Basic information

2026/2024(INI) INI - Own-initiative procedure	Procedure completed
Hybrid warfare and the protection of the EU's territorial integrity and critical security and defence infrastructure **Subject** 6.10 Common foreign and security policy (CFSP) 6.10.02 Common security and defence policy (CSDP); WEU, NATO	

Key players

European Parliament

Committee responsible	Rapporteur	Appointed
SEDE Security and Defence	JUKNEVIČIENĖ Rasa (EPP)	15/12/2025
	Shadow rapporteur CEPEDA José (S&D) BAY Christophe (PfE) TERHEŞ Cristian (ECR) PAET Urmas (Renew) SØVNDAL Villy (Greens/EFA) KYLLÖNEN Merja (The Left)	

Key events

Date	Event	Reference	Summary
12/03/2026	Committee referral announced in Parliament		
15/07/2026	Vote in committee		
20/07/2026	Committee report tabled for plenary	A10-0212/2026	
15/09/2026	Debate in Parliament		
16/09/2026	Decision by Parliament	T10-0303/2026	Summary
16/09/2026	Results of vote in Parliament		

Technical information

Procedure reference	2026/2024(INI)

Procedure type	INI - Own-initiative procedure
Procedure subtype	Initiative
Legal basis	Rules of Procedure EP 55
Stage reached in procedure	Procedure completed
Committee dossier	SEDE/10/05372

Documentation gateway

European Parliament

Document type	Committee	Reference	Date	Summary
Committee draft report		PE788.818	08/05/2026	
Amendments tabled in committee		PE789.927	11/06/2026	
Committee report tabled for plenary, single reading		A10-0212/2026	20/07/2026	
Text adopted by Parliament, single reading		T10-0303/2026	16/09/2026	Summary

Meetings with interest representatives published in line with the Rules of Procedure

Rapporteurs, Shadow Rapporteurs and Committee Chairs

Transparency

Name	Role	Committee	Date	Interest representatives
CEPEDA José	Shadow rapporteur	SEDE	01/06/2026	European Cyber Security Organisation
CEPEDA José	Shadow rapporteur	SEDE	28/05/2026	Microsoft Corporation
CEPEDA José	Shadow rapporteur	SEDE	27/05/2026	Alto Intelligence
JUKNEVIČIENĖ Rasa	Rapporteur	SEDE	17/03/2026	Vestas Wind Systems A/S
CEPEDA José	Shadow rapporteur	SEDE	12/02/2026	Alto Intelligence

Hybrid warfare and the protection of the EU’s territorial integrity and critical security and defence infrastructure

2026/2024(INI) - 16/09/2026 - Text adopted by Parliament, single reading

The European Parliament adopted by 470 votes to 129, with 62 abstentions, a resolution on hybrid warfare and the protection of the EU’s territorial integrity and critical security and defence infrastructure.

Hybrid warfare: between war and peace

Parliament stressed that hybrid operations are deliberate, combined, intelligence-led and coordinated acts by states, including through non-state actors, intermediaries and proxies. They are designed to appear as isolated incidents and remain below the threshold of armed conflict, while having the potential to produce effects comparable to conventional aggression. The primary objective of hybrid warfare is to destabilise, divide and undermine the EU and its Member States by exploiting systemic vulnerabilities, and weakening their security, resilience and democratic foundations, and their defence readiness.

Parliament affirmed that Russia, acting directly or via multiple proxies such as Belarus, is the **gravest hybrid-threat state actor** targeting the EU and its Member States. It stressed that EU must adopt a **comprehensive approach** to hybrid threats that addresses not only Russian and Belarusian activities but also the growing strategic role of China, Iran and North Korea in enabling and amplifying hostile actions against European interests and security.

The Commission and the Council are invited to assess **the adequacy of existing EU legal frameworks** for addressing hybrid threats, close identified gaps, and treat sub-threshold hybrid operations that cannot be addressed through law enforcement alone as collective security matters, requiring a combined civil-military response.

Information warfare, cognitive security and societal resilience

Parliament expressed concern at the growing scale of cognitive warfare together with foreign information manipulation and interference, which aims to erode societal trust in democratic institutions, increase polarisation, undermine democratic decision-making and public support for European security and defence, including support for Ukraine. AI tools - deepfakes, algorithmic amplification and automated account networks - make influence operations faster, cheaper and harder to detect.

The resolution stressed that information manipulation and interference activities carried out from abroad must be **treated as a serious security threat** requiring an operational approach, better coordination and collaboration among Member States at all levels, including **early detection**, adequate response options and stronger protection of democratic processes, particularly during electoral periods.

Given that hybrid threats target society as a whole, Parliament believes that resilience against hybrid threats must extend beyond military, technical and institutional measures by bringing together public authorities, the private sector, civil society, academia and independent media to strengthen democratic trust, public awareness and societal preparedness, thereby fostering a new European security culture. Members stressed the need to **strengthen public resilience** to foreign information manipulation and interference and called on the Commission to take further steps by **providing cognitive vulnerability mapping and resilience benchmarks**.

Cybersecurity

Cyberattacks have become a central element of hybrid campaigns that leverage the increasing digitalisation of critical sectors such as healthcare, finance and energy. Parliament called for mechanisms to combat information manipulation and interference activities conducted from abroad to be **systematically integrated with cybersecurity capabilities** in order to detect coordinated manipulation infrastructures, identify those responsible, and neutralise them at an early stage.

Members recommended that the Commission examine proposals to establish **a more harmonised framework** to assist Member States in the planning, operational coordination, and implementation of cyber operations. They called for greater harmonisation of **incident reporting** obligations and key legal concepts across EU cybersecurity and resilience frameworks. The Commission and Member States, in cooperation with NATO, should examine the legal, procedural, and operational prerequisites for proportionate, legally compliant **cyber countermeasures**.

Critical infrastructure

Parliament condemned the hybrid attacks targeting the EU's critical infrastructure – in particular energy, transport, communications and satellite infrastructure, including that for military mobility, maritime infrastructure, and submarine cables. It urged the Commission and the Member States to establish, within the framework of the next Multiannual Financial Framework (2028-2034), a European legal and financial framework guaranteeing sufficient protection and resilience for critical energy infrastructure. More generally, it is essential to strengthen surveillance, detection, and defence capabilities against air and maritime threats.

Parliament called for the swift implementation of the Critical Entity Resilience (CER) Directive and the NIS2 Directive, which represent significant steps forward in strengthening resilience against hybrid attacks.

The resolution called on Member States to conduct regular **preparedness and resilience exercises** for critical infrastructure, including joint exercises, and to urgently provide the **priority capabilities** identified in the White Paper on European Defence, particularly in the areas of air and missile defence, drones and counter-drone systems.

Considering the EU's structural dependence on high-risk non-EU countries, particularly China, Members called on the Commission to redouble its efforts to **reduce strategic dependencies** and on Member States to diversify supply chains and **prioritise European and like-minded suppliers** in strategic sectors whenever security considerations so require.

The resolution urged Member States to increase **intelligence sharing** and stressed the obligation to systematically incorporate data-driven and intelligence-based assessments into EU crisis planning and management. It affirmed that the **Single Intelligence Analysis Capability** (SIAC) should be the single hub for intelligence within the European institutions.