Official Journal
of the European Union

EN
L series

2025/173

27.1.2025

COUNCIL IMPLEMENTING REGULATION (EU) 2025/173

of 27 January 2025

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 one of the measures included in the Union's framework for a joint diplomatic response to malicious cyber activities, namely the Cyber Diplomacy Toolbox, and are a vital instrument to prevent, deter, discourage and respond to such activities.

(3) Malicious cyber activities against critical infrastructure or essential services, including through the use of ransomware and wipers, the targeting of supply chains and cyber-espionage, including intellectual property theft activities, are increasing in number, frequency and sophistication. With their disruptive and destructive effects, those activities pose a systemic threat to the Union's security, economy and democracy and to society at large.

(4) In 2020, cyber-attacks with a significant effect were carried out against Estonia. Cyber-attacks targeting the computer systems of multiple institutions were conducted with the aim of using the data to threaten the security of Estonia. Those cyber-attacks concerned the storage of classified information.

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

(6) 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, 27 January 2025.

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

In Annex I to Regulation (EU) 2019/796, the following entries are added under the heading ‘A. Natural persons’:

	Name	Identifying information	Reasons	Date of listing
‘15.	Nikolay Alexandrovich KORCHAGIN	Николай Александрович Корчагин Date of birth: 16.9.1997 Nationality: Russian Gender: male Associated entity: Main Directorate of the General Staff of the Armed Forces of the Russian Federation	Nikolay Korchagin is involved in and responsible for cyber-attacks with a significant effect by conducting intelligence activities directed against Estonia and gaining access to a computer system illegally. Nikolay Korchagin is an officer of military unit 29155 of the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GRU). In that role, he is involved in and responsible for cyber-attacks against computer systems with the aim of collecting data from the data systems of multiple institutions, which independently or in combination, give an overview of the cyber security policy of Estonia, the cyber capabilities of the state, sensitive personal data and other sensitive data, with the aim of using the data to threaten the security of Estonia. The attacks therefore concern the storage of classified information. The attacks concerned allies and partners of Estonia. Therefore, Nikolay Korchagin is involved in and responsible for cyber-attacks with a significant effect which constitute an external threat to a Member State.	27.1.2025
16.	Vitaly SHEVCHENKO	Виталий Шевченко Date of birth: 1.9.1997 Nationality: Russian Gender: male Associated entity: Main Directorate of the General Staff of the Armed Forces of the Russian Federation	Vitaly Shevchenko is involved in and responsible for cyber-attacks with a significant effect by conducting intelligence activities directed against Estonia and gaining access to a computer system illegally. Vitaly Shevchenko is an officer of military unit 29155 of the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GRU). In that role, he is involved in and responsible for cyber-attacks against computer systems with the aim of collecting data from the data systems of multiple institutions, which independently or in combination, give an overview of the cyber security policy of Estonia, the cyber capabilities of the state, sensitive personal data and other sensitive data, with the aim of using the data to threaten the security of Estonia. The attacks therefore concern the storage of classified information. The attacks concerned allies and partners of Estonia. Therefore, Vitaly Shevchenko is involved in and responsible for cyber-attacks with a significant effect which constitute an external threat to a Member State.	27.1.2025

ELI: http://data.europa.eu/eli/reg_impl/2025/173/oj

	Name	Identifying information	Reasons	Date of listing
17.	Yuriy Fedorovich DENISOV	Юрий Федорович Денисов Date of birth: 17.6.1980 Nationality: Russian Gender: male Associated entity: Main Directorate of the General Staff of the Armed Forces of the Russian Federation	Yuriy Denisov is involved in and responsible for cyber-attacks with a significant effect by conducting intelligence activities directed against Estonia and gaining access to a computer system illegally. Yuriy Denisov is an officer of military unit 29155 of the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GRU). In that role, he is involved in and responsible for cyber-attacks against computer systems with the aim of collecting data from the data systems of multiple institutions, which independently or in combination, give an overview of the cyber security policy of Estonia, the cyber capabilities of the state, sensitive personal data and other sensitive data, with the aim of using the data to threaten the security of Estonia. The attacks therefore concern the storage of classified information. The attacks concerned allies and partners of Estonia. Therefore, Yuriy Denisov is involved in and responsible for cyber-attacks with a significant effect which constitute an external threat to a Member State.	27.1.2025’