Raad van de
Europese Unie

Brussel, 13 mei 2024
(OR. en)

8500/24

LIMITE

CORLX 354
CFSP/PESC 510
CYBER 108
JAI 570
FIN 339

WETGEVINGSBESLUITEN EN ANDERE INSTRUMENTEN

Betreft:	BESLUIT VAN DE RAAD tot wijziging van Besluit (GBVB) 2019/797 betreffende beperkende maatregelen tegen cyberaanvallen die de Unie of haar lidstaten bedreigen

BESLUIT (GBVB) 2024/… VAN DE RAAD

van …

tot wijziging van Besluit (GBVB) 2019/797 betreffende beperkende maatregelen tegen cyberaanvallen die de Unie of haar lidstaten bedreigen

DE RAAD VAN DE EUROPESE UNIE,

Gezien het Verdrag betreffende de Europese Unie, en met name artikel 29,

Gezien het voorstel van de hoge vertegenwoordiger van de Unie voor buitenlandse zaken en veiligheidsbeleid,

Overwegende hetgeen volgt:

(1) De Raad heeft op 17 mei 2019 Besluit (GBVB) 2019/797[1] vastgesteld.

(2) Besluit (GBVB) 2019/797 is van toepassing tot en met 18 mei 2025. Op basis van een evaluatie van dat besluit moet de geldigheid van de daarin opgenomen beperkende maatregelen tot die datum worden verlengd.

(3) Gezien de aanhoudende en toenemende kwaadwillige cyberactiviteiten, waaronder activiteiten gericht tegen derde landen, moet de motivering voor het opnemen van zes personen en twee entiteiten in de lijst van aan beperkende maatregelen onderworpen natuurlijke en rechtspersonen, entiteiten en lichamen in de bijlage bij Verordening (EU) 2019/797, worden geactualiseerd.

(4) Besluit (GBVB) 2019/797 moet daarom dienovereenkomstig worden gewijzigd,

HEEFT HET VOLGENDE BESLUIT VASTGESTELD:

[1] Besluit (GBVB) 2019/797 van de Raad van 17 mei 2019 betreffende beperkende maatregelen tegen cyberaanvallen die de Unie of haar lidstaten bedreigen (PB L 129 I van 17.5.2019, blz. 13).

Artikel 1

Besluit (GBVB) 2019/797 wordt als volgt gewijzigd:

1) artikel 10 wordt vervangen door:

"*Artikel 10*

Dit besluit is van toepassing tot en met 18 mei 2025 en wordt voortdurend geëvalueerd.";

2) de bijlage wordt gewijzigd overeenkomstig de bijlage bij dit besluit.

Artikel 2

Dit besluit treedt in werking op de dag na die van de bekendmaking ervan in het *Publicatieblad van de Europese Unie*.

Gedaan te …,

Voor de Raad
De voorzitter

BIJLAGE

De bijlage bij Besluit (GBVB) 2019/797 (“Lijst van de in de artikelen 4 en 5 bedoelde natuurlijke personen en rechtspersonen, entiteiten en lichamen”) wordt als volgt gewijzigd:

1) in de lijst onder ‘A. Natuurlijke personen”, worden de vermeldingen 3 tot en met 8 vervangen door:

	Naam	Identificatiegegevens	Motivering	Datum van plaatsing op de lijst
“3.	Alexey Valeryevich MININ	Алексей Валерьевич МИНИН Geboortedatum: 27.5.1972 Geboorteplaats: oblast Perm, Russische Socialistische Federatieve Sovjetrepubliek (nu de Russische Federatie) Paspoortnummer: 120017582 Afgegeven door het ministerie van Buitenlandse Zaken van de Russische Federatie Geldigheidsduur: van 17.4.2017 tot en met 17.4.2022 Locatie: Moskou, Russische Federatie Nationaliteit: Russisch Geslacht: man	Alexey Minin nam deel aan een poging tot cyberaanval met mogelijk aanzienlijke gevolgen tegen de Organisatie voor het verbod van chemische wapens (OPCW) in Nederland en aan cyberaanvallen met aanzienlijke gevolgen tegen derde landen. Als ondersteunend medewerker inzake menselijke inlichtingen van het hoofddirectoraat van de generale staf van de strijdkrachten van de Russische Federatie (GU/GRU) maakte Alexey Minin deel uit van een vierkoppig team van de Russische militaire inlichtingendienst dat in april 2018 ongeautoriseerde toegang probeerde te verkrijgen tot het wifi-netwerk van de OPCW in Den Haag, Nederland. De poging tot cyberaanval was bedoeld om het wifi-netwerk van de OPCW te hacken hetgeen, indien de actie succesvol was geweest, de veiligheid van het netwerk en de lopende onderzoeksactiviteiten van de OPCW zou hebben aangetast. De Nederlandse Militaire Inlichtingen- en Veiligheidsdienst heeft de poging tot cyberaanval verstoord en zo ernstige schade aan de OPCW voorkomen. Een grand jury in het westelijke district van Pennsylvania (Verenigde Staten van Amerika) heeft Alexey Minin aangeklaagd als medewerker van het hoofddirectoraat van de Russische inlichtingendienst (GRU) voor het hacken van computers, wire fraud (fraude middels elektronische verbindingen), identiteitsdiefstal onder verzwarende omstandigheden en witwassen van geld.	30.7.2020

	Naam	Identificatiegegevens	Motivering	Datum van plaatsing op de lijst
4.	Aleksei Sergeyvich MORENETS	Алексей Сергеевич МОРЕНЕЦ Geboortedatum: 31.7.1977 Geboorteplaats: oblast Moermansk, Russische Socialistische Federatieve Sovjetrepubliek (nu de Russische Federatie) Paspoortnummer: 100135556 Afgegeven door het ministerie van Buitenlandse Zaken van de Russische Federatie Geldigheidsduur: van 17.4.2017 tot en met 17.4.2022 Locatie: Moskou, Russische Federatie Nationaliteit: Russisch Geslacht: man	Aleksei Morenets nam deel aan een poging tot cyberaanval met mogelijk aanzienlijke gevolgen tegen de Organisatie voor het verbod van chemische wapens (OPCW) in Nederland en aan cyberaanvallen met aanzienlijke gevolgen tegen derde landen. Als cyberoperator van het hoofddirectoraat van de generale staf van de strijdkrachten van de Russische Federatie (GU/GRU) maakte Aleksei Morenets deel uit van een vierkoppig team van de Russische militaire inlichtingendienst dat in april 2018 ongeautoriseerde toegang probeerde te verkrijgen tot het wifi-netwerk van de OPCW in Den Haag, Nederland. De poging tot cyberaanval was bedoeld om het wifi-netwerk van de OPCW te hacken hetgeen, indien de actie succesvol was geweest, de veiligheid van het netwerk en de lopende onderzoeksactiviteiten van de OPCW zou hebben aangetast. De Nederlandse Militaire Inlichtingen- en Veiligheidsdienst heeft de poging tot cyberaanval verstoord en zo ernstige schade aan de OPCW voorkomen. Een grand jury in het westelijke district van Pennsylvania (Verenigde Staten van Amerika) heeft Aleksei Morenets aangeklaagd als lid van militaire eenheid 26165,voor het hacken van computers, wire fraud (fraude middels elektronische verbindingen), identiteitsdiefstal onder verzwarende omstandigheden en witwassen van geld.	30.7.2020

	Naam	Identificatiegegevens	Motivering	Datum van plaatsing op de lijst
5.	Evgenii Mikhaylovich SEREBRIAKOV	Евгений Михайлович СЕРЕБРЯКОВ Geboortedatum: 26.7.1981 Geboorteplaats: Koersk, Russische Socialistische Federatieve Sovjetrepubliek (nu de Russische Federatie) Paspoortnummer: 100135555 Afgegeven door het ministerie van Buitenlandse Zaken van de Russische Federatie Geldigheidsduur: van 17.4.2017 tot en met 17.4.2022 Locatie: Moskou, Russische Federatie Nationaliteit: Russisch Geslacht: man	Evgenii Serebriakov nam deel aan een poging tot cyberaanval met mogelijk aanzienlijke gevolgen tegen de Organisatie voor het verbod van chemische wapens (OPCW) in Nederland en aan cyberaanvallen met aanzienlijke gevolgen tegen derde landen. Als cyberoperator van het hoofddirectoraat van de generale staf van de strijdkrachten van de Russische Federatie (GU/GRU) maakte Evgenii Serebriakov deel uit van een vierkoppig team van de Russische militaire inlichtingendienst dat in april 2018 ongeautoriseerde toegang probeerde te verkrijgen tot het wifi-netwerk van de OPCW in Den Haag, Nederland. Die poging tot cyberaanval was bedoeld om het wifi-netwerk van de OPCW te hacken hetgeen, indien de actie succesvol was geweest, de veiligheid van het netwerk en de lopende onderzoeksactiviteiten van de OPCW zou hebben aangetast. De Nederlandse Militaire Inlichtingen- en Veiligheidsdienst heeft de poging tot cyberaanval verstoord en zo ernstige schade aan de OPCW voorkomen. Sinds het voorjaar van 2022 leidt Evgenii Serebriakov de actor en hackersgroep “Sandworm” (alias “Sandworm Team”, “BlackEnergy Group”, “Voodoo Bear”, “Quedagh”, “Olympic Destroyer” en “Telebots”), die verbonden is met eenheid 74455 van het hoofddirectoraat van de Russische inlichtingendienst (GRU). Sandworm heeft cyberaanvallen uitgevoerd op Oekraïne, onder meer op Oekraïense overheidsinstanties, sinds het begin van de Russische aanvalsoorlog tegen Oekraïne.	30.7.2020

	Naam	Identificatiegegevens	Motivering	Datum van plaatsing op de lijst
6.	Oleg Mikhaylovich SOTNIKOV	Олег Михайлович СОТНИКОВ Geboortedatum: 24.8.1972 Geboorteplaats: Koersk, Russische Socialistische Federatieve Sovjetrepubliek (nu de Russische Federatie) Paspoortnummer: 120018866 Afgegeven door het ministerie van Buitenlandse Zaken van de Russische Federatie Geldigheidsduur: van 17.4.2017 tot en met 17.4.2022 Locatie: Moskou, Russische Federatie Nationaliteit: Russisch Geslacht: man	Oleg Sotnikov nam deel aan een poging tot cyberaanval met mogelijk aanzienlijke gevolgen tegen de Organisatie voor het verbod van chemische wapens (OPCW) in Nederland en aan cyberaanvallen met aanzienlijke gevolgen tegen derde landen. Als ondersteunend medewerker inzake menselijke inlichtingen van het hoofddirectoraat van de generale staf van de strijdkrachten van de Russische Federatie (GU/GRU) maakte Oleg Sotnikov deel uit van een vierkoppig team van de Russische militaire inlichtingendienst dat in april 2018 ongeautoriseerde toegang probeerde te verkrijgen tot het wifi-netwerk van de OPCW in Den Haag, Nederland. De poging tot cyberaanval was bedoeld om het wifi-netwerk van de OPCW te hacken hetgeen, indien de actie succesvol was geweest, de veiligheid van het netwerk en de lopende onderzoeksactiviteiten van de OPCW zou hebben aangetast. De Nederlandse Militaire Inlichtingen- en Veiligheidsdienst heeft de poging tot cyberaanval verstoord en zo ernstige schade aan de OPCW voorkomen. Een grand jury in het westelijke district van Pennsylvania (Verenigde Staten van Amerika) heeft Oleg Sotnikov aangeklaagd als medewerker van het hoofddirectoraat van de Russische inlichtingendienst (GRU) voor het hacken van computers, wire fraud (fraude middels elektronische verbindingen), identiteitsdiefstal onder verzwarende omstandigheden en witwassen van geld.	30.7.2020

	Naam	Identificatiegegevens	Motivering	Datum van plaatsing op de lijst
7.	Dmitry Sergeyevich BADIN	Дмитрий Сергеевич БАДИН Geboortedatum: 15.11.1990 Geboorteplaats: Koersk, Russische Socialistische Federatieve Sovjetrepubliek (nu de Russische Federatie) Nationaliteit: Russisch Geslacht: man	Dmitry Badin nam deel aan een cyberaanval met aanzienlijke gevolgen tegen het Duitse federaal parlement (Deutscher Bundestag) en aan cyberaanvallen met aanzienlijke gevolgen tegen derde landen. Als militaire-inlichtingenofficier van het 85e hoofdcentrum voor speciale diensten (GTsSS) van het hoofddirectoraat van de generale staf van de krijgsmacht van de Russische Federatie (GU/GRU) maakte Dmitry Badin deel uit van een team van Russische militaire-inlichtingenofficieren die in april en mei 2015 een cyberaanval hebben uitgevoerd tegen het Duitse federaal parlement. Die cyberaanval was gericht tegen het informaticasysteem van het parlement en belemmerde het functioneren van dat systeem dagenlang. Er werd een aanzienlijke hoeveelheid gegevens gestolen en de e-mailaccounts van verscheidene parlementsleden, alsook die van voormalig bondskanselier Angela Merkel, werden getroffen. Een grand jury in het westelijke district van Pennsylvania (Verenigde Staten van Amerika) heeft Dmitry Badin aangeklaagd als lid van militaire eenheid 26165,voor het hacken van computers, wire fraud (fraude middels elektronische verbindingen), identiteitsdiefstal onder verzwarende omstandigheden en witwassen van geld.	22.10.2020

	Naam	Identificatiegegevens	Motivering	Datum van plaatsing op de lijst
8.	Igor Olegovich KOSTYUKOV	Игорь Олегович КОСТЮКОВ Geboortedatum: 21.2.1961 Nationaliteit: Russisch Geslacht: man	Igor Kostyukov is thans hoofd van het hoofddirectoraat van de generale staf van de krijgsmacht van de Russische Federatie (GU/GRU), waar hij voorheen de eerste adjunct van de directeur was. Een van de eenheden onder zijn bevel is het 85e hoofdcentrum voor speciale diensten (GTsSS) (ook bekend als “militaire eenheid 26165”, “APT28”, “Fancy Bear”, “Sofacy Group”, “Pawn Storm” en “Strontium”). In die hoedanigheid is Igor Kostyukov verantwoordelijk voor de cyberaanvallen die door het GTsSS zijn uitgevoerd, waaronder ook cyberaanvallen met aanzienlijke gevolgen die een externe bedreiging vormen voor de Unie of haar lidstaten. Meer bepaald namen militaire-inlichtingenofficieren van het GTsSS deel aan de cyberaanval tegen het Duitse federaal parlement (Deutscher Bundestag) in april en mei 2015 en aan de poging tot cyberaanval bedoeld om het wifi-netwerk van de Organisatie voor het verbod van chemische wapens (OPCW) in Nederland te hacken in april 2018. De cyberaanval tegen het Duitse federaal parlement was gericht tegen het informaticasysteem van het parlement en belemmerde het functioneren van dat systeem dagenlang. Er werd een aanzienlijke hoeveelheid gegevens gestolen en de e-mailaccounts van verscheidene parlementsleden, alsook die van voormalig bondskanselier Angela Merkel, werden getroffen.”	22.10.2020”;

2) in de lijst onder “B. Rechtspersonen, entiteiten en lichamen” worden de vermeldingen 3 en 4 vervangen door:

	Naam	Identificatiegegevens	Motivering	Datum van plaatsing op de lijst
“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) (hoofdcentrum voor speciale technologieën (GTsST) van het hoofddirectoraat van de generale staf van de strijdkrachten van de Russische Federatie (GU/GRU))	Adres: 22 Kirova Street, Moscow, Russian Federation (Moskou, Russische Federatie)	Het hoofdcentrum voor speciale technologieën (GTsST) van het hoofddirectoraat van de generale staf van de strijdkrachten van de Russische Federatie (GU/GRU), dat ook bekend is onder veldpostnummer 74455, is betrokken bij cyberaanvallen met aanzienlijke gevolgen die afkomstig zijn van buiten de Unie en een externe bedreiging vormen voor de Unie of haar lidstaten, en bij cyberaanvallen met aanzienlijke gevolgen tegen derde landen, waaronder de cyberaanvallen van juni 2017 bekend onder de namen “NotPetya” en “EternalPetya” en de cyberaanvallen tegen een Oekraïens elektriciteitsnet in de winter van 2015 en 2016. “NotPetya” of “EternalPetya” maakte gegevens ontoegankelijk voor een aantal bedrijven in de Unie, in Europa in ruimere zin, en wereldwijd, door computers aan te vallen met gijzelsoftware en door de toegang tot gegevens te blokkeren, wat onder meer tot aanzienlijke economische verliezen heeft geleid. De cyberaanval op een Oekraïens elektriciteitsnet leidde ertoe dat delen ervan tijdens de winter werden uitgeschakeld.	30.7.2020

	Naam	Identificatiegegevens	Motivering	Datum van plaatsing op de lijst
			De actor bekend als „Sandworm” (ook bekend als “Sandworm Team”, “BlackEnergy Group”, “Voodoo Bear”, “Quedagh”, “Olympic Destroyer” en “Telebots”), die ook achter de aanval op het elektriciteitsnet in Oekraïne zat, heeft “NotPetya” of “EternalPetya” uitgevoerd. Sandworm heeft cyberaanvallen uitgevoerd op Oekraïne, onder meer op Oekraïense overheidsinstanties en Oekraïense kritieke infrastructuur, sinds het begin van de Russische aanvalsoorlog tegen Oekraïne. Bij die cyberaanvallen gaat het onder meer om spearphishing-operaties, kwaadaardige software en aanvallen met gijzelsoftware. Het hoofdcentrum voor speciale technologieën van het hoofddirectoraat van de generale staf van de strijdkrachten van de Russische Federatie speelt een actieve rol bij de door Sandworm uitgevoerde cyberactiviteiten en kan aan Sandworm worden gelinkt.	

	Naam	Identificatiegegevens	Motivering	Datum van plaatsing op de lijst
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) (85e hoofdcentrum voor speciale diensten (GTsST) van het hoofddirectoraat van de generale staf van de strijdkrachten van de Russische Federatie (GU/GRU))	Adres: Komsomol'skiy Prospekt, 20, Moscow, 119146, Russian Federation (Moskou, Russische Federatie)	Het 85e hoofdcentrum voor speciale diensten (GTsST) van het hoofddirectoraat van de generale staf van de strijdkrachten van de Russische Federatie (GU/GRU) (ook bekend als “militaire eenheid 26165”, “APT28”, “Fancy Bear”, “Sofacy Group”, “Pawn Storm” en ”Strontium”) is betrokken bij cyberaanvallen met aanzienlijke gevolgen die een externe bedreiging vormen voor de Unie of haar lidstaten, en bij cyberaanvallen met aanzienlijke gevolgen tegen derde landen. Meer bepaald namen militaire-inlichtingenofficieren van het GTsSS deel aan de cyberaanval tegen het Duitse federaal parlement (Deutscher Bundestag) in april en mei 2015 en aan de poging tot cyberaanval bedoeld om het wifi-netwerk van de Organisatie voor het verbod van chemische wapens (OPCW) in Nederland te hacken in april 2018. De cyberaanval tegen het Duitse federaal parlement was gericht tegen het informaticasysteem van het parlement en belemmerde het functioneren van dat systeem dagenlang. Er werd een aanzienlijke hoeveelheid gegevens gestolen en de e-mailaccounts van verscheidene parlementsleden, alsook die van bondskanselier Angela Merkel, werden getroffen. Sinds het begin van de Russische aanvalsoorlog tegen Oekraïne werden er door het GTsSS cyberaanvallen (spearphishing-operaties en aanvallen gebaseerd op kwaadaardige software) uitgevoerd tegen Oekraïne.	22.10.2020”.