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

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

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 States[(1)], 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,

Whereas:

(1) On 17 May 2019 the Council adopted Regulation (EU) 2019/796.

(2) Targeted restrictive measures against cyber-attacks with a significant effect which constitute an external threat to the Union or its Member States are among the measures included in the Union's framework for a joint diplomatic response to malicious cyber-activities (the cyber diplomacy toolbox) and are a vital instrument to deter and respond to such activities. Restrictive measures can also be applied in response to cyber-attacks with a significant effect against third States or international organisations, where deemed necessary to achieve common foreign and security policy objectives set out in the relevant provisions of Article 21 of the Treaty on European Union.

(3) On 16 April 2018 the Council adopted conclusions in which it firmly condemned the malicious use of information and communications technologies, including in the cyber-attacks publicly known as 'WannaCry' and 'NotPetya', which caused significant damage and economic loss in the Union and beyond. On 4 October 2018 the Presidents of the European Council and of the European Commission and the High Representative of the Union for Foreign Affairs and Security Policy (the 'High Representative') expressed serious concerns in a joint statement about an attempted cyber-attack to undermine the integrity of the Organisation for the Prohibition of Chemical Weapons (OPCW) in the Netherlands, an aggressive act which demonstrated contempt for the solemn purpose of the OPCW. In a declaration made on behalf of the Union on 12 April 2019, the High Representative urged actors to stop undertaking malicious cyber-activities that aim to undermine the Union's integrity, security and economic competiveness, including acts of cyber-enabled theft of intellectual property.

Such cyber-enabled thefts include those carried out by the actor publicly known as 'APT10' ('Advanced Persistent Threat 10').

(4) In this context, and to prevent, discourage, deter and respond to continuing and increasing malicious behaviour in cyberspace, six natural persons and three entities or bodies should be included in the list of natural and legal persons, entities and bodies subject to restrictive measures set out in Annex I to Regulation (EU) 2019/796. Those persons and entities or bodies are responsible for, provided support for or were involved in, or facilitated cyber-attacks or attempted cyber-attacks, including the attempted cyber-attack against the OPCW and the cyber-attacks publicly known as 'WannaCry' and 'NotPetya', as well as 'Operation Cloud Hopper'.

(5) Regulation (EU) 2019/796 should therefore be amended accordingly,

HAS ADOPTED THIS REGULATION:

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 date 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 Brussels, 30 July 2020.

For the Council

The President

M. ROTH

***Changes to legislation:** There are currently no known outstanding effects for the Council Implementing Regulation (EU) 2020/1125. (See end of Document for details)*

ANNEX

The following persons and entities or bodies are added to the list of natural and legal persons, entities and bodies set out in Annex I to Regulation (EU) 2019/796:

A. Natural persons

	Name	**Identifying information**	**Reasons**	**Date of listing**
1.	GAO Qiang	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" 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
			The actor publicly known as "APT10" ("Advanced	

Changes to legislation: *There are currently no known outstanding effects for the Council Implementing Regulation (EU) 2020/1125. (See end of Document for details)*

			Persistent Threat 10") (a.k.a. "Red Apollo", "CVNX", "Stone Panda", "MenuPass" and "Potassium") carried out "Operation Cloud Hopper". 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	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	30.7.2020

***Changes to legislation:** There are currently no known outstanding effects for the Council Implementing Regulation (EU) 2020/1125. (See end of Document for details)*

			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”.	
			Zhang Shilong can be linked to APT10, including through the malware he developed and tested in	