Council of the European Union

Brussels, 5 May 2026
(OR. en)

7281/26

LIMITE

CORLX 271
CFSP/PESC 388
CYBER 113
JAI 338
FIN 406

LEGISLATIVE ACTS AND OTHER INSTRUMENTS

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

COUNCIL DECISION (CFSP) 2026/…

of …

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) Decision (CFSP) 2019/797 applies until 18 May 2028.

(3) On the basis of a review of the Annex to Decision (CFSP) 2019/797, the application of the measures set out in Articles 4 and 5 of that Decision as regards the natural and legal persons, entities, and bodies listed in that Annex should be extended until 18 May 2027. Furthermore, the reasons for including four persons and one entity in the list of natural and legal persons, entities and bodies subject to restrictive measures should be updated.

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

HAS ADOPTED THIS DECISION:

[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 129I, 17.5.2019, p. 13, ELI: http://data.europa.eu/eli/dec/2019/797/oj).

Article 1

Decision (CFSP) 2019/797 is amended as follows:

(1) Article 10 is replaced by the following:

‘*Article 10*

This Decision shall apply until 18 May 2028 and shall be kept under constant review. The measures set out in Articles 4 and 5 shall apply as regards the natural and legal persons, entities and bodies listed in the Annex until 18 May 2027.’;

(2) the Annex is amended in accordance with the Annex to this Decision.

Article 2

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

Done at …, …

For the Council
The President

ANNEX

The Annex to Decision (CFSP) 2019/797 is amended as follows:

(1) under the heading ‘A. Natural Persons’, entries 1, 2, 13 and 14 are replaced by the following corresponding entries:

	Name	Identifying information	Reasons	Date of listing
‘1.	GAO Qiang	Date of birth: 4 October 1983 Place of birth: Shandong Province, China Address: Room 1102, Guanfu Mansion, 46 Xinkai Road, Hedong District, Tianjin, China Nationality: Chinese Gender: male	Gao Qiang is linked to the “APT10” (“Advanced Persistent Threat 10”) umbrella (a.k.a. “Red Apollo”, “CVNX”, “Stone Panda”, “MenuPass” and “Potassium”), and has been involved in “Operation Cloud Hopper”, a series of cyber-attacks with a significant effect originating from outside the Union and constituting an external threat to the Union or its Member States and of cyber-attacks with a significant effect against third States. “Operation Cloud Hopper” has targeted information systems of multinational companies in six continents, including companies located in the Union, and gained unauthorised access to commercially sensitive data, resulting in significant economic loss. Gao Qiang is associated with APT10 command and control infrastructure. Moreover, Huaying Haitai, a company used by APT10, and designated for providing support to and facilitating “Operation Cloud Hopper”, employed Gao Qiang. He is also associated with Zhang Shilong, who is linked to APT10 and who has also been employed by Huaying Haitai.	30.7.2020

	Name	Identifying information	Reasons	Date of listing
2.	ZHANG Shilong	Date of birth: 10 September 1981 Place of birth: China Address: Hedong, Yuyang Road No 121, Tianjin, China Nationality: Chinese Gender: male	Zhang Shilong is linked to the "APT10" ("Advanced Persistent Threat 10") umbrella (a.k.a. "Red Apollo", "CVNX", "Stone Panda", "MenuPass" and "Potassium"), and has been involved in "Operation Cloud Hopper", a series of cyber-attacks with a significant effect originating from outside the Union and constituting an external threat to the Union or its Member States and of cyber-attacks with a significant effect against third States. "Operation Cloud Hopper" has targeted information systems of multinational companies in six continents, including companies located in the Union, and gained unauthorised access to commercially sensitive data, resulting in significant economic loss. Zhang Shilong is associated with APT10, including through the malware he developed and tested in connection with the cyber-attacks carried out by APT10. Moreover, Huaying Haitai, a company used by APT10, and designated for providing support to and facilitating "Operation Cloud Hopper", employed Zhang Shilong. He is associated with Gao Qiang, who is linked to APT10 and who has also been employed by Huaying Haitai.	30.7.2020

	Name	Identifying information	Reasons	Date of listing
13.	Mikhail Mikhailovich TSAREV	Михаил Михайлович ЦАРЕВ Date of birth: 20.4.1989 Place of birth: Serpukhov, Russian Federation Nationality: Russian Address: Serpukhov Gender: male	Mikhail Mikhailovich Tsarev took part in cyberattacks with a significant effect, which constitute an external threat to EU Member States. Mikhail Mikhailovich Tsarev, also known by the online monikers “Mango”, “Alexander Grachev”, “Super Misha”, “Ivanov Mixail”, “Misha Krutysha”, and “Nikita Andreevich Tsarev” is a key-player in the deployment of the “Conti” and “Trickbot” malware programs and is involved in the Russia-based threat group “Wizard Spider”. Wizard Spider continues to evolve and intensify its operations. The Conti and Trickbot malware programs were created and developed by Wizard Spider. Wizard Spider has conducted ransomware campaigns in a variety of sectors, including essential services such as health and banking. The group has infected computers worldwide and their malware has been developed into a highly modular malware suite. Campaigns by Wizard Spider, using malware such as Conti, “Ryuk” TrickBot or Black Basta, are responsible for substantial economic damage in the European Union. Mikhail Mikhailovich Tsarev is therefore involved in cyberattacks with a significant effect, which constitute an external threat to the Union or its Member States.	24.6.2024

	Name	Identifying information	Reasons	Date of listing
14.	Maksim Sergeevich GALOCHKIN	Максим Сергеевич ГАЛОЧКИН Date of birth: 19.5.1982 Place of birth: Abakan, Russian Federation Nationality: Russian Gender: male	Maksim Galochkin took part in cyberattacks with a significant effect, which constitute an external threat to EU Member States. Maksim Galochkin is also known by the online monikers “Benalen”, “Bentley”, “Volhvb”, “volhvb”, “manuel”, “Max17” and “Crypt”. Galochkin is a key player in the deployment of the “Conti” and “Trickbot” malware programs and is involved in the Russia-based threat group “Wizard Spider”. He has led a group of testers, with responsibilities for the development, supervision, and implementation of tests for the TrickBot malware program, created and deployed by Wizard Spider. Wizard Spider continues to evolve and intensify its operations. Wizard Spider has conducted ransomware campaigns in a variety of sectors, including essential services such as health and banking. The group has infected computers worldwide and their malware has been developed into a highly modular malware suite. Campaigns by Wizard Spider, using malware such as Conti, “Ryuk” TrickBot or Black Basta, are responsible for substantial economic damage in the European Union. Maksim Galochkin is therefore involved in cyberattacks with a significant effect, which constitute an external threat to the Union or its Member States.	24.6.2024’;

(2) under the heading ‘B. Legal persons, entities and bodies’, entry 1 is replaced by the following:

	Name	Identifying information	Reasons	Date of listing
‘1.	Tianjin Huaying Haitai Science and Technology Development Co. Ltd (Huaying Haitai)	a.k.a.: Haitai Technology Development Co. Ltd Location: Tianjin, China	Huaying Haitai provided financial, technical or material support for and facilitated “Operation Cloud Hopper”, a series of cyber-attacks with a significant effect originating from outside the Union and constituting an external threat to the Union or its Member States and of cyber-attacks with a significant effect against third States. “Operation Cloud Hopper” has targeted information systems of multinational companies in six continents, including companies located in the Union, and gained unauthorised access to commercially sensitive data, resulting in significant economic loss. The actor publicly known as “APT10” (“Advanced Persistent Threat 10”) (a.k.a. “Red Apollo”, “CVNX”, “Stone Panda”, “MenuPass” and “Potassium”) carried out “Operation Cloud Hopper”. Huaying Haitai can be linked to APT10. Moreover, Huaying Haitai employed Gao Qiang and Zhang Shilong, who are both designated in connection with “Operation Cloud Hopper”. Huaying Haitai is therefore also associated with Gao Qiang and Zhang Shilong.	30.7.2020’.