2025/887

13.5.2025

COUNCIL DECISION (CFSP) 2025/887

of 12 May 2025

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 from 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) Decision (CFSP) 2019/797 applies until 18 May 2025. On the basis of a review of that Decision, the Council considers that its application should be extended until 18 May 2028.

(3) On the basis of a review of the Annex to Decision (CFSP) 2019/797, the application of the measures set out in Articles 4 and 5 of that Decision as regards the natural and legal persons, entities and bodies listed in that Annex should be extended until 18 May 2026. Furthermore, the reasons for including six persons in the list of natural and legal persons, entities and bodies subject to restrictive measures should be updated.

(4) Decision (CFSP) 2019/797 should therefore be amended accordingly,

HAS ADOPTED THIS DECISION:

Article 1

Decision (CFSP) 2019/797 is amended as follows:

(1) Article 10 is replaced by the following:

'*Article 10*

This Decision shall apply until 18 May 2028 and shall be kept under constant review. The measures set out in Articles 4 and 5 shall apply as regards the natural and legal persons, entities and bodies listed in the Annex until 18 May 2026.';

(2) the Annex is amended in accordance with the Annex to this Decision.

Article 2

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

Done at Brussels, 12 May 2025.

For the Council

The President

B. NOWACKA

[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, ELI: http://data.europa.eu/eli/dec/2019/797/oj).

ANNEX

In the Annex to Decision (CFSP) 2019/797, under the heading ‘A. Natural persons’, entries 3 to 8 are replaced by the following:

	Name	Identifying information	Reasons	Date of listing
‘3.	Alexey Valeryevich MININ	Алексей Валерьевич МИНИН Date of birth: 27.5.1972 Place of birth: Perm Oblast, Russian SFSR (now Russian Federation) Passport number: 120017582 Issued by: Ministry of Foreign Affairs of the Russian Federation Validity: from 17.4.2017 until 17.4.2022 Location: Moscow, Russian Federation Nationality: Russian Gender: male	Alexey Minin took part in an attempted cyber-attack with a potentially significant effect against the Organisation for the Prohibition of Chemical Weapons (OPCW) in the Netherlands and in cyber-attacks with a significant effect against third States. As a human intelligence support officer of the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GU/GRU), Alexey Minin was part of a team of four Russian military intelligence officers who attempted to gain unauthorised access to the Wi-Fi network of the OPCW in The Hague, the Netherlands, in April 2018. The attempted cyber-attack was aimed at hacking into the Wi-Fi network of the OPCW, which, if successful, would have compromised the security of the network and the OPCW’s ongoing investigatory work. The Netherlands Defence Intelligence and Security Service (Militaire Inlichtingen- en Veiligheidsdienst) disrupted the attempted cyber-attack, thereby preventing serious damage to the OPCW. A grand jury in the Western District of Pennsylvania (United States of America) has indicted Alexey Minin, as an officer of the GRU, for computer hacking, wire fraud, aggravated identity theft and money laundering. The GRU remains active in carrying out cyber-attacks against the Union or its Member States. As a member of the GRU, Alexey Minin is therefore involved in cyber-attacks with a significant effect, including attempted cyber-attacks with a potentially significant effect, which constitute an external threat to the Union or its Member States.	30.7.2020

	Name	Identifying information	Reasons	Date of listing
4.	Aleksei Sergeyvich MORENETS	Алексей Сергеевич МОРЕНЕЦ Date of birth: 31.7.1977 Place of birth: Murmanskaya Oblast, Russian SFSR (now Russian Federation) Passport number: 100135556 Issued by: Ministry of Foreign Affairs of the Russian Federation Validity: from 17.4.2017 until 17.4.2022 Location: Moscow, Russian Federation Nationality: Russian Gender: male	Aleksei Morenets took part in an attempted cyber-attack with a potentially significant effect against the Organisation for the Prohibition of Chemical Weapons (OPCW) in the Netherlands and in cyber-attacks with a significant effect against third States. As a cyber-operator for the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GU/GRU), Aleksei Morenets was part of a team of four Russian military intelligence officers who attempted to gain unauthorised access to the Wi-Fi network of the OPCW in The Hague, the Netherlands, in April 2018. The attempted cyber-attack was aimed at hacking into the Wi-Fi network of the OPCW, which, if successful, would have compromised the security of the network and the OPCW's ongoing investigatory work. The Netherlands Defence Intelligence and Security Service (Militaire Inlichtingen- en Veiligheidsdienst) disrupted the attempted cyber-attack, thereby preventing serious damage to the OPCW. A grand jury in the Western District of Pennsylvania (United States of America) has indicted Aleksei Morenets, as assigned to Military Unit 26165, for computer hacking, wire fraud, aggravated identity theft and money laundering. The GRU remains active in carrying out cyber-attacks against the Union or its Member States. As a member of the GRU, Aleksei Morenets is therefore involved in cyber-attacks with a significant effect, including attempted cyber-attacks with a potentially significant effect, which constitute an external threat to the Union or its Member States.	30.7.2020

	Name	Identifying information	Reasons	Date of listing
5.	Evgenii Mikhaylovich SEREBRIAKOV	Евгений Михайлович СЕРЕБРЯКОВ Date of birth: 26.7.1981 Place of birth: Kursk, Russian SFSR (now Russian Federation) Passport number: 100135555 Issued by: Ministry of Foreign Affairs of the Russian Federation Validity: from 17.4.2017 until 17.4.2022 Location: Moscow, Russian Federation Nationality: Russian Gender: male	Evgenii Serebriakov took part in an attempted cyber-attack with a potentially significant effect against the Organisation for the Prohibition of Chemical Weapons (OPCW) in the Netherlands and in cyber-attacks with a significant effect against third States. As a cyber-operator for the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GU/GRU), Evgenii Serebriakov was part of a team of four Russian military intelligence officers who attempted to gain unauthorised access to the Wi-Fi network of the OPCW in The Hague, the Netherlands, in April 2018. The attempted cyber-attack was aimed at hacking into the Wi-Fi network of the OPCW, which, if successful, would have compromised the security of the network and the OPCW's ongoing investigatory work. The Netherlands Defence Intelligence and Security Service (Militaire Inlichtingen- en Veiligheidsdienst) disrupted the attempted cyber-attack, thereby preventing serious damage to the OPCW. Since spring 2022, Evgenii Serebriakov is leading "Sandworm" (a.k.a. "Sandworm Team", "BlackEnergy Group", "Voodoo Bear", "Quedagh", "Olympic Destroyer" and "Telebots"), an actor and hacking group affiliated with Unit 74455 of the Russian Main Intelligence Directorate. Sandworm has carried out cyber-attacks on Ukraine, including Ukrainian government agencies, following Russia's war of aggression against Ukraine. The GRU remains active in carrying out cyber-attacks against the Union or its Member States. As a member of the GRU, Evgenii Serebriakov is therefore involved in cyber-attacks with a significant effect, including attempted cyber-attacks with a potentially significant effect, which constitute an external threat to the Union or its Member States.	30.7.2020

	Name	Identifying information	Reasons	Date of listing
6.	Oleg Mikhaylovich SOTNIKOV	Олег Михайлович СОТНИКОВ Date of birth: 24.8.1972 Place of birth: Ulyanovsk, Russian SFSR (now Russian Federation) Passport number: 120018866 Issued by: Ministry of Foreign Affairs of the Russian Federation Validity: from 17.4.2017 until 17.4.2022 Location: Moscow, Russian Federation Nationality: Russian Gender: male	Oleg Sotnikov took part in an attempted cyber-attack with a potentially significant effect against the Organisation for the Prohibition of Chemical Weapons (OPCW) in the Netherlands and in cyber-attacks with a significant effect against third States. As a human intelligence support officer of the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GU/GRU), Oleg Sotnikov was part of a team of four Russian military intelligence officers who attempted to gain unauthorised access to the Wi-Fi network of the OPCW in The Hague, the Netherlands, in April 2018. The attempted cyber-attack was aimed at hacking into the Wi-Fi network of the OPCW, which, if successful, would have compromised the security of the network and the OPCW's ongoing investigatory work. The Netherlands Defence Intelligence and Security Service (Militaire Inlichtingen- en Veiligheidsdienst) disrupted the attempted cyber-attack, thereby preventing serious damage to the OPCW. A grand jury in the Western District of Pennsylvania (United States of America) has indicted Oleg Sotnikov, as an officer of the GRU, for computer hacking, wire fraud, aggravated identity theft and money laundering. The GRU remains active in carrying out cyber-attacks against the Union or its Member States. As a member of the GRU, Oleg Sotnikov is therefore involved in cyber-attacks with a significant effect, including attempted cyber-attacks with a potentially significant effect, which constitute an external threat to the Union or its Member States.	30.7.2020

	Name	Identifying information	Reasons	Date of listing
7.	Dmitry Sergeyevich BADIN	Дмитрий Сергеевич БАДИН Date of birth: 15.11.1990 Place of birth: Kursk, Russian SFSR (now Russian Federation) Nationality: Russian Gender: male	Dmitry Badin took part in a cyber-attack with a significant effect against the German federal parliament (Deutscher Bundestag) and in cyber-attacks with a significant effect against third States. As a military intelligence officer of the 85th Main Centre for Special Services (GTsSS) of the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GU/GRU), Dmitry Badin was part of a team of Russian military intelligence officers who conducted a cyber-attack against the German federal parliament in April and May 2015. That cyber-attack targeted the parliament's information system and affected its operation for several days. A significant amount of data was stolen and the email accounts of several MPs, as well as of former Chancellor Angela Merkel, were affected. A grand jury in the Western District of Pennsylvania (United States of America) has indicted Dmitry Badin, as assigned to Military Unit 26165, for computer hacking, wire fraud, aggravated identity theft and money laundering. The GRU remains active in carrying out cyber-attacks against the Union or its Member States. As a member of the GRU, Dmitry Badin is therefore involved in cyber-attacks with a significant effect, including attempted cyber-attacks with a potentially significant effect, which constitute an external threat to the Union or its Member States.	22.10.2020

ELI: http://data.europa.eu/eli/dec/2025/887/oj

	Name	Identifying information	Reasons	Date of listing
8.	Igor Olegovich KOSTYUKOV	Игорь Олегович КОСТЮКОВ Date of birth: 21.2.1961 Nationality: Russian Gender: male	Igor Kostyukov is the current Head of the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GU/GRU), where he previously served as First Deputy Head. One of the units under his command is the 85th Main Centre for Special Services (GTsSS) (a.k.a. "Military Unit 26165", "APT28", "Fancy Bear", "Sofacy Group", "Pawn Storm" and "Strontium"). In this capacity, Igor Kostyukov is responsible for cyber-attacks carried out by the GTsSS, including those with a significant effect constituting an external threat to the Union or its Member States. In particular, military intelligence officers of the GTsSS took part in the cyber-attack against the German federal parliament (Deutscher Bundestag) in April and May 2015 and the attempted cyber-attack aimed at hacking into the Wi-Fi network of the Organisation for the Prohibition of Chemical Weapons (OPCW) in the Netherlands in April 2018. The cyber-attack against the German federal parliament targeted the parliament's information system and affected its operation for several days. A significant amount of data was stolen and email accounts of several MPs, as well as of former Chancellor Angela Merkel, were affected. The GRU remains active in carrying out cyberattacks against the Union or its Member States. As a member of the GRU, Igor Kostyukov is therefore involved in cyber-attacks with a significant effect, including attempted cyber-attacks with a potentially significant effect, which constitute an external threat to the Union or its Member States.	22.10.2020'