Official Journal
of the European Union

EN
L series

2026/2546

16.11.2026

COUNCIL DECISION (CFSP) 2026/2546

of 16 November 2026

amending Decision (CFSP) 2019/797 concerning restrictive measures against cyber-attacks threatening the Union or its Member States

THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on European Union and in particular Article 29 thereof,

Having regard to the proposal from the High Representative of the Union for Foreign Affairs and Security Policy,

Whereas:

(1) On 17 May 2019, the Council adopted Decision (CFSP) 2019/797 [1].

(2) As part of the sustained, tailored and coordinated Union action against persistent cyber threat actors, one entity should be added to the list of natural and legal persons, entities and bodies subject to restrictive measures set out in the Annex to Decision (CFSP) 2019/797. That entity is responsible for cyber-attacks with a significant effect which constitute an external threat to the Union or its Member States, as well as for cyber-attacks with a significant effect against third States.

(3) Decision (CFSP) 2019/797 should therefore be amended accordingly,

HAS ADOPTED THIS DECISION:

Article 1

The Annex to Decision (CFSP) 2019/797 is amended in accordance with the Annex to this Decision.

Article 2

This Decision shall enter into force on the date of its publication in the *Official Journal of the European Union*.

Done at Brussels, 16 November 2026.

For the Council

The President

K. KALLAS

[1] Council Decision (CFSP) 2019/797 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States (OJ L 129 I, 17.5.2019, p. 13, ELI: http://data.europa.eu/eli/dec/2019/797/oj).

ANNEX

In the Annex to Decision (CFSP) 2019/797, the following entry is added under the heading ‘B. Legal persons, entities and bodies’:

	Name	Identifying information	Reasons	Date of listing
‘12.	NoName057(16)	Aliases: 05716nnm, Nnm05716, NoName057, NoName05716	NoName057(16) is a pro-Russian hacker group that first emerged in March 2022 and claims responsibility for cyber-attacks on government bodies, critical infrastructure, and private companies of Ukraine, the United States of America and Member States. NoName057(16) uses the DDoSia toolkit, through which it conducts denial-of-service (DDoS) attacks by repeatedly issuing network requests to target websites. Following those attacks, the group claims responsibility for those attacks, addresses targets and issues threats on the dark web or through Telegram channels. NoName057(16) is engaged in cyber-attacks with a significant effect which constitute an external threat to the Union or its Member States. NoName057(16) has targeted services necessary for the maintenance of essential social and economic activities and critical state functions of Member States, including governmental portals, military intelligence services, political parties and candidates during electoral processes, the energy and industrial sector, transport infrastructure, water supply facilities, banks, financial institutions and online payment services, and national post offices. NoName057(16) is therefore responsible for cyber-attacks with a significant effect which constitute an external threat to Member States. NoName057(16) is also responsible for cyber-attacks with a significant effect against third States.	16.11.2026’