NEUVOSTON PÄÄTÖS (YUTP) 2020/1127,

annettu 30 päivänä heinäkuuta 2020,

unionia tai sen jäsenvaltioita uhkaavien kyberhyökkäysten vastaisista rajoittavista toimenpiteistä annetun päätöksen (YUTP) 2019/797 muuttamisesta

EUROOPAN UNIONIN NEUVOSTO, joka

ottaa huomioon Euroopan unionista tehdyn sopimuksen ja erityisesti sen 29 artiklan,

ottaa huomioon unionin ulkoasioiden ja turvallisuuspolitiikan korkean edustajan ehdotuksen,

sekä katsoo seuraavaa:

(1) Neuvosto hyväksyi 17 päivänä toukokuuta 2019 päätöksen (YUTP) 2019/797 ([1]).

(2) Unionille tai sen jäsenvaltioille ulkoisen uhkan muodostavien vaikutukseltaan merkittävien kyberhyökkäysten vastaiset kohdennetut rajoittavat toimenpiteet kuuluvat yhteistä diplomaattista vastausta haitallisiin kybertoimiin koskevien unionin puitteiden (kyberdiplomatian välineistö) toimenpiteisiin ja ovat erittäin tärkeä väline, jolla estetään tällainen toiminta ja vastataan siihen. Rajoittavia toimenpiteitä voidaan soveltaa myös vastauksena kolmansiin valtioihin tai kansainvälisiin järjestöihin kohdistuviin vaikutukseltaan merkittäviin kyberhyökkäyksiin, jos tämä katsotaan tarpeelliseksi Euroopan unionista tehdyn sopimuksen 21 artiklan asiaankuuluvissa määräyksissä määrättyjen yhteisen ulko- ja turvallisuuspolitiikan tavoitteiden saavuttamiseksi.

(3) Neuvosto antoi 16 päivänä huhtikuuta 2018 päätelmät, joissa se tuomitsi vakaasti tieto- ja viestintätekniikan käytön haitantekotarkoituksessa, mukaan lukien julkisuudessa nimillä ”WannaCry” ja ”NotPetya” tunnetut kyberhyökkäykset, jotka aiheuttivat huomattavaa vahinkoa ja taloudellista tappiota unionissa ja muualla. Eurooppa-neuvoston puheenjohtaja, Euroopan komission puheenjohtaja ja unionin ulkoasioiden ja turvallisuuspolitiikan korkea edustaja, jäljempänä ’korkea edustaja’, ilmaisivat 4 päivänä lokakuuta 2018 antamassaan yhteisessä lausumassa vakavan huolensa kyberhyökkäysyrityksestä, jolla pyrittiin horjuttamaan Alankomaissa sijaitsevan kemiallisten aseiden kieltojärjestön (OPCW) koskemattomuutta; kyseessä oli aggressiivinen toimi, joka oli osoitus OPCW:n perimmäisen tarkoituksen halventamisesta. Korkea edustaja kehotti 12 päivänä huhtikuuta 2019 unionin puolesta antamassaan julkilausumassa toimijoita lopettamaan haitalliset kybertoimet, joiden tavoitteena on heikentää unionin yhtenäisyyttä, turvallisuutta ja talouden kilpailukykyä, mukaan lukien kyberympäristöä hyväksi käyttäen tehdyt teollis- ja tekijänoikeuksiin kohdistuvat varkaudet. Tällaisia varkauksia kyberympäristöä hyväksi käyttäen on tehnyt muun muassa toimija, joka julkisuudessa tunnetaan nimellä ”APT10” (”Advanced Persistent Threat 10”).

(4) Tässä yhteydessä ja kybertoimintaympäristössä esiintyvän haitallisen käyttäytymisen jatkumisen ja lisääntymisen torjumiseksi, hillitsemiseksi ja estämiseksi sekä siihen reagoimiseksi, kuusi luonnollista henkilöä ja kolme yhteisöä tai elintä olisi sisällytettävä päätöksen (YUTP) 2019/797 liitteessä olevaan luetteloon luonnollisista henkilöistä, oikeushenkilöistä, yhteisöistä ja elimistä, joihin kohdistetaan rajoittavia toimenpiteitä. Kyseiset henkilöt ja yhteisöt tai elimet ovat vastuussa kyberhyökkäyksistä tai niiden yrityksistä taikka antoivat tukea niille tai osallistuivat niihin tai helpottivat niiden toteuttamista, mukaan lukien OPCW:tä vastaan tehty kyberhyökkäysyritys sekä kyberhyökkäykset, jotka julkisuudessa tunnetaan nimillä ”WannaCry” ja ”NotPetya” sekä ”Operation Cloud Hopper”.

(5) Päätös (YUTP) 2019/797 olisi näin ollen muutettava vastaavasti,

ON HYVÄKSYNYT TÄMÄN PÄÄTÖKSEN:

1 artikla

Muutetaan päätöksen (YUTP) 2019/797 liite tämän päätöksen liitteen mukaisesti.

([1]) Neuvoston päätös (YUTP) 2019/797, annettu 17 päivänä toukokuuta 2019, unionia tai sen jäsenvaltioita uhkaavien kyberhyökkäysten vastaisista rajoittavista toimenpiteistä (EUVL L 129 I, 17.5.2019, s. 13).

2 artikla

Tämä päätös tulee voimaan sinä päivänä, jona se julkaistaan *Euroopan unionin virallisessa lehdessä*.

Tehty Brysselissä 30 päivänä heinäkuuta 2020.

Neuvoston puolesta
Puheenjohtaja
M. ROTH

LIITE

Lisätään seuraavat henkilöt ja yhteisöt tai elimet päätöksen (YUTP) 2019/797 liitteessä olevaan luetteloon luonnollisista henkilöistä, oikeushenkilöistä, yhteisöistä ja elimistä:

”A. Luonnolliset henkilöt

	Nimi	Tunnistustiedot	Luetteloon merkitsemisen perusteet	Luetteloon merkitsemisen päivämäärä
1.	GAO Qiang	Syntymäpaikka: Shandongin maakunta, Kiina Osoite: Room 1102, Guanfu Mansion, 46 Xinkai Road, Hedong District, Tianjin, Kiina Kansalaisuus: kiinalainen Sukupuoli: mies	Gao Qiang on osallistunut ”Operation Cloud Hopper” nimellä tunnettuun sarjaan vaikutukseltaan merkittäviä kyberhyökkäyksiä, jotka ovat peräisin unionin ulkopuolelta ja jotka muodostavat unionille tai sen jäsenvaltioille ulkoisen uhkan, ja vaikutukseltaan merkittäviä kyberhyökkäyksiä kolmansia valtioita vastaan. ”Operation Cloud Hopper” -kyberhyökkäysten kohteena olivat monikansallisten yhtiöiden tietojärjestelmät kuudella mantereella, mukaan lukien unionissa sijaitsevat yhtiöt; hyökkäyksissä päästiin luvattomasti kaupallisesti arkaluonteisiin tietoihin, mistä aiheutui huomattavaa taloudellista tappiota. ”Operation Cloud Hopper” -kyberhyökkäykset toteutti toimija, joka julkisuudessa tunnetaan nimellä ”APT10” (”Advanced Persistent Threat 10”) (alias ”Red Apollo”, ”CVNX”, ”Stone Panda”, ”MenuPass” ja ”Potassium”). Gao Qiang voidaan yhdistää APT10:een, myös, koska hänellä on yhteyksiä APT10:n johtamis- ja valvontarakenteeseen. Lisäksi Gao Qiang on työskennellyt Huaying Haitai -yhtiössä, joka on nimetty yhteisöksi, joka antaa tukea ”Operation Cloud Hopper” -kyberhyökkäyksille ja helpottaa niiden toteuttamista. Hänellä on yhteyksiä Zhang Shilongiin, joka myös on nimetty ”Operation Cloud Hopper” -kyberhyökkäysten yhteydessä. Gao Qiangilla on siis yhteyksiä sekä Huaying Haitai -yhtiöön että Zhang Shilongiin.	30.7.2020
2.	ZHANG Shilong	Osoite: Hedong, Yuyang Road No 121, Tianjin, Kiina Kansalaisuus: kiinalainen Sukupuoli: mies	Zhang Shilong on osallistunut ”Operation Cloud Hopper” nimellä tunnettuun sarjaan vaikutukseltaan merkittäviä kyberhyökkäyksiä, jotka ovat peräisin unionin ulkopuolelta ja jotka muodostavat unionille tai sen jäsenvaltioille ulkoisen uhkan, ja vaikutukseltaan merkittäviä kyberhyökkäyksiä kolmansia valtioita vastaan. ”Operation Cloud Hopper” -kyberhyökkäysten kohteena ovat olleet monikansallisten yhtiöiden tietojärjestelmät kuudella mantereella, mukaan lukien unionissa sijaitsevat yhtiöt; hyökkäyksissä päästiin luvattomasti kaupallisesti arkaluonteisiin tietoihin, mistä aiheutui huomattavaa taloudellista tappiota. ”Operation Cloud Hopper” -kyberhyökkäykset toteutti toimija, joka julkisuudessa tunnetaan nimellä ”APT10” (”Advanced Persistent Threat 10”) (alias ”Red Apollo”, ”CVNX”, ”Stone Panda”, ”MenuPass” ja ”Potassium”).	30.7.2020

			Zhang Shilong voidaan yhdistää APT10:een, myös APT10:n toteuttamien kyberhyökkäysten yhteydessä hänen kehittämänsä ja testaamansa haittaohjelman kautta. Lisäksi Zhang Shilong on työskennellyt Huaying Haitai -yhtiössä, joka on nimetty yhteisöksi, joka antaa tukea ”Operation Cloud Hopper” -kyberhyökkäyksille ja helpottaa niiden toteuttamista. Hänellä on yhteyksiä Gao Qiangiin, joka myös on nimetty ”Operation Cloud Hopper” -kyberhyökkäysten yhteydessä. Zhang Shilongilla on siis yhteyksiä sekä Huaying Haitai -yhtiöön että Gao Qiangiin.	
3.	Alexey Valeryevich MININ	Алексей Валерьевич МИНИН Syntymäaika: 27.5.1972 Syntymäpaikka: Permin alue, Venäjän SFNT (nykyinen Venäjän federaatio) Passin numero: 120017582 Myöntänyt: Venäjän federaation ulkoministeriö Voimassa: 17.4.2017–17.4.2022 Oleskelupaikka: Moskova, Venäjän federaatio Kansalaisuus: venäläinen Sukupuoli: mies	Alexey Minin osallistui yritykseen toteuttaa mahdollisesti vaikutukseltaan merkittävä kyberhyökkäys Alankomaissa sijaitsevaa kemiallisten aseiden kieltojärjestöä (OPCW) vastaan. Venäjän federaation asevoimien yleisesikunnan pääosaston (GU/GRU) henkilötiedustelun tukiupseerina Alexey Minin kuului neljän venäläisen sotilastiedustelu-upseerin ryhmään, joka huhtikuussa 2018 yritti päästä luvattomasti Alankomaiden Haagissa sijaitsevan OPCW:n langattomaan verkkoon. Kyberhyökkäysyrityksen tavoitteena oli tehdä tietomurto OPCW:n langattomaan verkkoon; jos hyökkäys olisi onnistunut, se olisi vaarantanut verkon turvallisuuden ja OPCW:n meneillään olevat tutkinnat. Alankomaiden sotilastiedustelu- ja turvallisuuspalvelu (DISS) (Militaire Inlichtingen- en Veiligheidsdienst – MIVD) keskeytti kyberhyökkäysyrityksen ja näin esti vakavien vahinkojen aiheutumisen OPCW:lle.	30.7.2020
4.	Aleksei Sergeyvich MORENETS	Алексей Сергеевич МОРЕНЕЦ Syntymäaika: 31.7.1977 Syntymäpaikka: Murmanskin alue, Venäjän SFNT (nykyinen Venäjän federaatio) Passin numero: 100135556 Myöntänyt: Venäjän federaation ulkoministeriö Voimassa: 17.4.2017–17.4.2022 Oleskelupaikka: Moskova, Venäjän federaatio Kansalaisuus: venäläinen Sukupuoli: mies	Aleksei Morenets osallistui yritykseen toteuttaa mahdollisesti vaikutukseltaan merkittävä kyberhyökkäys Alankomaissa sijaitsevaa kemiallisten aseiden kieltojärjestöä (OPCW) vastaan. Venäjän federaation asevoimien yleisesikunnan pääosaston (GU/GRU) kyberoperaattorina Aleksei Morenets kuului neljän venäläisen sotilastiedustelu-upseerin ryhmään, joka huhtikuussa 2018 yritti päästä luvattomasti Alankomaiden Haagissa sijaitsevan OPCW:n langattomaan verkkoon. Kyberhyökkäysyrityksen tavoitteena oli tehdä tietomurto OPCW:n langattomaan verkkoon; jos hyökkäys olisi onnistunut, se olisi vaarantanut verkon turvallisuuden ja OPCW:n meneillään olevat tutkinnat. Alankomaiden sotilastiedustelu- ja turvallisuuspalvelu (DISS) (Militaire Inlichtingen- en Veiligheidsdienst – MIVD) keskeytti kyberhyökkäysyrityksen ja näin esti vakavien vahinkojen aiheutumisen OPCW:lle.	30.7.2020

5.	Evgenii Mikhaylovich SEREBRIAKOV	Евгений Михайлович СЕРЕБРЯКОВ Syntymäaika: 26.7.1981 Syntymäpaikka: Kurskin alue, Venäjän SFNT (nykyinen Venäjän federaatio) Passin numero: 100135555 Myöntänyt: Venäjän federaation ulkoministeriö Voimassa: 17.4.2017–17.4.2022 Oleskelupaikka: Moskova, Venäjän federaatio Kansalaisuus: venäläinen Sukupuoli: mies	Evgenii Serebriakov osallistui yritykseen toteuttaa mahdollisesti vaikutukseltaan merkittävä kyberhyökkäys Alankomaissa sijaitsevaa kemiallisten aseiden kieltojärjestöä (OPCW) vastaan. Venäjän federaation asevoimien yleisesikunnan pääosaston (GU/GRU) kyberoperaattorina Evgenii Serebriakov kuului neljän venäläisen sotilastiedustelu-upseerin ryhmään, joka huhtikuussa 2018 yritti päästä luvattomasti Alankomaiden Haagissa sijaitsevan OPCW:n langattomaan verkkoon. Kyberhyökkäysyrityksen tavoitteena oli tehdä tietomurto OPCW:n langattomaan verkkoon; jos hyökkäys olisi onnistunut, se olisi vaarantanut verkon turvallisuuden ja OPCW:n meneillään olevat tutkinnat. Alankomaiden sotilastiedustelu- ja turvallisuuspalvelu (DISS) (Militaire Inlichtingen- en Veiligheidsdienst – MIVD) keskeytti kyberhyökkäysyrityksen ja näin esti vakavien vahinkojen aiheutumisen OPCW:lle.	30.7.2020
6.	Oleg Mikhaylovich SOTNIKOV	Олег Михайлович СОТНИКОВ Syntymäaika: 24.8.1972 Syntymäpaikka: Uljanovskin alue, Venäjän SFNT (nykyinen Venäjän federaatio) Passin numero: 120018866 Myöntänyt: Venäjän federaation ulkoministeriö Voimassa: 17.4.2017–17.4.2022 Oleskelupaikka: Moskova, Venäjän federaatio Kansalaisuus: venäläinen Sukupuoli: mies	Oleg Sotnikov osallistui yritykseen toteuttaa mahdollisesti vaikutukseltaan merkittävä kyberhyökkäys Alankomaissa sijaitsevaa kemiallisten aseiden kieltojärjestöä (OPCW) vastaan. Venäjän federaation asevoimien yleisesikunnan pääosaston (GU/GRU) henkilötiedustelun tukiupseerina Oleg Sotnikov kuului neljän venäläisen sotilastiedustelu-upseerin ryhmään, joka huhtikuussa 2018 yritti päästä luvattomasti Alankomaiden Haagissa sijaitsevan OPCW:n langattomaan verkkoon. Kyberhyökkäysyrityksen tavoitteena oli tehdä tietomurto OPCW:n langattomaan verkkoon; jos hyökkäys olisi onnistunut, se olisi vaarantanut verkon turvallisuuden ja OPCW:n meneillään olevat tutkinnat. Alankomaiden sotilastiedustelu- ja turvallisuuspalvelu (DISS) (Militaire Inlichtingen- en Veiligheidsdienst – MIVD) keskeytti kyberhyökkäysyrityksen ja näin esti vakavien vahinkojen aiheutumisen OPCW:lle.	30.7.2020

B. Oikeushenkilöt, yhteisöt ja elimet

	Nimi	Tunnistustiedot	Luetteloon merkitsemisen perusteet	Luetteloon merkitsemisen päivämäärä
1.	Tianjin Huaying Haitai Science and Technology Development Co. Ltd (Huaying Haitai)	Alias: Haitai Technology Development Co. Ltd Paikka: Tianjin, Kiina	Huaying Haitai -yhtiö antoi taloudellista, teknistä tai aineellista tukea ja helpotti toimia, jotka liittyivät ”Operation Cloud Hopper” nimellä tunnettuun sarjaan vaikutukseltaan merkittäviä kyberhyökkäyksiä, jotka ovat peräisin unionin ulkopuolelta ja jotka muodostavat unionille tai sen jäsenvaltioille ulkoisen uhkan, ja vaikutukseltaan merkittäviä kyberhyökkäyksiä kolmansia valtioita vastaan.	30.7.2020

			”Operation Cloud Hopper” -kyberhyökkäysten kohteena ovat olleet monikansallisten yhtiöiden tietojärjestelmät kuudella mantereella, mukaan lukien unionissa sijaitsevat yhtiöt; hyökkäyksissä päästiin luvattomasti kaupallisesti arkaluonteisiin tietoihin, mistä aiheutui huomattavaa taloudellista tappiota. ”Operation Cloud Hopper” -kyberhyökkäykset toteutti toimija, joka julkisuudessa tunnetaan nimellä ”APT10” (”Advanced Persistent Threat 10”) (alias ”Red Apollo”, ”CVNX”, ”Stone Panda”, ”MenuPass” ja ”Potassium”). Huaying Haitai -yhtiö voidaan yhdistää APT10:een. Lisäksi Huaying Haitai -yhtiössä työskentelivät Gao Qiang ja Zhang Shilong, jotka molemmat on nimetty ”Operation Cloud Hopper” -kyberhyökkäysten yhteydessä. Huaying Haitai -yhtiöllä on siis yhteyksiä sekä Gao Qiangiin että Zhang Shilongiin.	
2.	Chosun Expo	Alias: Chosen Expo; Korea Export Joint Venture Paikka: Korean demokraattinen kansantasavalta	Chosun Expo -yhtiö antoi taloudellista, teknistä tai aineellista tukea ja helpotti toimia, jotka liittyivät sarjaan vaikutukseltaan merkittäviä kyberhyökkäyksiä, jotka ovat peräisin unionin ulkopuolelta ja jotka muodostavat unionille tai sen jäsenvaltioille ulkoisen uhkan, ja vaikutukseltaan merkittäviä kyberhyökkäyksiä kolmansia valtioita vastaan, mukaan lukien kyberhyökkäykset, jotka julkisuudessa tunnetaan nimellä ”WannaCry”, ja kyberhyökkäykset Puolan rahoitustarkastuslaitosta ja Sony Pictures Entertainment -yhtiötä vastaan sekä Bangladesh Bank -pankkiin tehty kybervarkaus ja Vietnam Tien Phong Bank -pankkiin tehty kybervarkausyritys. ”WannaCry” -kyberhyökkäykset sekoittivat tietojärjestelmät eri puolilla maailmaa kohdistamalla niihin kiristyshaittaohjelman ja estämällä pääsyn tietoihin. Ne vaikuttivat yhtiöiden tietojärjestelmiin unionissa ja myös jäsenvaltioiden keskeisten palvelujen ja taloudellisten toimintojen ylläpitämiseksi välttämättömiin palveluihin liittyviin tietojärjestelmiin. ”WannaCry” -kyberhyökkäykset toteutti toimija, joka julkisuudessa tunnetaan nimellä ”APT38” (”Advanced Persistent Threat 38”) tai ”Lazarus Group”. Chosun Expo -yhtiö voidaan yhdistää APT38:aan/Lazarus Groupiin, myös kyberhyökkäyksissä käytettyjen tilien kautta.	30.7.2020
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)	Osoite: 22 Kirova Street, Moskova, Venäjän federaatio	Venäjän federaation asevoimien yleisesikunnan pääosaston (GU/GRU) erikoisteknologioiden pääkeskus (GTsST), johon viitataan myös kenttäpostinumeronsa 74455 mukaan, on vastuussa vaikutukseltaan merkittävistä kyberhyökkäyksistä, jotka ovat peräisin unionin ulkopuolelta ja jotka muodostavat unionille tai sen jäsenvaltioille ulkoisen uhkan, ja vaikutukseltaan merkittävistä kyberhyökkäyksistä kolmansia valtioita vastaan, mukaan lukien kesäkuussa 2017 tehdyt kyberhyökkäykset, jotka julkisuudessa tunnetaan nimellä ”NotPetya” tai ”EternalPetya”, ja Ukrainan sähköverkkoon talvella 2015–2016 kohdistetut kyberhyökkäykset.	30.7.2020”

			”NotPetya”- tai ”EternalPetya”-kyberhyökkäykset tekivät tietojen käytön mahdottomaksi useissa yhtiöissä unionissa, muualla Euroopassa ja maailmanlaajuisesti kohdistamalla tietokoneisiin kiristyshaittaohjelman ja estämällä pääsyn tietoihin, mistä aiheutui muun muassa huomattavaa taloudellista tappiota. Ukrainan sähköverkko oli siihen kohdistetun kyberhyökkäyksen vuoksi talvella osittain kytkettynä pois toiminnasta. ”NotPetya”- tai ”EternalPetya”-kyberhyökkäykset toteutti toimija, joka julkisuudessa tunnetaan nimellä ”Sandworm” (alias ”Sandworm Team”, ”BlackEnergy Group”, ”Voodoo Bear”, ”Quedagh”, ”Olympic Destroyer” ja ”Telebots”) ja joka on myös vastuussa hyökkäyksestä Ukrainan sähköverkkoa vastaan. Venäjän federaation asevoimien yleisesikunnan pääosaston erikoisteknologioiden pääkeskuksella on aktiivinen rooli ”Sandwormin” kybertoiminnassa, ja se voidaan yhdistää ”Sandwormiin”.	