►B

PADOMES LĒMUMS (KĀDP) 2019/797

(2019. gada 17. maijs),

par ierobežojošiem pasākumiem pret kiberuzbrukumiem, kuri apdraud Savienību vai tās dalībvalstis

(OV L 129I, 17.5.2019., 13. lpp.)

Grozīts ar:

		Oficiālais Vēstnesis		
		Nr.	Lappuse	Datums
►M1	Padomes Lēmums (KĀDP) 2020/651 (2020. gada 14. maijs)	L 153	4	15.5.2020.
►M2	Padomes Lēmums (KĀDP) 2020/1127 (2020. gada 30. jūlijs)	L 246	12	30.7.2020.
►M3	Padomes Lēmums (KĀDP) 2020/1537 (2020. gada 22. oktobris)	L 351 I	5	22.10.2020.
►M4	Padomes Lēmums (KĀDP) 2020/1748 (2020. gada 20. novembris)	L 393	19	23.11.2020.
►M5	Padomes Lēmums (KĀDP) 2021/796 (2021. gada 17. maijs)	L 174 I	1	18.5.2021.

Labota ar:

►C1	Kļūdu labojums, OV L 230, 17.7.2020., 36. lpp. (2019/797)

▼B

PADOMES LĒMUMS (KĀDP) 2019/797

(2019. gada 17. maijs),

par ierobežojošiem pasākumiem pret kiberuzbrukumiem, kuri apdraud Savienību vai tās dalībvalstis

1. pants

1. Šo lēmumu piemēro kiberuzbrukumiem ar būtisku ietekmi, tostarp kiberuzbrukumu mēģinājumiem ar potenciāli būtisku ietekmi, kuri ir ārējs apdraudējums Savienībai vai tās dalībvalstīm.

2. Kiberuzbrukumi, kas ir ārējs apdraudējums, ietver tādus,

a) kuri ir cēlušies vai tiek veikti no kādas vietas ārpus Savienības;

b) kuros izmanto infrastruktūru ārpus Savienības;

c) kurus veic jebkāda fiziska vai juridiska persona, vienība vai struktūra, kas veic uzņēmējdarbību vai darbojas ārpus Savienības; vai

d) kurus veic ar jebkādas fiziskas vai juridiskas personas, vienības vai struktūras, kas darbojas ārpus Savienības, atbalstu, tās vadībā vai kontrolē.

3. Šajā nolūkā kiberuzbrukumi ir darbības, kas ietver jebko no turpmāk minētā:

a) piekļuvi informācijas sistēmām;

b) iejaukšanos informācijas sistēmā;

c) iejaukšanos datos; vai

d) datu pārtveršanu,

ja šādas darbības nav pienācīgi pilnvarojis īpašnieks vai cits sistēmas vai datu vai to daļas tiesību turētājs, vai tās nav atļautas saskaņā ar Savienības vai attiecīgās dalībvalsts tiesību aktiem.

4. Kiberuzbrukumi, kas ir apdraudējums dalībvalstīm, ietver tos, kuri ietekmē informācijas sistēmas, kas cita starpā ir saistītas ar:

a) kritisko infrastruktūru, tostarp zemūdens kabeļiem un kosmosā palaistiem objektiem, kura ir būtiska vitālo sabiedrisko funkciju uzturēšanai, veselības, drošuma, drošības, cilvēku ekonomiskās vai sociālās labklājības nodrošināšanai;

b) pakalpojumiem, kas ir vajadzīgi būtisku sabiedrisko un/vai ekonomisko darbību uzturēšanai, jo īpaši enerģētikas (elektrība, nafta un gāze); transporta (gaisa, dzelzceļa, ūdens un autotransports); banku; finanšu tirgus infrastruktūru; veselības aprūpes (veselības aprūpes

▼B

sniedzēji, slimnīcas un privātās klīnikas); dzeramā ūdens piegādes un izplatīšanas; digitālās infrastruktūras nozarēs; un jebkurā citā nozarē, kas ir būtiska attiecīgajai dalībvalstij;

c) kritiskām valsts funkcijām, jo īpaši šādās jomās: aizsardzība, iestāžu pārvaldība un darbība, tostarp saistībā ar publiskām vēlēšanām vai balsošanas procesu, saimnieciskās un civilās infrastruktūras darbība, iekšējā drošība un ārējās attiecības, tostarp ar diplomātisko pārstāvniecību starpniecību;

d) klasificētas informācijas glabāšanu vai apstrādi; vai

e) valdības vienībām reaģēšanai uz apdraudējumiem.

5. Pie kiberuzbrukumiem, kas apdraud Savienību, pieder tie, kas tiek veikti pret Savienības iestādēm, struktūrām, birojiem un aģentūrām, tās delegācijām trešās valstīs vai starptautiskām organizācijām, tās kopējās drošības un aizsardzības politikas (KDAP) operācijām un misijām un tās īpašajiem pārstāvjiem.

6. Ja tas tiek uzskatīts par nepieciešamu attiecīgajos Līguma par Eiropas Savienību 21. panta noteikumos minēto KĀDP mērķu sasniegšanai, ierobežojošos pasākumus saskaņā ar šo lēmumu var arī piemērot, reaģējot uz būtiskas ietekmes kiberuzbrukumiem pret trešām valstīm vai starptautiskām organizācijām.

2. pants

Šajā lēmumā piemēro šādas definīcijas:

a) "informācijas sistēmas" ir ierīces vai savstarpēji savienotu vai saistītu ierīču kopums, no kurām viena vai vairākas ierīces saskaņā ar programmu automātiski apstrādā digitālos datus, kā arī digitālie dati, ko minētās ierīces vai ierīču kopums glabā, apstrādā, izgūst vai sūta, lai nodrošinātu savu darbību, izmantošanu, aizsargāšanu un uzturēšanu;

b) "iejaukšanās informācijas sistēmā" ir informācijas sistēmas darbības kavēšana vai pārtraukšana, ievadot, sūtot, bojājot, dzēšot, pasliktinot, pārveidojot vai slāpējot digitālos datus vai padarot šādus datus nepieejamus;

c) "iejaukšanās datos" ir digitālo datu dzēšana, bojāšana, pasliktināšana, mainīšana vai slāpēšana informācijas sistēmā vai darbība, padarot šādus datus nepieejamus; tajā ietilpst arī datu, naudaslīdzekļu, saimniecisko resursu vai intelektuālā īpašuma tiesību zādzība;

d) "datu pārtveršana" ir tas, ka ar tehniskiem līdzekļiem pārtver uz informācijas sistēmu, no tās vai tās ietvaros nepubliski sūtītus digitālos datus, tostarp šādus digitālos datus saturošu elektromagnētisko starojumu no informācijas sistēmas.

▼B

3. pants

Starp faktoriem, kas nosaka, vai kiberuzbrukumam ir 1. panta 1. punktā minētā būtiskā ietekme, ir jebkurš no turpmāk minētajiem:

a) kiberuzbrukuma joma, mērogs, ietekme vai tā radīto traucējumu smaguma pakāpe, tostarp ekonomiskajām un sabiedriskajām darbībām, pamatpakalpojumiem, kritiskajām valsts funkcijām, sabiedriskajai kārtībai vai sabiedrības drošībai;

b) skarto fizisko vai juridisko personu, vienību vai struktūru skaits;

c) attiecīgo dalībvalstu skaits;

d) izraisīto ekonomisko zaudējumu apjoms, kas radies, piemēram, liela apjoma līdzekļu, ekonomisko resursu vai intelektuālā īpašuma zādzības dēļ;

e) saimnieciskais ieguvums, ko likumpārkāpējs saņēmis pats vai kas nodrošināts citiem; vai

f) nozagto datu daudzums vai būtība vai datu aizsardzības pārkāpumu mērogs; vai

g) to komerciāli sensitīvo datu veids, kuriem ir piekļūts.

4. pants

1. Dalībvalstis veic pasākumus, kas ir vajadzīgi, lai nepieļautu, ka to teritorijās ieceļo vai tās tranzītā šķērso:

a) fiziskas personas, kas ir atbildīgas par kiberuzbrukumiem vai kiberuzbrukumu mēģinājumiem;

b) fiziskas personas, kas sniedz finansiālu, tehnisku vai materiālu atbalstu vai ir citādi iesaistītas kiberuzbrukumos vai kiberuzbrukumu mēģinājumos, tostarp tos plānojot, sagatavojot, tajos piedaloties, tos vadot, palīdzot vai mudinot tos veikt, vai ar darbību vai bezdarbību atvieglojot to veikšanu;

c) fiziskas personas, kuras ir saistītas ar a) un b) apakšpunktā minētajām personām,

kā uzskaitīts pielikumā.

2. Šā panta 1. punkts neliek dalībvalstij aizliegt saviem valstspiederīgajiem ieceļot tās teritorijā.

3. Šā panta 1. punkts neskar gadījumus, ja kādai dalībvalstij ir starptautiskajās tiesībās paredzēti pienākumi, konkrēti:

a) kā starptautiskas starpvaldību organizācijas uzņēmējvalstij;

b) kā valstij, kurā tiek rīkota starptautiska konference, ko sasauc Apvienoto Nāciju Organizācija vai kas notiek tās aizbildnībā;

c) saskaņā ar daudzpusēju nolīgumu, ar ko piešķir privilēģijas un imunitāti; vai

d) ievērojot 1929. gada Samierināšanās līgumu (Laterāna pakts), ko noslēdza Svētais Krēsls (Vatikāna Pilsētvalsts) un Itālija.

▼B

4. Šā panta 3. punktu uzskata par piemērojamu arī gadījumos, kad dalībvalsts ir Eiropas Drošības un sadarbības organizācijas (EDSO) uzņēmējvalsts.

5. Padome tiek pienācīgi informēta par visiem gadījumiem, kad dalībvalsts piešķir izņēmumu saskaņā ar 3. vai 4. punktu.

6. Dalībvalstis var piešķirt izņēmumus no 1. punktā paredzētajiem pasākumiem, ja ceļošana ir attaisnojama steidzamu humanitāru vajadzību dēļ vai tā tiek veikta, lai apmeklētu starpvaldību sanāksmes vai sanāksmes, kuras atbalsta vai rīko Savienība, vai kuras rīko dalībvalsts, kas ir EDSO prezidentvalsts, ja tajās norisinās politiskais dialogs, ar ko tieši atbalsta ierobežojošo pasākumu politikas mērķus, tostarp drošību un stabilitāti kibertelpā.

7. Dalībvalstis var arī piešķirt izņēmumus attiecībā uz pasākumiem, kas noteikti saskaņā ar 1. punktu, ja ieceļošana vai teritorijas šķērsošana ir nepieciešama tiesas procesa nolūkā.

8. Dalībvalsts, kas vēlas piešķirt 6. vai 7. punktā minētos izņēmumus, par to rakstiski paziņo Padomei. Izņēmumu uzskata par piešķirtu, ja vien viens vai vairāki Padomes locekļi rakstiski neiebilst divās darba dienās no dienas, kad saņemts paziņojums par ierosināto izņēmumu. Ja viens vai vairāki Padomes locekļi iebilst, Padome ar kvalificētu balsu vairākumu var pieņemt lēmumu piešķirt ierosināto izņēmumu.

9. Gadījumos, kad dalībvalsts saskaņā ar 3., 4., 6., 7. vai 8. punktu atļauj pielikumā uzskaitītajām personām ieceļot savā teritorijā vai to šķērsot tranzītā, atļauju piešķir tikai un vienīgi tādam nolūkam, kādam tā ir paredzēta, un tikai tām personām, uz kurām tā tieši attiecas.

5. pants

1. Iesaldē visus līdzekļus un saimnieciskos resursus, kas pieder, ir īpašumā, turējumā vai kontrolē:

a) fiziskām vai juridiskām personām, vienībām vai struktūrām, kuras ir atbildīgas par kiberuzbrukumiem vai kiberuzbrukumu mēģinājumiem;

b) fiziskām vai juridiskām personām, vienībām vai struktūrām, kuras sniedz finansiālu, tehnisku vai materiālu atbalstu vai ir citādi iesaistītas kiberuzbrukumos vai kiberuzbrukumu mēģinājumos, tostarp tos plānojot, sagatavojot, tajos piedaloties, tos vadot, palīdzot vai mudinot tos veikt, vai ar darbību vai bezdarbību atvieglojot to veikšanu;

c) fiziskām vai juridiskām personām, vienībām vai struktūrām, kuras ir saistītas ar a) un b) apakšpunktā minētajām fiziskajām vai juridiskajām personām, vienībām vai struktūrām,

kā uzskaitīts pielikumā.

▼B

2. Nekādi līdzekļi vai saimnieciskie resursi netiek darīti tieši vai netieši pieejami pielikumā uzskaitītajām fiziskajām vai juridiskajām personām, vienībām vai struktūrām vai to interesēs.

3. Atkāpjoties no 1. un 2. punkta, dalībvalstu kompetentās iestādes var atļaut atsevišķu iesaldēto līdzekļu vai saimniecisko resursu atbrīvošanu vai arī atsevišķus iesaldētos līdzekļus vai saimnieciskos resursus darīt pieejamus ar tādiem nosacījumiem, kādus tās uzskata par atbilstīgiem, ja tā ir konstatējusi, ka attiecīgie līdzekļi vai saimnieciskie resursi ir:

a) ►C1 vajadzīgi, lai segtu pielikumā uzskaitīto fizisko vai juridisko personu, vienību vai struktūru pamatvajadzības un šādu fizisko personu apgādājamo ģimenes locekļu pamatvajadzības, ◄ tostarp maksājumus par pārtikas produktiem, īri vai hipotēku, zālēm un medicīnisko aprūpi, nodokļu, apdrošināšanas prēmiju un komunālo pakalpojumu maksājumus;

b) paredzēti vienīgi samērīgai samaksai par kvalificētu darbu vai atlīdzībai par izdevumiem, kas saistīti ar juridiskiem pakalpojumiem;

c) paredzēti vienīgi komisijas maksai vai apkalpošanas maksai par iesaldēto līdzekļu vai saimniecisko resursu parasto turēšanu vai pārvaldību;

d) nepieciešami ārkārtas izdevumiem ar noteikumu, ka attiecīgā kompetentā iestāde pārējo dalībvalstu kompetentajām iestādēm un Komisijai vismaz divas nedēļas pirms atļaujas piešķiršanas ir sniegusi pamatojumu, kāpēc tā uzskata, ka būtu jāpiešķir īpaša atļauja; vai

e) ir paredzēti, lai veiktu maksājumus tādas diplomātiskās vai konsulārās pārstāvniecības vai tādas starptautiskas organizācijas kontā, kurai ar starptautiskām tiesībām ir noteikta imunitāte, vai lai veiktu maksājumus no šādas pārstāvniecības vai organizācijas konta – ciktāl šādi maksājumi ir paredzēti izmantošanai šīs diplomātiskās vai konsulārās pārstāvniecības vai starptautiskās organizācijas oficiālajiem mērķiem.

Attiecīgā dalībvalsts informē pārējās dalībvalstis un Komisiju par visām atļaujām, kas piešķirtas saskaņā ar šo punktu.

4. Atkāpjoties no 1. punkta, dalībvalstu kompetentās iestādes var atļaut konkrētu iesaldētu līdzekļu vai saimniecisko resursu atbrīvošanu ar noteikumu, ka ir ievēroti šādi nosacījumi:

a) uz līdzekļiem vai saimnieciskajiem resursiem attiecas šķīrējtiesas nolēmums, kas ir pieņemts pirms dienas, kad 1. punktā minētā fiziskā vai juridiskā persona, vienība vai struktūra tika iekļauta pielikumā minētajā sarakstā, vai pirms vai pēc minētās dienas Savienībā pieņemts tiesas vai administratīvs nolēmums vai attiecīgajā dalībvalstī izpildāms tiesas nolēmums;

▼B

b) līdzekļus vai saimnieciskos resursus izmantos vienīgi, lai apmierinātu prasījumus, kas izriet no šāda nolēmuma vai kas ir atzīti par spēkā esošiem ar šādu nolēmumu, ievērojot ierobežojumus, kuri noteikti piemērojamos normatīvajos aktos, ar ko reglamentē tiesības, kas ir personām, kurām ir šādi prasījumi;

c) nolēmums nav pieņemts kādas pielikumā uzskaitītas fiziskas vai juridiskas personas, vienības vai struktūras interesēs; un

d) nolēmuma atzīšana nav pretrunā attiecīgās dalībvalsts sabiedriskajai kārtībai.

Attiecīgā dalībvalsts informē pārējās dalībvalstis un Komisiju par visām atļaujām, kas piešķirtas saskaņā ar šo punktu.

5. Šā panta 1. punkts neliedz pielikumā uzskaitītai fiziskai vai juridiskai personai, vienībai vai struktūrai veikt maksājumus saskaņā ar līgumu, kas noslēgts pirms datuma, kurā minētā fiziskā vai juridiskā persona, vienība vai struktūra tika iekļauta sarakstā, ar noteikumu, ka attiecīgā dalībvalsts ir konstatējusi, ka maksājumu tieši vai netieši nesaņem 1. punktā minētā fiziskā vai juridiskā persona, vienība vai struktūra.

6. Šā panta 2. punktu nepiemēro iesaldētu kontu papildināšanai ar:

a) procentiem vai citiem ieņēmumiem no minētajiem kontiem;

b) maksājumiem, kuri paredzēti līgumos, nolīgumos vai saistībās, kas noslēgtas vai radušās pirms dienas, kad uz minētajiem kontiem attiecināja 1. un 2. punktā paredzētos pasākumus; vai

c) maksājumiem, kuri paredzēti Savienībā pieņemtā tiesas, administratīvā vai šķīrējtiesas nolēmumā vai attiecīgajā dalībvalstī izpildāmā tiesas nolēmumā,

ar noteikumu, ka uz visiem šādiem procentiem, cita veida ieņēmumiem un maksājumiem joprojām attiecas 1. punktā paredzētie pasākumi.

6. pants

1. Padome, vienprātīgi lemjot pēc kādas dalībvalsts vai Savienības Augstā pārstāvja ārlietās un drošības politikas jautājumos priekšlikuma, izveido un groza pielikumā iekļauto sarakstu.

2. Padome 1. punktā minēto lēmumu, tostarp pamatojumu iekļaušanai sarakstā, paziņo attiecīgajai fiziskajai vai juridiskajai personai, vienībai vai struktūrai vai nu tieši, ja ir zināma tās adrese, vai publicējot paziņojumu, dodot minētajai fiziskajai vai juridiskajai personai, vienībai vai struktūrai iespēju iesniegt savus apsvērumus.

3. Ja ir iesniegti apsvērumi vai būtiski jauni pierādījumi, Padome pārskata 1. punktā minētos lēmumus un atbilstīgi informē attiecīgo fizisko vai juridisko personu, vienību vai struktūru.

▼B

7. pants

1. Pielikumā norāda pamatojumu 4. un 5. pantā minēto fizisko vai juridisko personu, vienību un struktūru iekļaušanai sarakstā.

2. Pielikumā iekļauj informāciju, kas nepieciešama, lai identificētu attiecīgās fiziskās vai juridiskās personu, vienības vai struktūras, ja tāda ir pieejama. Attiecībā uz fiziskām personām šāda informācija var ietvert: vārdu, uzvārdu un pieņemtos vārdus; dzimšanas datumu un vietu; valstspiederību; pases un personas apliecības numuru; dzimumu; adresi, ja tā ir zināma; un amatu vai profesiju. Attiecībā uz juridiskām personām, vienībām vai struktūrām šāda informācija var ietvert nosaukumus, reģistrācijas vietu un datumu, reģistrācijas numuru un darījumdarbības vietu.

8. pants

Prasījumus saistībā ar jebkādu līgumu vai darījumu, kura izpildi tieši vai netieši, pilnīgi vai daļēji ietekmē pasākumi, kas piemēroti saskaņā ar šo lēmumu, tostarp prasījumus par atlīdzinājuma saņemšanu vai citus šāda veida prasījumus, piemēram, prasījumus par kompensāciju vai garantijas nodrošinātus prasījumus, jo īpaši prasījumus pagarināt vai samaksāt jebkura veida galvojumu, garantiju vai atlīdzību, jo īpaši finanšu garantijas vai finanšu atlīdzību, pagarinājumu vai samaksu, neizpilda, ja tos iesniedz:

a) norādītās fiziskās vai juridiskās personas, vienības vai struktūras, kuras uzskaitītas pielikumā;

b) jebkura fiziska vai juridiska persona, vienība vai struktūra, kas darbojas ar kādas a) apakšpunktā minētās fiziskās vai juridiskās personas, vienības vai struktūras starpniecību vai tās vārdā.

9. pants

Lai šajā lēmumā izklāstīto pasākumu ietekme būtu pēc iespējas lielāka, Savienība aicina trešās valstis pieņemt šajā lēmumā paredzētajiem pasākumiem līdzīgus ierobežojošus pasākumus.

▼M5

10. pants

Šo lēmumu piemēro līdz 2022. gada 18. maijam un pastāvīgi pārskata. To atjauno vai attiecīgi groza, ja Padome uzskata, ka lēmuma mērķi nav sasniegti.

▼B

11. pants

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

▼B

PIELIKUMS

Lēmuma 4. un 5. pantā minēto fizisko un juridisko personu, vienību un struktūru saraksts

▼M2

A. Fiziskas personas

	Vārds	Identifikācijas informācija	Pamatojums	Sarakstā iekļaušanas datums
▼M4				
1.	GAO Qiang	Dzimšanas datums: 1983. gada 4. oktobris 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. "*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*.	30.7.2020.
2.	ZHANG Shilong	Dzimšanas datums: 1981. gada 10. septembris Dzimšanas vieta: Ķīna 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.	30.7.2020.

▼M4

	Vārds	Identifikācijas informācija	Pamatojums	Sarakstā iekļaušanas datums
			“*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*”). *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*.	

▼M2

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 *OPCWWiFi* tīklam Hāgā, Nīderlandē. Kiberuzbrukuma mēģinājuma mērķis bija ielauzties *OPCWWiFi* 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.

▼M2

	Vārds	Identifikācijas informācija	Pamatojums	Sarakstā iekļaušanas datums
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 *OPCWWiFi* tīklam Hāgā, Nīderlandē. Kiberuzbrukuma mēģinājuma mērķis bija ielauzties *OPCWWiFi* 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 *OPCWWiFi* tīklam Hāgā, Nīderlandē. Kiberuzbrukuma mēģinājuma mērķis bija ielauzties *OPCWWiFi* 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.

▼M2

	Vārds	Identifikācijas informācija	Pamatojums	Sarakstā iekļaušanas datums
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 *OPCWWiFi* tīklam Hāgā, Nīderlandē. Kiberuzbrukuma mēģinājuma mērķis bija ielauzties *OPCWWiFi* 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.
▼M3				
7.	Dmitry Sergeyevich BADIN	Дмитрий Сергеевич БАДИН Dzimšanas datums: 1990. gada 15. novembris Dzimšanas vieta: *Kursk*, Krievijas PFSR (tagad Krievijas Federācija) Valstspiederība: Krievijas Dzimums: vīrietis	*Dmitry Badin* piedalījās kiberuzbrukumā ar būtisku ietekmi pret Vācijas federālo parlamentu (*Deutscher Bundestag*). Būdams militārās izlūkošanas virsnieks Krievijas Federācijas Bruņoto spēku Ģenerālštāba Galvenās pārvaldes (*GU/GRU*) 85. Speciālo dienestu galvenajā centrā (*85th Main Centre for Special Services – GTsSS*), *Dmitry Badin* bija Krievijas militārās izlūkošanas virsnieku komandā, kura 2015. gada aprīlī un maijā veica kiberuzbrukumu pret Vācijas federālo parlamentu (*Deutscher Bundestag*). 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 kancleres *Angela Merkel* e-pasta konti.	22.10.2020.

▼M3

	Vārds	Identifikācijas informācija	Pamatojums	Sarakstā iekļaušanas datums
8.	Igor Olegovich KOSTYUKOV	Игорь Олегович КОСТЮКОВ Dzimšanas datums: 1961. gada 21. februāris Valstspiederība: Krievijas 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*), kuru pazīst arī kā "militāro vienību 26165" (nozares iesaukas: "*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 piedalījās kiberuzbrukumā pret Vācijas federālo parlamentu (*Deutscher Bundestag*), kas notika 2015. gada aprīlī un maijā, un 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 kancleres *Angela Merkel* e-pasta konti.	22.10.2020.

▼M2

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.	30.7.2020.

▼M2

	Nosaukums	Identifikācijas informācija	Pamatojums	Sarakstā iekļaušanas datums
			“*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*.	
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. “*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.	30.7.2020.

▼M2

	Nosaukums	Identifikācijas informācija	Pamatojums	Sarakstā iekļaušanas datums
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. "*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*.	30.7.2020.

▼M3

4.	Krievijas Federācijas Bruņoto spēku Ģenerālštāba Galvenās pārvaldes (*GU/GRU*) 85. Speciālo dienestu galvenais centrs (*85th Main Centre for Special Services – GTsSS*)	Adrese: *Komsomol'skiy Prospekt*, 20, *Moscow*, 119146, Krievijas Federācija	Krievijas Federācijas Bruņoto spēku Ģenerālštāba Galvenās pārvaldes (*GU/GRU*) 85. Speciālo dienestu galvenais centrs (*GTsSS*), kuru pazīst arī kā "militāro vienību 26165" (nozares iesaukas: "*APT28*", "*Fancy Bear*", "*Sofacy Group*", "*Pawn Storm*" un "*Strontium*"), ir atbildīgs par kiberuzbrukumiem ar būtisku ietekmi, kas ir ārējs apdraudējums Savienībai vai tās dalībvalstīm.	22.10.2020.

▼M3

	Nosaukums	Identifikācijas informācija	Pamatojums	Sarakstā iekļaušanas datums
			Konkrēti, *GTsSS* militārās izlūkošanas virsnieki piedalījās kiberuzbrukumā pret Vācijas federālo parlamentu (*Deutscher Bundestag*), kas notika 2015. gada aprīlī un maijā, un 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 kancleres *Angela Merkel* e-pasta konti.	