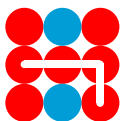
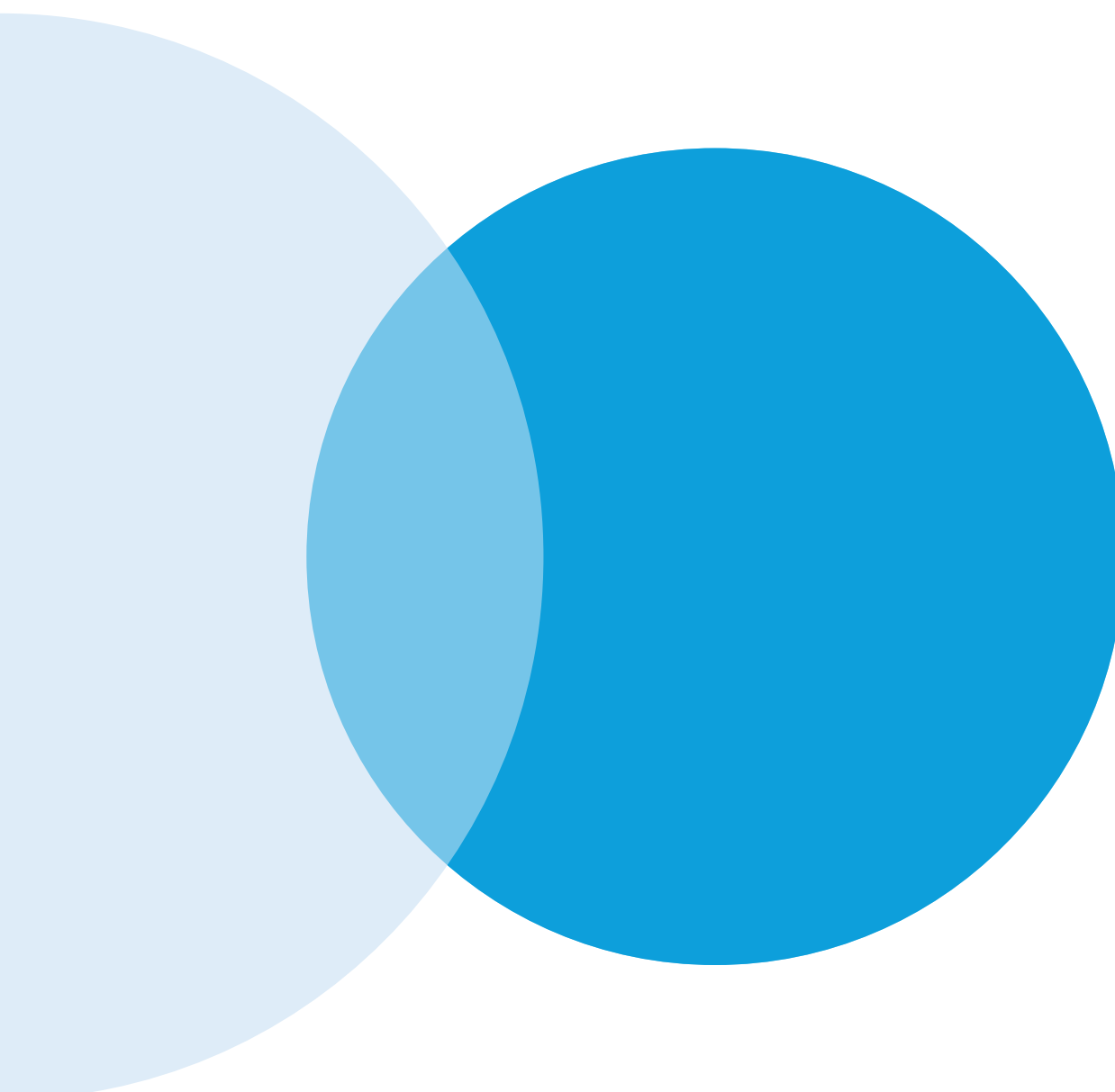




Hybrid CoE key themes for 2023



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 2023

Introduction

In 2022, the Euro-Atlantic security environment worsened significantly due to the Russian war against Ukraine and its consequences for international relations. The confrontation deepened between Russia and China on one side and Western democracies on the other, with authoritarian states continuing their large-scale hybrid threat operations against the West throughout the year.

Hybrid CoE continued to implement its previously agreed work plan, while adjusting to the demands of the new worsening security environment. With the war against Ukraine ongoing, Hybrid CoE has addressed the use of hybrid threat instruments in that context and analyzed the probable long-term implications of the war for hybrid threat methods, as used by Russia and other authoritarian states. The Centre also started to study those hybrid threat instruments whose use intensified in parallel with the war.

Given the urgency of the situation in Ukraine, and the country's common interests with Hybrid CoE in understanding the evolving nature of hybrid warfare, cooperation between Ukraine and Hybrid CoE has been elevated to the level of an enhanced partnership. This status allows for a more systematic exploration of mutual interests across Hybrid CoE and enables capacity-building efforts in support of Ukraine, within the means and capabilities of the Centre. To this end, contacts have been intensified between Ukrainian authorities and the Centre.

With the pandemic easing, the Centre has been able to resume its normal outreach

functions, including training and exercise activities. Apart from the newly established Hybrid 101 training module, different types of training events and exercises have been offered to the Participating States in the framework of many workstrands, such as those on deterrence, hybrid warfare, election training, open-source intelligence, maritime hybrid threats and Arctic hybrid threats, to mention just a few. The large multiannual Resilient Civilians project funded by NATO's Science for Peace programme concluded with a major conference and exercise that took place in Helsinki in April. In 2022, the Centre's work on countering disinformation was boosted thanks to a major grant received from the US Global Engagement Center at the US State Department.

Hybrid CoE's key themes and approaches to countering hybrid threats in 2023

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 sharing 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 2023 can be divided into three major fields of interest:

- Strengthening knowledge about **the particular characteristics of hybrid threats and making proposals to counter them.**
- Strengthening knowledge about **hybrid threat action as a part of the strategies and policies of actors using them,** and creating 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 workstrands planned under these three main themes.

Strengthening knowledge about the particular characteristics of hybrid threats 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 ways of using them. There are thus many particularities, ranging from the use of various interfaces to causing

confusion and ambiguity, and further to the use of proxies, which make the detection of responsible actors difficult. They are all aimed at preventing the target from effectively responding to the action and protecting itself against it. As a consequence, hybrid threats usually occur in many domains simultaneously, and are designed to remain below the threshold of detection and attribution.

Hybrid CoE continues to study 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 Deterrence workstrand, which has progressed from its initial conceptual analysis phase into a module consisting of a cross-government exercise. The goal is to increase understanding of how deterrence theory can be applied to the hybrid threat environment, what the various policy instruments are, and how the EU and NATO can best be involved in this activity. COI Hybrid Influence (HI) is leading the project and will continue offering exercises to the Participating States and multilateral platforms such as the Joint Expeditionary Force (JEF), as well as publishing a further set of case studies.

Several workstrands are planned for 2023 where the particularities of hybrid threat action will be analyzed by mapping their emergence within a specific geopolitical region or in a thematic context. Building on the Eastern Partnership Trend Report (2022), the Research and Analysis (R&A) function will focus on patterns and trends of hybrid threat activities taking

place in Moldova. The work on hybrid threat potential in and towards the Arctic will be continued through case studies on how hybrid threats are manifesting at local, national and regional levels amongst the Participating States. Arctic infrastructures will be another focus area for this work.

The workstrand on identifying trends in the global economy from the hybrid threat point of view, which started in 2022, will continue to pursue its aim of producing a trend report and an expanded network of practitioners and experts. In 2023, this work will be complemented with new aspects focusing on relevant Chinese economic activities. The first deals with forms of Chinese economic coercion in Southeast Asia, and the second will focus on Chinese acquisition of strategic capabilities through foreign direct investment, joint ventures and research collaboration. This work is based on joint efforts between COI V&R and the R&A function.

Another key effort to map and identify emerging hybrid threat activities takes the form of Hybrid CoE's internal open-source monitoring system – Monitoring, Assessment and Reporting Group Capability (MSG) – 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 monthly reports for the Centre's networks, focusing on actors and thematic fields of hybrid threat activity (Russia, China, the Arctic, Deterrence, etc.). In 2023, the monitoring capacity will be continued with a focus on hybrid threat activities in general, and new emerging threats and trends in particular.

In addition to bi-monthly reports provided for Hybrid CoE's networks, a second annual report will be launched built on the data and findings from that year. MSG is a Centre-wide project involving participants from all of the Centre's functions, monitoring hybrid threat activity in their field of interest. At the same time, it serves as an important tool for the Centre's internal professional development.

The workstrand launched by COI Vulnerabilities and Resilience (V&R) in 2022 in the field of 'instrumentalized migration', which focuses on the use of illegal migration as a hybrid threat instrument, will continue mapping legal vulnerabilities on the basis of the results of the first expert studies presented at an event organized for the Participating States at the end of 2022. Further steps in the workstrand – in terms of legal vulnerabilities to be studied – will be decided in that context on the basis of the outcomes of the first expert reports.

Hybrid warfare has constituted a workstrand for COI Strategy and Defence (S&D), from both a conceptual and an empirical point of view. After a discussion with key stakeholders, this work will take three directions in 2023. First, a specific wargame has been designed to practise and train command and control capabilities in a hybrid threat environment, as well as a digital OSINT-based platform to analyze and share lessons learned from the Russian war against Ukraine. Second, the use of military exercises will be studied as a particular form of hybrid warfare to collect experiences and practices, and to learn to counter the use of this tool. Third, alongside the ongoing work on monitoring

the hybrid threat aspects of the Russian war against Ukraine, the workstrand will continue to analyze and assess the possible hybrid threat potential of climate change and different aspects of human security.

Finally, the Centre's work on enhancing knowledge about the particularities of hybrid threat action will continue in the thematic fields of cyber and modern technologies, which will be continued in a more focused form by COI S&D. The results of an earlier project on Hybrid Warfare: Future & Technologies (HYFUTEC) will be used to enhance knowledge about possibilities to mitigate the offensive potential of modern disruptive technologies through established arms control mechanisms. The hybrid cyber power project will focus on the cognitive aspects of the cyber and information domains as means and targets for hybrid threat activities. Based on the annual cyber symposium, regular Hybrid CoE cyber papers will continue to be published.

Strengthening knowledge about hybrid threat action as a part of the strategies and policies of actors using them, and creating ideas about how to cope with them.

Another key theme in Hybrid CoE's work plan deals with hybrid threat action as a part of the broader strategies and policies of actors using them. This approach is designed to enhance knowledge about similarities and differences between different 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 action.

Two key workstrands planned for 2023 will shed light on hybrid threat actors: the first is a project led by the R&A function, extending the earlier work on comparing and contrasting the strategic cultures of authoritarian states ("Seeing Red"), resulting in a major report on the topic in 2022. 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, enhancing efforts to anticipate and counter hybrid threats. In 2023, the workstrand will focus on the role of China in the framework of the Russian war against Ukraine, studying in particular how China has positioned itself in the Global South. This project, which is linked to the work on Chinese economic statecraft presented in the context of the workstrand on the global economy, will take advantage of the Centre's strengthened expertise on China.

Another workstrand under the leadership of COI HI will build on the taxonomy of non-state actors (NSAs) functioning as proxies in hybrid threat operations, published in 2022. The goal of the workstrand is to help practitioners detect, deter and mitigate hybrid threats caused by the use of non-state actors. A substantial scoping report planned for 2023 aims to improve understanding of the operationalization of NSAs by hostile state sponsors, to explore how NSAs generate effects, and to develop indicators and warnings to help practitioners identify the employment of NSAs as a tool for hybrid threat operations.

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 2023 deals with identifying Western actors' vulnerabilities to hybrid threats, and building resilience and response capabilities.

One of the key focal points for this work deals with the broad democratic vulnerabilities of Western societies. The ongoing workstrand on Safeguarding Democratic Processes, led by COI HI, will be continued. It encompasses situational awareness (especially through open-source intelligence training), public/private engagement (focusing on large tech companies), analysis of disinformation tools used to challenge Western democracy, and training to counter election interference. The disinformation elements of this workstrand will be emphasised in 2023 to continue to meet the key demands and current requirements of the Participating States. Running in parallel with COI HI's work is a disinformation project that will be continued by the Training & Exercises function, consisting of an exercise that will be provided for the Participating States.

In 2023, the theme of democratic vulnerabilities will be addressed within a new R&A- led workstrand on cognitive intrusion and democratic vulnerability. This workstrand builds on the work of a multidisciplinary expert group focusing on trends of cognitive threats undermining forms of democratic governance. A consortium of key partners from the Participating States has been planned for this work-

strand, which will provide support and function in close cooperation with the aforementioned COI HI-led workstrand.

COI V&R will continue with the workstrand on Maritime Hybrid Threats, focusing among other things on legal vulnerabilities in the framework of international law at sea. An updated (2022) handbook consisting of different legal scenarios will continue to be presented to interested stakeholder groups, accompanied by training events based on it.

Another workstrand with the general goal of mapping important vulnerabilities is the COI V&R-led work on Aviation and Space, which will culminate in the publication of both a conceptual paper on the space domain, as well as the mapping of future trends regarding hybrid threats. An expert network is being built in support of the Centre's work in this field.

Within COI V&R's workstrand on Resilience, Hybrid CoE's cooperation with the Joint Research Centre of the European Commission (JRC) will be continued. In 2022, this cooperation led to the publication of a major report on resilience and will now be focusing on conceptualizing escalation in the landscape of hybrid threats.

The final theme in the context of the study of Western states' vulnerabilities to hybrid threats deals with existing forms of preparedness in the form of governmental structures and legislation. Hybrid CoE plans to gradually extend the work on mapping Participating States' different 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. By highlighting similarities and differences, this comparative analysis of the approaches aims to provide good practices and allow administrations to learn from each other. This work will now be continued, firstly by relating the findings to the framework of the EU's (Strategic Compass) and NATO's (Strategic Concept) visions for countering hybrid threats. Secondly, more focused efforts will be made by R&A to map governance structures and legislation put in place to counter hybrid threats within Nordic countries.

Hybrid CoE's operational modes for 2023

Hybrid CoE's Helsinki-based office currently hosts 40 members of staff representing 15 different nationalities and a wide variety of professional backgrounds. Secondments from the Participating States – currently 16 experts – play an important role in this context as the Centre leads and coordinates Hybrid CoE's multifaceted international activities. In 2022, there was a relatively heavy staff turnover due in part to the rotation of secondees. The Centre also received new secondments from the Czech Republic, Iceland and Hungary, and the first full-time Swedish secondment. In 2023, a modest growth in staffing is expected.

Hybrid CoE's operational modes combine a wide range of activities to ensure that the Centre is a 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 studies and reports commissioned from the Centre's academic and practitioner expert networks. Various types of training events, exercises and capabilities provided for different audiences form an important part of the Centre's commitment to applying work to counter hybrid threats. Furthermore, the Centre and its experts will continue the work to raise awareness of the threat environment among the general public in its Participating States, including through the media.

Networks and partnerships

As Hybrid CoE is a network-based organization, its networks and partnerships will also play a key role – and will be developed further – in 2023. In 2020, the Centre's IR unit 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 2022, the Centre's national points of contact gathered for their first-ever meeting in Helsinki 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 meetings and visits at various levels.

Hybrid CoE will also continue its close cooperation with the EU institutions (the Commission, including DG DEFIS and the Joint Research Centre, the Council and its bodies including the EEAS, the European Defence Agency and the European Security and Defence College, as well as the European Parliament including its com-

mittees and secretariat). It will continue to support the incoming Council Presidencies in the Horizontal Working Party and other committees and events. Hybrid CoE's experts will present their work to the relevant political and military bodies of NATO (including the Hybrid Analysis Branch of the Joint Intelligence and Security Division, the Emerging Security Challenges Division, and the Enablement and Resilience Section of the Defence Policy and Planning Division). The annual High Level Retreat, bringing together leading EU and NATO officials, will continue to provide an informal platform for discussions between the two organizations.

During 2023, the Centre will continue its work to deepen and structure its various partnerships. The cooperation with third countries will be systematized based on an internal policy. The cooperation models will include the possibility of opening up selected Centre activities and output, based on a case-by-case assessment by the Centre. Cooperation with Ukraine will be further defined in a common framework document. Cooperation with international and non-governmental organizations will also be further systematized as the Centre's networks continue to grow.

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 – 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 will provide additional

tools for the Centre 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 remove impediments to cross-societal, intra-governmental approaches aimed at reducing the effects of hybrid threats on individual member state societies and institutions. The Training and Exercises function continues to support the Centre's work by taking a pragmatic approach through the development of original hybrid threat-related training and exercise programmes. In 2023, Training and Exercises will expand the reach of the Centre by providing expertise in 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 counter-hybrid threat tools to strengthen knowledge and build institutional muscle memory to counter future hybrid effects. Continuing to produce innovative ways to explore the spectrum of hybrid threats in a pragmatic way, the Training and Exercises function will look at ways in which wargaming can provide a platform to better strengthen democratic institutions, communicate with populations, and develop a whole-of-society approach to recognizing, responding to, and defending against threats such as disinformation. Through funding from the US Global Engagement Center, Training and Exercises has been leading a series

of events that allows participants to develop and employ their own strategies to counter disinformation through the use of a virtual exercise platform.

In 2023, the Hybrid 101 training module will be offered to the Participating States and other stakeholders, consisting of topical presentations and briefings. The wargaming course organized in 2021 and 2022 is anticipated to run in 2023 as well. Likewise, the disinformation exercise that was provided for the Participating States in 2022, thanks to the grant from the US Global Engagement Center, will stay on the agenda on a smaller scale.

COI V&R is preparing to share its expertise in a new format called “Light exercises”, where Participating States’ own exercises would be supported by a specialist team. The team’s task would be to explain Hybrid Threats and Comprehensive Resilience and to produce a “Red scenario” through open-source intelligence and reconnaissance. The actual exercise would be conducted by the Participating State itself, and the Hybrid CoE team would not get involved in operational assessments.

The catalogue of training events and exercises included in the *News for Networks* newsletter since 2021 has proved to be a useful tool and will continue to be published in 2023.

Publications

Through its publications, the Centre will continue working on delivering timely and tailored analysis and advice on hybrid threat-related issues. The Centre’s publications range from short paper formats such as the Strategic Anal-

ysis papers, which aim to seed discussion, to longer edited Research Reports designed to contribute to the existing academic body of knowledge, as well as more focused manuals and lessons learned, which present timely and targeted recommendations, and Records, which present workshop and exercise summaries and project outcomes. The papers are divided into public and limited release publications. The public publications are aimed at a broader audience, while the limited release publications cover more targeted and sensitive subjects.

During 2023, the Centre’s aim is to reinforce external communication about its publications to ensure that Hybrid CoE is leading the discussion on hybrid threats, as well as providing timely and practical insights for the Participating States, NATO and the EU. Publication releases targeted both at the Centre’s networks and the general public will be developed in order to increase the reach of new publications across the Centre’s stakeholder groups.

Events and conferences

After the outbreak of the COVID-19 pandemic, Hybrid CoE shifted its modus operandi from organizing physical events to running all of the activities online. This practice will remain a part of the Centre’s activities in parallel with the increasing number of physical events.

In 2023, Hybrid CoE will launch a new virtual event series called Hybrid CoE Talks, comprising regular moderated interviews in a virtual format, designed to foster dialogue and engage the audience. The purpose of the new virtual event series is to take up new emerging trends

within the hybrid threat field, as well as to highlight topical work carried out at the Centre. The new concept also aims at increasing the Centre's visibility and broadening its networks.

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 to contributing to the public discussion on hybrid threats.

The functions will gradually increase the number of physical meetings and events to maximize interaction with Participating State practitioners and other stakeholders in the framework of all workstrands. In 2023, the Centre will organize major events on themes cutting across its work plan, including one larger conference in the latter part of the year. The High Level Retreat will bring leading EU and NATO practitioners together to discuss important hybrid threat-related topics.

Key plans for Hybrid CoE's administration for 2023

During summer 2022, Hybrid CoE acquired additional office space to accommodate the growing number of staff. The new extension, 220 square metres in area, has workstations for ten members of staff. In 2023, a modest increase in both directly employed and seconded staff members is expected.

The task of the Communications team is to support Hybrid CoE in achieving its goals via timely and effective communication. In 2022, the implementation of the new communi-

cations strategy got underway and brought some changes to the Centre's communications approach and toolbox. In 2023, the Comms team will be working to finalize the extensive development projects started in 2022 (the construction of a proper contact database and extranet and the renewal of the Centre's intranet), and to promote the use of the new services. The Centre's two newsletters, the publicly available Hybrid CoE Newsletter and the limited release News for Networks, will also be further developed in 2023 in response to the feedback received from the Centre's points of contact. In addition, a project to create a toolkit for the Participating States to help raise awareness of hybrid threats within their populations will be started in 2023.

Impact assessment of Hybrid CoE's work

A mechanism for impact assessment has been prepared 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, will be fully operational during 2022, enabling the Centre to more systematically monitor the performance and effectiveness of its work and activities and, when necessary, to adjust its efforts. The first results of the impact assessment will be included in the 2022 Annual Report.



Hybrid CoE

The European Centre of Excellence
for Countering Hybrid Threats