MARCH 2022
#EUDefence
#StrategicCompass

COUNTERING HYBRID THREATS

Hybrid threats influence and exploit vulnerabilities to incur damage below the threshold of overt aggression. They are a mixture of coercive and subversive activities, conventional and unconventional methods, used in a coordinated manner across multiple domains. Authoritarian regimes are increasingly attempting to undermine the EU's shared democratic values and polarise our societies for their own purposes using different types of hybrid activities, such as information manipulation, cyber-attacks, lawfare, economic coercion, or 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 is crucial for making Member States aware of the challenges, informing decision making and developing a common strategic culture.

Resilience - the EU's resilience concept includes our ability to prevent, withstand and recover from crises, including multifaceted hybrid attacks. The EU also supports the resilience building of its neighbours and can use CSDP missions to this end.

Response options can range from diplomatic engagement, CSDP and crisis response mechanisms, to rapid response teams and restrictive measures.

Cooperation - the EU is committed to working on countering hybrid threats with international partners and organisations as well as with other stakeholders from civil society. It is crucial not just to make our own societies more resilient, but also those close to our borders and beyond.

In the **Strategic Compass** for Security and Defence, Member States expressed their intention to establish an **EU hybrid toolbox,** which could comprise preventive, cooperative, stability-building, restrictive and support measures. It would focus on (1) identifying complex and multifaceted hybrid campaigns, and (2) coordinating tailor-made and cross-sectoral responses to them. Acting as an overall framework, it would bring together other relevant response mechanisms and instruments, such as the **cyber diplomacy toolbox** and the proposed **Foreign Information Manipulation and Interference (FIMI) toolbox**. It would improve the effectiveness and coherence of different actions, and therefore bring added value to the EU's capabilities in responding to hybrid threats.

EU-NATO COOPERATION

- Joint Declarations of Warsaw and Brussels (2016 and 2018).
- 20 out of the 74 common proposals for cooperation are related to countering hybrid threats (e.g. enhancing resilience, situational awareness and countering disinformation).

HYBRID RISK SURVEYS TO PARTNERS

- Goal is to help partners in the neighbourhood to strengthen their resilience to hybrid threats.
- Support measures to mitigate the identified risks and vulnerabilities through existing projects or ad hoc support.