Rada
Európskej únie

V Bruseli 13. mája 2024
(OR. en)

8500/24

LIMITE

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

LEGISLATÍVNE AKTY A INÉ PRÁVNE AKTY

Predmet:	ROZHODNUTIE RADY, ktorým sa mení rozhodnutie (SZBP) 2019/797 o reštriktívnych opatreniach proti kybernetickým útokom ohrozujúcim Úniu alebo jej členské štáty

ROZHODNUTIE RADY (SZBP) 2024/…

z ...,

ktorým sa mení rozhodnutie (SZBP) 2019/797 o reštriktívnych opatreniach proti kybernetickým útokom ohrozujúcim Úniu alebo jej členské štáty

RADA EURÓPSKEJ ÚNIE,

so zreteľom na Zmluvu o Európskej únii, a najmä jej článok 29,

so zreteľom na návrh vysokého predstaviteľa Únie pre zahraničné veci a bezpečnostnú politiku,

keďže:

(1) Rada 17. mája 2019 prijala rozhodnutie (SZBP) 2019/797[1].

(2) Rozhodnutie (SZBP) 2019/797 sa uplatňuje do 18. mája 2025. Na základe preskúmania uvedeného rozhodnutia by sa platnosť reštriktívnych opatrení, ktoré sú v ňom stanovené, mala predĺžiť do tohto dátumu.

(3) Vzhľadom na pokračujúce a rastúce škodlivé správanie v kybernetickom priestore vrátane správania namiereného proti tretím štátom by sa malo aktualizovať odôvodnenie zaradenia šiestich osôb a dvoch subjektov na zoznam fyzických a právnických osôb, subjektov a orgánov, na ktoré sa vzťahujú reštriktívne opatrenia, uvedený v prílohe k rozhodnutiu (SZBP) 2019/797.

(4) Rozhodnutie (SZBP) 2019/797 by sa preto malo zodpovedajúcim spôsobom zmeniť,

PRIJALA TOTO ROZHODNUTIE:

[1] Rozhodnutie Rady (SZBP) 2019/797 zo 17. mája 2019 o reštriktívnych opatreniach proti kybernetickým útokom ohrozujúcim Úniu alebo jej členské štáty (Ú. v. EÚ L 129I, 17.5.2019, s. 13).

Článok 1

Rozhodnutie (SZBP) 2019/797 sa mení takto:

1. Článok 10 sa nahrádza takto:

„*Článok 10*

Toto rozhodnutie sa uplatňuje do 18. mája 2025 a pravidelne sa preskúmava.“;

2. Príloha sa mení v súlade s prílohou k tomuto rozhodnutiu.

Článok 2

Toto rozhodnutie nadobúda účinnosť dňom nasledujúcim po jeho uverejnení v *Úradnom vestníku Európskej únie*.

V ...

Za Radu
predseda/predsedníčka

PRÍLOHA

Príloha k rozhodnutiu (SZBP) 2019/797 („Zoznam fyzických a právnických osôb, subjektov a orgánov podľa článkov 4 a 5“) sa mení takto:

1. V zozname s nadpisom „A. Fyzické osoby“, sa záznamy 3 až 8 nahrádzajú takto:

	Meno a priezvisko	Informácie o totožnosti	Odôvodnenie	Dátum zaradenia do zoznamu
„3.	Alexey Valeryevich MININ	Алексей Валерьевич МИНИН Dátum narodenia: 27.5.1972 Miesto narodenia: Permská oblasť, RSFSR (v súčasnosti Ruská federácia) Číslo cestovného pasu: 120017582 Vydaný: Ministerstvom zahraničných vecí Ruskej federácie Platnosť: od 17.4. 2017 do 17.4.2022 Miesto: Moskva, Ruská federácia Štátna príslušnosť: ruská Pohlavie: muž	Alexej Minin (Alexey Minin) sa podieľal na pokuse o kybernetický útok s potenciálne závažným vplyvom proti Organizácii pre zákaz chemických zbraní (OPCW) v Holandsku a na kybernetických útokoch so závažným vplyvom proti tretím štátom. Ako príslušník na podporu spravodajstva z ľudských zdrojov na Hlavnom riaditeľstve Generálneho štábu Ozbrojených síl Ruskej federácie (GU/GRU) bol Alexej Minin členom tímu štyroch príslušníkov ruskej vojenskej spravodajskej služby, ktorí sa v apríli 2018 pokúsili o neoprávnený prístup do siete wi-fi OPCW v holandskom Haagu. Tento pokus o kybernetický útok bol zameraný na nabúranie siete wi-fi OPCW, ktoré by v prípade úspechu ohrozilo bezpečnosť siete a prebiehajúce vyšetrovanie OPCW. Holandská Obranná spravodajská a bezpečnostná služba (Militaire Inlichtingen- en Veiligheidsdienst) pokus o kybernetický útok narušila, a tak zabránila spôsobeniu závažnej ujmy OPCW. Veľká porota Západného dištriktu štátu Pensylvánia (Spojené štáty americké) obvinila Alexeja Minina ako príslušníka ruského hlavného riaditeľstva spravodajskej služby (GRU) z hackerstva, podvodu prostredníctvom elektronickej komunikácie, krádeže totožnosti s priťažujúcimi okolnosťami a prania špinavých peňazí.	30.7.2020

	Meno a priezvisko	Informácie o totožnosti	Odôvodnenie	Dátum zaradenia do zoznamu
4.	Aleksei Sergeyvich MORENETS	Алексей Сергеевич МОРЕНЕЦ Dátum narodenia: 31.7.1977 Miesto narodenia: Murmanská oblasť, RSFSR (v súčasnosti Ruská federácia) Číslo cestovného pasu: 100135556 Vydaný: Ministerstvom zahraničných vecí Ruskej federácie Platnosť: od 17.4.2017 do 17.4.2022 Miesto: Moskva, Ruská federácia Štátna príslušnosť: ruská Pohlavie: muž	Alexej Morenec (Aleksei Morenets) sa podieľal na pokuse o kybernetický útok s potenciálne závažným vplyvom proti Organizácii pre zákaz chemických zbraní (OPCW) v Holandsku a na kybernetických útokoch so závažným vplyvom proti tretím štátom. Ako kybernetický operátor Hlavného riaditeľstva Generálneho štábu Ozbrojených síl Ruskej federácie (GU/GRU) bol Alexej Morenec členom tímu štyroch príslušníkov ruskej vojenskej spravodajskej služby, ktorí sa v apríli 2018 pokúsili o neoprávnený prístup do siete wi-fi OPCW v holandskom Haagu. Tento pokus o kybernetický útok bol zameraný na nabúranie siete wi-fi OPCW, ktoré by v prípade úspechu ohrozilo bezpečnosť siete a prebiehajúce vyšetrovanie OPCW. Holandská Obranná spravodajská a bezpečnostná služba (Militaire Inlichtingen- en Veiligheidsdienst) pokus o kybernetický útok narušila, a tak zabránila spôsobeniu závažnej ujmy OPCW. Veľká porota Západného dištriktu štátu Pensylvánia (Spojené štáty americké) obvinila Alexeja Morenca, prideleného k vojenskej jednotke 26165, z hackerstva, podvodu prostredníctvom elektronickej komunikácie, krádeže totožnosti s priťažujúcimi okolnosťami a prania špinavých peňazí.	30.7.2020

	Meno a priezvisko	Informácie o totožnosti	Odôvodnenie	Dátum zaradenia do zoznamu
5.	Evgenii Mikhaylovich SEREBRIAKOV	Евгений Михайлович СЕРЕБРЯКОВ Dátum narodenia: 26.7.1981 Miesto narodenia: Kursk, RSFSR (v súčasnosti Ruská federácia) Číslo cestovného pasu: 100135555 Vydaný: Ministerstvom zahraničných vecí Ruskej federácie Platnosť: od 17.4. 2017 do 17.4.2022 Miesto: Moskva, Ruská federácia Štátna príslušnosť: ruská Pohlavie: muž	Jevgenij Serebriakov (Evgenii Serebriakov) sa podieľal na pokuse o kybernetický útok s potenciálne závažným vplyvom proti Organizácii pre zákaz chemických zbraní (OPCW) v Holandsku a na kybernetických útokoch so závažným vplyvom proti tretím štátom. Ako kybernetický operátor Hlavného riaditeľstva Generálneho štábu Ozbrojených síl Ruskej federácie (GU/GRU) bol Jevgenij Serebriakov členom tímu štyroch príslušníkov ruskej vojenskej spravodajskej služby, ktorí sa v apríli 2018 pokúsili o neoprávnený prístup do siete wi-fi OPCW v holandskom Haagu. Tento pokus o kybernetický útok bol zameraný na nabúranie siete wi-fi OPCW, ktoré by v prípade úspechu ohrozilo bezpečnosť siete a prebiehajúce vyšetrovanie OPCW. Holandská Obranná spravodajská a bezpečnostná služba (Militaire Inlichtingen- en Veiligheidsdienst) pokus o kybernetický útok narušila, a tak zabránila spôsobeniu závažnej ujmy OPCW. Od jari 2022 vedie Jevgenij Serebriakov aktérsku a hackerskú skupinu „Sandworm“ (alias „Sandworm Team“, „BlackEnergy Group“, „Voodoo Bear“, „Quedagh“, „Olympic Destroyer“ a „Telebots“), pridruženú k jednotke 74455 ruského hlavného riaditeľstva spravodajskej služby. Sandworm podniká od začiatku ruskej útočnej vojny proti Ukrajine kybernetické útoky proti Ukrajine, a to aj proti ukrajinským orgánom štátnej správy.	30.7.2020

	Meno a priezvisko	Informácie o totožnosti	Odôvodnenie	Dátum zaradenia do zoznamu
6.	Oleg Mikhaylovich SOTNIKOV	Олег Михайлович СОТНИКОВ Dátum narodenia: 24.8.1972 Miesto narodenia: Ulianovsk, RSFSR (v súčasnosti Ruská federácia) Číslo cestovného pasu: 120018866 Vydaný: Ministerstvom zahraničných vecí Ruskej federácie Platnosť: od 17.4.2017 do 17.4.2022 Miesto: Moskva, Ruská federácia Štátna príslušnosť: ruská Pohlavie: muž	Oleg Sotnikov sa podieľal na pokuse o kybernetický útok s potenciálne závažným vplyvom proti Organizácii pre zákaz chemických zbraní (OPCW) v Holandsku a na kybernetických útokoch so závažným vplyvom proti tretím štátom. Ako príslušník na podporu spravodajstva z ľudských zdrojov na Hlavnom riaditeľstve Generálneho štábu Ozbrojených síl Ruskej federácie (GU/GRU) bol Oleg Sotnikov členom tímu štyroch príslušníkov ruskej vojenskej spravodajskej služby, ktorí sa v apríli 2018 pokúsili o neoprávnený prístup do siete wi-fi OPCW v holandskom Haagu. Tento pokus o kybernetický útok bol zameraný na nabúranie siete wi-fi OPCW, ktoré by v prípade úspechu ohrozilo bezpečnosť siete a prebiehajúce vyšetrovanie OPCW. Holandská Obranná spravodajská a bezpečnostná služba (Militaire Inlichtingen- en Veiligheidsdienst) pokus o kybernetický útok narušila, a tak zabránila spôsobeniu závažnej ujmy OPCW. Veľká porota Západného dištriktu štátu Pensylvánia obvinila Olega Sotnikova ako príslušníka ruského hlavného riaditeľstva spravodajskej služby (GRU) z hackerstva, podvodu prostredníctvom elektronickej komunikácie, krádeže totožnosti s priťažujúcimi okolnosťami a prania špinavých peňazí.	30.7.2020

	Meno a priezvisko	Informácie o totožnosti	Odôvodnenie	Dátum zaradenia do zoznamu
7.	Dmitry Sergeyevich BADIN	Дмитрий Сергеевич БАДИН Dátum narodenia: 15.11.1990 Miesto narodenia: Kursk, RSFSR (v súčasnosti Ruská federácia) Štátna príslušnosť: ruská Pohlavie: muž	Dmitrij Badin (Dmitry Badin) sa podieľal na kybernetickom útoku so závažným vplyvom proti nemeckému spolkovému snemu (Deutscher Bundestag) a na kybernetických útokoch so závažným vplyvom proti tretím štátom. Ako vojenský spravodajský dôstojník 85. hlavného centra pre špeciálne služby (GCSS) Hlavného riaditeľstva Generálneho štábu Ozbrojených síl Ruskej federácie (GU/GRU) bol Dmitrij Badin členom tímu príslušníkov ruskej vojenskej spravodajskej služby, ktorí v apríli a máji 2015 podnikli kybernetický útok proti nemeckému spolkovému snemu. Tento kybernetický útok sa zameral na informačný systém snemu a na niekoľko dní narušil jeho prevádzku. Odcudzil sa pri ňom výrazný objem údajov a boli zasiahnuté e-mailové účty niekoľkých poslancov, ako aj bývalej kancelárky Angely Merkelovej. Veľká porota Západného dištriktu štátu Pensylvánia (Spojené štáty americké) obvinila Dmitrija Badina, prideleného k vojenskej jednotke 26165, z hackerstva, podvodu prostredníctvom elektronickej komunikácie, krádeže totožnosti s priťažujúcimi okolnosťami a prania špinavých peňazí.	22.10.2020

	Meno a priezvisko	Informácie o totožnosti	Odôvodnenie	Dátum zaradenia do zoznamu
8.	Igor Olegovich KOSTYUKOV	Игорь Олегович КОСТЮКОВ Dátum narodenia: 21.2.1961 Štátna príslušnosť: ruská Pohlavie: muž	Igor Kosťukov (Igor Kostyukov) je aktuálnym náčelníkom Hlavného riaditeľstva Generálneho štábu Ozbrojených síl Ruskej federácie (GU/GRU), kde predtým pôsobil ako prvý námestník. K jednotkám pod jeho velením patrí aj 85. hlavné centrum pre špeciálne služby (GCSS) (alias „vojenská jednotka 26165“, „APT28“, „Fancy Bear“, „Sofacy Group“, „Pawn Storm“ a „Strontium“). V tejto funkcii zodpovedá Igor Kosťukov za kybernetické útoky GCSS vrátane útokov so závažným vplyvom, ktoré predstavujú vonkajšiu hrozbu pre Úniu alebo jej členské štáty. Vojenskí spravodajskí dôstojníci 85. hlavného centra pre špeciálne služby (GCSS) sa konkrétne podieľali na kybernetickom útoku proti nemeckému spolkovému snemu (Deutscher Bundestag), v apríli a máji 2015, a na pokuse o kybernetický útok v apríli 2018, ktorý mal za cieľ nabúranie siete wi-fi Organizácie pre zákaz chemických zbraní (OPCW) v Holandsku. Kybernetický útok proti nemeckému spolkovému snemu sa zameral na informačný systém snemu a na niekoľko dní narušil jeho prevádzku. Odcudzil sa pri ňom výrazný objem údajov a boli zasiahnuté e-mailové účty niekoľkých poslancov, ako aj bývalej kancelárky Angely Merkelovej.	22.10.2020“;

2. V zozname s nadpisom „B) Právnické osoby, subjekty a orgány“ sa záznamy 3 a 4 nahrádzajú takto:

	Názov	Informácie o totožnosti	Odôvodnenie	Dátum zaradenia do zoznamu
„3.	Hlavné stredisko pre špeciálne technológie (GCST) Hlavného riaditeľstva Generálneho štábu ozbrojených síl Ruskej federácie (GU/GRU)	Adresa: 22 Kirova Street, Moscow, Russian Federation	Hlavné stredisko pre špeciálne technológie (GCST) Hlavného riaditeľstva Generálneho štábu Ozbrojených síl Ruskej federácie (GU/GRU), označované tiež ako 74455 podľa svojho poštového smerovacieho čísla, sa podieľa na kybernetických útokoch so závažným vplyvom a pôvodom mimo Únie, ktoré predstavujú vonkajšiu hrozbu pre Úniu alebo jej členské štáty, a kybernetických útokoch so závažným vplyvom proti tretím štátom, a to vrátane kybernetických útokov verejne známych ako „NotPetya“ alebo „EternalPetya“ v júni 2017 a kybernetických útokov zameraných na ukrajinskú energetickú sieť v zime 2015 a 2016. Útoky „NotPetya“ a „EternalPetya“ spôsobili neprístupnosť údajov vo viacerých spoločnostiach v Únii, inde v Európe a vo svete prostredníctvom ransomvéru a zablokovania prístupu k údajom, čo viedlo k značným hospodárskym stratám. Kybernetické útoky na ukrajinskú energetickú sieť viedli k čiastočným výpadkom siete počas zimy.	30.7.2020

	Názov	Informácie o totožnosti	Odôvodnenie	Dátum zaradenia do zoznamu
			Útok „NotPetya“ alebo „EternalPetya“ uskutočnil aktér, ktorý je verejne známy ako „Sandworm“ (alias „Sandworm Team“, „BlackEnergy Group“, „Voodoo Bear“, „Quedagh“, „Olympic Destroyer“ a „Telebots“) a stojí aj za útokom na ukrajinskú energetickú sieť. Sandworm podniká od začiatku ruskej útočnej vojny proti Ukrajine kybernetické útoky proti Ukrajine, a to aj proti ukrajinským orgánom štátnej správy a ukrajinskej kritickej infraštruktúre. K týmto kybernetickým útokom patria spearphishingové kampane, malvérové a ransomvérové útoky. Hlavné stredisko pre špeciálne technológie Hlavného riaditeľstva Generálneho štábu Ozbrojených síl Ruskej federácie zohráva aktívnu úlohu pri kybernetických aktivitách skupiny Sandworm a možno konštatovať prepojenie naň.	

	Názov	Informácie o totožnosti	Odôvodnenie	Dátum zaradenia do zoznamu
4.	85. hlavné centrum pre špeciálne služby (GCSS) Hlavného riaditeľstva Generálneho štábu ozbrojených síl Ruskej federácie (GU/GRU)	Adresa: Komsomol'skiy Prospekt, 20, Moscow, 119146, Russian Federation	85. hlavné centrum pre špeciálne služby (GCSS) Hlavného riaditeľstva Generálneho štábu Ozbrojených síl Ruskej federácie (GU/GRU) (alias „vojenská jednotka 26165“, „APT28“, „Fancy Bear“, „Sofacy Group“, „Pawn Storm“ a „Strontium“) sa podieľa na kybernetických útokoch so závažným vplyvom, ktoré predstavujú vonkajšiu hrozbu pre Úniu alebo jej členské štáty, a kybernetických útokoch so závažným vplyvom proti tretím štátom. Vojenskí spravodajskí dôstojníci 85. hlavného centra pre špeciálne služby (GCSS) sa konkrétne podieľali na kybernetickom útoku proti nemeckému spolkovému snemu (Deutscher Bundestag), v apríli a máji 2015, a na pokuse o kybernetický útok v apríli 2018, ktorý mal za cieľ nabúranie siete wi-fi Organizácie pre zákaz chemických zbraní (OPCW) v Holandsku. Kybernetický útok proti nemeckému spolkovému snemu sa zameral na informačný systém snemu a na niekoľko dní narušil jeho prevádzku. Odcudzil sa pri ňom výrazný objem údajov a boli zasiahnuté e-mailové účty niekoľkých poslancov, ako aj bývalej kancelárky Angely Merkelovej. Od začiatku ruskej útočnej vojny proti Ukrajine podniká GCSS proti Ukrajine kybernetické (spearphishingové a malvérové) útoky.	22.10.2020“.