Eiropas Savienības
Padome

Briselē, 2024. gada 13. maijā
(OR. en)

8500/24

LIMITE

CORLX 354
CFSP/PESC 510
CYBER 108
JAI 570
FIN 339

LEĢISLATĪVIE AKTI UN CITI DOKUMENTI

Temats:	PADOMES LĒMUMS, ar ko groza Lēmumu (KĀDP) 2019/797 par ierobežojošiem pasākumiem pret kiberuzbrukumiem, kuri apdraud Savienību vai tās dalībvalstis

PADOMES LĒMUMS (KĀDP) 2024/…

(... gada ...),

ar ko groza Lēmumu (KĀDP) 2019/797 par ierobežojošiem pasākumiem pret kiberuzbrukumiem, kuri apdraud Savienību vai tās dalībvalstis

EIROPAS SAVIENĪBAS PADOME,

ņemot vērā Līgumu par Eiropas Savienību un jo īpaši tā 29. pantu,

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

tā kā:

(1) Padome 2019. gada 17. maijā pieņēma Lēmumu (KĀDP) 2019/797[1].

(2) Lēmumu (KĀDP) 2019/797 piemēro līdz 2025. gada 18. maijam. Pamatojoties uz minētā lēmuma pārskatīšanu, tajā noteikto ierobežojošo pasākumu spēkā esamība būtu jāpagarina līdz minētajai dienai.

(3) Ņemot vērā nepārtrauktu un arvien spēcīgāku ļaunprātīgu rīcību kibertelpā, tostarp rīcību, kas vērsta pret trešām valstīm, būtu jāatjaunina pamatojumi sešu personu un divu vienību iekļaušanai Lēmuma (KĀDP) 2019/797 pielikumā izklāstītajā to fizisko un juridisko personu, vienību un struktūru sarakstā, kurām piemēro ierobežojošus pasākumus.

(4) Tādēļ Lēmums (KĀDP) 2019/797 būtu attiecīgi jāgroza,

IR PIEŅĒMUSI ŠO LĒMUMU.

[1] Padomes Lēmums (KĀDP) 2019/797 (2019. gada 17. maijs) par ierobežojošiem pasākumiem pret kiberuzbrukumiem, kuri apdraud Savienību vai tās dalībvalstis (OV L 129 I, 17.5.2019., 13. lpp.).

1. pants

Lēmumu (KĀDP) 2019/797 groza šādi:

1) lēmuma 10. pantu aizstāj ar šādu:

"*10. pants*

Šo lēmumu piemēro līdz 2025. gada 18. maijam un pastāvīgi pārskata.";

2) pielikumu groza saskaņā ar šā lēmuma pielikumu.

2. pants

Šis lēmums stājas spēkā nākamajā dienā pēc tā publicēšanas *Eiropas Savienības Oficiālajā Vēstnesī*.

...,

Padomes vārdā –
priekšsēdētājs / priekšsēdētāja

PIELIKUMS

Lēmuma (KĀDP) 2019/797 pielikumu (“Lēmuma 4. un 5. pantā minēto fizisko un juridisko personu, vienību un struktūru saraksts”) groza šādi:

1) sarakstā “A. Fiziskas personas” 3. līdz 8. ierakstu aizstāj ar šādiem ierakstiem:

	Vārds	Identifikācijas informācija	Pamatojums	Sarakstā iekļaušanas datums
"3.	Alexey Valeryevich MININ	Алексей Валерьевич МИНИН Dzimšanas datums: 27.5.1972. Dzimšanas vieta: *Perm Oblast*, Krievijas PFSR (tagad Krievijas Federācija) Pases numurs: 120017582 Izdevusi Krievijas Federācijas Ārlietu ministrija Derīga no 17.4. 2017. līdz 17.4.2022. Vieta: *Moscow*, Krievijas Federācija Valstspiederība: Krievija Dzimums: vīrietis	*Alexey Minin* piedalījās kiberuzbrukuma ar potenciāli būtisku ietekmi mēģinājumā pret Ķīmisko ieroču aizlieguma organizāciju (*OPCW*) Nīderlandē un kiberuzbrukumos ar būtisku ietekmi pret trešām valstīm. 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 (*Militaire Inlichtingen- en Veiligheidsdienst*) apturēja kiberuzbrukuma mēģinājumu, tādējādi novēršot nopietnu kaitējumu *OPCW*. Pensilvānijas rietumu apgabala zvērināto tiesa (Amerikas Savienotās Valstis) ir apsūdzējusi *Alexey Minin*, kurš bija Krievijas Galvenās izlūkošanas pārvaldes (*GRU*) virsnieks, par datoruzlaušanu, krāpšanu, izmantojot elektroniskos sakaru līdzekļus, identitātes zādzību vainu pastiprinošos apstākļos un nelikumīgi iegūtu līdzekļu legalizēšanu.	30.7.2020.

	Vārds	Identifikācijas informācija	Pamatojums	Sarakstā iekļaušanas datums
4.	Aleksei Sergeyvich MORENETS	Алексей Сергеевич МОРЕНЕЦ Dzimšanas datums: 31.7.1977. Dzimšanas vieta: *Murmanskaya Oblast*, Krievijas PFSR (tagad Krievijas Federācija) Pases numurs: 100135556 Izdevusi Krievijas Federācijas Ārlietu ministrija Derīga no 17.4.2017. līdz 17.4.2022. Vieta: *Moscow*, Krievijas Federācija Valstspiederība: Krievija Dzimums: vīrietis	*Aleksei Morenets* piedalījās kiberuzbrukuma ar potenciāli būtisku ietekmi mēģinājumā pret Ķīmisko ieroču aizlieguma organizāciju (*OPCW*) Nīderlandē un kiberuzbrukumos ar būtisku ietekmi pret trešām valstīm. 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 (*Militaire Inlichtingen- en Veiligheidsdienst*) apturēja kiberuzbrukuma mēģinājumu, tādējādi novēršot nopietnu kaitējumu *OPCW*. Pensilvānijas rietumu apgabala zvērināto tiesa (Amerikas Savienotās Valstis) ir apsūdzējusi *Aleksei Morenets*, kurš bija norīkots militārajā vienībā 26165, par datoruzlaušanu, krāpšanu, izmantojot elektroniskos sakaru līdzekļus, identitātes zādzību vainu pastiprinošos apstākļos un nelikumīgi iegūtu līdzekļu legalizēšanu.	30.7.2020.

	Vārds	Identifikācijas informācija	Pamatojums	Sarakstā iekļaušanas datums
5.	Evgenii Mikhaylovich SEREBRIAKOV	Евгений Михайлович СЕРЕБРЯКОВ Dzimšanas datums: 26.7.1981. Dzimšanas vieta: *Kursk*, Krievijas PFSR (tagad Krievijas Federācija) Pases numurs: 100135555 Izdevusi Krievijas Federācijas Ārlietu ministrija Derīga no 17.4. 2017. līdz 17.4.2022. Vieta: *Moscow*, Krievijas Federācija Valstspiederība: Krievija Dzimums: vīrietis	*Evgenii Serebriakov* piedalījās kiberuzbrukuma ar potenciāli būtisku ietekmi mēģinājumā pret Ķīmisko ieroču aizlieguma organizāciju (*OPCW*) Nīderlandē un kiberuzbrukumos ar būtisku ietekmi pret trešām valstīm. 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 (*Militaire Inlichtingen- en Veiligheidsdienst*) apturēja kiberuzbrukuma mēģinājumu, tādējādi novēršot nopietnu kaitējumu *OPCW*. Kopš 2022. gada pavasara *Evgenii Serebriakov* vada ar Krievijas Galvenās izlūkošanas pārvaldes 74455. nodaļu saistītu aktoru un datoruzlaušanas grupu "*Sandworm*" (jeb "*Sandworm Team*", "*BlackEnergy Group*", "*Voodoo Bear*", "*Quedagh*", "*Olympic Destroyer*" un "*Telebots*"). Kopš sācies Krievijas agresijas karš pret Ukrainu, *Sandworm* ir veicis kiberuzbrukumus Ukrainai, tostarp Ukrainas valdības aģentūrām.	30.7.2020.

	Vārds	Identifikācijas informācija	Pamatojums	Sarakstā iekļaušanas datums
6.	Oleg Mikhaylovich SOTNIKOV	Олег Михайлович СОТНИКОВ Dzimšanas datums: 24.8.1972. Dzimšanas vieta: *Ulyanovsk*, Krievijas PFSR (tagad Krievijas Federācija) Pases numurs: 120018866 Izdevusi Krievijas Federācijas Ārlietu ministrija Derīga no 17.4.2017. līdz 17.4.2022. Vieta: *Moscow*, Krievijas Federācija Valstspiederība: Krievija Dzimums: vīrietis	*Oleg Sotnikov* piedalījās kiberuzbrukuma ar potenciāli būtisku ietekmi mēģinājumā pret Ķīmisko ieroču aizlieguma organizāciju (*OPCW*) Nīderlandē un kiberuzbrukumos ar būtisku ietekmi pret trešām valstīm. 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 (*Militaire Inlichtingen- en Veiligheidsdienst*) apturēja kiberuzbrukuma mēģinājumu, tādējādi novēršot nopietnu kaitējumu *OPCW*. Pensilvānijas rietumu apgabala zvērināto tiesa ir apsūdzējusi *Oleg Sotnikov*, kurš bija Krievijas Galvenās izlūkošanas pārvaldes (*GRU*) virsnieks, par datoruzlaušanu, krāpšanu, izmantojot elektroniskos sakaru līdzekļus, identitātes zādzību vainu pastiprinošos apstākļos un nelikumīgi iegūtu līdzekļu legalizēšanu.	30.7.2020.

	Vārds	Identifikācijas informācija	Pamatojums	Sarakstā iekļaušanas datums
7.	Dmitry Sergeyevich BADIN	Дмитрий Сергеевич БАДИН Dzimšanas datums: 15.11.1990. Dzimšanas vieta: *Kursk*, Krievijas PFSR (tagad Krievijas Federācija) Valstspiederība: Krievija Dzimums: vīrietis	*Dmitry Badin* piedalījās kiberuzbrukumā ar būtisku ietekmi pret Vācijas federālo parlamentu (*Deutscher Bundestag*) un kiberuzbrukumos ar būtisku ietekmi pret trešām valstīm. Būdams militārās izlūkošanas virsnieks Krievijas Federācijas Bruņoto spēku Ģenerālštāba Galvenās pārvaldes (*GU/GRU*) 85. Speciālo dienestu galvenajā centrā, *Dmitry Badin* bija Krievijas militārās izlūkošanas virsnieku komandā, kura 2015. gada aprīlī un maijā veica kiberuzbrukumu pret Vācijas federālo parlamentu. Minētā kiberuzbrukuma mērķis bija parlamenta informācijas sistēma, un tas ietekmēja tās darbību uz vairākām dienām. Tika nozagts nozīmīgs datu apjoms, un tika skarti vairāku parlamenta deputātu, kā arī bijušās kancleres *Angela Merkel* e-pasta konti. Pensilvānijas rietumu apgabala zvērināto tiesa (Amerikas Savienotās Valstis) ir apsūdzējusi *Dmitry Badin*, kurš bija norīkots militārajā vienībā 26165, par datoruzlaušanu, krāpšanu, izmantojot elektroniskos sakaru līdzekļus, identitātes zādzību vainu pastiprinošos apstākļos un nelikumīgi iegūtu līdzekļu legalizēšanu.	22.10.2020.

	Vārds	Identifikācijas informācija	Pamatojums	Sarakstā iekļaušanas datums
8.	Igor Olegovich KOSTYUKOV	Игорь Олегович КОСТЮКОВ Dzimšanas datums: 21.2.1961. Valstspiederība: Krievija Dzimums: vīrietis	*Igor Kostyukov* ir Krievijas Federācijas Bruņoto spēku Ģenerālštāba Galvenās pārvaldes (*GU/GRU*) pašreizējais priekšnieks; pirms tam viņš bija priekšnieka pirmā vietnieka amatā. Viena no vienībām, ko viņš komandē, ir 85. Speciālo dienestu galvenais centrs (*85th Main Centre for Special Services – GTsSS*) (jeb "militārā vienība 26165", "*APT28*", "*Fancy Bear*", "*Sofacy Group*", "*Pawn Storm*" un "*Strontium*"). Šajā amatā *Igor Kostyukov* ir atbildīgs par kiberuzbrukumiem, ko veicis *GTsSS*, tostarp par kiberuzbrukumiem ar būtisku ietekmi, kas ir ārējs apdraudējums Savienībai vai tās dalībvalstīm. Konkrēti, *GTsSS* militārās izlūkošanas virsnieki 2015. gada aprīlī un maijā piedalījās kiberuzbrukumā pret Vācijas federālo parlamentu (*Deutscher Bundestag*), kā arī kiberuzbrukuma mēģinājumā, kas bija vērsts uz Ķīmisko ieroču aizlieguma organizācijas (*OPCW*) WiFi tīkla uzlaušanu 2018. gada aprīlī Nīderlandē. Kiberuzbrukuma pret Vācijas federālo parlamentu mērķis bija parlamenta informācijas sistēma, un tas ietekmēja tās darbību uz vairākām dienām. Tika nozagts nozīmīgs datu apjoms, un tika skarti vairāku parlamenta deputātu, kā arī bijušās kancleres *Angela Merkel* e-pasta konti.	22.10.2020.”;

2) sarakstā “B. Juridiskas personas, vienības un struktūras” 3. un 4. ierakstu aizstāj ar šādiem ierakstiem:

	Nosaukums	Identifikācijas informācija	Pamatojums	Sarakstā iekļaušanas datums
“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)	Adrese: *22 Kirova Street, Moscow, Russian Federation*	Krievijas Federācijas Bruņoto spēku Ģenerālštāba (*GU/GRU*) Galvenais īpašo tehnoloģiju centrs (*GTsST*) (*The Main Centre for Special Technologies (GTsST) of the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GU/GRU)*), zināms arī ar lauka pasta numuru 74455, ir iesaistīts kiberuzbrukumos ar būtisku ietekmi, kuru izcelsme ir ārpus Savienības un kuri rada ārēju apdraudējumu Savienībai vai tās dalībvalstīm, un kiberuzbrukumos ar būtisku ietekmi uz trešām valstīm, tostarp kiberuzbrukumiem, kas publiski zināmi kā “*NotPetya*” vai “*EternalPetya*”, 2017. gada 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.

	Nosaukums	Identifikācijas informācija	Pamatojums	Sarakstā iekļaušanas datums
			"*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. Kopš sācies Krievijas agresijas karš pret Ukrainu, *Sandworm* ir veicis kiberuzbrukumus Ukrainai, tostarp Ukrainas valdības aģentūrām un Ukrainas kritiskajai infrastruktūrai. Minētie kiberuzbrukumi ietver mērķētu pikšķerēšanu, ļaunprogrammatūras un izspiedējprogrammatūras uzbrukumus. Krievijas Federācijas Bruņoto spēku Ģenerālštāba Galvenajam īpašo tehnoloģiju centram ir aktīva loma *Sandworm* veiktajās kiberdarbībās, un tas var būt saistīts ar *Sandworm*.	

	Nosaukums	Identifikācijas informācija	Pamatojums	Sarakstā iekļaušanas datums
4.	85th Main Centre for Special Services (GTsSS) of the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GU/GRU)	Adrese: *Komsomol'skiy Prospekt, 20, Moscow, 119146, Russian Federation*	Krievijas Federācijas Bruņoto spēku Ģenerālštāba Galvenās pārvaldes (*GU/GRU*) 85. Speciālo dienestu galvenais centrs (*GTsSS*) (*85th Main Centre for Special Services (GTsSS) of the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GU/GRU)*) (jeb "militārā vienība 26165", "*APT28*", "*Fancy Bear*", "*Sofacy Group*", "*Pawn Storm*" un "*Strontium*") ir iesaistīts kiberuzbrukumos ar būtisku ietekmi, kuri rada ārēju apdraudējumu Savienībai vai tās dalībvalstīm, un kiberuzbrukumos ar būtisku ietekmi pret trešām valstīm. Konkrēti, *GTsSS* militārās izlūkošanas virsnieki 2015. gada aprīlī un maijā piedalījās kiberuzbrukumā pret Vācijas federālo parlamentu (*Deutscher Bundestag*), kā arī kiberuzbrukuma mēģinājumā, kas bija vērsts uz Ķīmisko ieroču aizlieguma organizācijas (*OPCW*) WiFi tīkla uzlaušanu 2018. gada aprīlī Nīderlandē. Kiberuzbrukuma pret Vācijas federālo parlamentu mērķis bija parlamenta informācijas sistēma, un tas ietekmēja tās darbību uz vairākām dienām. Tika nozagts nozīmīgs datu apjoms, un tika skarti vairāku parlamenta deputātu, kā arī bijušās kancleres *Angela Merkel* e-pasta konti. Kopš sācies Krievijas agresijas karš pret Ukrainu, *GTsSS* ir veicis kiberuzbrukumus (mērķētu pikšķerēšanu un ļaunprogrammatūras uzbrukumus) pret Ukrainu.	22.10.2020.".