II

(Niet-wetgevingshandelingen)

VERORDENINGEN

UITVOERINGSVERORDENING (EU) 2020/1536 VAN DE RAAD

van 22 oktober 2020

tot uitvoering van Verordening (EU) 2019/796 betreffende beperkende maatregelen tegen cyberaanvallen die de Unie of haar lidstaten bedreigen

DE RAAD VAN DE EUROPESE UNIE,

Gezien het Verdrag betreffende de werking van de Europese Unie,

Gezien Verordening (EU) 2019/796 van de Raad van 17 mei 2019 betreffende beperkende maatregelen tegen cyberaanvallen die de Unie of haar lidstaten bedreigen ([1]), en met name artikel 13, lid 1,

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 Verordening (EU) 2019/796 vastgesteld.

(2) Gerichte beperkende maatregelen tegen cyberaanvallen met aanzienlijke gevolgen die een externe bedreiging vormen voor de Unie of haar lidstaten, vallen onder de maatregelen binnen het Uniekader voor een gezamenlijke diplomatieke respons op kwaadwillige cyberactiviteiten (het instrumentarium voor cyberdiplomatie) en zijn een cruciaal instrument om dergelijke activiteiten tegen te gaan en te beantwoorden.

(3) Teneinde aanhoudend en toenemend kwaadwillig cybergedrag te voorkomen, te ontmoedigen, tegen te gaan en erop te reageren, moeten twee natuurlijke personen en één lichaam worden toegevoegd aan de in bijlage I bij Verordening (EU) 2019/796 opgenomen lijst van natuurlijke personen en rechtspersonen, entiteiten en lichamen die aan beperkende maatregelen onderworpen zijn. Die personen en dat lichaam zijn verantwoordelijk voor of waren betrokken bij cyberaanvallen met aanzienlijke gevolgen die een externe bedreiging vormen voor de Unie of haar lidstaten, meer bepaald de cyberaanval tegen het Duitse federaal parlement (Deutscher Bundestag) in april en mei 2015.

(4) Bijlage I bij Verordening (EU) 2019/796 moet daarom dienovereenkomstig worden gewijzigd,

HEEFT DE VOLGENDE VERORDENING VASTGESTELD:

Artikel 1

Bijlage I bij Verordening (EU) 2019/796 wordt gewijzigd overeenkomstig de bijlage bij deze verordening.

([1]) PB L 129 I van 17.5.2019, blz. 1.

Artikel 2

Deze verordening treedt in werking op de datum van de bekendmaking ervan in het *Publicatieblad van de Europese Unie*.

Deze verordening is verbindend in al haar onderdelen en is rechtstreeks toepasselijk in elke lidstaat.

Gedaan te Brussel, 22 oktober 2020.

Voor de Raad
De voorzitter
M. ROTH

BIJLAGE

De volgende vermeldingen worden toegevoegd aan de lijst van natuurlijke personen en rechtspersonen, entiteiten en lichamen in bijlage I bij Verordening (EU) 2019/796:

A. Natuurlijke personen

	Naam	Identificatiegegevens	Motivering	Datum van plaatsing op de lijst
"7.	Dmitry Sergeyevich BADIN	Дмитрий Сергеевич Бадин Geboortedatum: 15 november 1990 Geboorteplaats: Koersk, Russische Socialistische Federatieve Sovjetrepubliek (nu de Russische Federatie) Nationaliteit: Russisch Geslacht: man	Dmitry Badin nam deel aan een cyberaanval tegen het Duitse federaal parlement (Deutscher Bundestag) die aanzienlijke gevolgen heeft teweeggebracht. 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 dat in april en mei 2015 een cyberaanval heeft uitgevoerd tegen het Duitse federaal parlement (Deutscher Bundestag). 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 er werd schade berokkend aan de e-mailaccounts van verscheidene parlementsleden, alsook aan die van bondskanselier Angela Merkel.	22.10.2020
8.	Igor Olegovich KOSTYUKOV	Игорь Олегович Костюков Geboortedatum: 21 februari 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" (in de branche ook bekend als "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 inbraak in het wifi-netwerk van de Organisatie voor het verbod van chemische wapens (OVCW) in april 2018 in Nederland. 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 er werd schade berokkend aan de e-mailaccounts van verscheidene parlementsleden, alsook aan die van bondskanselier Angela Merkel.	22.10.2020"

B. Rechtspersonen, entiteiten en lichamen

	Naam	Identificatiegegevens	Motivering	Datum van plaatsing op de lijst
"4.	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, Moskou, 119146, 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" (in de branche ook bekend als "APT28", "Fancy Bear", "Sofacy Group", "Pawn Storm" en "Strontium"), is verantwoordelijk voor 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 inbraak in het wifi-netwerk van de Organisatie voor het verbod van chemische wapens (OVCW) in april 2018 in Nederland. 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 er werd schade berokkend aan de e-mailaccounts van verscheidene parlementsleden, alsook aan die van bondskanselier Angela Merkel.	22.10.2020"