The OSCE Secretariat bears no responsibility for the content of this document and circulates it without altering its content. The distribution by OSCE Conference Services of this document is without prejudice to OSCE decisions, as set out in documents agreed by OSCE participating States.

PC.DEL/700/25
4 July 2025

ENGLISH only

EUROPEAN UNION

OSCE Permanent Council 1526
Vienna, 3 July 2025

EU Statement on Malign Activity in the OSCE Region

1. The European Union remains deeply concerned by the growing trend of malign activities across the OSCE area, which threaten our common security, undermine trust, and violate international law, including the core principles enshrined in the Helsinki Final Act and subsequent OSCE documents.

2. We strongly condemn all types of hybrid activities against the European Union and its Member States as well as against its partners. We condemn in particular Russia's continued hybrid campaign, including sabotage, disruption of critical infrastructure, cyber-attacks, information manipulation and interference, and attempts to undermine democracy, including in the electoral process. In this context, the EU welcomes the adoption of additional listings under the framework for restrictive measures in view of Russia's destabilising activities, and the broadened scope of this regime. The EU and the Member States will continue to strengthen their resilience and make full use of all means available, including the EU hybrid toolbox, to specifically prevent, deter and respond to Russia's hybrid threats.

3. As illustrated also by successive EEAS Reports on Foreign Information Manipulation and Interference (FIMI), Russia has engaged in a systematic, international campaign of media manipulation and distortion of facts in order to enhance its strategy of destabilising its neighbouring countries and the EU and its Member States. Russia must uphold its international obligations and commitments and stop its state-controlled disinformation and other malign activities.

4. The EU and its Member States, together with international partners, stand in solidarity with Czechia regarding the malicious cyber campaign that targeted its Ministry of Foreign Affairs. On 28 May, Czechia determined the cyber-attack has been perpetrated by Threat Actor APT 31 that is associated with the Ministry of State Security of China. In recent years, malicious cyber activities linked to China and targeting the EU and its Member States have increased and we have urged Chinese authorities to take action against malicious cyber activities undertaken from their territory.

5. We strongly condemn malicious cyber activities and call upon all states to refrain from such behaviour, to respect international law and to adhere to the United Nations framework of responsible state behaviour in cyberspace, which all UN Member States have endorsed. The EU reaffirms its strong commitment to prevent, deter and respond to malicious behaviour in cyberspace and stands ready to take further action when necessary, in line with its Cyber Diplomacy Toolbox. We will continue to cooperate with our international partners to promote due diligence and responsible state behaviour in cyberspace, with the aim to ensure a global, open, free, stable and secure cyberspace.

6. As the world becomes more interconnected and interdependent, certain economic flows and activities can present a risk to our security. The EU supports efforts to diversify supply routes, invest in green and digital infrastructure, address risks to the resilience of our supply chains and the security of critical infrastructure, enhance technological competitiveness, counter the weaponisation of economic dependencies and the instrumentalisation of migration, and improve crisis preparedness. The EU stands ready to continue working with OSCE participating States and Partners for Co-operation to address the challenges and opportunities in these areas.

Albania, Andorra, Bosnia and Herzegovina, Iceland, Montenegro, North Macedonia, Norway, Republic of Moldova, San Marino and Ukraine align themselves with this statement.