NÕUKOGU OTSUS (ÜVJP) 2020/1127,

30. juuli 2020,

millega muudetakse otsust (ÜVJP) 2019/797 piiravate meetmete kohta, millega takistada liitu või selle liikmesriike ähvardavaid küberrünnete

EUROOPA LIIDU NÕUKOGU,

võttes arvesse Euroopa Liidu lepingut, eriti selle artiklit 29,

võttes arvesse liidu välisasjade ja julgeolekupoliitika kõrge esindaja ettepanekut

ning arvestades järgmist:

(1) Nõukogu võttis 17. mail 2019 vastu otsuse (ÜVJP) 2019/797 ([1]).

(2) Sihipärased piiravad meetmed märkimisväärse mõjuga küberrünnete vastu, mis kujutavad liidule või selle liikmesriikidele välist ohtu, on osa pahatahtlikule kübertegevusele liidu ühise diplomaatilise reageerimise raamistikku („küberdiplomaatia meetmete kogum“) kuuluvatest meetmetest ning oluline vahend sellise tegevuse ärahoidmiseks ja sellele reageerimiseks. Piiravaid meetmeid võib kohaldada ka vastusena märkimisväärse mõjuga küberrünnetele, mis on suunatud kolmandate riikide või rahvusvaheliste organisatsioonide vastu, kui seda peetakse vajalikuks Euroopa Liidu lepingu artikli 21 asjakohastes sätetes sätestatud ühiste välis- ja julgeolekupoliitika eesmärkide saavutamiseks.

(3) Nõukogu võttis 16. aprillil 2018 vastu järeldused, milles ta mõistis kindlalt hukka info- ja kommunikatsioonitehnoloogia pahatahtliku kasutamise, sealhulgas WannaCry ja NotPetya nime all tuntud küberrünnetes, mis tekitasid suurt kahju ja majanduslikku kahjumit nii liidus kui ka mujal. Euroopa Ülemkogu eesistuja ja Euroopa Komisjoni president ning liidu välisasjade ja julgeolekupoliitika kõrge esindaja („kõrge esindaja“) väljendasid oma 4. oktoobri 2018. aasta ühisavalduses tõsist muret seoses küberrünnetega, mille eesmärk oli õõnestada Keemiarelvade Keelustamise Organisatsiooni (OPCW) terviklikkust Madalmaades; tegemist oli agressiivse teoga, millega näidati üles vaenulikkust OPCW ametliku eesmärgi vastu. 12. aprillil 2019 liidu nimel tehtud avalduses kutsus kõrge esindaja pooli üles lõpetama liidu terviklikkuse, turvalisuse ja majandusliku konkurentsivõime kahjustamise eesmärgil küberruumis toimuv pahatahtlik tegevus, sealhulgas küberruumi kasutades toime pandud intellektuaalomandi vargused. Need küberruumi kasutades toime pandud vargused hõlmavad ka selliseid vargusi, mille korraldaja on üldsusele tuntud kui APT10 (Advanced Persistent Threat 10).

(4) Sellega seoses ning küberruumis jätkuva ja kasvava pahatahtliku käitumise ennetamiseks, takistamiseks, ärahoidmiseks ja sellele reageerimiseks tuleks otsuse (ÜVJP) 2019/797 lisas esitatud nende füüsiliste ja juriidiliste isikute, üksuste ja asutuste loetellu, kelle suhtes kohaldatakse piiravaid meetmeid, kanda kuus füüsilist isikut ja kolm üksust või asutust. Need isikud, üksused ja asutused vastutavad küberrünnete või küberrünnete katsete eest, toetasid neid või olid nendega seotud või hõlbustasid neid, sealhulgas OPCW vastu suunatud küberrünnete katsed ning WannaCry ja NotPetya, samuti operatsiooni Cloud Hopper nime all tuntud küberründed.

(5) Otsust (ÜVJP) 2019/797 tuleks seetõttu vastavalt muuta,

ON VASTU VÕTNUD KÄESOLEVA OTSUSE:

Artikkel 1

Otsuse (ÜVJP) 2019/797 lisa muudetakse vastavalt käesoleva otsuse lisale.

([1]) Nõukogu 17. mai 2019. aasta otsus (ÜVJP) 2019/797 piiravate meetmete kohta, millega takistada liitu või selle liikmesriike ähvardavaid küberrünnete (ELT L 129 I, 17.5.2019, lk 13).

Artikkel 2

Käesolev otsus jõustub *Euroopa Liidu Teatajas* avaldamise päeval.

Brüssel, 30. juuli 2020

Nõukogu nimel
eesistuja
M. ROTH

LISA

Järgmised isikud, üksused ja asutused lisatakse otsuse (EL) 2019/797 lisas esitatud füüsiliste või juriidiliste isikute, üksuste ja asutuste loetellu.

„A. Füüsilised isikud

	Nimi	Tuvastamisandmed	Põhjused	Loetellu kandmise kuupäev
1.	GAO Qiang	Sünnikoht: Shandongi provints, Hiina Aadress: Room 1102, Guanfu Mansion, 46 Xinkai Road, Hedong District, Tianjin, Hiina Kodakondsus: Hiina Sugu: mees	Gao Qiang on seotud operatsiooniga Cloud Hopper, mis on selliste väljastpoolt liitu pärinevate märkimisväärse mõjuga küberrünnete seeria, mis kujutavad liidule või selle liikmesriikidele välisohtu, ning märkimisväärse mõjuga küberrünnete seeria, mis on suunatud kolmandate riikide vastu. Operatsiooni Cloud Hopper käigus rünnati rahvusvaheliste ettevõtjate infosüsteeme kuues maailmajaos, sealhulgas liidus asuvate ettevõtjate omasid, ning saadi loata juurdepääs tundlikele äriandmetele, põhjustades sellega suurt majanduslikku kahju. Operatsiooni Cloud Hopper korraldaja on tuntud nime all APT10 (Advanced Persistent Threat 10) (teise nimega Red Apollo, CVNX, Stone Panda, MenuPass ja Potassium). Gao Qiangi võib olla seotud APT10ga, sealhulgas APT10 juhtimis- ja kontrollitaristuga. Lisaks töötas Gao Qiang Huaying Haitai heaks, mis on operatsiooni Cloud Hopper toetamise ja hõlbustamise eest loetellu kantud üksus. Tal on sidemed Zhang Shilongiga, kes on samuti kantud loetellu seoses operatsiooniga Cloud Hopper. Gao Qiangi seostatakse seega nii Huaying Haitai kui ka Zhang Shilongiga.	30.7.2020
2.	ZHANG Shilong	Aadress: Hedong, Yuyang Road nr 121, Tianjin, Hiina Kodakondsus: Hiina Sugu: mees	Zhang Shilong on seotud operatsiooniga Cloud Hopper, mis on selliste väljastpoolt liitu pärinevate märkimisväärse mõjuga küberrünnete seeria, mis kujutavad liidule või selle liikmesriikidele välisohtu, ning märkimisväärse mõjuga küberrünnete seeria, mis on suunatud kolmandate riikide vastu. Operatsiooni Cloud Hopper käigus rünnati rahvusvaheliste ettevõtjate infosüsteeme kuues maailmajaos, sealhulgas liidus asuvate ettevõtjate omasid, ning saadi loata juurdepääs tundlikele äriandmetele, põhjustades sellega suurt majanduslikku kahju. Operatsiooni Cloud Hopper korraldaja on tuntud nime all APT10 (Advanced Persistent Threat 10) (teise nimega Red Apollo, CVNX, Stone Panda, MenuPass ja Potassium).	30.7.2020

			Zhang Shilong võib olla seotud APT10ga, sealhulgas seoses pahavaraga, mille ta APT10 poolt toime pandud küberrünnetega seoses välja töötas ja testis. Lisaks töötas Zhang Shilong Huaying Haitai heaks, mis on operatsiooni Cloud Hopper toetamise ja hõlbustamise eest loetellu kantud üksus. Tal on sidemed Gao Qiangiga, kes on samuti kantud loetellu seoses operatsiooniga Cloud Hopper. Zhang Shilongi seostatakse seega nii Huaying Haitai kui ka Gao Qiangiga.	
3.	Alexey Valeryevich MININ	Алексей Валерьевич МИНИН Sünniaeg: 27. mai 1972 Sünnikoht: Permi oblast, Venemaa NFSV (praegune Venemaa Föderatsioon) Pass nr: 120017582 Välja andnud: Venemaa Föderatsiooni välisministeerium Kehtivusaeg: 17. aprillist 2017 kuni 17. april lini 2022 Asukoht: Moskva, Venemaa Föderatsioon Kodakondsus: Venemaa Sugu: mees	Alexey Minin osales küberründekatses, millel oleks võinud olla potentsiaalselt märkimisväärne mõju Keemiarelvade Keelustamise Organisatsioonile (OPCW) Madalmaades. Venemaa Föderatsiooni relvajõudude peastaabi peadirektoraadi (GU/GRU) inimluure tugiohvitserina kuulus Alexey Minin neljast Venemaa sõjaväeluureohvitserist koosnevasse rühma, kes püüdsid 2018. aasta aprillis saada loata juurdepääsu OPCW WiFi võrgule Madalmaades Haagis. Küberründekatse eesmärk oli häkkida sisse OPCW WiFi võrku, mis edu korral oleks ohustanud võrgu turvalisust ja OPCW käimasolevat uurimistegevust. Madalmaade kaitsealase luure- ja julgeolekuteenistus (DISS) (Militaire Inlichtingen- en Veiligheidsdienst – MIVD) takistas küberründekatse lõpuleviimist, hoides seeläbi ära tõsise kahju OPCW-le.	30.7.2020
4.	Aleksei Sergeyvich MORENETS	Алексей Сергеевич МОРЕНЕЦ Sünniaeg: 31. juuli 1977 Sünnikoht: Murmanski oblast, Venemaa NFSV (praegune Venemaa Föderatsioon) Pass nr: 100135556 Välja andnud: Venemaa Föderatsiooni välisministeerium Kehtivusaeg: 17. aprillist 2017 kuni 17. april lini 2022 Asukoht: Moskva, Venemaa Föderatsioon Kodakondsus: Venemaa Sugu: mees	Aleksei Morenets osales küberründekatses, millel oleks võinud olla potentsiaalselt märkimisväärne mõju Keemiarelvade Keelustamise Organisatsioonile (OPCW) Madalmaades. Venemaa Föderatsiooni relvajõudude peastaabi peadirektoraadi (GU/GRU) küberspetsialistina kuulus Aleksei Morenets neljast Venemaa sõjaväeluureohvitserist koosnevasse rühma, kes püüdsid 2018. aasta aprillis saada loata juurdepääsu OPCW WiFi võrgule Madalmaades Haagis. Küberründekatse eesmärk oli häkkida sisse OPCW WiFi võrku, mis edu korral oleks ohustanud võrgu turvalisust ja OPCW käimasolevat uurimistegevust. Madalmaade kaitsealase luure- ja julgeolekuteenistus (DISS) (Militaire Inlichtingen- en Veiligheidsdienst – MIVD) takistas küberründekatse lõpuleviimist, hoides seeläbi ära tõsise kahju OPCW-le.	30.7.2020

5.	Evgenii Mikhaylovich SEREBRIAKOV	Евгений Михайлович СЕРЕБРЯКОВ Sünniaeg: 26. juuli 1981 Sünnikoht: Kursk, Venemaa NFSV (praegune Venemaa Föderatsioon) Pass nr: 100135555 Välja andnud: Venemaa Föderatsiooni välisministeerium Kehtivusaeg: 17. aprillist 2017 kuni 17. aprillini 2022 Asukoht: Moskva, Venemaa Föderatsioon Kodakondsus: Venemaa Sugu: mees	Evgenii Serebriakov osales küberründekatses, millel oleks võinud olla potentsiaalselt märkimisväärne mõju Keemiarelvade Keelustamise Organisatsioonile (OPCW) Madalmaades. Venemaa Föderatsiooni relvajõudude peastaabi peadirektoraadi (GU/GRU) küberspetsialistina kuulus Evgenii Serebriakov neljast Venemaa sõjaväeluureohvitserist koosnevasse rühma, kes püüdsid 2018. aasta aprillis saada loata juurdepääsu OPCW WiFi võrgule Madalmaades Haagis. Küberründekatse eesmärk oli häkkida sisse OPCW WiFi võrku, mis edu korral oleks ohustanud võrgu turvalisust ja OPCW käimasolevat uurimistegevust. Madalmaade kaitsealase luure- ja julgeolekuteenistus (DISS) (Militaire Inlichtingen- en Veiligheidsdienst – MIVD) takistas küberründekatse lõpuleviimist, hoides seeläbi ära tõsise kahju OPCW-le.	30.7.2020
6.	Oleg Mikhaylovich SOTNIKOV	Олег Михайлович СОТНИКОВ Sünniaeg: 24. august 1972 Sünnikoht: Uljanovsk, Venemaa NFSV (praegune Venemaa Föderatsioon) Pass nr: 120018866 Välja andnud: Venemaa Föderatsiooni välisministeerium Kehtivusaeg: 17. aprillist 2017 kuni 17. aprillini 2022 Asukoht: Moskva, Venemaa Föderatsioon Kodakondsus: Venemaa Sugu: mees	Oleg Sotnikov osales küberründekatses, millel oleks võinud olla potentsiaalselt märkimisväärne mõju Keemiarelvade Keelustamise Organisatsioonile (OPCW) Madalmaades. Venemaa Föderatsiooni relvajõudude peastaabi peadirektoraadi (GU/GRU) inimluure tugiohvitserina kuulus Oleg Sotnikov neljast Venemaa sõjaväeluureohvitserist koosnevasse rühma, kes püüdsid 2018. aasta aprillis saada loata juurdepääsu OPCW WiFi võrgule Madalmaades Haagis. Küberründekatse eesmärk oli häkkida sisse OPCW WiFi võrku, mis edu korral oleks ohustanud võrgu turvalisust ja OPCW käimasolevat uurimistegevust. Madalmaade kaitsealase luure- ja julgeolekuteenistus (DISS) (Militaire Inlichtingen- en Veiligheidsdienst – MIVD) takistas küberründekatse lõpuleviimist, hoides seeläbi ära tõsise kahju OPCW-le.	30.7.2020

B. Juriidilised isikud, üksused ja asutused

	Nimi	Tuvastamisandmed	Põhjused	Loetellu kandmise kuupäev
1.	Tianjin Huaying Haitai Science and Technology Development Co. Ltd (Huaying Haitai)	Teise nimega: Haitai Technology Development Co. Ltd Asukoht: Tianjin, Hiina	Huaying Haitai pakkus rahalist, tehnilist või materiaalset toetust ja aitas kaasa operatsioonile Cloud Hopper, mis on selliste väljastpoolt liitu pärinevate märkimisväärse mõjuga küberrünnete seeria, mis kujutavad liidule või selle liikmesriikidele välisohtu, ning selliste märkimisväärse mõjuga küberrünnete seeria, mis on suunatud kolmandate riikide vastu.	30.7.2020

			Operatsiooni Cloud Hopper käigus rünnati rahvusvaheliste ettevõtjate infosüsteeme kuues maailmajaos, sealhulgas liidus asuvate ettevõtjate omasid, ning saadi loata juurdepääs tundlikele äriandmetele, põhjustades sellega suurt majanduslikku kahju. Operatsiooni Cloud Hopper korraldaja on tuntud nime all APT10 (Advanced Persistent Threat 10) (teise nimega Red Apollo, CVNX, Stone Panda, MenuPass ja Potassium). Huaying Haitai võib olla seotud APT10ga. Lisaks töötasid Huaying Haitai heaks Gao Qiang ja Zhang Shilong, kes mõlemad on kantud loetellu seoses operatsiooniga Cloud Hopper. Huaying Haitaid seostatakse seega Gao Qiangi ja Zhang Shilongiga.	
2.	Chosun Expo	Teise nimega: Chosen Expo; Korea Export Joint Venture Asukoht: KRDV	Chosun Expo pakkus rahalist, tehnilist või materiaalset toetust ja aitas kaasa mitmetele väljastpoolt liitu pärinevatele märkimisväärse mõjuga küberrünnetele, mis kujutavad liidule või selle liikmesriikidele välisohtu, ning märkimisväärse mõjuga küberrünnetele, mis on suunatud kolmandate riikide vastu, sealhulgas WannaCry nime all tuntud küberründed ning küberründed Poola finantsjärelevalveameti ja Sony Pictures Entertainmenti vastu, samuti kübervargus pangas Bangladesh Bank ja kübervarguse katse pangas Vietnam Tien Phong Bank. WannaCry häiris infosüsteeme kogu maailmas, rünnates lunavara abil infosüsteeme ja tõkestades juurdepääsu andmetele. See mõjutas liidu ettevõtjate infosüsteeme, sealhulgas infosüsteeme, mis on seotud elutähtsate teenustega ja majandustegevuse säilitamiseks vajalike teenustega liikmesriikides. Küberründe WannaCry korraldajad on tuntud nime all APT38 (Advanced Persistent Threat 38) või Lazarus Group. Chosun Expo võib olla seotud APT38-ga/Lazarus Groupiga, sealhulgas küberründe jaoks kasutatud kontode kaudu.	30.7.2020
3.	Venemaa Föderatsiooni relvajõudude peastaabi (GU/GRU) peadirektoraadi eritehnoloogia põhikeskus (GTsST)	Aadress: 22 Kirova Street, Moscow, Russian Federation	Venemaa Föderatsiooni relvajõudude peastaabi peadirektoraadi (GU/GRU) eritehnoloogia põhikeskus (GTsST), mida tuntakse ka selle sihtnumbri 74455 all, vastutab väljastpoolt liitu pärinevate märkimisväärse mõjuga küberrünnete eest, mis kujutavad liidule või selle liikmesriikidele välisohtu, ning märkimisväärse mõjuga küberrünnete eest, mis on suunatud kolmandate riikide vastu, sealhulgas 2017. aasta juunis toimunud küberründed, mida tuntakse NotPetya või EternalPetya nime all ning 2015. aasta ja 2016. aasta talvel toimunud küberründed Ukraina elektrivõrguettevõtja vastu.	30.7.2020“

			Küberrünne NotPetya ehk EternalPetya muutis andmed kättesaamatuks paljudes ettevõtetes liidus, laiemalt Euroopas ja maailmas, rünnates lunavara abil arvuteid ja blokeerides andmetele juurdepääsu, mis muu hulgas põhjustas suurt majanduslikku kahju. Ukraina elektrivõrguettevõtja vastu suunatud küberründe tulemusena oli talvel osa elektrivõrgust välja lülitatud. NotPetya ehk EternalPetya korraldaja oli Sandworm (teise nimega Sandworm Team, BlackEnergy Group, Voodoo Bear, Quedagh, Olympic Destroyer ja Telebots), kes on samuti Ukraina elektrivõrguettevõtja vastu suunatud rünnaku taga. Venemaa Föderatsiooni relvajõudude peastaabi peadirektoraadi eritehnoloogia põhikeskusel on aktiivne roll Sandwormi kübertegevuses ja seda saab seostada Sandwormiga.	