







COUNTERING HYBRID THREATS

The increased use of hybrid strategies and operations by state and non-state actors poses a **threat to security and shared democratic values** of the EU Member States and our partner countries. These threats include, for instance, information manipulation, cyber-attacks, lawfare, economic coercion, and the instrumentalisation of migrants.

THE EU'S APPROACH TO COUNTERING HYBRID THREATS

While countering hybrid threats is primarily a national responsibility, the EU facilitates Member States' cooperation, develops policy solutions and encourages sharing best practices. The EU's policy framework on countering hybrid threats contains two major documents: the **2016 Joint Framework on Countering Hybrid Threats** and the **2018 Joint Communication on increasing resilience and bolstering capabilities to address hybrid threats**.

The EU counter-hybrid threats policy is based on four lines of action:

			
Situational awareness Ensuring that Member States have a common understanding of the challenges affecting the EU, as basis for taking targeted action.	Resilience Making the EU and its partners better prepared to prevent, withstand and recover from hybrid attacks, including through CSDP missions.	Response Using the full range of EU tools to respond to hybrid attacks from diplomatic and restrictive measures, to CSDP missions and crisis response mechanisms.	Cooperation Working with international partners and organisations, as well as with civil societies, to improve our responses and resilience against hybrid threats.

As agreed in the **Strategic Compass** for Security and Defence, an **EU hybrid toolbox** was established in 2022. It comprises preventive, cooperative, stability-building, restrictive and support measures.

The purpose of the toolbox is to help

- identify complex and multifaceted hybrid campaigns,
- coordinate tailor-made and cross-sectoral responses to them.

Acting as an overall framework, it brings together other relevant response mechanisms and instruments, such as the **cyber diplomacy toolbox** and the **foreign information manipulation and interference (FIMI) toolbox**. It improves the effectiveness and coherence of various actions, and therefore brings added value to the EU's capabilities in responding to hybrid threats.

EU Hybrid Rapid Response Teams

The EU is creating teams drawing from sectoral national and EU civilian and military expertise to support Member States, CSDP missions and operations and partner countries to counter hybrid threats.



EU-NATO COOPERATION

- 20 out of the 74 common proposals for cooperation are related to countering hybrid threats (e.g. enhancing resilience, situational awareness and countering disinformation).
- Structured Dialogue on Resilience and the well-established cooperation on resilience since 2022.
- EU-NATO Task Force on Resilience of Critical Infrastructure launched in 2023 to focus on four key areas: transport, energy, space and digital infrastructure.



HYBRID RISK SURVEYS TO PARTNERS

- The surveys help identify the gaps and vulnerabilities of partner countries, prepare recommendations and consider support measures based on these.
- The Hybrid Risk Survey carried out with Moldova in 2022 served as basis for the launch of the EU Partnership Mission, deployed to support Moldova counter hybrid threats.