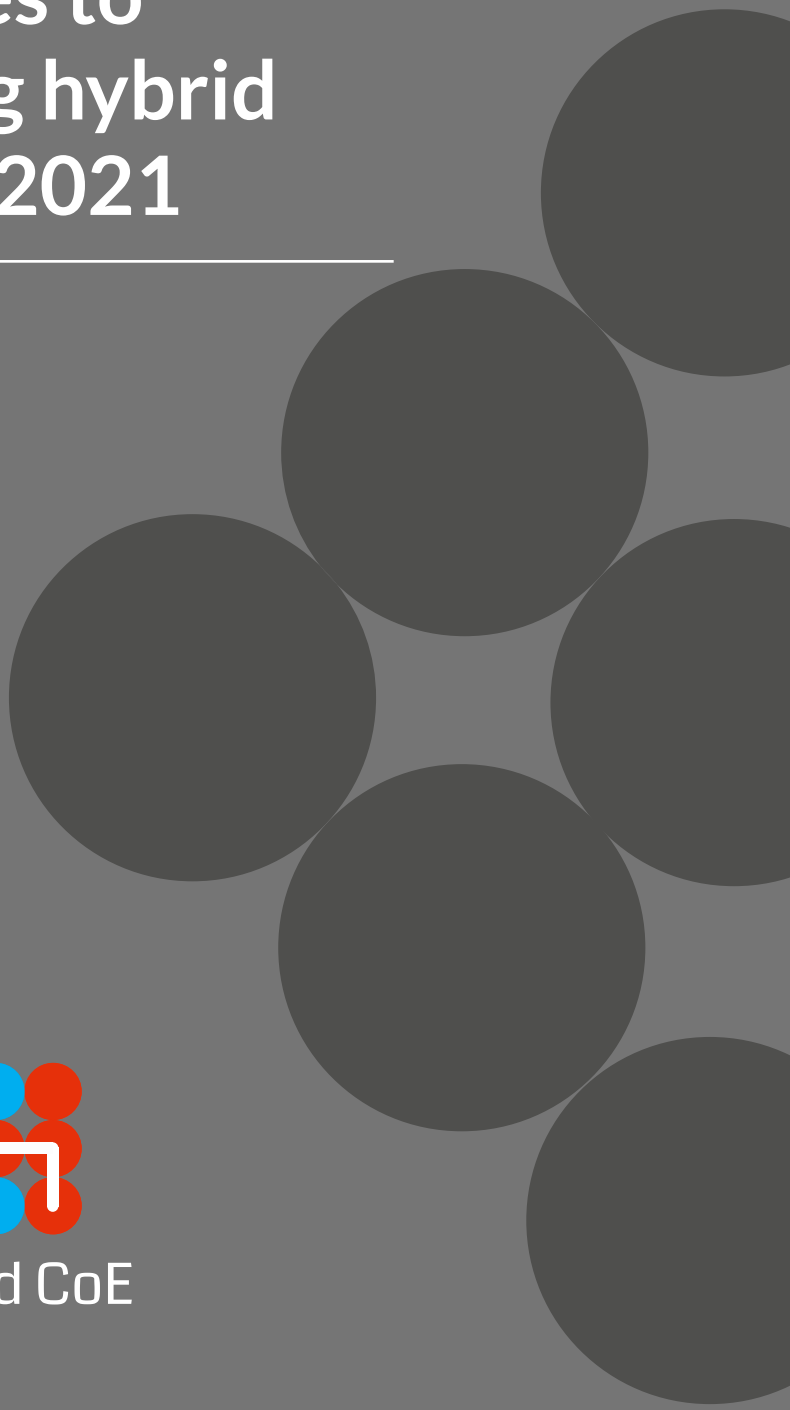
Hybrid CoE's key themes and approaches to countering hybrid threats in 2021



Hybrid CoE

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

Hybrid CoE is an international hub for practitioners and experts, building participating states' and institutions' capabilities and enhancing EU-NATO cooperation in countering hybrid threats located in Helsinki, Finland

HYBRID COE'S KEY THEMES AND APPROACHES TO COUNTERING HYBRID THREATS IN 2021

Hybrid CoE's key goal is defined in its constitutive document (Memorandum of Understanding) as follows: "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". Hybrid CoE fulfils this goal by providing a platform for its participants to come together, share best practices, build their capabilities, test new ideas and defend themselves against hybrid threats. As a hub of expertise, the Centre leads the discussion on countering hybrid threats through research, the sharing of best practices, and giving policy recommendations.

The Centre's Helsinki-based office currently hosts 34 staff members representing 11 different nationalities and a wide variety of professional backgrounds. Secondments from Participating States – currently amounting to 15 experts – play an important role in this context as the Centre leads and coordinates the multifaceted international activities of Hybrid CoE.

Hybrid CoE engages in a wide range of dynamic activities to ensure its leadership in promoting a greater understanding of hybrid threats. Events ranging from small brainstorming sessions and sets of consecutive workshops to large-scale meetings and conferences are underpinned by the Centre's own research activities, as well as studies and reports commissioned by the Centre's academic and practitioner expert networks. Various forms of training, exercises and tools provided for different audiences comprise an important part of Hybrid CoE's commitment to countering hybrid threats.

As the Centre is a network-based organization, its networks and partnerships play a key role, and will also be developed further in 2021. In 2020, Hybrid CoE conducted a comprehensive mapping of the expectations and interests of its Participating States vis-à-vis the Centre, and this work will continue in various forms in 2021.

Hybrid CoE will also continue its close cooperation with EU institutions (Commission, Council, EEAS, European Parliament, including actors such as the Joint Research Centre and the European Security and Defence College), and will support the incoming Council Presidencies in the Horizontal Working Party and in the POC meetings of the Hybrid Fusion Cell. Hybrid CoE will continue its cooperation with NATO (including with the Hybrid Analysis Branch and Defence Policy and Planning Division), while the annual High-Level Retreat bringing together leading EU and NATO officials will continue to provide an informal platform for discussions between the two institutions.

The work plan for 2021 can be divided into three major fields, enhancing knowledge of:

- the particular characteristics of hybrid threats and their operational logic, and making proposals to counter them;
- hybrid threat action as a part of the strategies and policies of actors in charge of them, and producing ideas on how to cope with them;
- the key vulnerabilities of Western societies with respect to hybrid threats and providing ideas on how to address them.

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

Hybrid CoE continues its work in 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 **Deterrence project**.

The second phase of the project is currently underway and, based on a series of case studies and a strategic game, seeks to develop the skills and understanding of practitioners in Participating States. The first phase of the project explored how

deterrence is applied against hybrid threats and culminated in the publication of the Deterrence Playbook.

A project on the **Arctic** analyzes the nature and forms of hybrid threats in and to this region. The project findings can inform the revision of the EU's Joint Communication on the EU's Arctic Policy and ensure consideration of hybrid threats in the Participating States' Arctic policies and strategies.

Hybrid CoE supports the Portuguese EU presidency by studying the hybrid threat challenge and its elements in the **EU's Southern Neighbourhood**. The project consists of the preparation of a trend report and maritime scenarios and exercises.

Another key effort to map and identify emerging hybrid threat activities takes the form of an internal monitoring system – **Monitoring Assessment and Reporting Group Capability (MSG)** – established in spring 2020 to monitor hybrid threat activities in the COVID-19 framework. The system has produced monthly reports for the Centre's networks, focusing on thematic fields of hybrid activity. In 2021, the MSG will be continued with a focus on general hybrid threat activities and newly emerging threats and trends in particular.

Hybrid CoE will also continue enhancing knowledge of the particularities of hybrid threat action in the thematic fields of **cyber and modern technologies**. The results of an earlier project on Hybrid Warfare: Future & Technologies (HYFUTECH) will be used to increase knowledge of the use of modern technologies in improving multidomain situational awareness. The cyber-power project will continue to focus on the interlinkages between both cyber power and the cyber domain and hybrid action.

Enhancing knowledge of hybrid threat action as a part of the strategies and policies of actors in charge of them, and producing ideas on how to cope with them.

Another key theme in the Centre's work plan deals with hybrid threat action as a part of the broader strategies and policies of actors in charge of them. This approach is designed to enhance knowledge of the similarities and differ-ences between various actors, as well as the more detailed political logic behind the selection of means used. The final goal of the work is to generate ideas on how to cope with these forms of action.

Two key workstrands planned for 2021 will shed light on hybrid threat actors. The first is a project launched in 2020 dealing with the **strategic cultures of authoritarian states**, which will also produce a manual on the topic in 2021.

Another workstrand will build on earlier work on **non-state actors** functioning as proxies in hybrid operations, and deepen the approach towards a systematic analysis of key groups of non-state actors, their operational mode, and political framework. The broader goal is to prepare to mitigate, deter and prevent hybrid threats caused by the use of non-state actors.

A third workstrand with a clearly actor-centric focus deals with the field of **international finance and markets**, where geoeconomic policies and tools are increasingly used as hybrid instruments. In 2021, the workstrand will produce a baseline study on the theme, as well as a more detailed assessment of the use of foreign direct investment and money laundering as tools for hybrid action.

Enhancing knowledge of the key vulnerabilities of Western societies with respect to hybrid threats and providing ideas on how to address them.

The third key theme for Hybrid CoE's work in 2021 deals with identifying Western actors' vulnerabilities to hybrid threats, and with building resilience.

One of the Centre's leading joint workstrands in this field deals with **legal resilience** and the way in which existing normative frameworks, international or national, may be used by hybrid threat actors to challenge security and stability in the transatlantic community. This workstrand will firstly draw together the results of previous work carried out on the topic at the Centre, such as knowledge of vulnerabilities in the maritime context, or legal resilience within the EU and NATO, as developed in a joint project with the University of Exeter in 2020.

In 2021, earlier work on the topic will be complemented with new focus areas identifying gaps

and vulnerabilities in legal systems that can be used against Western societies to exert hybrid threats. This work is intended to lead to recommendations for national and international actors on how to eliminate or remove vulnerabilities from legislation.

Hybrid CoE's work on **critical infrastructure** will continue to address different forms of the public-private partnership. The goal is to bring together both groups of actors to raise awareness and discuss their division of labour in critical infrastructure protection vis-à-vis hybrid threats.

A new topic related to broad societal vulnerabilities deals with **aviation**, for which the key vulnerabilities to be addressed deal with the emerging role of satellites and their risk potential in a hybrid threat context.

An entirely new workstrand will focus on the **Strategies and policies of the Centre's Participating States in countering hybrid threats**. By highlighting similarities and differences, this comparative analysis of the approaches aims to provide best practices and to allow administrations to learn from each other.

The final workstrand under the theme of enhancing resilience deals with key issues in **safeguarding democratic processes**. This new workstrand builds on earlier work on election interference (with training events) and situational awareness. The lessons learned during those projects will now be extended by complementing the agenda of challenges to democracy with some new elements, and by strengthening the foundation of the election training activities, which will continue in a slightly revised form. Changes in the information environment are in a key position in this context, and hence close cooperation with social media platforms will continue in order to study and monitor their role in hybrid operations that challenge democratic processes.

Hybrid CoE