



Council of the
European Union

**Brussels, 29 October 2020
(OR. en)**

12473/20

LIMITE

**CORLX 520
CFSP/PESC 935
CYBER 205
JAI 881
FIN 803**

PROPOSAL

From: High Representative of the Union for Foreign Affairs and Security Policy, signed by Ms. Helga SCHMID, Secretary General

date of receipt: 29 October 2020

To: Mr Jeppe TRANHOLM-MIKKELSEN, Secretary-General of the Council of the European Union

Subject: Proposal of the High Representative of the Union for Foreign Affairs and Security Policy to the Council for a Council Decision amending Decision (CFSP) 2019/797 concerning restrictive measures against cyber-attacks threatening the Union or its Member States

Delegations will find attached document HR(2020) 165.

Encl.: HR(2020) 165

HR(2020) 165
Limited

EUROPEAN EXTERNAL ACTION SERVICE



GREFFE

**Proposal of the High Representative of the Union for Foreign Affairs and Security
Policy to the Council**

of 29/10/2020

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

HR(2020) 165
Limited

HR(2020) 165

Limited

COUNCIL DECISION (CFSP) 2020/...

of [dd/mm/2020]

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 of 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) On 30 July 2020, the Council adopted Decision (CFSP) 2020/1127 ⁽²⁾, which added six natural persons and three entities or bodies to the list of natural and legal persons, entities and bodies subject to restrictive measures in the Annex to Decision (CFSP) 2019/797.
- (3) Updated information has been received for two listings.
- (4) The Annex to 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 day following that of its publication in the *Official Journal of the European Union*.

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).

² Council Decision (CFSP) 2020/1127 of 30 July 2020 amending Decision (CFSP) 2019/797 concerning restrictive measures against cyber-attacks threatening the Union or its Member States (OJ L 246, 30.7.2020, p. 12).

HR(2020) 165
Limited

Done at Brussels,

For the Council
The President

HR(2020) 165
Limited

ANNEX

In the Annex to Decision (CFSP) 2019/797, under the subheading ‘A. Natural Persons’, entries 1 and 2 are replaced by the following entries:

A. Natural persons

	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	<p>Gao Qiang is 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.</p> <p>“Operation Cloud Hopper” 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.</p> <p>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”.</p> <p>Gao Qiang can be linked to APT10, including through his association with APT10 command and control infrastructure. Moreover, Huaying Haitai, an entity designated for providing support to and facilitating “Operation Cloud Hopper”, employed Gao Qiang. He has links with Zhang Shilong, who is also designated in connection with “Operation Cloud Hopper”. Gao Qiang is therefore associated with both Huaying Haitai and Zhang Shilong</p>	30.7.2020

HR(2020) 165
Limited

2.	ZHANG Shilong	<p>Date of birth: 10 September 1981</p> <p>Place of birth: China</p> <p>Address: Hedong, Yuyang Road No 121, Tianjin, China</p> <p>Nationality: Chinese</p> <p>Gender: male</p>	<p>Zhang Shilong is 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.</p> <p>“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.</p> <p>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”.</p> <p>Zhang Shilong can be linked to APT10, including through the malware he developed and tested in connection with the cyber-attacks carried out by APT10. Moreover, Huaying Haitai, an entity designated for providing support to and facilitating “Operation Cloud Hopper”, employed Zhang Shilong. He has links with Gao Qiang, who is also designated in connection with “Operation Cloud Hopper”. Zhang Shilong is therefore associated with both Huaying Haitai and Gao Qiang.</p>	30. 30.7.2020’