Eiropas Savienības
Padome

Briselē, 2026. gada 7. jūlijā
(OR. en)

8643/26

LIMITE

CORLX 388
CFSP/PESC 584
CYBER 192
JAI 505
FIN 592

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) 2026/...

(... 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 Augstās pārstāves ārlietās un drošības politikas jautājumos priekšlikumu,

tā kā:

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

(2) Kā daļu no noturīgas, pielāgotas un koordinētas Savienības darbības pret pastāvīgiem kiberdraudu aktoriem Lēmuma (KĀDP) 2019/797 pielikumā ietvertajā to fizisko un juridisko personu, vienību un struktūru sarakstā, kurām piemēro ierobežojošus pasākumus, būtu jāpievieno astoņas fiziskas personas un četras vienības. Minētās personas un vienības ir atbildīgas par kiberuzbrukumiem ar būtisku ietekmi, kuri ir ārējs apdraudējums Savienībai vai tās dalībvalstīm, atbalsta šādus kiberuzbrukumus vai ir iesaistītas tajos.

(3) 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 129I, 17.5.2019., 13. lpp., ELI: http://data.europa.eu/eli/dec/2019/797/oj).

1. pants

Lēmuma (KĀDP) 2019/797 pielikumu groza saskaņā ar šā lēmuma pielikumu.

2. pants

Šis lēmums stājas spēkā dienā, kad to publicē *Eiropas Savienības Oficiālajā Vēstnesī*.

..., ...

Padomes vārdā –
priekšsēdētājs/priekšsēdētāja

PIELIKUMS

Lēmuma (KĀDP) 2019/797 pielikumu groza šādi:

1) iedaļā "A. Fiziskas personas" pievieno šādus ierakstus:

	Vārds	Identifikācijas informācija	Pamatojums	Sarakstā iekļaušanas datums
"20.	Vitaly Nikolayevich KOVALEV	Виталий Николаевич КОВАЛЕВ jeb: "Bentley", "Bergen", "Alex Konor", "Benny", "Ben", "Stern" Dzimšanas datums: 23.6.1988. Adrese: *Serebristy Bulvar 34 (Serebristyy Bul'var); krp 1; flt 528; 197341; St Petersburg*, Krievijas Federācija Valstspiederība: Krievijas Dzimums: vīrietis Saistītās vienības: *TrickBot*, *Wizard Spider*, *Conti*	*Vitaly Kovalev* ir augsta ranga persona saistībā ar ļaunprogrammatūru "*Trickbot*" un "*Conti*". Viņš arī ir pazīstams ar tiešsaistes iesaukām "*Bentley*", "*Bergen*", "*Alex Konor*", "*Benny*", "*Ben*" un "*Stern*". "*Conti*" un "*Trickbot*" sākotnēji izveidoja un attīstīja "*Wizard Spider*". "*Wizard Spider*" ir īstenojis izspiešanas kampaņas ar programmatūras palīdzību dažādās nozarēs, tostarp tādās pamatpakalpojumu nozarēs kā veselības aprūpe un banku pakalpojumi, ir inficējis datorus visā pasaulē, un to ļaunprogrammatūra ir attīstījusies par ļoti modulāru ļaunprogrammatūras komplektu. "*Wizard Spider*" kampaņas, kurās izmanto tādu ļaunprogrammatūru kā "*Conti*" un "*TrickBot*", ir atbildīgas par būtisku ekonomisko kaitējumu Eiropas Savienībā. Tāpēc *Vitaly Kovalev* ir atbildīgs par kiberuzbrukumiem ar būtisku ietekmi, kuri ir ārējs apdraudējums Savienībai vai tās dalībvalstīm, un ir iesaistīts tajos.	[+]

[+] OV: lūgums ievietot šā lēmuma publicēšanas datumu.

	Vārds	Identifikācijas informācija	Pamatojums	Sarakstā iekļaušanas datums
21.	Alexander Alexandrovich VOLOSOVIK	Александр Александрович ВОЛОСОВИК Dzimšanas datums: 30.1.1983. Dzimšanas vieta: PSRS Valstspiederība: Krievijas Pases numurs: 762988138 Dzimums: vīrietis Saistītās vienības: *Yalishanda*, *LARVA-34*, *podzemniyl*, *Ohyeahhellno*, *Stas_vl*, *downlow*	*Alexander Volosovik* ir uzņēmuma *Media Land LLC* īpašnieks. Kopš 2016. gada "ložnecaurlaidīgas" mitināšanas pakalpojumu sniedzējs *Media Land LLC* ir veicinājis daudz un dažādu ļaunprogrammatūras uzbrukumu gan Savienībā, gan visā pasaulē, piedāvājot mitināšanas pakalpojumus, kas slēpj lietotāju identitāti un pretojas tiesībaizsardzības iestāžu pieprasījumiem izņemt saturu. *Media Land LLC* radīja iespēju veikt plaša mēroga izspiedējprogrammatūras operācijas, vadības un kontroles pakalpojumus un pikšķerēšanas operācijas, kas vērstas pret kritisko infrastruktūru un pamatpakalpojumiem dalībvalstīs, tādējādi radot ievērojamus finansiālus zaudējumus. Operācijas, kuru norisi veicināja *Media Land LLC*, cita starpā ietver "*LockBit*", "*EvilCorp*" un "*BlackBasta*". Tādējādi *Media Land LLC* ir iesaistīts kiberuzbrukumos ar būtisku ietekmi, kuri ir ārējs apdraudējums Savienībai vai tās dalībvalstīm. *Alexander Volosovik*, būdams *Media Land LLC* īpašnieks, ir atbildīgs par šiem kiberuzbrukumiem un ir tajos iesaistīts. Viņš arī ir saistīts ar *Media Land LLC*.	+

+ OV: lūgums ievietot šā lēmuma publicēšanas datumu.

	Vārds	Identifikācijas informācija	Pamatojums	Sarakstā iekļaušanas datums
22.	Denis Olegovich DEGTYARENKO	Денис Олегович ДЕГТЯРЕНКО jeb: “Dena” Dzimšanas datums: 9.10.1989. Dzimšanas vieta: PSRS Valstspiederība: Krievijas Dzimums: vīrietis Adrese: *130 Lenina Avenue, Novy Gorod microdistrict, Orsk, Orenburg Region*, Krievijas Federācija	*Denis Degtyarenko* jeb “*Dena*” ir Krievijas hakeris, kurš darbojas *CARR* (*Cyber Army of Russia Reborn*) labā. *CARR* ir bijusi atbildīga par kiberuzbrukumiem, kas vērsti pret pakalpojumiem, kuri nepieciešami būtiskas saimnieciskās darbības un kritiski svarīgu valsts funkciju uzturēšanai dalībvalstīs, kā arī infrastruktūrai Ukrainā un citās trešās valstīs. *CARR* ir saistīta ar Krievijas Federācijas bruņoto spēku ģenerālštāba galvenās pārvaldes (*GRU*) galveno speciālo tehnoloģiju centru (*GTsST*). *GTsST* joprojām veic kiberuzbrukumus pret Savienību vai tās dalībvalstīm. Starp *CARR* mērķiem ir valdības aģentūras, finanšu iestādes, mediji un kritiskā infrastruktūra dalībvalstīs un Amerikas Savienotajās Valstīs. *CARR* ir veikusi izkliedētās pakalpojumatteices (*DDoS*) uzbrukumus Ukrainā un pret valdībām un uzņēmumiem valstīs, kuras ir atbalstījušas Ukrainu. Tādējādi *Denis Degtyarenko*, *CARR* galvenais hakeris, ir iesaistīts kiberuzbrukumos ar būtisku ietekmi, tostarp kiberuzbrukumu ar potenciāli būtisku ietekmi mēģinājumos, kuri ir ārējs apdraudējums dalībvalstīm, kā arī pret trešām valstīm. Būdams *CARR* dalībnieks, viņš arī ir saistīts ar *GTsST*.	[+]

[+] OV: lūgums ievietot šā lēmuma publicēšanas datumu.

	Vārds	Identifikācijas informācija	Pamatojums	Sarakstā iekļaušanas datums
23.	Yuliya Vladimirovna PANKRATOVA	Юлия Владимировна ПАНКРАТОВА jeb: "YUliYA" Dzimšanas datums: 6.4.1984. Dzimšanas vieta: PSRS Valstspiederība: Krievijas Dzimums: sieviete Adrese: *130 Lenina Avenue, Novy Gorod microdistrict, Orsk, Orenburg Region*, Krievijas Federācija	*Yuliya Pankratova* ir Krievijas hakere, kas ir darbojusies *CARR* (*Cyber Army of Russia Reborn*) labā un pēc tam dibinājusi un turpinājusi darboties *Z-Pentest* labā. *CARR* ir bijusi atbildīga par kiberuzbrukumiem pret pakalpojumiem, kuri nepieciešami būtiskas saimnieciskās darbības un kritiski svarīgu valsts funkciju uzturēšanai dalībvalstīs, kā arī pret infrastruktūru Ukrainā un citās trešās valstīs. *CARR* ir saistīta ar Krievijas Federācijas bruņoto spēku ģenerālštāba galvenās pārvaldes (*GRU*) galveno speciālo tehnoloģiju centru (*GTsST*). *GTsST* joprojām veic kiberuzbrukumus pret Savienību vai tās dalībvalstīm. Starp *CARR* mērķiem ir valdības aģentūras, finanšu iestādes, mediji un kritiskā infrastruktūra dalībvalstīs un Amerikas Savienotajās Valstīs. *CARR* ir veikusi izkliedētās pakalpojumatteices (*DDoS*) uzbrukumus Ukrainā un pret valdībām un uzņēmumiem valstīs, kuras ir atbalstījušas Ukrainu.	+

+ OV: lūgums ievietot šā lēmuma publicēšanas datumu.

	Vārds	Identifikācijas informācija	Pamatojums	Sarakstā iekļaušanas datums
			Z-Pentest ir atbildīgs par kiberuzbrukumiem ar būtisku ietekmi, kas cita starpā vērsti pret pakalpojumiem, kuri nepieciešami būtisku darbību uzturēšanai dalībvalstīs. Tādējādi *Yuliya Pankratova*, *CARR* un *Z-Pentest* primārā hakere, ir iesaistīta kiberuzbrukumos ar būtisku ietekmi, tostarp kiberuzbrukumu ar potenciāli būtisku ietekmi mēģinājumos, kuri ir ārējs apdraudējums dalībvalstīm, kā arī pret trešām valstīm. Viņa arī ir saistīta ar *Z-Pentest*.	

	Vārds	Identifikācijas informācija	Pamatojums	Sarakstā iekļaušanas datums
24.	Maksim Evgenevich VORONIN	Максим Евгеньевич ВОРОНИН jeb: “Daugn0” Valstspiederība: iespējams, Krievijas Dzimums: vīrietis	*Maksim Voronin* jeb *Daugn0* ir iesaistīts informācijas zagšanas ļaunprogrammatūras *LummaC2* (pazīstama arī kā *Lumma Infostealer*, *Lumma Stealer*) izstrādē, izplatīšanā un pārdošanā. *LummaC2* ir ļaunprogrammatūras kā pakalpojuma (*MaaS*) platforma, ko izmanto, lai zagtu sensitīvus datus, pārlūku akreditācijas datus, kriptomakus vai sistēmas informāciju, lai inficētajās ierīcēs izvietotu papildu ļaunprogrammatūru kriptovalūtas zagšanas un spiegošanas kampaņu nolūkos. Kiberuzbrukumus, kuros iesaistīta ļaunprogrammatūra *LummaC2*, izmanto arī finansiāli motivēti kiberapdraudētāji, piemēram, *Storm-113*, *Storm-1607*, *Storm-1674*, *Octo Tempest* un citi. Ļaunprogrammatūra *LummaC2* ir izmantota kiberuzbrukumiem kritiskām valsts funkcijām un pakalpojumiem, kas nepieciešami būtisku sociālo un saimniecisko darbību uzturēšanai dalībvalstīs. 2024. un 2025. gadā *LummaC2* bija viens no pasaulē visvairāk izmantotajiem informācijas zagšanas rīkiem. Tāpēc *Maksim Voronin*, būdams *LummaC2* izstrādātājs, izplatītājs un pārdevējs, ir iesaistīts kiberuzbrukumos ar būtisku ietekmi, kuri ir ārējs apdraudējums dalībvalstīm, un veicina tos.	[+]

[+] OV: lūgums ievietot šā lēmuma publicēšanas datumu.

	Vārds	Identifikācijas informācija	Pamatojums	Sarakstā iekļaušanas datums
25.	Maksim Aleksandrovich GORDIENKO jeb: Maxim Alexandrovich GORDIENKO	Максим Александрович ГОРДИЕНКО jeb: “Lummaseller” Valstspiederība: iespējams, Krievijas Dzimums: vīrietis	*Maksim Gordienko* jeb *Lummaseller* ir iesaistīts informācijas zagšanas ļaunprogrammatūras *LummaC2* (pazīstama arī kā *Lumma Infostealer*, *Lumma Stealer*) izstrādē un izplatīšanā. *LummaC2* ir ļaunprogrammatūras kā pakalpojuma (*MaaS*) platforma, ko izmanto, lai zagtu sensitīvus datus, pārlūku akreditācijas datus, kriptomakus vai sistēmas informāciju, lai inficētajās ierīcēs izvietotu papildu ļaunprogrammatūru kriptovalūtas zagšanas un spiegošanas kampaņu nolūkos. Kiberuzbrukumus, kuros iesaistīta ļaunprogrammatūra *LummaC2*, izmanto arī finansiāli motivēti kiberapdraudētāji, piemēram, *Storm-113*, *Storm-1607*, *Storm-1674*, *Octo Tempest* un citi. Ļaunprogrammatūra *LummaC2* ir izmantota kiberuzbrukumiem kritiskām valsts funkcijām un pakalpojumiem, kas nepieciešami būtisku sociālo un saimniecisko darbību uzturēšanai dalībvalstīs. 2024. un 2025. gadā *LummaC2* bija viens no pasaulē visvairāk izmantotajiem informācijas zagšanas rīkiem. Tāpēc *Maksim Gordienko*, būdams *LummaC2* izstrādātājs, izplatītājs un pārdevējs, ir iesaistīts kiberuzbrukumos ar būtisku ietekmi, kuri ir ārējs apdraudējums dalībvalstīm, un veicina tos.	[+]

[+] OV: lūgums ievietot šā lēmuma publicēšanas datumu.

	Vārds	Identifikācijas informācija	Pamatojums	Sarakstā iekļaušanas datums
26.	Evgeniy Viktorovich BASHEV	Евгений Викторович БАШЕВ Dzimšanas datums: 25.1.1980. Dzimšanas vieta: PSRS Valstspiederība: Krievijas Dzimums: vīrietis Saistītās personas: *Denis Igorevich Denisenko*, *Yuriy Fedorovich Denisov*, *Dmitriy Yuryevich Goloshubov*, *Nikolay Alexandrovich Korchagin* Saistītās vienības: *GRU* vienība Nr. 29155, *"Impuls" LLC*	*Evgeniy Bashev* ir Krievijas militārās izlūkošanas pārvaldes *GRU* vienības Nr. 29155 loceklis. Vienībā viņš atbalsta un veicina kiberuzbrukumus ar būtisku ietekmi pret dalībvalstīm, cita starpā kontrolējot serveri "*Aegon*", ko izmanto uzlaušanas operācijām. Konkrēti, viņš sniedz tehnisku un materiālu atbalstu *GRU* vienības Nr. 29155 kiberuzbrukumiem ar sava uzņēmuma "*Impulse*" *LLC* starpniecību, kas palīdzēja nodrošināt operatīvo segumu, infrastruktūru un maksājumus, kā arī pārvaldīja tehniskos līdzekļus, tostarp serverus, kurus izmanto kiberuzbrukumiem. Viņš arī koordinēja sadarbību starp *GRU* struktūrām un ārējiem hakeru tīkliem. Kiberuzbrukumi, ko viņš veicināja, bija vērsti pret kritiski svarīgām valsts funkciju sistēmām un pakalpojumiem, kas nepieciešami būtisku sociālo vai saimniecisko darbību uzturēšanai dalībvalstīs, jo īpaši transporta nozarē. *WhisperGate* kampaņas ietvaros *GRU* vienība Nr. 29155 vērsās pret Ukrainas kritisko infrastruktūru.	+

+ OV: lūgums ievietot šā lēmuma publicēšanas datumu.

	Vārds	Identifikācijas informācija	Pamatojums	Sarakstā iekļaušanas datums
			Tādējādi *Evgeniy Bashev* sniedz tehnisku un materiālu atbalstu kiberuzbrukumiem ar būtisku ietekmi, tostarp kiberuzbrukumu ar potenciāli būtisku ietekmi mēģinājumiem, kuri ir ārējs apdraudējums dalībvalstīm, kā arī kiberuzbrukumiem ar būtisku ietekmi pret trešo valsti, vai ir citādi iesaistīts tajos. Būdams īpašnieks un ģenerāldirektors, viņš ir saistīts ar uzņēmumu "*Impulse*" *LLC*. Būdams *GRU* vienības Nr. 29155 loceklis, viņš arī ir saistīts ar minēto vienību.	

	Vārds	Identifikācijas informācija	Pamatojums	Sarakstā iekļaušanas datums
27.	Roman Alexandrovich PUNTUS	Роман Александрович ПУНТУС Dzimšanas vieta: Krievijas Federācija Valstspiederība: Krievijas Dzimums: vīrietis Saistītās personas: *Denis Igorevich Denisenko*, *Yuriy Fedorovich Denisov*, *Dmitriy Yuryevich Goloshubov*, *Nikolay Alexandrovich Korchagin*, *Evgeniy Viktorovich Bashev* Saistītās vienības: *GRU* vienība Nr. 29155	*Roman Puntus* ir Krievijas militārās izlūkošanas aģentūras *GRU* vienības Nr. 29155 loceklis. Vienībā viņam ir vadoša loma tādu kiberuzbrukumu organizēšanā un koordinēšanā, kuriem ir būtiska ietekme uz dalībvalstīm. Viņš arī atbalsta vienības iekšējo kiberspēju attīstīšanu, tostarp, veicot personāla (piemēram, hakeru un programmētāju) vervēšanu un uzraudzību. Izveidojot aizsegsabiedrību "*Aegeon-Impulse*", viņš palīdzēja nodrošināt kiberoperāciju loģistikas un finanšu aspektus. Viņam koordinējot, vienība īstenoja kiberuzbrukumus, kuri bija vērsti pret kritiski svarīgām valsts funkciju sistēmām un pakalpojumiem, kas nepieciešami būtisku sociālo vai saimniecisko darbību uzturēšanai dalībvalstīs, jo īpaši transporta nozarē. *WhisperGate* kampaņas ietvaros *GRU* vienība Nr. 29155 vērsās pret Ukrainas kritisko infrastruktūru.	[+]";

[+] OV: lūgums ievietot šā lēmuma publicēšanas datumu.

	Vārds	Identifikācijas informācija	Pamatojums	Sarakstā iekļaušanas datums
			Tādējādi *Roman Puntus* ir atbildīgs par kiberuzbrukumiem ar būtisku ietekmi, tostarp par kiberuzbrukumu ar potenciāli būtisku ietekmi mēģinājumiem, kuri ir ārējs apdraudējums dalībvalstīm, kā arī par kiberuzbrukumiem ar būtisku ietekmi pret trešo valsti, vai ir citādi iesaistīts tajos. Būdams *GRU* vienības Nr. 29155 loceklis, viņš arī ir saistīts ar minēto vienību.	

2) iedaļā “B. Juridiskas personas, vienības un struktūras” pievieno šādus ierakstus:

	Nosaukums	Identifikācijas informācija	Pamatojums	Sarakstā iekļaušanas datums
“8.	Media Land LLC	Adrese: *Tsvetnochnaya st., 16 Litera P, Room 27, Moskovskaya Zastava Municipal District, St Petersburg, 196006*, Krievijas Federācija Vienības veids: sabiedrība ar ierobežotu atbildību Reģistrācijas vieta: *St Petersburg* Reģistrācijas datums: 19.10.2015. Reģistrācijas Nr.: 1152536009900 Galvenā uzņēmējdarbības vieta: *St Petersburg*, Krievijas Federācija Saistītā vienība: *ML.Cloud*	Kopš 2016. gada “ložnecaurlaidīgas” mitināšanas pakalpojumu sniedzējs *Media Land LLC* ir veicinājis daudz un dažādu ļaunprogrammatūras uzbrukumu gan pret dalībvalstīm, gan visā pasaulē, piedāvājot mitināšanas pakalpojumus, kas slēpj lietotāju identitāti un pretojas tiesībaizsardzības iestāžu pieprasījumiem izņemt saturu, tādējādi radot ievērojamus finansiālus zaudējumus. *Media Land LLC* radīja iespēju veikt plaša mēroga izspiedējprogrammatūras operācijas, vadības un kontroles pakalpojumus un pikšķerēšanas operācijas, kas vērstas pret kritisko infrastruktūru un pamatpakalpojumiem dalībvalstīs. Operācijas, kuru norisi veicināja *Media Land LLC*, cita starpā ietver “*LockBit*”, “*EvilCorp*” un “*BlackBasta*”. Tādējādi *Media Land LLC* ir iesaistīts kiberuzbrukumos ar būtisku ietekmi, kuri ir ārējs apdraudējums dalībvalstīm.	+

+ OV: lūgums ievietot šā lēmuma publicēšanas datumu.

	Nosaukums	Identifikācijas informācija	Pamatojums	Sarakstā iekļaušanas datums
9.	*ML.Cloud*	Adrese: *Brivibas iela 52, Riga, LV-1011*, Latvija; Krievijas Federācija, *Kazan, Peterburgskaya st. 52* Reģistrācijas vieta: Rīga Saistītā persona: *Alexander Volosovik* Citas saistītās vienības: Media Land LLC	*ML.Cloud* ir *Media Land LLC* māsasuzņēmums un nodrošina *Media Land LLC* tehnisko infrastruktūru. Kopš 2016. gada "ložnecaurlaidīgas" mitināšanas pakalpojumu sniedzējs *Media Land LLC* ir veicinājis daudz un dažādu ļaunprogrammatūras uzbrukumu gan pret dalībvalstīm, gan visā pasaulē, piedāvājot mitināšanas pakalpojumus, kas slēpj lietotāju identitāti un pretojas tiesībaizsardzības iestāžu pieprasījumiem izņemt saturu, tādējādi radot ievērojamus finansiālus zaudējumus. *Media Land LLC* radīja iespēju veikt plaša mēroga izspiedējprogrammatūras operācijas, vadības un kontroles pakalpojumus un pikšķerēšanas operācijas, kas vērstas pret kritisko infrastruktūru un pamatpakalpojumiem dalībvalstīs. Operācijas, kuru norisi veicināja *Media Land LLC*, cita starpā ietver "*LockBit*", "*EvilCorp*" un "*BlackBasta*". Tādējādi *Media Land LLC* ir iesaistīts kiberuzbrukumos, kas ir ārējs apdraudējums ar būtisku ietekmi uz ES dalībvalstīm. Tādējādi *ML Cloud* sniedz tehnisku atbalstu kiberuzbrukumiem ar būtisku ietekmi, kuri ir ārējs apdraudējums dalībvalstīm.	[+]

[+] OV: lūgums ievietot šā lēmuma publicēšanas datumu.

	Nosaukums	Identifikācijas informācija	Pamatojums	Sarakstā iekļaušanas datums
10.	“Impuls” LLC	Общество с ограниченной ответственностью “Импульс” Adrese: 344015, Krievijas Federācija, *Rostov Region, Rostov-on-Don, ul. Eremenko, d. 56, k. 6, apt.* 88 Vienības veids: sabiedrība ar ierobežotu atbildību Reģistrācijas vieta: *Interdistrict Inspectorate of the Federal Tax Service No. 26 for the Rostov Region, 344019, Rostov-on-Don, ul. Myasnikova, d. 52/32*, Krievijas Federācija Reģistrācijas datums: 27.9.2010.	*“Impuls” LLC* ir Krievijas uzņēmums, kas pieder *Evgeniy Viktorovich Bashev*, kurš ir Krievijas militārās izlūkošanas pārvaldes *GRU* vienības Nr. 29155 loceklis. Uzņēmums sniedz tehnisku un materiālu atbalstu kiberuzbrukumiem un kiberuzbrukumu mēģinājumiem, ko veic *GRU* vienība Nr. 29155. Konkrēti, *“Impuls” LLC* darbojas kā operatīvais starpnieks, kas ļauj veikt ar uzlaušanu saistītas darbības ar tāda uzņēmuma starpniecību, kurš formāli nav saistīts ar Krievijas valsti. Uzņēmums koordinēja operatīvo segumu, infrastruktūru un maksājumus saistībā ar kiberuzbrukumiem, un bija saistīts ar tehniskajiem līdzekļiem, tostarp serveriem, ko izmantoja hakeru darbības atbalstam. Jo īpaši *“Impuls” LLC* radīja iespējas sadarbībai starp *GRU* struktūrām un ārējiem hakeru tīkliem. Kiberuzbrukumi, ko veicina *“Impuls” LLC*, ir vērsti pret kritiski svarīgām valsts funkcijām un pakalpojumiem, kas nepieciešami būtisku sociālo un saimniecisko darbību uzturēšanai dalībvalstīs, jo īpaši transporta nozarē. *WhisperGate* kampaņas ietvaros *GRU* vienība Nr. 29155 vērsās pret Ukrainas kritisko infrastruktūru.	+

+ OV: lūgums ievietot šā lēmuma publicēšanas datumu.

	Nosaukums	Identifikācijas informācija	Pamatojums	Sarakstā iekļaušanas datums
		Reģistrācijas Nr.: INN (ИНН): 6168033776; OGRN (ОГРН): 1106194004850 Galvenā uzņēmējdarbības vieta: Krievijas Federācija Saistītās personas: *Evgeniy Bashev* Saistītās vienības: *GRU* vienība Nr. 29155	Tādējādi *"Impuls" LLC* sniedz tehnisku un materiālu atbalstu kiberuzbrukumiem ar būtisku ietekmi, kuri ir ārējs apdraudējums dalībvalstīm, kā arī kiberuzbrukumiem ar būtisku ietekmi pret trešo valsti, vai ir citādi iesaistīts tajos.	

	Nosaukums	Identifikācijas informācija	Pamatojums	Sarakstā iekļaušanas datums
11.	Z-Pentest	jeb: “Z-Pentest Alliance”, “Z-Alliance” Galvenā uzņēmējdarbības vieta: Krievijas Federācija Saistītās personas: *Yuliya Pankratova* Saistītās vienības: *Cyber Army of Russia/CARR* *X.com* konts: *ZPentest* (konta darbība apturēta) *Telegram* konts: *Zpentestalliance*	*Z-pentest* ir prokrieviska haktīvistu grupa, kuras sastāvā ir locekļi no *CARR* (*Cyber Army of Russia Reborn*) un *NoName057* un kura visā pasaulē vēršas pret kritisko infrastruktūru, jo īpaši enerģētikas un ūdensapgādes nozari. Jo īpaši grupa 2024. gada decembrī uzbruka Dānijas ūdensapgādes uzņēmumam. Tādējādi *Z-Pentest* ir atbildīgs par kiberuzbrukumiem ar būtisku ietekmi, kuri ir ārējs apdraudējums dalībvalstīm.	[+]”.

[+] OV: lūgums ievietot šā lēmuma publicēšanas datumu.