Council of the European Union

Brussels, 5 May 2025
(OR. en)

6991/25

LIMITE

CORLX 301
CFSP/PESC 431
RELEX 319
CYBER 71
JAI 304
FIN 292

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) 2025/…

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 States[1], and in particular Article 13 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, ELI: http://data.europa.eu/eli/reg/2019/796/oj.

Whereas:

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

(2) The Council has reviewed the list of natural and legal persons, entities and bodies in Annex I to Regulation (EU) 2019/796. On the basis of that review, the reasons for including six persons in the list of natural and legal persons, entities and bodies subject to restrictive measures should be updated.

(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 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 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	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.	30.7.2020

	Name	Identifying information	Reasons	Date of listing
		Location: Moscow, Russian Federation Nationality: Russian Gender: male	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.	

	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	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.	30.7.2020

	Name	Identifying information	Reasons	Date of listing
		Location: Moscow, Russian Federation Nationality: Russian Gender: male	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.	

	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.	30.7.2020

	Name	Identifying information	Reasons	Date of listing
			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.	

	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.	30.7.2020

	Name	Identifying information	Reasons	Date of listing
			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.	

	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

	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.	22.10.2020'

	Name	Identifying information	Reasons	Date of listing
			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.	