybrid threats deals with the 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. In 2023, the R&A function mapped the governmental structures and legislation put in place to counter hybrid threats in Nordic countries. As a next step, this work will focus on policymaking, legislation and governmental solutions in FDI screening in a selection of countries.

Hybrid CoE's operational modes for 2025

Hybrid CoE's Helsinki-based office currently employs 44 members of staff, representing 18 different nationalities and diverse professional backgrounds. Secondees from the Participating States – currently 18 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 networks of academic and practitioner experts. 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 reached a major milestone in 2024 when the last eligible EU member states and NATO allies joined as Participating States. This concludes the Centre's expansion phase, but having 36 Participating States also poses an increased challenge for the Centre in terms of providing sufficient and meaningful value to all Participating States. Hybrid CoE will therefore slightly readjust its focus on engaging new and existing Participating States in a more proactive manner. The Centre will also begin to implement

its new internal policy on Strategic Partnerships, focusing on key civil society actors.

As a network-based organization, Hybrid CoE's networks and partnerships will continue to play a key role in this effort. The Centre's International Relations (IR) unit has been organizing the Annual Bilateral Consultations since 2020 to comprehensively map the expectations and interests of its Participating States, the EU and NATO vis-à-vis the Centre. This work will continue on an annual basis, and the consultations will be developed to generate more coherent feedback to support work planning for the following year.

In addition to the annual consultations, continuous dialogue with the Centre's key stakeholders in Participating States, as well as with EU and NATO institutions, is a vital part of its activities. This dialogue takes place regularly through roadshows to the capitals of Participating States and through different types of meetings and visits to the Centre at various levels. The Centre will take a more proactive approach to outreach by leveraging its entire staff to build networks more systematically, engage with Participating States, the EU and NATO, and facilitate discussions between EU and NATO members.

In 2024, for the second time, Hybrid CoE invited the Centre's national points of contact to a meeting in Helsinki to discuss common practices and expectations concerning the Centre's work, and to learn more about its activities. These formal meetings, open to all Participating States, the EU and NATO, will continue on a biennial basis. Hybrid CoE will also systematically engage the POC network to facilitate the Centre's engagements in the respective Participating States. Hybrid CoE will continue to take a strategic approach to visits to the Centre, focusing on visits by key partners from the Participating States, the EU and NATO.

Hybrid CoE will continue its close cooperation with the EU institutions, including the Commission's key Directorates-General, the Council and its bodies, including the EEAS, the EDA and the ESDC, as well as the European Parliament, including its committees and Secretariat. The Horizontal Working Party on Enhancing Resilience and Countering Hybrid Threats continues to be an important channel for Hybrid CoE to contribute to the work of the rotating presidencies of the Council of the European Union.

Close cooperation will also continue with NATO. Hybrid CoE's experts will present their work to its relevant political and military bodies, as well as at many NATO events. The annual High-Level Retreat organized by Hybrid CoE will continue to provide an informal platform for discussion between the two organizations, bringing together leading EU and NATO officials. Hybrid CoE also remains available to support any potential iterations of the EU-NATO Foresight Seminar.

The Centre will continue its work to deepen and structure its various partnerships in 2025. In 2023, an internal policy on third-country partnerships was established for partnerships with non-EU and non-NATO countries. The policy introduces the possibility of opening selected activities and outputs to third countries, and the Centre will build on this policy on a case-by-

case assessment. Cooperation with Ukraine will be further developed in line with this policy and the 'enhanced partnership' framework.

In 2024, an internal policy was established on Strategic Partnerships with civil society actors, such as think tanks, and international and non-governmental organizations. This policy will be implemented from 2025 onwards with the aim of managing key partnerships of mutual benefit more efficiently and contributing to the whole-of-society response and visibility of the Centre among the broader public.

R&A will continue to support the Centre's work by building on its expert pools, further establishing networks with the transatlantic academic and research community. An assessment of the forms and composition of the pools has recently taken place, ensuring their full representativeness with respect to the Participating States. The EU-HYBNET project – to be concluded in 2025 – will provide the Centre with an additional tool for creating networks and partnerships with new actors.

Trainings and Exercises

Through its versatile Training and Exercises function, Hybrid CoE is uniquely positioned to overcome obstacles, such as coordination challenges and communication gaps, which may hinder cross-societal and intra-governmental approaches aimed at reducing the effects of hybrid threats on the societies and institutions of Participating States. T&E continues to support the Centre's work by developing original hybrid threat-related training and exercise programmes. In 2025, T&E will continue to provide expertise for both NATO and EU exercises, build Participating States' capacity through in-person and online training opportunities, and design original exercises informed by the conceptualization of hybrid threats. Exercises continue to be the most effective way to offer the network of practitioners an opportunity to apply counter-hybrid threat tools, strengthen knowledge, and build institutional muscle memory to counter the potential impact of future hybrid threats.

T&E continues to devise innovative ways to explore the spectrum of hybrid threats in a pragmatic manner, and will again use wargaming simulations to provide a platform for strengthening democratic institutions, communicating with populations, and developing a whole-of-society approach to identifying, responding to, and countering threats such as disinformation. Based on continued interest from Participating States, T&E will continue the Countering Disinformation Wargame (CDWG) series of events, which will allow participants to develop and deploy their own strategies to counter disinformation using a virtual exercise platform. With the assistance of COI HI, the CDWG programme will more closely examine the manifestation of disinformation and serve as a capstone event in late 2025.

In response to requests stemming from the Annual Bilateral Consultations, T&E will develop and facilitate a tabletop exercise on economic coercion. It will seek to strengthen the resilience of governments and the financial sector against economic coercion, focusing on potential threats from Russia and China, and designed to facilitate informative exchanges among participating

governments regarding current policies and procedures. It will culminate in an in-person exercise simulating a hybrid threat incident. This incident will involve aspects such as a cybersecurity breach and physical infrastructure damage, which could disrupt the digital operations of the financial sector. By enabling representatives to scrutinize and deliberate on their readiness to respond to such scenarios, the exercise aims to foster a deeper understanding of vulnerabilities and enhance collaborative strategies among nations facing economic pressures and coercive tactics.

In 2025, the Hybrid 101 training module will continue to be offered to Participating States, consisting of topical presentations and briefings; the programme can also be tailored to meet specific needs. In addition to two national exercises, the wargaming course is also planned for 2025, marking the fifth iteration of this unique event.

In 2021, the Centre started compiling a catalogue of training and exercises to provide a better overview of its programme and the options available to its stakeholders. This practice will continue in 2025, and the training catalogue will continue to be updated on the Centre's extranet.

Publications

Publications represent one of the cornerstones of the Centre's knowledge production and awareness-raising activities. Through its publications, the Centre will continue to disseminate timely and tailored situational awareness and analysis of hybrid threats and their countermeasures. In 2025, the Centre will further streamline its publication production to ensure that publications are produced in the most cost-efficient way and that each publication supports the strategic goals of the Centre. Its open-access publications will focus on leading the public discussion on hybrid threats, while its limited release products, aimed solely at officials in its Participating States and organizations, will provide bespoke situational awareness on hybrid threats and best practices to counter them.

Encouraged by the positive response to its Monthly Monitoring Reports and the Hybrid Threat Trend Outlook, in 2025 the Centre will seek more detailed feedback on these products from the Participating States and organizations, with the goal of developing the products further to best meet the needs of the Centre's core audiences.

Events and conferences

A wide range of events, including training sessions, exercises, workshops and courses, constitute an integral part of Hybrid CoE's dissemination of knowledge about hybrid threats, as well as engagement with its networks. In 2025, the Centre will organize major events on themes that cut across its work plan, including three large conferences in the Western Balkans.

The Centre will continue to organize events in both online and physical formats, depending on the goal and scope of the respective activities. In addition, hybrid events, which allow for both physical and online participation, will be organized where appropriate to facilitate remote engagement with the Centre.

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

Key plans for Hybrid CoE's administration in 2025

Development of the Centre's organization and staffing will be a key focus for the administration in 2025. There is an increasing need to strengthen the organization by creating new positions, both within the administrative teams and the content functions. The growing number of expert positions needs to be balanced by enlarging the administrative and support functions. The Centre's premises also need to be adapted to accommodate the growing staff. A further extension of the current premises was started in 2024 and will be finalized in 2025. The security of Hybrid CoE's offices, including ICT security, remains a key target for the Centre's administrative development efforts. This work is aimed at ensuring a safe and secure working environment for the Centre and its staff and is being carried out in cooperation with the Finnish Security and Intelligence Service (Supo).

The Communications team will continue to support Hybrid CoE in achieving its objectives via timely and effective communications. In 2025, the Centre's communications strategy will be updated to reflect changes in the Euro-Atlantic security environment, as well as the recent expansion of participation in Hybrid CoE to include all EU member states and NATO allies.

During 2025, the Communications team will work on updating the Centre's website as a platform for providing topical research and analysis on countering hybrid threats in an easy-to-consume format. During the year, particular emphasis will be placed on the effective dissemination of the Centre's research and knowledge to its stakeholders by enhancing the accessibility of the Hybrid CoE extranet, and by reaching out to media representatives in the Participating States.

Broadening the Centre's network of practitioners and increasing the number of subscribers to its limited release News for Networks newsletter, and to the publicly available Hybrid CoE Newsletter, also remain among the priorities for the year.

Impact assessment of Hybrid CoE's work

An impact assessment mechanism, based on the continuous data collection and feedback provided on the Centre's activities, has been fully operational since 2022. It consists of both quantitative and qualitative indicators enabling the Centre to systematically monitor the performance and effectiveness of its work and activities, and to adjust its efforts when necessary. The impact assessment process will be further developed in 2025 to better capture formal feedback from the Participating States on the Centre's activities. The latest results of the impact assessment will be included in the 2024 Annual Report.

Hybrid CoE

The European Centre of Excellence
for Countering Hybrid Threats