PADOMES ĪSTENOŠANAS REGULA (ES) 2020/1125

(2020. gada 30. jūlijs),

ar ko īsteno Regulu (ES) 2019/796 par ierobežojošiem pasākumiem pret kiberuzbrukumiem, kuri apdraud Savienību vai tās dalībvalstis

EIROPAS SAVIENĪBAS PADOME,

ņemot vērā Līgumu par Eiropas Savienības darbību,

ņemot vērā Padomes Regulu (ES) 2019/796 (2019. gada 17. maijs) par ierobežojošiem pasākumiem pret kiberuzbrukumiem, kuri apdraud Savienību vai tās dalībvalstis ([1]), un jo īpaši tās 13. panta 1. punktu,

ņemot vērā Savienības Augstā pārstāvja ārlietās un drošības politikas jautājumos priekšlikumu,

tā kā:

(1) Padome 2019. gada 17. maijā pieņēma Regulu (ES) 2019/796.

(2) Mērķtiecīgi ierobežojoši pasākumi pret kiberuzbrukumiem ar būtisku ietekmi, kas ir ārējs apdraudējums Savienībai vai tās dalībvalstīm, ir to pasākumu skaitā, kuri iekļauti Savienības satvarā vienotai diplomātiskajai reakcijai uz ļaunprātīgām kiberdarbībām (kiberdiplomātijas instrumentu kopums), un ir svarīgs instruments, lai atturētu no šādām darbībām un reaģētu uz tām. Ierobežojošus pasākumus var arī piemērot, reaģējot uz kiberuzbrukumiem ar būtisku ietekmi, kas veikti pret trešām valstīm vai starptautiskām organizācijām, ja tas tiek uzskatīts par nepieciešamu, lai sasniegtu Līguma par Eiropas Savienību 21. panta attiecīgajos noteikumos izklāstītos kopējos ārpolitikas un drošības politikas mērķus.

(3) Padome 2018. gada 16. aprīlī pieņēma secinājumus, kuros tā stingri nosodīja informācijas un komunikācijas tehnoloģiju ļaunprātīgu izmantošanu, tostarp kiberuzbrukumos, kas publiski zināmi kā "*WannaCry*" un "*NotPetya*" un kas izraisīja nozīmīgu kaitējumu un ekonomiskus zaudējumus Savienībā un ārpus tās. 2018. gada 4. oktobrī Eiropadomes un Eiropas Komisijas priekšsēdētāji un Savienības Augstā pārstāve ārlietās un drošības politikas jautājumos ("Augstā pārstāve") kopīgajā paziņojumā pauda nopietnas bažas par mēģinājumu veikt kiberuzbrukumu Ķīmisko ieroču aizlieguma organizācijai (*OPCW*) Nīderlandē nolūkā graut tās integritāti – agresīvu aktu, ar ko tika izrādīta necieņa *OPCW* svarīgajai sūtībai. Augstā pārstāve Savienības vārdā sniegtā deklarācijā 2019. gada 12. aprīlī mudināja attiecīgos aktorus izbeigt īstenot ļaunprātīgas kiberdarbības, kuru mērķis ir graut Savienības integritāti, drošību un ekonomisko konkurētspēju, tostarp tādas intelektuālā īpašuma zādzības, ko iespējamu dara kibertelpa. Šādas zādzības, ko iespējamu dara kibertelpa, ietver zādzības, ko veicis aktors, kas publiski zināms kā "*APT10*" ("*Advanced Persistent Threat 10*").

(4) Šajā sakarā un lai novērstu un nepieļautu nepārtrauktu un arvien spēcīgāku ļaunprātīgu rīcību kibertelpā, atturētu no tās un reaģētu uz to, Regulas (ES) 2019/796 I pielikumā ietvertajā to fizisko un juridisko personu, vienību un struktūru sarakstā, kurām piemēro ierobežojošus pasākumus, būtu jāiekļauj sešas fiziskas personas un trīs vienības vai struktūras. Minētās personas un vienības vai struktūras ir atbildīgas par kiberuzbrukumiem vai kiberuzbrukumu mēģinājumiem, tostarp kiberuzbrukuma mēģinājumiem pret *OPCW* un kiberuzbrukumiem, kas publiski zināmi kā "*WannaCry*" un "*NotPetya*", kā arī "*Operation Cloud Hopper*", vai ir tos atbalstījušas, vai bijušas tajos iesaistītas vai ir tos sekmējušas.

(5) Tāpēc Regula (ES) 2019/796 būtu attiecīgi jāgroza,

IR PIEŅĒMUSI ŠO REGULU.

1. pants

Regulas (ES) 2019/796 I pielikumu groza saskaņā ar šīs regulas pielikumu.

([1]) OV L 129I, 17.5.2019., 1. lpp.

2. pants

Šī regula stājas spēkā dienā, kad to publicē *Eiropas Savienības Oficiālajā Vēstnesī*.

Šī regula uzliek saistības kopumā un ir tieši piemērojama visās dalībvalstīs.

Briselē, 2020. gada 30. jūlijā

Padomes vārdā –
priekšsēdētājs
M. ROTH

PIELIKUMS

Regulas (ES) 2019/796 I pielikumā iekļauto fizisko un juridisko personu, vienību un struktūru sarakstu papildina ar turpmāk minētajām personām un vienībām vai struktūrām:

"A. Fiziskas personas

	Vārds	Identifikācijas informācija	Pamatojums	Sarakstā iekļaušanas datums
1.	GAO Qiang	Dzimšanas vieta: *Shandong* province, Ķīna Adrese: Room 1102, Guanfu Mansion, 46 Xinkai Road, Hedong District, Tianjin, China Valstspiederība: Ķīnas Dzimums: vīrietis	*Gao Qiang* ir iesaistīts "*Operation Cloud Hopper*" – virknē kiberuzbrukumu ar būtisku ietekmi, kuru izcelsme ir ārpus Savienības un kuri rada ārēju apdraudējumu Savienībai vai tās dalībvalstīm, un ar būtisku ietekmi uz trešām valstīm. "*Operation Cloud Hopper*" bija vērsta pret daudznacionālu uzņēmumu informācijas sistēmām, kuri atrodas sešos kontinentos, tostarp to uzņēmumu informācijas sistēmām, kuri atrodas Savienībā, un tās ietvaros neatļauti piekļuva komerciāli sensitīviem datiem, tādējādi radot ievērojamus ekonomiskus zaudējumus.	30.7.2020.
			"*Operation Cloud Hopper*" veica aktors, kas publiski zināms kā "*APT10*" ("*Advanced Persistent Threat 10*") (jeb "*Red Apollo*", "*CVNX*", "*Stone Panda*", "*MenuPass*" un "*Potassium*"). *Gao Qiang* var būt saistīts ar *APT10*, tostarp esot saistīts ar *APT10* vadības un kontroles infrastruktūru. Turklāt *Gao Qiang* bija nodarbināts *Huaying Haitai* – vienībā, kas iekļauta sarakstā, jo sniedza atbalstu "*Operation Cloud Hopper*" un sekmēja to. Viņam ir saiknes ar *Zhang Shilong*, kurš arī ir iekļauts sarakstā saistībā ar "*Operation Cloud Hopper*". Tāpēc *Gao Qiang* ir saistīts gan ar *Huaying Haitai*, gan ar *Zhang Shilong*.	
2.	ZHANG Shilong	Adrese: Hedong, Yuyang Road No 121, Tianjin, China Valstspiederība: Ķīnas Dzimums: vīrietis	*Zhang Shilong* ir iesaistīts "*Operation Cloud Hopper*" – virknē kiberuzbrukumu ar būtisku ietekmi, kuru izcelsme ir ārpus Savienības un kuri rada ārēju apdraudējumu Savienībai vai tās dalībvalstīm, un ar būtisku ietekmi uz trešām valstīm. "*Operation Cloud Hopper*" bija vērsta pret daudznacionālu uzņēmumu informācijas sistēmām, kuri atrodas sešos kontinentos, tostarp to uzņēmumu informācijas sistēmām, kuri atrodas Savienībā, un tās ietvaros neatļauti piekļuva komerciāli sensitīviem datiem, tādējādi radot ievērojamus ekonomiskus zaudējumus. "*Operation Cloud Hopper*" veica aktors, kas publiski zināms kā "*APT10*" ("*Advanced Persistent Threat 10*") (jeb "*Red Apollo*", "*CVNX*", "*Stone Panda*", "*MenuPass*" un "*Potassium*").	30.7.2020.
			Zhang Shilong var būt saistīts ar *APT10*, tostarp saistībā ar ļaunprogrammatūru, ko viņš izstrādāja un testēja saistībā ar *APT10* veiktajiem kiberuzbrukumiem. Turklāt *Zhang Shilong* bija nodarbināts *Huaying Haitai* – vienībā, kas iekļauta sarakstā, jo sniedza atbalstu "*Operation Cloud Hopper*" un sekmēja to. Viņam ir saiknes ar *Gao Qiang*, kurš arī ir iekļauts sarakstā saistībā ar "*Operation Cloud Hopper*". Tāpēc *Zhang Shilong* ir saistīts gan ar *Huaying Haitai*, gan ar *Gao Qiang*.	

3.	Alexey Valeryevich MININ	Алексей Валерьевич МИНИН Dzimšanas datums: 1972. gada 27. maijs Dzimšanas vieta: *Perm Oblast,* Krievijas PFSR (tagad Krievijas Federācija) Pases numurs: 120017582 Izdevusi Krievijas Federācijas Ārlietu ministrija Derīga no 2017. gada 17. aprīļa līdz 2022. gada 17. aprīlim Vieta: *Moscow,* Krievijas Federācija Valstspiederība: Krievijas Dzimums: vīrietis	*Alexey Minin* piedalījās kiberuzbrukuma ar potenciāli būtisku ietekmi mēģinājumā pret Ķīmisko ieroču aizlieguma organizāciju (*OPCW*) Nīderlandē. Būdams cilvēku veiktas izlūkošanas atbalsta virsnieks Krievijas Federācijas Bruņoto spēku Ģenerālštāba Galvenajā pārvaldē (*GU/GRU*), *Alexey Minin* bija četru Krievijas militārās izlūkošanas virsnieku komandā, kuri 2018. gada aprīlī mēģināja neatļauti piekļūt *OPCW WiFi* tīklam Hāgā, Nīderlandē. Kiberuzbrukuma mēģinājuma mērķis bija ielauzties *OPCW WiFi* tīklā – ja tas izdotos, būtu tikusi apdraudēta tīkla drošība un *OPCW* notiekošais izmeklēšanas darbs. Nīderlandes Aizsardzības izlūkošanas un drošības dienests (*DISS*) (*Militaire Inlichtingen- en Veiligheidsdienst – MIVD*) apturēja kiberuzbrukuma mēģinājumu, tādējādi novēršot nopietnu kaitējumu *OPCW*.	30.7.2020.
4.	Aleksei Sergeyvich MORENETS	Алексей Сергеевич МОРЕНЕЦ Dzimšanas datums: 1977. gada 31. jūlijs Dzimšanas vieta: *Murmanskaya Oblast,* Krievijas PFSR (tagad Krievijas Federācija) Pases numurs: 100135556 Izdevusi Krievijas Federācijas Ārlietu ministrija Derīga no 2017. gada 17. aprīļa līdz 2022. gada 17. aprīlim Vieta: *Moscow,* Krievijas Federācija Valstspiederība: Krievijas Dzimums: vīrietis	*Aleksei Morenets* piedalījās kiberuzbrukuma ar potenciāli būtisku ietekmi mēģinājumā pret Ķīmisko ieroču aizlieguma organizāciju (*OPCW*) Nīderlandē. Būdams kiberoperāciju darbinieks Krievijas Federācijas Bruņoto spēku Ģenerālštāba Galvenajā pārvaldē (*GU/GRU*), *Aleksei Morenets* bija četru Krievijas militārās izlūkošanas virsnieku komandā, kuri 2018. gada aprīlī mēģināja neatļauti piekļūt *OPCW WiFi* tīklam Hāgā, Nīderlandē. Kiberuzbrukuma mēģinājuma mērķis bija ielauzties *OPCW WiFi* tīklā – ja tas izdotos, būtu tikusi apdraudēta tīkla drošība un *OPCW* notiekošais izmeklēšanas darbs. Nīderlandes Aizsardzības izlūkošanas un drošības dienests (*DISS*) (*Militaire Inlichtingen- en Veiligheidsdienst – MIVD*) apturēja kiberuzbrukuma mēģinājumu, tādējādi novēršot nopietnu kaitējumu *OPCW*.	30.7.2020.
5.	Evgenii Mikhaylovich SEREBRIAKOV	Евгений Михайлович СЕРЕБРЯКОВ Dzimšanas datums: 1981. gada 26. jūlijs Dzimšanas vieta: *Kursk,* Krievijas PFSR (tagad Krievijas Federācija) Pases numurs: 100135555 Izdevusi Krievijas Federācijas Ārlietu ministrija Derīga no 2017. gada 17. aprīļa līdz 2022. gada 17. aprīlim Vieta: *Moscow,* Krievijas Federācija Valstspiederība: Krievijas Dzimums: vīrietis	*Evgenii Serebriakov* piedalījās kiberuzbrukuma ar potenciāli būtisku ietekmi mēģinājumā pret Ķīmisko ieroču aizlieguma organizāciju (*OPCW*) Nīderlandē. Būdams kiberoperāciju darbinieks Krievijas Federācijas Bruņoto spēku Ģenerālštāba Galvenajā pārvaldē (*GU/GRU*), *Evgenii Serebriakov* bija četru Krievijas militārās izlūkošanas virsnieku komandā, kuri 2018. gada aprīlī mēģināja neatļauti piekļūt *OPCW WiFi* tīklam Hāgā, Nīderlandē. Kiberuzbrukuma mēģinājuma mērķis bija ielauzties *OPCW WiFi* tīklā – ja tas izdotos, būtu tikusi apdraudēta tīkla drošība un *OPCW* notiekošais izmeklēšanas darbs. Nīderlandes Aizsardzības izlūkošanas un drošības dienests (*DISS*) (*Militaire Inlichtingen- en Veiligheidsdienst – MIVD*) apturēja kiberuzbrukuma mēģinājumu, tādējādi novēršot nopietnu kaitējumu *OPCW*.	30.7.2020.

6.	Oleg Mikhaylovich SOTNIKOV	Олег Михайлович СОТНИКОВ Dzimšanas datums: 1972. gada 24. augusts Dzimšanas vieta: *Ulyanovsk*, Krievijas PFSR (tagad Krievijas Federācija) Pases numurs: 120018866 Izdevusi Krievijas Federācijas Ārlietu ministrija Derīga no 2017. gada 17. aprīļa līdz 2022. gada 17. aprīlim Vieta: *Moscow*, Krievijas Federācija Valstspiederība: Krievijas Dzimums: vīrietis	*Oleg Sotnikov* piedalījās kiberuzbrukuma ar potenciāli būtisku ietekmi mēģinājumā pret Ķīmisko ieroču aizlieguma organizāciju (*OPCW*) Nīderlandē. Būdams cilvēku veiktas izlūkošanas atbalsta virsnieks Krievijas Federācijas Bruņoto spēku Ģenerālštāba Galvenajā pārvaldē (*GU/GRU*), *Oleg Sotnikov* bija četru Krievijas militārās izlūkošanas virsnieku komandā, kuri 2018. gada aprīlī mēģināja neatļauti piekļūt *OPCW WiFi* tīklam Hāgā, Nīderlandē. Kiberuzbrukuma mēģinājuma mērķis bija ielauzties *OPCW WiFi* tīklā – ja tas izdotos, būtu tikusi apdraudēta tīkla drošība un *OPCW* notiekošais izmeklēšanas darbs. Nīderlandes Aizsardzības izlūkošanas un drošības dienests (*DISS*) (*Militaire Inlichtingen- en Veiligheidsdienst – MIVD*) apturēja kiberuzbrukuma mēģinājumu, tādējādi novēršot nopietnu kaitējumu *OPCW*.	30.7.2020.

B. Juridiskas personas, vienības un struktūras

	Nosaukums	Identifikācijas informācija	Pamatojums	Sarakstā iekļaušanas datums
1.	Tianjin Huaying Haitai Science and Technology Development Co. Ltd (Huaying Haitai)	jeb *Haitai Technology Development Co. Ltd* Vieta: *Tianjin*, Ķīna	*Huaying Haitai* sniedza finansiālu, tehnisku vai materiālu atbalstu "*Operation Cloud Hopper*" – virknei kiberuzbrukumu ar būtisku ietekmi, kuru izcelsme ir ārpus Savienības un kuri rada ārēju apdraudējumu Savienībai vai tās dalībvalstīm, un ar būtisku ietekmi uz trešām valstīm – un sekmēja to. "*Operation Cloud Hopper*" bija vērsta pret daudznacionālu uzņēmumu informācijas sistēmām, kuri atrodas sešos kontinentos, tostarp to uzņēmumu informācijas sistēmām, kuri atrodas Savienībā, un tās ietvaros neatļauti piekļuva komerciāli sensitīviem datiem, tādējādi radot ievērojamus ekonomiskus zaudējumus. "*Operation Cloud Hopper*" veica aktors, kas publiski zināms kā "*APT10*" ("*Advanced Persistent Threat 10*") (jeb "*Red Apollo*", "*CVNX*", "*Stone Panda*", "*MenuPass*" un "*Potassium*"). *Huaying Haitai* var būt saistīts ar *APT10*. Turklāt *Huaying Haitai* nodarbināja *Gao Qiang* un *Zhang Shilong*, kuri abi ir iekļauti sarakstā saistībā ar "*Operation Cloud Hopper*". Tāpēc *Huaying Haitai* ir saistīts ar *Gao Qiang* un *Zhang Shilong*.	30.7.2020.
2.	Chosun Expo	jeb *Chosen Expo; Korea Export Joint Venture* Vieta: KTDR	*Chosun Expo* sniedza finansiālu, tehnisku vai materiālu atbalstu virknei kiberuzbrukumu ar būtisku ietekmi, kuru izcelsme ir ārpus Savienības un kuri rada ārēju apdraudējumu Savienībai vai tās dalībvalstīm, un ar būtisku ietekmi uz trešām valstīm, tostarp kiberuzbrukumiem, kas publiski zināmi kā "*WannaCry*", un kiberuzbrukumiem pret Polijas Finanšu uzraudzības iestādi un "*Sony Pictures Entertainment*", kā arī kiberzādzībai no *Bangladesh Bank* un kiberzādzības mēģinājumam no *Vietnam Tien Phong Bank*, un sekmēja tos.	30.7.2020.

			"*WannaCry*" traucēja informācijas sistēmu darbību visā pasaulē, uzbrūkot informācijas sistēmām ar izspiedējprogrammatūru un bloķējot piekļuvi datiem. Tā ietekmēja uzņēmumu informācijas sistēmas ESavienībāS, tostarp informācijas sistēmas, kas saistītas ar pakalpojumiem, kuri nepieciešami pamatpakalpojumu un saimnieciskās darbības uzturēšanai dalībvalstīs. "*WannaCry*" veica aktors, kas publiski zināms kā "*APT38*" ("*Advanced Persistent Threat 38*") vai "*Lazarus Group*". *Chosun Expo* var būt saistīts ar *APT38*/*Lazarus Group*, tostarp ar kiberuzbrukumiem izmantoto kontu starpniecību.	
3.	Krievijas Federācijas Bruņoto spēku Ģenerālštāba (*GU*/*GRU*) Galvenais īpašo tehnoloģiju centrs (*GTsST*)	Adrese: Kirova iela 22, Maskava, Krievijas Federācija	Krievijas Federācijas Bruņoto spēku Ģenerālštāba (*GU*/*GRU*) Galvenais īpašo tehnoloģiju centrs (*GTsST*), zināms arī ar lauka pasta numuru 74455, ir atbildīgs par kiberuzbrukumiem ar būtisku ietekmi, kuru izcelsme ir ārpus Savienības un kuri rada ārēju apdraudējumu Savienībai vai tās dalībvalstīm, un par kiberuzbrukumiem ar būtisku ietekmi uz trešām valstīm, tostarp kiberuzbrukumiem, kas publiski zināmi kā "*NotPetya*" vai "*EternalPetya*", 2017. gad jūnijā un kiberuzbrukumiem, kas vērsti pret Ukrainas elektrotīklu, 2015. un 2016. gada ziemā. "*NotPetya*" vai "*EternalPetya*" padarīja datus nepieejamus vairākos uzņēmumos Savienībā, citviet Eiropā un pasaulē, uzbrūkot datoriem ar izspiedējprogrammatūru un bloķējot piekļuvi datiem, kas cita starpā radīja ievērojamus ekonomiskus zaudējumus. Kiberuzbrukums Ukrainas elektrotīklam noveda pie tā, ka tā daļas ziemā tika atslēgtas.	30.7.2020."
			"*NotPetya*" vai "*EternalPetya*" veica aktors, kas ir publiski zināms kā "*Sandworm*" (jeb "*Sandworm Team*", "*BlackEnergy Group*", "*Voodoo Bear*", "*Quedagh*", "*Olympic Destroyer*" un "*Telebots*") un kas stāv arī aiz uzbrukuma Ukrainas elektrotīklam. Krievijas Federācijas Bruņoto spēku Ģenerālštāba Galvenajam īpašo tehnoloģiju centram ir aktīva loma *Sandworm* veiktajās kiberdarbībās, un tas var būt saistīts ar *Sandworm*.	