Council of the
European Union

Brussels, 13 May 2024
(OR. en)

8502/24

LIMITE

CORLX 356
CFSP/PESC 512
RELEX 467
CYBER 110
JAI 572
FIN 341

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) 2024/…

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(1) thereof,

Having regard to the proposal from the High Representative of the Union for Foreign Affairs and Security Policy,

[1] OJ L 129 I, 17.5.2019, p. 1.

Whereas:

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

(2) In the light of continuing and increasing malicious behaviour in cyberspace, including behaviour directed against third States, the reasons for including six persons and two entities 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 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

Annex I to Regulation (EU) 2019/796 (‘List of natural and legal persons, entities and bodies referred to in Article 3’) is amended as follows:

(1) in the list headed ‘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 Russian Main Intelligence Directorate (GRU), for computer hacking, wire fraud, aggravated identity theft and money laundering.	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.	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.	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 has indicted Oleg Sotnikov, as an officer of the Russian Main Intelligence Directorate (GRU), for computer hacking, wire fraud, aggravated identity theft and money laundering.	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.	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. 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.	22.10.2020';

(2) in the list headed ‘B. Legal persons, entities and bodies’, entries 3 and 4 are replaced by the following:

	Name	Identifying information	Reasons	Date of listing
‘3.	Main Centre for Special Technologies (GTsST) of the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GU/GRU)	Address: 22 Kirova Street, Moscow, Russian Federation	The Main Centre for Special Technologies (GTsST) of the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GU/GRU), also known by its field post number 74455, is involved in cyber-attacks with a significant effect originating from outside the Union and constituting an external threat to the Union or its Member States and in cyber-attacks with a significant effect against third States, including the cyber-attacks publicly known as “NotPetya” or “EternalPetya” in June 2017 and the cyber-attacks directed at a Ukrainian power grid in the winter of 2015 and 2016. “NotPetya” or “EternalPetya” rendered data inaccessible in a number of companies in the Union, wider Europe and worldwide, by targeting computers with ransomware and blocking access to data, resulting amongst others in significant economic loss. The cyber-attack on a Ukrainian power grid resulted in parts of it being switched off during winter.	30.7.2020

	Name	Identifying information	Reasons	Date of listing
			The actor publicly known as “Sandworm” (a.k.a. “Sandworm Team”, “BlackEnergy Group”, “Voodoo Bear”, “Quedagh”, “Olympic Destroyer” and “Telebots”), which is also behind the attack on the Ukrainian power grid, carried out “NotPetya” or “EternalPetya”. Sandworm has carried out cyber-attacks against Ukraine, including Ukrainian government agencies and Ukrainian critical infrastructure, following Russia’s war of aggression against Ukraine. Those cyber-attacks include spear-phishing campaigns, malware and ransomware attacks. The Main Centre for Special Technologies of the Main Directorate of the General Staff of the Armed Forces of the Russian Federation has an active role in the cyber-activities undertaken by Sandworm and can be linked to Sandworm.	

	Name	Identifying information	Reasons	Date of listing
4.	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)	Address: Komsomol'skiy Prospekt, 20, Moscow, 119146, Russian Federation	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) (a.k.a. "Military Unit 26165", "APT28", "Fancy Bear", "Sofacy Group", "Pawn Storm" and "Strontium") is involved in cyber-attacks with a significant effect constituting an external threat to the Union or its Member States and in cyber-attacks with a significant effect against third 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. Following Russia's war of aggression against Ukraine, cyber-attacks by the GTsSS (spear-phishing and malware-based attacks) were carried out against Ukraine.	22.10.2020'.