PC.DEL/744/26
16 July 2026

ENGLISH
Original: FRENCH

Delegation of France

STATEMENT BY THE DELEGATION OF FRANCE AT THE 1573rd MEETING OF THE OSCE PERMANENT COUNCIL

16 July 2026

Current issue on hybrid threats (raised by the United Kingdom)

France would like to thank the United Kingdom for having placed an item on hybrid threats on the agenda and aligns itself with the statements by the European Union and NATO, but allow me to add a few comments in a national capacity.

France condemns in the strongest possible terms the cyberattacks carried out on French territory by Russia against French strategic interests.

For several years now, France has been the target of persistent malicious cyberactivities for espionage purposes conducted by the 16th Centre of the Federal Security Service of the Russian Federation (FSB), and more specifically by its Unit 61240, which is tasked with targeting France.

Building on the Turla intrusion set, the FSB has specifically targeted email accounts belonging to the Armed Forces Ministry since 2017, along with the network of the Ministry for Europe and Foreign Affairs at the French Embassy in Moscow in 2018. In 2019, unauthorized access to a computer server belonging to a justice sector entity was detected. In February 2025, a research institute specialized in sensitive technologies and working for the French defence industry was also targeted by cyberattacks carried out by the FSB's 16th Centre, resulting in the exfiltration of a significant amount of data.

Many of our European partners are faced with a similar situation, as the European Union has pointed out on behalf of its 27 Member States. France is directly involved in European collective efforts to prevent or respond to cyberincidents, including those related to the activities of that specific actor.

In recent years, Russia has continuously intensified its malicious cyberactivities, targeting Ukraine and its supporters in particular. Russia is strengthening its own offensive cybercapabilities, while also relying on a diverse ecosystem of non-State actors, including so-called hacktivist groups, for destabilization purposes. In response to these actions, the European Union adopted a new package of sanctions on 13 July, under the EU cybersecurity framework, against nine individuals and four entities that are part of this malicious cyber ecosystem, including a group that has claimed responsibility for destabilization activities against the 2024 Paris Olympic and Paralympic Games.

These cyberactivities are one aspect of the growing hybrid threats targeting EU Member States in the context of Russia's war of aggression against Ukraine, which also encompass information manipulation campaigns, interference in democratic processes, airspace violations and other destabilizing activities.

Russia's malicious cyberactivities are unacceptable and unworthy of a permanent member of the United Nations Security Council. Furthermore, they are contrary to the principles of the United Nations normative framework for responsible State behaviour in cyberspace, which Russia has endorsed. France reaffirms its commitment to the United Nations normative framework and urges Russia to respect its undertakings in this regard.

Alongside its partners and in line with international law, France is determined to use all the means at its disposal to anticipate, deter and respond to destabilizing activities targeting it in cyberspace, including in the run-up to the forthcoming 2027 election.

The technical departments of the Cyber Crisis Coordination Centre (C4) – which brings together the French Cybersecurity Agency, the Directorate-General for External Security, the Directorate-General for Internal Security, the Directorate-General for Armaments and the Cyberdefence Command – are today publishing a joint report on malicious cyberactivities conducted by Russia against French interests using the Turla intrusion set; the report is based on cyberattack attribution work carried out within the C4.

Lastly, I should like to support Canada's call for the OSCE to play an active role in combating these malicious cyberactivities.

I would be grateful if the Chairmanship could kindly attach this statement to the journal of the day.