Hybrid CoE
The European Centre of Excellence for Countering Hybrid Threats

Frequently asked questions on hybrid threats

What are hybrid threats?

Hybrid threats are harmful activities that are planned and carried out with malign intent. They aim to undermine a target, such as a state or an institution, through a variety of means, often combined. Such means include information manipulation, cyberattacks, economic influence or coercion, covert political manoeuvring, coercive diplomacy, or threats of military force. Hybrid threats describe a wide array of harmful activities with different goals, ranging from influence operations and interference all the way to hybrid warfare.

Who are the actors behind hybrid threats?

Hybrid threats are used by authoritarian states and regimes, and by non-state actors (NSAs), which often act as proxies for authoritarian regimes. Examples of hybrid threat actors include Russia, China, and Iran. Non-state hybrid threat actors can include groups, movements or entities, which are used or co-opted to fulfil certain strategic objectives. One such example is the Wagner Group, a private military company (PMC) which operates in several states worldwide.

Why do authoritarian states resort to hybrid threats?

Authoritarian states aim to fulfil their strategic objectives, such as increased global influence and power, by means of interfering in and influencing other states. Hybrid threats are a cost-efficient way to achieve these objectives and affect the processes and institutions of democratically governed states. Hybrid threat actors seek to avoid both accountability for, and countermeasures against, their hostile activities. Hence, hybrid threats are designed in such a way that detecting and defending against them is difficult. They are devised to remain under a threshold which could constitute or be perceived as (an act of) war against the attacked state.

How do hybrid activities threaten us?

Hybrid threats aim to restrict the political room for manoeuvre by targeted states, including by undermining their citizens' sense of security. They are designed to create fear or anxiety, and sow distrust towards authorities and other people, citizens, or groups. They target and exploit vulnerabilities inherent in democratic systems of government and in the fabric of democratic societies, such as political rights and individual liberties. By using hybrid threat activities, malign actors seek to aggravate wedges in society, to undermine social cohesion and trust among citizens and towards their democratic institutions.

When and where have hybrid threats been used against democracies?

Before its full-scale invasion of Ukraine in February 2022, **Russia** had conducted an intensive hybrid threat campaign against Ukraine. This included disinformation campaigns, cyberattacks against state institutions and critical infrastructure, diplomatic coercion, co-opting of officials and business leaders, and an (undeclared) military intervention in Eastern Ukraine and Crimea. When this campaign failed to achieve Russia's objectives in Ukraine, Russia launched a full-scale war of aggression against its neighbouring state – while continuing to use a range of hybrid threat activities across other domains.

Taiwan is a constant target of hybrid threats from mainland **China** and the Chinese Communist Party. These threats include economic and military coercion, as well as information operations that aim to further the strategic objectives of China's Communist Party in Taiwan.

After Russia's interference in the 2016 US presidential election, similar influencing campaigns have been observed in several European states. The goals of such hybrid threat activities included the discrediting of electoral processes, increasing societal polarization, and/or support for parties and candidates that were perceived as well-disposed towards authoritarianism.

What can we do to defend ourselves against hybrid threats?

To defend democratic societies against hybrid threats, hostile foreign influence must be countered through intensified cooperation – both within societies, and within and across governments. The first step is to raise awareness of hybrid threats. Additionally, careful attention is required regarding abuses of the information environment and civil liberties by hostile actors. Democratic states duly need to foster resilience against these threats in both government and the broader civil society. Examples of resilience-building measures include improving media literacy or protection of critical infrastructure. Democratic states should aim to have a broad toolbox of instruments of power that can be used in a strategic and coordinated manner.

Hybrid CoE
The European Centre of Excellence for Countering Hybrid Threats

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.