



Council of the
European Union

Brussels, 10 November 2020
(OR. en)

12476/20

LIMITE

CORLX 523
CFSP/PESC 938
RELEX 838
CYBER 208
JAI 884
FIN 806

LEGISLATIVE ACTS AND OTHER INSTRUMENTS

Subject: COUNCIL IMPLEMENTING REGULATION implementing Regulation (EU) 2019/796 concerning restrictive measures against cyber-attacks threatening the Union or its Member States

COUNCIL IMPLEMENTING REGULATION (EU) 2020/...

of ...

**implementing Regulation (EU) 2019/796
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 the Functioning of the European Union,

Having regard to Council Regulation (EU) 2019/796 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States¹, and in particular Article 13(1) thereof,

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

¹ OJ L 129I, 17.5.2019, p. 1.

Whereas:

- (1) On 17 May 2019 the Council adopted Regulation (EU) 2019/796.
- (2) On 30 July 2020 the Council adopted implementing Regulation (EU) 2020/1125¹, 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 set out in Annex I to Regulation (EU) 2019/796.
- (3) Updated information has been received for two listings of natural persons.
- (4) Regulation (EU) 2019/796 should therefore be amended accordingly,

HAS ADOPTED THIS REGULATION:

¹ Council Implementing Regulation (EU) 2020/1125 of 30 July 2020 implementing Regulation (EU) 2019/796 concerning restrictive measures against cyber-attacks threatening the Union or its Member States (OJ L 246, 30.7.2020, p. 4).

Article 1

Annex I to Regulation (EU) 2019/796 is amended in accordance with the Annex to this Regulation.

Article 2

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

This Regulation shall be binding in its entirety and directly applicable in all Member States.

Done at ...,

For the Council

The President

ANNEX

In Annex I to Regulation (EU) 2019/796, under the subheading 'A. Natural Persons', entries 1 and 2 are replaced by the following 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 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. 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".	30.7.2020

	Name	Identifying information	Reasons	Date of listing
			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.	
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 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.	30.7.2020'

	Name	Identifying information	Reasons	Date of listing
			<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>	
