# UITVOERINGSVERORDENING (EU) 2020/1125 VAN DE RAAD

## van 30 juli 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. Indien zulks nodig wordt geacht ter verwezenlijking van gemeenschappelijke doelstellingen wat betreft buitenlands en veiligheidsbeleid die in de relevante bepalingen van artikel 21 van het Verdrag betreffende de Europese Unie zijn vermeld, kunnen beperkende maatregelen eveneens worden toegepast als respons op cyberaanvallen met aanzienlijke gevolgen tegen derde landen of internationale organisaties.

(3) De Raad heeft op 16 april 2018 conclusies aangenomen waarin hij het kwaadwillige gebruik van informatie- en communicatietechnologieën met klem veroordeelde; daaronder vielen ook de cyberaanvallen bekend als "WannaCry" en "NotPetya", die aanzienlijke schade en economisch verlies hebben berokkend in en buiten de Unie. De voorzitter van de Europese Raad, de voorzitter van de Europese Commissie en de hoge vertegenwoordiger van de Unie voor buitenlandse zaken en veiligheidsbeleid (de "hoge vertegenwoordiger") hebben op 4 oktober 2018 in een gemeenschappelijke verklaring hun diepe bezorgdheid geuit over een poging tot cyberaanval waarmee geprobeerd werd de integriteit van de Organisatie voor het verbod van chemische wapens (OPCW) in Nederland te ondermijnen, een agressieve daad die blijk gaf van minachting voor de belangrijke taak van de OPCW. In een verklaring namens de Unie op 12 april 2019 heeft de hoge vertegenwoordiger er bij de betrokken actoren op aangedrongen kwaadwillige cyberactiviteiten die erop gericht zijn de integriteit, veiligheid en het economisch concurrentievermogen van de Unie te ondermijnen — waaronder ook een aantal gevallen van cyberdiefstal van intellectuele eigendom — te staken. Daaronder vallen ook de cyberdiefstallen uitgevoerd door de actor die bekend staat als "APT10" ("Advanced Persistent Threat 10").

(4) In dit verband, en teneinde aanhoudend en toenemend kwaadwillig cybergedrag te voorkomen, te ontmoedigen, tegen te gaan en te beantwoorden, moeten zes natuurlijke personen en drie entiteiten of lichamen 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 entiteiten of lichamen zijn verantwoordelijk voor, hebben steun verstrekt voor of waren betrokken bij cyberaanvallen, of hebben dergelijke aanvallen gefaciliteerd of pogingen tot cyberaanvallen ondernomen, onder meer de poging tot cyberaanval tegen de OPCW en de cyberaanvallen bekend als "WannaCry", "NotPetya" en "Operation Cloud Hopper".

(5) 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 129I 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, 30 juli 2020.

*Voor de Raad*
*De voorzitter*
M. ROTH

*BIJLAGE*

De volgende personen en entiteiten of lichamen 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 |
|---|---|---|---|---|
| 1. | GAO Qiang | Geboorteplaats: Provincie Shandong, China<br>Adres: Room 1102, Guanfu Mansion, 46 Xinkai Road, Hedong District, Tianjin, China<br>Nationaliteit: Chinees<br>Geslacht: man | Gao Qiang is betrokken bij "Operation Cloud Hopper", een reeks cyberaanvallen afkomstig van buiten de Unie die aanzienlijke gevolgen hebben en een externe bedreiging vormen voor de Unie of haar lidstaten, en een reeks cyberaanvallen die aanzienlijke gevolgen voor derde landen hebben. "Operation Cloud Hopper" was gericht op informatiesystemen van multinationale ondernemingen op zes continenten, waaronder in de Unie gevestigde ondernemingen, en heeft het mogelijk gemaakt ongeautoriseerde toegang te verkrijgen tot commercieel gevoelige gegevens, wat tot significante economische verliezen heeft geleid.<br><br>De actor bekend als "APT10" ("Advanced Persistent Threat 10") (alias "Red Apollo", "CVNX", "Stone Panda", "MenuPass" en "Potassium") voerde "Operation Cloud Hopper" uit.<br>Gao Qiang kan worden gelinkt aan APT10, onder meer door zijn banden met de commando- en controle-infrastructuur van APT10. Bovendien had Huaying Haitai, een entiteit die op de lijst is geplaatst voor het ondersteunen en faciliteren van "Operation Cloud Hopper", Gao Qiang in dienst. Hij heeft banden met Zhang Shilong, die ook op de lijst is geplaatst in verband met "Operation Cloud Hopper". Gao Qiang heeft derhalve banden met zowel Huaying Haitai als Zhang Shilong. | 30.7.2020 |
| 2. | ZHANG Shilong | Adres: Hedong, Yuang Road nr. 121, Tianjin, China<br>Nationaliteit: Chinees<br>Geslacht: man | Zhang Shilong is betrokken bij "Operation Cloud Hopper", een reeks cyberaanvallen afkomstig van buiten de Unie die aanzienlijke gevolgen hebben en een externe bedreiging vormen voor de Unie of haar lidstaten, en een reeks cyberaanvallen die aanzienlijke gevolgen voor derde landen hebben.<br>"Operation Cloud Hopper" was gericht op informatiesystemen van multinationale ondernemingen op zes continenten, waaronder in de Unie gevestigde ondernemingen, en heeft het mogelijk gemaakt ongeautoriseerde toegang te verkrijgen tot commercieel gevoelige gegevens, wat tot significante economische verliezen heeft geleid.<br>De actor bekend als "APT10" ("Advanced Persistent Threat 10") (ook bekend als "Red Apollo", "CVNX", "Stone Panda", "MenuPass" en "Potassium") voerde "Operation Cloud Hopper" uit.<br><br>Zhang Shilong kan worden gelinkt aan APT10, onder meer door de malware die hij heeft ontwikkeld en getest in verband met de door APT10 uitgevoerde cyberaanvallen. Bovendien had Huaying Haitai, een entiteit die op de lijst is geplaatst voor het ondersteunen en faciliteren van "Operation Cloud Hopper", Zhang Shilong in dienst. Hij heeft banden met Gao Qiang, die ook op de lijst is geplaatst in verband met "Operation Cloud Hopper". Zhang Shilong heeft derhalve banden met zowel Huaying Haitai als Gao Qiang. | 30.7.2020 |

| | | | | |
|---|---|---|---|---|
| 3. | Alexey Valeryevich MININ | Алексей Валерьевич МИНИН<br>Geboortedatum: 27 mei 1972<br>Geboorteplaats: oblast Perm, Russische Socialistische Federatieve Sovjetrepubliek (nu de Russische Federatie)<br>Paspoortnummer: 120017582<br>Afgegeven door het ministerie van Buitenlandse Zaken van de Russische Federatie Geldigheidsduur: van 17 april 2017 tot en met 17 april 2022<br>Locatie: Moskou, Russische Federatie<br>Nationaliteit: Russisch<br>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.<br>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, die, indien deze succesvol was geweest, de veiligheid van het netwerk en de lopende onderzoeksactiviteiten van de OPCW zou hebben aangetast. De Nederlandse Militaire Inlichtingen- en Veiligheidsdienst (MIVD) heeft de poging tot cyberaanval verstoord en zo ernstige schade aan de OPCW voorkomen. | 30.7.2020 |
| 4. | Aleksei Sergeyvich MORENETS | Алексей Сергеевич МОРЕНЕЦ<br>Geboortedatum: 31 juli 1977<br>Geboorteplaats: oblast Moermansk, Russische Socialistische Federatieve Sovjetrepubliek (nu de Russische Federatie)<br>Paspoortnummer: 100135556<br>Afgegeven door het ministerie van Buitenlandse Zaken van de Russische Federatie Geldigheidsduur: van 17 april 2017 tot en met 17 april 2022<br>Locatie: Moskou, Russische Federatie<br>Nationaliteit: Russisch<br>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.<br>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 die, indien deze succesvol was geweest, de veiligheid van het netwerk en de lopende onderzoeksactiviteiten van de OPCW zou hebben aangetast. De Nederlandse Militaire Inlichtingen- en Veiligheidsdienst (MIVD) heeft de poging tot cyberaanval verstoord en zo ernstige schade aan de OPCW voorkomen. | 30.7.2020 |
| 5. | Evgenii Mikhaylovich SEREBRIAKOV | Евгений Михайлович СЕРЕБРЯКОВ<br>Geboortedatum: 26 juli 1981<br>Geboorteplaats: Koersk, Russische Socialistische Federatieve Sovjetrepubliek (nu de Russische Federatie)<br>Paspoortnummer: 100135555<br>Afgegeven door het ministerie van Buitenlandse Zaken van de Russische Federatie Geldigheidsduur: van 17 april 2017 tot en met 17 april 2022<br>Locatie: Moskou, Russische Federatie<br>Nationaliteit: Russisch<br>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.<br>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. De poging tot cyberaanval was bedoeld om het wifi-netwerk van de OPCW te hacken die, indien deze succesvol was geweest, de veiligheid van het netwerk en de lopende onderzoeksactiviteiten van de OPCW zou hebben aangetast. De Nederlandse Militaire Inlichtingen- en Veiligheidsdienst (MIVD) heeft de poging tot cyberaanval verstoord en zo ernstige schade aan de OPCW voorkomen. | 30.7.2020 |

| | | | | |
|---|---|---|---|---|
| 6. | Oleg Mikhaylovich SOTNIKOV | Олег Михайлович СОТНИКОВ<br>Geboortedatum: 24 augustus 1972<br>Geboorteplaats: Oeljanovsk, Russische Socialistische Federatieve Sovjetrepubliek (nu de Russische Federatie)<br>Paspoortnummer: 120018866<br>Afgegeven door het ministerie van Buitenlandse Zaken van de Russische Federatie Geldigheidsduur: van 17 april 2017 tot en met 17 april 2022<br>Locatie: Moskou, Russische Federatie<br>Nationaliteit: Russisch<br>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.<br>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 die, indien deze succesvol was geweest, de veiligheid van het netwerk en de lopende onderzoeksactiviteiten van de OPCW zou hebben aangetast. De Nederlandse Militaire Inlichtingen- en Veiligheidsdienst (MIVD) heeft de poging tot cyberaanval verstoord en zo ernstige schade aan de OPCW voorkomen. | 30.7.2020 |

B. Rechtspersonen, entiteiten en lichamen

| | Naam | Identificatiegegevens | Motivering | Datum van plaatsing op de lijst |
|---|---|---|---|---|
| 1. | Tianjin Huaying Haitai Science and Technology Development Co. Ltd (Huaying Haitai) | Ook bekend als: Haitai Technology Development Co. Ltd.<br>Locatie: Tianjin, China | Huaying Haitai heeft financiële, technische of materiële steun verleend voor “Operation Cloud Hopper”, een reeks cyberaanvallen afkomstig van buiten de Unie die aanzienlijke gevolgen hebben en een externe bedreiging vormen voor de Unie of haar lidstaten, en een reeks cyberaanvallen die aanzienlijke gevolgen voor derde landen hebben, en heeft die operatie gefaciliteerd.<br>“Operation Cloud Hopper” was gericht op informatiesystemen van multinationale ondernemingen op zes continenten, waaronder in de Unie gevestigde ondernemingen, en heeft het mogelijk gemaakt ongeautoriseerde toegang te verkrijgen tot commercieel gevoelige gegevens, wat tot significante economische verliezen heeft geleid.<br>De actor bekend als “APT10” (“Advanced Persistent Threat 10”) (ook bekend als “Red Apollo”, “CVNX”, “Stone Panda”, “MenuPass” en “Potassium”) voerde “Operation Cloud Hopper” uit.<br>Huaying Haitai kan worden gelinkt aan APT10. Bovendien was Huaying Haitai de werkgever van Gao Qiang en Zhang Shilong, die beiden op de lijst zijn geplaatst in verband met “Operation Cloud Hopper”. Huaying Haitai heeft derhalve banden met Gao Qiang en Zhang Shilong. | 30.7.2020 |
| 2. | Chosun Expo | Ook bekend als: Chosen Expo; Korea Export Joint Venture<br>Locatie: Democratische Volksrepubliek Korea | Chosun Expo heeft financiële, technische of materiële steun verleend voor een reeks cyberaanvallen afkomstig van buiten de Unie die aanzienlijke gevolgen hebben en een externe bedreiging vormen voor de Unie of haar lidstaten, en een reeks cyberaanvallen die aanzienlijke gevolgen voor derde landen hebben, waaronder de cyberaanvallen bekend onder de naam “WannaCry” en de cyberaanvallen tegen de Poolse autoriteit voor financieel toezicht en Sony Pictures Entertainment, alsook de cyberdiefstal bij de centrale bank van Bangladesh en de poging tot cyberdiefstal bij de Vietnamese Tien Phong Bank, en heeft deze cyberaanvallen gefaciliteerd. | 30.7.2020 |

| | | | | |
|---|---|---|---|---|
| | | | "WannaCry" verstoorde informatiesystemen in de hele wereld door ze met ransomware aan te vallen en door de toegang tot gegevens te blokkeren. Dit heeft gevolgen gehad voor informatiesystemen van ondernemingen in de Unie, onder meer informatiesystemen in verband met diensten voor het in stand houden van essentiële diensten en economische activiteiten in de lidstaten.<br>De actor bekend als "APT38" ("Advanced Persistent Threat 38") of de "Lazarus-groep" hebben "WannaCry" uitgevoerd.<br>Chosun Expo kan worden gelinkt aan APT38/de Lazarus-groep, onder meer via de rekeningen die zijn gebruikt voor de cyberaanvallen. | |
| 3. | Het 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, 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 verantwoordelijk voor cyberaanvallen afkomstig van buiten de Unie die aanzienlijke gevolgen hebben en een externe bedreiging vormen voor de Unie of haar lidstaten, en voor cyberaanvallen die aanzienlijke gevolgen voor derde landen hebben, waaronder de cyberaanvallen van juni 2017 bekend onder de namen "NotPetya" of "EternalPetya" en de cyberaanvallen tegen een Oekraïens elektriciteitsnet in de winter van 2015 en 2016.<br>"NotPetya" of "EternalPetya" maakte gegevens ontoegankelijk voor een aantal bedrijven in de Unie, Europa in ruimere zin, en de hele wereld, door computers aan te vallen met ransomware en door de toegang tot gegevens te blokkeren, wat onder meer tot significante economische verliezen heeft geleid. De cyberaanval op een Oekraïens elektriciteitsnet leidde ertoe dat delen ervan tijdens de winter werden uitgeschakeld. | 30.7.2020" |
| | | | 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.<br>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. | |