Official Journal
of the European Union

EN
L series

2026/589

16.3.2026

COUNCIL IMPLEMENTING REGULATION (EU) 2026/589

of 16 March 2026

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) As part of the sustained, tailored and coordinated Union action against persistent cyber threat actors, two natural persons and three entities 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 natural persons and entities are responsible for, or involved in, cyber-attacks with a significant effect which constitute an external threat to the Union or its Member States.

(3) Annex I to 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, 16 March 2026.

For the Council

The President

K. KALLAS

[1] OJ L 129 I, 17.5.2019, p. 1, ELI: http://data.europa.eu/eli/reg/2019/796/oj.

ANNEX

Annex I to Regulation (EU) 2019/796 is amended as follows:

(1) the following entries are added under the heading ‘A. Natural persons’:

	Name	Identifying information	Reasons	Date of listing
‘18.	CHEN Cheng	陈诚 (Chinese spelling) Aliases: Jesse Chen lengmo l3n6m0 Date of birth: 20.10.1984 Place of birth: Yancheng, Jiangsu, China Nationality: Chinese Gender: male	Chen Cheng is a Chinese businessman, co-founder and one of the general managers (Chief Operating Officer) of Anxun Information Technology Co. Ltd. He is also a legal representative of the Sichuan branch of that company. Anxun Information Technology Co. Ltd., also known as i-Soon, is a company based in the People’s Republic of China (PRC) that offers “hacking-for-hire” services. Anxun Information Technology Co. Ltd. has targeted critical infrastructure and critical State functions of Member States and accessed and sold classified information. Furthermore, Anxun Information Technology Co. Ltd. has attacked governments of various third States, thereby posing a threat to the common foreign and security policy (CFSP) objectives of the Union, as set out in Article 21(2), points (a) to (c), of the Treaty on European Union. Anxun Information Technology Co. Ltd. gains an important economic benefit from the services provided. Anxun Information Technology Co. Ltd. is therefore responsible for cyber-attacks with a significant effect which constitute an external threat to the Union and its Member States as well as attacks against third States. In this capacity, Chen Cheng is responsible for, and involved in, cyber-attacks with a significant effect which constitute an external threat to Member States as well as cyber-attacks with a significant effect against third States.	16.3.2026

	Name	Identifying information	Reasons	Date of listing
19.	WU Haibo	吴海波 (Chinese spelling) Aliases: shutdown shutd0wn POB: China Nationality: Chinese Gender: male	Wu Haibo is a Chinese businessman, co-founder and one of the general managers (Chief Executive Officer) of Anxun Information Technology Co. Ltd. He is also the legal representative, chairman and general manager of the Shanghai branch ("mothership") of Anxun Information Technology Co. Ltd. Furthermore, he is acting as the legal representative of the Sichuan branch of that company. Anxun Information Technology Co. Ltd., also known as i-Soon, is a company based in the People's Republic of China (PRC) that offers "hacking-for-hire" services. Anxun Information Technology Co. Ltd. has targeted critical infrastructure and critical State functions of Member States and accessed and sold classified information. Furthermore, Anxun Information Technology Co. Ltd. has attacked governments of various third States, thereby posing a threat to the common foreign and security policy (CFSP) objectives of the Union, as set out in Article 21(2), points (a) to (c), of the Treaty on European Union. Anxun Information Technology Co. Ltd. gains an important economic benefit from the services provided. Anxun Information Technology Co. Ltd. is therefore responsible for cyber-attacks with a significant effect which constitute an external threat to Member States as well as attacks against third States. Wu Haibo was involved in directing and encouraging attempted cyber-attacks with a significant effect against Member States. In this capacity, he is responsible for, and involved in, cyber-attacks with a significant effect which constitute an external threat to Member States as well as cyber-attacks with a significant effect against third States.	16.3.2026';

(2) the following entries are added under the heading ‘B. Legal persons, entities and bodies’:

	Name	Identifying information	Reasons	Date of listing
‘5.	Integrity Technology Group	永信至诚科技集团股份有限公司 (Chinese spelling) Alias: Beijing Integrity Technology Company Limited, Yongxin Zhicheng Technology Group Company Limited Address: Fenghao East Road, Room 103, Building6, No. 9, Beijing Haidian District, China Place of registration: Beijing, China Date of registration: 2.9.2010 Unified Social Credit Code: 91110108562135265P	Integrity Technology Group is a cybersecurity enterprise, based in the People’s Republic of China (PRC), that facilitated cyber-attacks linked to Advanced Persistent Threat (APT) Flax Typhoon. That APT used Integrity Technology Group’s products and technology to deploy its computer network exploitation activities. Integrity Technology Group’s products have been used since then to compromise and access Internet of Things devices in Member States, as well as in countries across Europe and globally. Between 2022 and 2023, Flax Typhoon accessed at least 65 600 Internet of Things devices in six Member States by using Integrity Technology Group’s products. Therefore, Integrity Technology Group’s commercial products and infrastructure were routinely used in cyber-attacks against Member States as well as third States. Consequently, by affecting information systems relating to digital infrastructure, Integrity Technology Group is providing technical and material support for cyber-attacks with a significant effect which constitute an external threat to Member States and third States.	16.3.2026

	Name	Identifying information	Reasons	Date of listing
6.	Emennet Pasargad	Alias: Anzu Team, Holy Souls, Aria Sepehr Ayandehsazan, Haywire Kitten Place of registration: Tehran, Iran Registration number: 554267 Principal place of business: Tehran, Iran	Emennet Pasargad is an Iranian cyber actor (company) that has targeted numerous entities, in particular, in Member States as well as in the United States (US). Emennet Pasargad, operating under the alias "Anzu Team", targeted digital infrastructure in Sweden and compromised a Swedish SMS service, affecting a large number of people. Furthermore, by acting under the alias "Holy Souls", the entity compromised the subscriber database of the French satirical magazine, Charlie Hebdo, and advertised it for sale on the dark web. Emennet Pasargad compromised advertising billboards during the Paris Olympic Games and displayed disinformation campaigns. Emennet Pasargad also attempted to interfere with the US presidential elections of 2020, threatening democracy and the rule of law, by obtaining confidential US voter information and gaining unauthorised access to a US media company's computer network. Emennet Pasargad is therefore responsible for cyber-attacks with a significant effect which constitute an external threat to Member States and for cyber-attacks with a significant effect against a third State.	16.3.2026

	Name	Identifying information	Reasons	Date of listing
7.	Anxun Information Technology Co. Ltd.	安洵信息技术有限公司 (Chinese spelling) Alias: i-Soon Address: Room 1002, Qiangqiang Building, No. 1318 Qixin Road, Minhang District, Shanghai Unified Social Credit Code: 91510105332025597A (Sichuan branch) Unified Social Credit Code: 91310116561906136G (Shanghai branch) Website: i-soon.net, isoon.net, i-soon.com.cn, isoonren.com, isoon.win Phone numbers: +862161119992, +8605645893417, +8613761671735, +864000665915 Email: shutdown@163.com, isoon2015@126.com, tao_tingting@i-soon.net, li_ping@i-soon.net	Anxun Information Technology Co. Ltd. is a company based in the People's Republic of China that offers "hacking-for-hire" services. It has targeted critical infrastructure and critical State functions of Member States and accessed and sold classified information. Furthermore, Anxun Information Technology Co. Ltd. has attacked governments of various third States, thereby posing a threat to the common foreign and security policy (CFSP) objectives of the Union, as set out in Article 21(2), points (a) to (c), of the Treaty on European Union. Anxun Information Technology Co. Ltd. gains an important economic benefit from the services provided. Anxun Information Technology Co. Ltd. is therefore responsible for cyber-attacks with a significant effect which constitute an external threat to Member States as well as for cyber-attacks with a significant effect against third States.	16.3.2026'.