PC.DEL/744/26
16 July 2026

Original: FRENCH

REPRÉSENTATION PERMANENTE
DE LA FRANCE AUPRÈS DE
L'ORGANISATION POUR
LA SÉCURITÉ ET
LA COOPÉRATION
EN EUROPE

Liberté
Égalité
Fraternité

CP 16/07/2026

Point d'actualité sur les menaces hybrides (soulevé par le Royaume-Uni)

Déclaration de la France

La France remercie le Royaume-Uni d'avoir inscrit un point sur les menaces hybrides à l'agenda et s'aligne sur les déclarations de l'UE et de l'OTAN, mais permettez-mois d'ajouter des remarques à titre national.

La France condamne avec la plus grande fermeté les cyber-attaques conduites sur son territoire par la Russie contre ses intérêts stratégiques.

Depuis plusieurs années, la France est la cible d'activités cyber malveillantes persistantes à des fins d'espionnage conduites par le 16e Centre du Service fédéral de sécurité russe (FSB), et plus particulièrement son unité 61240, chargée du ciblage de la France.

A l'appui du mode opératoire d'attaque (MOA) TURLA, le FSB a notamment visé des comptes de messagerie Internet du ministère des Armées depuis 2017, ainsi que le réseau du ministère de l'Europe et des Affaires étrangères à l'Ambassade de France à Moscou en 2018. En 2019, une compromission d'un serveur appartenant à une entité du secteur de la justice a été détectée. En février 2025, un institut de recherche sur les technologies sensibles travaillant pour l'industrie de défense française a également été visé par des cyberattaques conduites par le 16e Centre du FSB, conduisant à l'exfiltration d'un volume significatif de données.

Cette situation concerne aussi nombre de nos partenaires européens comme cela a été rappelé par l'Union européenne, au nom de ses 27 Etats membres. La France est directement impliquée dans des actions de solidarité européenne pour prévenir ou répondre à des incidents cyber, y compris liés aux activités de cet acteur spécifique.

Ces dernières années, la Russie n'a cessé d'intensifier ses actions cyber malveillantes, ciblant particulièrement l'Ukraine et ses soutiens. La Russie renforce ses propres capacités cyber-offensives, tout en s'appuyant, à des fins de déstabilisation, sur un écosystème diversifié d'acteurs non-étatiques, y compris des groupes soi-disant « hacktivistes ». Face à ces agissements, l'Union européenne a adopté ce 13 juillet un nouveau paquet de sanctions dans le cadre du régime cyber de l'UE à l'encontre de 9 individus et de 4 entités faisant partie de cet écosystème cyber malveillant, dont un groupe ayant revendiqué des actions de déstabilisation contre les Jeux de Paris en 2024.

Ces actions cyber sont l'une des dimensions de l'accroissement des menaces hybrides ciblant les États membres de l'Union européenne, dans le contexte de la guerre d'agression conduite par la Russie contre l'Ukraine : manipulations de l'information, ingérences dans les processus démocratiques, incursions aériennes et autres actions de déstabilisation.

Les activités cyber-malveillantes de la Russie sont inacceptables et indignes d'un membre permanent du Conseil de sécurité des Nations unies. Elles sont par ailleurs contraires aux principes du cadre normatif de comportement responsable des Etats dans le cyberespace des Nations unies auquel la Russie a souscrit. La France rappelle son attachement au cadre normatif porté par l'ONU et enjoint la Russie à respecter ses engagements en la matière.

Aux côtés de ses partenaires et dans le cadre du droit international, la France est résolue à employer l'ensemble des moyens à sa disposition pour anticiper, décourager et répondre aux actions déstabilisatrices qui la visent dans le cyberespace, y compris à l'approche des prochaines élections de 2027.

Les services techniques du Centre de coordination des crises cyber (C4) – regroupant l'Agence nationale de sécurité des systèmes d'information, la Direction générale de la sécurité extérieure, la Direction générale de la sécurité intérieure, la Direction générale de l'armement et le Commandement de la cyberdéfense – publient ce jour un rapport conjoint sur les activités cyber malveillantes conduites par la Russie contre des intérêts français avec le mode opératoire d'attaque TURLA, en s'appuyant sur des travaux d'imputation des cyberattaques conduits au sein du C4.

Enfin, je voudrais soutenir l'appel du Canada pour que l'OSCE joue un rôle actif pour lutter contre ces activités cyber malveillantes.

Je serais reconnaissante à la présidence de bien vouloir joindre cette déclaration au journal du jour./.