PC.DEL/748/26
16 July 2026

ENGLISH only

Permanent Mission of Ukraine
to the International Organizations in Vienna

Statement on Hybrid Threats in the OSCE Region
As delivered by the Permanent Representative of Ukraine to the International Organizations in Vienna, Yurii VITRENKO, to the 1573rd meeting of the Permanent Council, 16 July 2026

Mr. Chairperson,

Ukraine aligns itself with the statement of the European Union. I would also like to add several remarks in my national capacity.

We are grateful to the UK delegation for raising such an important issue. We see this as an important continuation of the discussion on Russia's hybrid activity that took place in the OSCE last year.

We commend the United Kingdom and the European Union for their first-ever joint cyber sanctions package announced on 13 July, targeting Russian state actors and criminal proxy networks responsible for destructive cyber and hybrid operations across Europe. This is the kind of coordinated action that the moment demands — and Ukraine calls on all participating States to follow suit.

Mr. Chairperson,

Russia's hybrid warfare is not a discrete phenomenon separate from its military aggression — it is an integral component of the same campaign. Cyberspace remains one of the key theatres of Russia's war against Ukraine. Russia systematically combines cyberattacks with kinetic strikes, disinformation, and other hybrid instruments, targeting public authorities, the energy sector, telecommunications, and critical infrastructure. Russian cyber operations have evolved from destructive attacks into covert and prolonged campaigns of cyber espionage, network persistence, and information-psychological influence.

Russia's propaganda funding is set to increase by an unprecedented 54% in 2026 — a clear signal that, unable to achieve its objectives on the battlefield, Moscow is doubling down on disinformation and hybrid pressure.

Although Ukraine remains Russia's primary target, our European partners are coming under growing pressure. Drone incursions, sabotage, attacks on undersea and critical infrastructure, airspace violations, interference in democratic elections — are becoming increasingly visible across the OSCE space. Russia is moving from the sustained pressure model tested in Ukraine to active hybrid operations against EU and NATO member states.

Mr. Chairperson,

Ukraine draws three practical conclusions for this Council.

First, hybrid threats must be treated as a primary security concern, not a secondary one. They are the instrument through which Russia currently projects power across the OSCE space while maintaining a degree of deniability.

Second, the response must be collective. Ukraine shares with its partners its unique frontline expertise in cyber defence, counter-disinformation, and resilience against information operations — expertise accumulated at enormous cost. We call on participating States to strengthen national cyber defences, develop threat

information-sharing mechanisms, improve attribution procedures, and introduce effective deterrence tools.

Third, hybrid threats are intensifying. It is time for the OSCE to do more. The organisation must deepen its work in this area, matching the scale of its response to the scale of the threat.

Russia cannot wage a war without consequence.

Thank you, Mr. Chairperson.