Vijeće
Europske unije

Bruxelles, 13. svibnja 2024.
(OR. en)

8500/24

LIMITE

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

ZAKONODAVNI AKTI I DRUGI INSTRUMENTI

Predmet:	ODLUKA VIJEĆA o izmjeni Odluke (ZVSP) 2019/797 o mjerama ograničavanja protiv kibernapada koji predstavljaju prijetnju Uniji ili njezinim državama članicama

ODLUKA VIJEĆA (ZVSP) 2024/...

od …

o izmjeni Odluke (ZVSP) 2019/797 o mjerama ograničavanja protiv kibernapada koji predstavljaju prijetnju Uniji ili njezinim državama članicama

VIJEĆE EUROPSKE UNIJE,

uzimajući u obzir Ugovor o Europskoj uniji, a posebno njegov članak 29.,

uzimajući u obzir prijedlog Visokog predstavnika Unije za vanjske poslove i sigurnosnu politiku,

budući da:

(1) Vijeće je 17. svibnja 2019. donijelo Odluku (ZVSP) 2019/797[1].

(2) Odluka (ZVSP) 2019/797 primjenjuje se do 18. svibnja 2025. Na temelju preispitivanja te odluke, valjanost u njoj utvrđenih mjera ograničavanja trebalo bi produljiti do tog datuma.

(3) S obzirom na kontinuirano i sve prisutnije zlonamjerno ponašanje u kibernetičkom prostoru, koje obuhvaća i ponašanje usmjereno protiv trećih država, trebalo bi za šest osoba i dva subjekta ažurirati razloge za uvrštenje na popis fizičkih i pravnih osoba, subjekata i tijela koji podliježu mjerama ograničavanja naveden u Prilogu Odluci (ZVSP) 2019/797.

(4) Odluku (ZVSP) 2019/797 trebalo bi stoga na odgovarajući način izmijeniti,

DONIJELO JE OVU ODLUKU:

[1] Odluka Vijeća (ZVSP) 2019/797 od 17. svibnja 2019. o mjerama ograničavanja protiv kibernapada koji predstavljaju prijetnju Uniji ili njezinim državama članicama (SL L 129I, 17.5.2019., str. 13.).

Članak 1.

Odluka (ZVSP) 2019/797 mijenja se kako slijedi:

1. članak 10. zamjenjuje se sljedećim:

„*Članak 10.*

Ova Odluka primjenjuje se do 18. svibnja 2025. te se redovito preispituje.”;

2. Prilog se mijenja u skladu s Prilogom ovoj Odluci.

Članak 2.

Ova Odluka stupa na snagu sljedećeg dana od dana objave u *Službenom listu Europske unije*.

Sastavljeno u …

Za Vijeće

Predsjednik/Predsjednica

PRILOG

Prilog Odluci (ZVSP) 2019/797 („Popis fizičkih i pravnih osoba, subjekata i tijela iz članaka 4. i 5.”) mijenja se kako slijedi:

1. na popisu pod naslovom „A. Fizičke osobe” unosi od 3. do 8. zamjenjuju se sljedećim:

	Ime	Identifikacijski podaci	Obrazloženje	Datum uvrštenja na popis
„3.	Alexey Valeryevich MININ	Алексей Валерьевич МИНИН Datum rođenja: 27.5.1972. Mjesto rođenja: Permska oblast, Ruski SFSR (sada Ruska Federacija) Broj putovnice: 120017582 Izdalo: Ministarstvo vanjskih poslova Ruske Federacije Vrijedi: od 17.4.2017. do 17. 4.2022. Lokacija: Moskva, Ruska Federacija Državljanstvo: rusko Spol: muški	Alexey Minin sudjelovao je u pokušaju kibernetičkog napada s potencijalno znatnim učinkom na Organizaciju za zabranu kemijskog oružja (OPCW) u Nizozemskoj i u kibernetičkim napadima sa znatnim učinkom protiv trećih država. Kao službenik za prikupljanje obavještajnih podataka osobnim kontaktima u okviru glavne uprave glavnog stožera oružanih snaga Ruske Federacije (GU/GRU), Alexey Minin bio je dio tima od četiriju ruskih vojnih obavještajnih službenika koji su pokušali neovlašteno pristupiti bežičnoj mreži OPCW-a u Haagu u Nizozemskoj u travnju 2018. Pokušaj kibernetičkog napada bio je usmjeren na hakiranje bežične mreže OPCW-a, što bi, da je bilo uspješno, ugrozilo sigurnost mreže i tekuće istražne radnje OPCW-a. Nizozemska obrambena obavještajna i sigurnosna služba (Militaire Inlichtingen- en Veiligheidsdienst) spriječila je pokušaj kibernetičkog napada i time izbjegla ozbiljnu štetu za OPCW. Velika porota u Zapadnom okrugu Pennsylvanije (Sjedinjene Američke Države) podigla je optužnicu protiv Alexeyja Minina, kao časnika Glavne ruske obavještajne uprave (GRU), za hakiranje računala, prijevaru elektroničkim sredstvima, tešku krađu identiteta i pranje novca.	30.7.2020.

	Ime	Identifikacijski podaci	Obrazloženje	Datum uvrštenja na popis
4.	Aleksei Sergeyvich MORENETS	Алексей Сергеевич МОРЕНЕЦ Datum rođenja: 31.7.1977. Mjesto rođenja: Murmanska oblast, Ruski SFSR (sada Ruska Federacija) Broj putovnice: 100135556 Izdalo: Ministarstvo vanjskih poslova Ruske Federacije Vrijedi: od 17.4.2017. do 17.4.2022. Lokacija: Moskva, Ruska Federacija Državljanstvo: rusko Spol: muški	Aleksei Morenets sudjelovao je u pokušaju kibernetičkog napada s potencijalno znatnim učinkom na Organizaciju za zabranu kemijskog oružja (OPCW) u Nizozemskoj i u kibernetičkim napadima sa znatnim učinkom protiv trećih država. Kao kibernetički operater glavne uprave glavnog stožera oružanih snaga Ruske Federacije (GU/GRU), Aleksei Morenets bio je dio tima od četiriju ruskih vojnih obavještajnih službenika koji su pokušali neovlašteno pristupiti bežičnoj mreži OPCW-a u Haagu u Nizozemskoj u travnju 2018. Pokušaj kibernetičkog napada bio je usmjeren na hakiranje bežične mreže OPCW-a, što bi, da je bilo uspješno, ugrozilo sigurnost mreže i tekuće istražne radove OPCW-a. Nizozemska obrambena obavještajna i sigurnosna služba (Militaire Inlichtingen- en Veiligheidsdienst) spriječila je pokušaj kibernetičkog napada i time izbjegla ozbiljnu štetu za OPCW. Velika porota u Zapadnom okrugu Pennsylvanije (Sjedinjene Američke Države) podigla je optužnicu protiv Alekseja Morenetsa, kao osobe dodijeljene vojnoj jedinici 26165, za hakiranje računala, prijevaru elektroničkim sredstvima, tešku krađu identiteta i pranje novca.	30.7.2020.

	Ime	Identifikacijski podaci	Obrazloženje	Datum uvrštenja na popis
5.	Evgenii Mikhaylovich SEREBRIAKOV	Евгений Михайлович СЕРЕБРЯКОВ Datum rođenja: 26.7.1981. Mjesto rođenja: Kursk, Ruski SFSR (sada Ruska Federacija) Broj putovnice: 100135555 Izdalo: Ministarstvo vanjskih poslova Ruske Federacije Vrijedi: od 17.4.2017. do 17.4.2022. Lokacija: Moskva, Ruska Federacija Državljanstvo: rusko Spol: muški	Evgenii Serebriakov sudjelovao je u pokušaju kibernetičkog napada s potencijalno znatnim učinkom na Organizaciju za zabranu kemijskog oružja (OPCW) u Nizozemskoj i u kibernetičkim napadima sa znatnim učinkom protiv trećih država. Kao kibernetički operater glavne uprave glavnog stožera oružanih snaga Ruske Federacije (GU/GRU), Evgenii Serebriakov bio je dio tima od četiriju ruskih vojnih obavještajnih službenika koji su pokušali neovlašteno pristupiti bežičnoj mreži OPCW-a u Haagu u Nizozemskoj u travnju 2018. Pokušaj kibernetičkog napada bio je usmjeren na hakiranje bežične mreže OPCW-a, što bi, da je bilo uspješno, ugrozilo sigurnost mreže i tekuće istražne radnje OPCW-a. Nizozemska obrambena obavještajna i sigurnosna služba (Militaire Inlichtingen- en Veiligheidsdienst) spriječila je pokušaj kibernetičkog napada i time izbjegla ozbiljnu štetu za OPCW. Evgenii Serebriakov od proljeća 2022. predvodi ‚Sandworm' (također poznat kao ‚Sandworm Team', ‚BlackEnergy Group', ‚Voodoo Bear', ‚Quedagh', ‚Olympic Destroyer' i ‚Telebots'), subjekt i hakersku skupinu povezanu s jedinicom 74455 Glavne ruske obavještajne uprave. Sandworm je izvršio kibernetičke napade na Ukrajinu, uključujući ukrajinske vladine agencije, slijedom agresivnog rata Rusije protiv Ukrajine.	30.7.2020.

	Ime	Identifikacijski podaci	Obrazloženje	Datum uvrštenja na popis
6.	Oleg Mikhaylovich SOTNIKOV	Олег Михайлович СОТНИКОВ Datum rođenja: 24.8.1972. Mjesto rođenja: Uljanovsk, Ruski SFSR (sada Ruska Federacija) Broj putovnice: 120018866 Izdalo: Ministarstvo vanjskih poslova Ruske Federacije Vrijedi: od 17.4.2017. do 17.4.2022. Lokacija: Moskva, Ruska Federacija Državljanstvo: rusko Spol: muški	Oleg Sotnikov sudjelovao je u pokušaju kibernetičkog napada s potencijalno znatnim učinkom na Organizaciju za zabranu kemijskog oružja (OPCW) u Nizozemskoj i u kibernetičkim napadima sa znatnim učinkom protiv trećih država. Kao službenik za prikupljanje obavještajnih podataka osobnim kontaktima u okviru glavne uprave glavnog stožera oružanih snaga Ruske Federacije (GU/GRU), Oleg Sotnikov bio je dio tima od četiriju ruskih vojnih obavještajnih službenika koji su pokušali neovlašteno pristupiti bežičnoj mreži OPCW-a u Haagu u Nizozemskoj u travnju 2018. Pokušaj kibernetičkog napada bio je usmjeren na hakiranje bežične mreže OPCW-a, što bi, da je bilo uspješno, ugrozilo sigurnost mreže i tekuće istražne radnje OPCW-a. Nizozemska obrambena obavještajna i sigurnosna služba (Militaire Inlichtingen- en Veiligheidsdienst) spriječila je pokušaj kibernetičkog napada i time izbjegla ozbiljnu štetu za OPCW. Velika porota u Zapadnom okrugu Pennsylvanije podigla je optužnicu protiv Olega Sotnikova, kao časnika Glavne ruske obavještajne uprave (GRU), za hakiranje računala, prijevaru elektroničkim sredstvima, tešku krađu identiteta i pranje novca.	30.7.2020.

	Ime	Identifikacijski podaci	Obrazloženje	Datum uvrštenja na popis
7.	Dmitry Sergeyevich BADIN	Дмитрий Сергеевич БАДИН Datum rođenja: 15.11.1990. Mjesto rođenja: Kursk, Ruski SFSR (sada Ruska Federacija) Državljanstvo: rusko Spol: muški	Dmitry Badin sudjelovao je u kibernetičkom napadu sa znatnim učinkom na Njemački savezni parlament (Deutscher Bundestag) i u kibernetičkim napadima sa znatnim učinkom protiv trećih država. Kao vojni obavještajni časnik 85. glavnog centra za specijalne službe (GTsSS) Glavne uprave Glavnog stožera oružanih snaga Ruske Federacije (GU/GRU) Dmitry Badin bio je dio tima ruskih vojnih obavještajnih časnika koji su izveli kibernetički napad na Njemački savezni parlament u travnju i svibnju 2015. Taj je kibernetički napad bio usmjeren na informacijski sustav Parlamenta i nekoliko je dana utjecao na njegovo funkcioniranje. Ukradena je znatna količina podataka i zahvaćeni su računi e-pošte više zastupnika u Parlamentu, kao i račun e-pošte bivše kancelarke Angele Merkel. Velika porota u Zapadnom okrugu Pennsylvanije (Sjedinjene Američke Države) podigla je optužnicu protiv Dmitryja Badina, kao osobe dodijeljene vojnoj jedinici 26165, za hakiranje računala, prijevaru elektroničkim sredstvima, tešku krađu identiteta i pranje novca.	22.10.2020.

	Ime	Identifikacijski podaci	Obrazloženje	Datum uvrštenja na popis
8.	Igor Olegovich KOSTYUKOV	Игорь Олегович КОСТЮКОВ Datum rođenja: 21.2.1961. Državljanstvo: rusko Spol: muški	Igor Kostyukov aktualni je načelnik Glavne uprave Glavnog stožera oružanih snaga Ruske Federacije (GU/GRU), gdje je prethodno obnašao dužnost prvog zamjenika načelnika. Među jedinicama pod njegovim zapovjedništvom nalazi se 85. glavni centar za specijalne službe (GTsSS) (također poznat kao ‚vojna jedinica 26165', ‚APT28', ‚Fancy Bear', ‚Sofacy Group', ‚Pawn Storm' i ‚Strontium'). U tom je svojstvu Igor Kostyukov odgovoran za kibernetičke napade koje je izveo GTsSS, uključujući kibernetičke napade sa znatnim učinkom koji predstavljaju vanjsku prijetnju Uniji ili njezinim državama članicama. Osobito, vojni obavještajni časnici GTsSS-a sudjelovali su u kibernetičkom napadu na Njemački savezni parlament (Deutscher Bundestag) u travnju i svibnju 2015. te pokušaju kibernetičkog napada s ciljem hakiranja bežične mreže Organizacije za zabranu kemijskog oružja (OPCW) u Nizozemskoj u travnju 2018. Kibernetički napad na Njemački savezni parlament bio je usmjeren na njegov informacijski sustav i nekoliko je dana utjecao na njegovo funkcioniranje. Ukradena je znatna količina podataka i zahvaćeni su računi e-pošte više zastupnika u Parlamentu, kao i račun e-pošte bivše kancelarke Angele Merkel.	22.10.2020."

2. na popisu pod naslovom „B. Pravne osobe, subjekti i tijela” unosi 3. i 4. zamjenjuju se sljedećim:

	Ime	Identifikacijski podaci	Obrazloženje	Datum uvrštenja na popis
”3.	Glavni centar za posebne tehnologije (GTsST) glavne uprave glavnog stožera oružanih snaga Ruske Federacije (GU/GRU)	Adresa: 22 Kirova Street, Moscow, Russian Federation	Glavni centar za posebne tehnologije (GTsST) Glavne uprave Glavnog stožera oružanih snaga Ruske Federacije (GU/GRU), poznat i pod brojem vojne pošte 74455, uključen je u kibernetičke napade sa znatnim učinkom koji potječu iz područja izvan Unije i predstavljaju vanjsku prijetnju Uniji ili njezinim državama članicama te kibernetičke napade sa znatnim učinkom na treće države, uključujući kibernetičke napade u lipnju 2017. koji su javnosti poznati kao ‚NotPetya’ ili ‚EternalPetya’ i kibernetičke napade na ukrajinsku energetsku mrežu tijekom zima 2015. i 2016. ‚NotPetya’ ili ‚EternalPetya’ onemogućili su pristup podacima u nizu društava u Uniji, široj Europi i svijetu tako što su računala napali ucjenjivačkim softverom i blokirali pristup podacima, što je, među ostalim, dovelo do znatnog gospodarskog gubitka. Kibernetički napad na ukrajinsku energetsku mrežu rezultirao je gašenjem dijelova te mreže tijekom zime.	30.7.2020.

	Ime	Identifikacijski podaci	Obrazloženje	Datum uvrštenja na popis
			Subjekt javnosti poznat pod nazivom ‚Sandworm' (također poznat kao ‚Sandworm Team', ‚BlackEnergy Group', ‚Voodoo Bear', ‚Quedagh', ‚Olympic Destroyer', i ‚Telebots'), koji također stoji iza napada na ukrajinsku energetsku mrežu, izvršio je napade ‚NotPetya' ili ‚EternalPetya'. Sandworm je izvršio kibernetičke napade na Ukrajinu, uključujući ukrajinske vladine agencije i ukrajinsku kritičnu infrastrukturu, slijedom agresivnog rata Rusije protiv Ukrajine. Ti kibernetički napadi uključuju kampanje ciljanog *phishinga*, štetne softvere i napade ucjenjivačkim softverom. Glavni centar za posebne tehnologije glavne uprave glavnog stožera oružanih snaga Ruske Federacije ima aktivnu ulogu u kibernetičkim aktivnostima koje provodi Sandworm i može se povezati sa subjektom Sandworm.	

	Ime	Identifikacijski podaci	Obrazloženje	Datum uvrštenja na popis
4.	85. glavni centar za specijalne službe (GTsSS) Glavne uprave Glavnog stožera oružanih snaga Ruske Federacije (GU/GRU)	Adresa: Komsomol'skiy Prospekt, 20, Moscow, 119146, Russian Federation	85. glavni centar za specijalne službe (GTsSS) Glavne uprave Glavnog stožera oružanih snaga Ruske Federacije (GU/GRU) (također poznat kao ‚vojna jedinica 26165', ‚APT28', ‚Fancy Bear', ‚Sofacy Group', ‚Pawn Storm' i ‚Strontium'), uključen je u kibernetičke napade sa znatnim učinkom koji predstavljaju vanjsku prijetnju Uniji ili njezinim državama članicama i u kibernetičke napade sa znatnim učinkom protiv trećih država. Osobito, vojni obavještajni časnici GTsSS-a sudjelovali su u kibernetičkom napadu na Njemački savezni parlament (Deutscher Bundestag) u travnju i svibnju 2015. te pokušaju kibernetičkog napada s ciljem hakiranja bežične mreže Organizacije za zabranu kemijskog oružja (OPCW) u Nizozemskoj u travnju 2018. Kibernetički napad na Njemački savezni parlament bio je usmjeren na njegov informacijski sustav i nekoliko je dana utjecao na njegovo funkcioniranje. Ukradena je znatna količina podataka i zahvaćeni su računi e-pošte više zastupnika u Parlamentu, kao i račun e-pošte bivše kancelarke Angele Merkel. Slijedom agresivnog rata Rusije protiv Ukrajine GTsSS izvršio je kibernetičke napade (ciljani *phishing* i napadi s pomoću štetnog softvera) protiv Ukrajine.	22.10.2020.".