Europos Sąjungos
Taryba

Briuselis, 2024 m. gegužės 13 d.
(OR. en)

8502/24

LIMITE

CORLX 356
CFSP/PESC 512
RELEX 467
CYBER 110
JAI 572
FIN 341

TEISĖS AKTAI IR KITI DOKUMENTAI

Dalykas:	TARYBOS ĮGYVENDINIMO REGLAMENTAS, kuriuo įgyvendinamas Reglamentas (ES) 2019/796 dėl ribojamųjų priemonių, skirtų kovai su kibernetiniais išpuoliais, keliančiais grėsmę Sąjungai arba jos valstybėms narėms

TARYBOS ĮGYVENDINIMO REGLAMENTAS (ES) 2024/…

… m. … … d.

kuriuo įgyvendinamas Reglamentas (ES) 2019/796 dėl ribojamųjų priemonių, skirtų kovai su kibernetiniais išpuoliais, keliančiais grėsmę Sąjungai arba jos valstybėms narėms

EUROPOS SĄJUNGOS TARYBA,

atsižvelgdama į Sutartį dėl Europos Sąjungos veikimo,

atsižvelgdama į 2019 m. gegužės 17 d. Tarybos reglamentą (ES) 2019/796 dėl ribojamųjų priemonių, skirtų kovai su kibernetiniais išpuoliais, keliančiais grėsmę Sąjungai arba jos valstybėms narėms[1], ypač į jo 13 straipsnio 1 dalį,

atsižvelgdama į Sąjungos vyriausiojo įgaliotinio užsienio reikalams ir saugumo politikai pasiūlymą,

[1] OL L 129I, 2019 5 17, p. 1.

kadangi:

(1) 2019 m. gegužės 17 d. Taryba priėmė Reglamentą (ES) 2019/796;

(2) atsižvelgiant į tebesitęsiantį ir aktyvėjantį piktavališką elgesį kibernetinėje erdvėje, įskaitant prieš trečiąsias valstybes nukreiptą elgesį, turėtų būti atnaujintos šešių asmenų ir dviejų subjektų įtraukimo į Reglamento (ES) 2019/796 I priede išdėstytą fizinių ir juridinių asmenų, subjektų ir organizacijų, kuriems taikomos ribojamosios priemonės, sąrašą priežastys;

(3) todėl Reglamento (ES) 2019/796 I priedas turėtų būti atitinkamai iš dalies pakeistas,

PRIĖMĖ ŠĮ REGLAMENTĄ:

1 straipsnis

Reglamento (ES) 2019/796 I priedas iš dalies keičiamas pagal šio reglamento priedą.

2 straipsnis

Šis reglamentas įsigalioja kitą dieną po jo paskelbimo *Europos Sąjungos oficialiajame leidinyje*.

Šis reglamentas privalomas visas ir tiesiogiai taikomas visose valstybėse narėse.

Priimta … …

Tarybos vardu
Pirmininkas / Pirmininkė

PRIEDAS

Reglamento (ES) 2019/796 I priedas („3 straipsnyje nurodytų fizinių ir juridinių asmenų, subjektų ir organizacijų sąrašas“) iš dalies keičiamas taip:

1) sąrašo su antrašte „A. Fiziniai asmenys“ 3–8 įrašai pakeičiami taip:

	Vardas, pavardė	Identifikuojamoji informacija	Įtraukimo į sąrašą priežastys	Įtraukimo į sąrašą data
„3.	Alexey Valeryevich MININ	Алексей Валерьевич МИНИН Gimimo data: 1972 5 27 Gimimo vieta: Permės sritis (Perm Oblast), Rusijos TFSR (dabar – Rusijos Federacija) Paso Nr.: 120017582 Išduotas: Rusijos Federacijos užsienio reikalų ministerijos Galioja: nuo 2017 4 17 iki 2022 4 17 Vieta: Maskva, Rusijos Federacija Pilietybė: Rusijos Lytis: vyras	Alexey Minin dalyvavo mėginant įvykdyti kibernetinį išpuolį, kuris galėjo padaryti didelį poveikį, prieš Cheminio ginklo uždraudimo organizaciją (OPCW) Nyderlanduose ir vykdant kibernetinius išpuolius, darančius didelį poveikį trečiosioms valstybėms. Rusijos Federacijos ginkluotųjų pajėgų generalinio štabo vyriausiosios valdybos (GU/GRU) žmonių žvalgybinės paramos pareigūnas Alexey Minin buvo keturių Rusijos karinės žvalgybos pareigūnų grupės, kuri 2018 m. balandžio mėn. mėgino įgyti neteisėtą prieigą prie OPCW Hagoje (Nyderlandai) belaidžio tinklo, narys. Mėginant įvykdyti kibernetinį išpuolį buvo siekiama įsilaužti į OPCW belaidį tinklą; jei šis mėginimas būtų buvęs sėkmingai įvykdytas, būtų kilusi grėsmė tinklo saugumui ir OPCW vykdomam tiriamajam darbui. Nyderlandų gynybos žvalgybos ir saugumo tarnyba (*Militaire Inlichtingen- en Veiligheidsdienst*) sužlugdė šį mėginimą įvykdyti kibernetinį išpuolį ir taip užkirto kelią galimybei padaryti didelę žalą OPCW. Pensilvanijos Vakarų apygardos (Jungtinės Amerikos Valstijos) didžioji žiuri yra pareiškusi Rusijos vyriausiosios žvalgybos valdybos (GRU) pareigūnui Alexey Minin kaltinimus dėl kompiuterinio įsilaužimo, sukčiavimo naudojantis ryšio priemonėmis, tapatybės vagystės sunkinančiomis aplinkybėmis ir pinigų plovimo.	2020 7 30

	Vardas, pavardė	Identifikuojamoji informacija	Įtraukimo į sąrašą priežastys	Įtraukimo į sąrašą data
4.	Aleksei Sergeyvich MORENETS	Алексей Сергеевич МОРЕНЕЦ Gimimo data: 1977 7 31 Gimimo vieta: Murmansko sritis (Murmanskaya Oblast), Rusijos TFSR (dabar – Rusijos Federacija) Paso Nr.: 100135556 Išduotas: Rusijos Federacijos užsienio reikalų ministerijos Galioja: nuo 2017 4 17 iki 2022 4 17 Vieta: Maskva, Rusijos Federacija Pilietybė: Rusijos Lytis: vyras	Aleksei Morenets dalyvavo mėginant įvykdyti kibernetinį išpuolį, kuris galėjo padaryti didelį poveikį, prieš Cheminio ginklo uždraudimo organizaciją (OPCW) Nyderlanduose ir vykdant kibernetinius išpuolius, darančius didelį poveikį trečiosioms valstybėms. Rusijos Federacijos ginkluotųjų pajėgų generalinio štabo vyriausiosios valdybos (GU/GRU) kibernetinės veiklos operatorius Aleksei Morenets buvo keturių Rusijos karinės žvalgybos pareigūnų grupės, kuri 2018 m. balandžio mėn. mėgino įgyti neteisėtą prieigą prie OPCW Hagoje (Nyderlandai) belaidžio tinklo, narys. Mėginant įvykdyti kibernetinį išpuolį buvo siekiama įsilaužti į OPCW belaidį tinklą; jei šis mėginimas būtų buvęs sėkmingai įvykdytas, būtų kilusi grėsmė tinklo saugumui ir OPCW vykdomam tiriamajam darbui. Nyderlandų gynybos žvalgybos ir saugumo tarnyba (*Militaire Inlichtingen- en Veiligheidsdienst*) sužlugdė šį mėginimą įvykdyti kibernetinį išpuolį ir taip užkirto kelią galimybei padaryti didelę žalą OPCW. Pensilvanijos Vakarų apygardos (Jungtinės Amerikos Valstijos) didžioji žiuri yra pareiškusi Aleksei Morenets, paskirtam į karinį dalinį 26165, kaltinimus dėl kompiuterinio įsilaužimo, sukčiavimo naudojantis ryšio priemonėmis, tapatybės vagystės sunkinančiomis aplinkybėmis ir pinigų plovimo.	2020 7 30

	Vardas, pavardė	Identifikuojamoji informacija	Įtraukimo į sąrašą priežastys	Įtraukimo į sąrašą data
5.	Evgenii Mikhaylovich SEREBRIAKOV	Евгений Михайлович СЕРЕБРЯКОВ Gimimo data: 1981 7 26 Gimimo vieta: Kurskas (Kursk), Rusijos TFSR (dabar – Rusijos Federacija) Paso Nr.: 100135555 Išduotas: Rusijos Federacijos užsienio reikalų ministerijos Galioja: nuo 2017 4 17 iki 2022 4 17 Vieta: Maskva, Rusijos Federacija Pilietybė: Rusijos Lytis: vyras	Evgenii Serebriakov dalyvavo mėginant įvykdyti kibernetinį išpuolį, kuris galėjo padaryti didelį poveikį, prieš Cheminio ginklo uždraudimo organizaciją (OPCW) Nyderlanduose ir vykdant kibernetinius išpuolius, darančius didelį poveikį trečiosioms valstybėms. Rusijos Federacijos ginkluotųjų pajėgų generalinio štabo vyriausiosios valdybos (GU/GRU) kibernetinės veiklos operatorius Evgenii Serebriakov buvo keturių Rusijos karinės žvalgybos pareigūnų grupės, kuri 2018 m. balandžio mėn. mėgino įgyti neteisėtą prieigą prie OPCW Hagoje (Nyderlandai) belaidžio tinklo, narys. Mėginant įvykdyti kibernetinį išpuolį buvo siekiama įsilaužti į OPCW belaidį tinklą; jei šis mėginimas būtų buvęs sėkmingai įvykdytas, būtų kilusi grėsmė tinklo saugumui ir OPCW vykdomam tiriamajam darbui. Nyderlandų gynybos žvalgybos ir saugumo tarnyba (*Militaire Inlichtingen- en Veiligheidsdienst*) sužlugdė šį mėginimą įvykdyti kibernetinį išpuolį ir taip užkirto kelią galimybei padaryti didelę žalą OPCW. Nuo 2022 m. pavasario Evgenii Serebriakov vadovauja subjektui ir įsilaužėlių grupei „Sandworm“ (dar žinomai kaip „Sandworm Team“, „BlackEnergy Group“, „Voodoo Bear“, „Quedagh“, „Olympic Destroyer“ ir „Telebots“), susijusiai su Rusijos vyriausiosios žvalgybos valdybos padaliniu 74455. Nuo Rusijos agresijos karo prieš Ukrainą pradžios „Sandworm“ vykdo kibernetinius išpuolius prieš Ukrainą, įskaitant Ukrainos vyriausybines agentūras.	2020 7 30

	Vardas, pavardė	Identifikuojamoji informacija	Įtraukimo į sąrašą priežastys	Įtraukimo į sąrašą data
6.	Oleg Mikhaylovich SOTNIKOV	Олег Михайлович СОТНИКОВ Gimimo data: 1972 8 24 Gimimo vieta: Uljanovskas (Ulyanovsk), Rusijos TFSR (dabar – Rusijos Federacija) Paso Nr.: 120018866 Išduotas: Rusijos Federacijos užsienio reikalų ministerijos Galioja: nuo 2017 4 17 iki 2022 4 17 Vieta: Maskva, Rusijos Federacija Pilietybė: Rusijos Lytis: vyras	Oleg Sotnikov dalyvavo mėginant įvykdyti kibernetinį išpuolį, kuris galėjo padaryti didelį poveikį, prieš Cheminio ginklo uždraudimo organizaciją (OPCW) Nyderlanduose ir vykdant kibernetinius išpuolius, darančius didelį poveikį trečiosioms valstybėms. Rusijos Federacijos ginkluotųjų pajėgų generalinio štabo vyriausiosios valdybos (GU/GRU) žmonių žvalgybinės paramos pareigūnas Oleg Sotnikov buvo keturių Rusijos karinės žvalgybos pareigūnų grupės, kuri 2018 m. balandžio mėn. mėgino įgyti neteisėtą prieigą prie OPCW Hagoje (Nyderlandai) belaidžio tinklo, narys. Mėginant įvykdyti kibernetinį išpuolį buvo siekiama įsilaužti į OPCW belaidį tinklą; jei šis mėginimas būtų buvęs sėkmingai įvykdytas, būtų kilusi grėsmė tinklo saugumui ir OPCW vykdomam tiriamajam darbui. Nyderlandų gynybos žvalgybos ir saugumo tarnyba (*Militaire Inlichtingen- en Veiligheidsdienst*) sužlugdė šį mėginimą įvykdyti kibernetinį išpuolį ir taip užkirto kelią galimybei padaryti didelę žalą OPCW. Pensilvanijos Vakarų apygardos didžioji žiuri yra pareiškusi Rusijos vyriausiosios žvalgybos valdybos (GRU) pareigūnui Oleg Sotnikov kaltinimus dėl kompiuterinio įsilaužimo, sukčiavimo naudojantis ryšio priemonėmis, tapatybės vagystės sunkinančiomis aplinkybėmis ir pinigų plovimo.	2020 7 30

	Vardas, pavardė	Identifikuojamoji informacija	Įtraukimo į sąrašą priežastys	Įtraukimo į sąrašą data
7.	Dmitry Sergeyevich BADIN	Дмитрий Сергеевич БАДИН Gimimo data: 1990 11 15 Gimimo vieta: Kurskas (Kursk), Rusijos TFSR (dabar – Rusijos Federacija) Pilietybė: Rusijos Lytis: vyras	Dmitry Badin dalyvavo vykdant didelį poveikį darantį kibernetinį išpuolį prieš Vokietijos Federalinį Parlamentą (*Deutscher Bundestag*) ir vykdant kibernetinius išpuolius, darančius didelį poveikį trečiosioms valstybėms. Rusijos Federacijos ginkluotųjų pajėgų generalinio štabo vyriausiosios valdybos (GU/GRU) 85-ojo pagrindinio specialiųjų tarnybų centro (GTsSS) karinės žvalgybos pareigūnas Dmitry Badin buvo Rusijos karinės žvalgybos pareigūnų grupės, kuri 2015 m. balandžio ir gegužės mėn. įvykdė kibernetinį išpuolį prieš Vokietijos Federalinį Parlamentą, narys. Tas kibernetinis išpuolis buvo nukreiptas prieš Parlamento informacinę sistemą ir sutrikdė jos veikimą keletui dienų. Buvo pavogta daug duomenų ir padarytas poveikis kelių parlamento narių bei buvusios kanclerės Angelos Merkel el. pašto paskyroms. Pensilvanijos Vakarų apygardos (Jungtinės Amerikos Valstijos) didžioji žiuri yra pareiškusi Dmitry Badin, paskirtam į karinį dalinį 26165, kaltinimus dėl kompiuterinio įsilaužimo, sukčiavimo naudojantis ryšio priemonėmis, tapatybės vagystės sunkinančiomis aplinkybėmis ir pinigų plovimo.	2020 10 22

	Vardas, pavardė	Identifikuojamoji informacija	Įtraukimo į sąrašą priežastys	Įtraukimo į sąrašą data
8.	Igor Olegovich KOSTYUKOV	Игорь Олегович КОСТЮКОВ Gimimo data: 1961 2 21 Pilietybė: Rusijos Lytis: vyras	Igor Kostyukov yra dabartinis Rusijos Federacijos ginkluotųjų pajėgų generalinio štabo vyriausiosios valdybos (GU/GRU) vadovas; anksčiau jis buvo šios valdybos vadovo pirmasis pavaduotojas. Vienas iš jam pavaldžių padalinių yra 85-asis pagrindinis specialiųjų tarnybų centras (GTsSS) (dar žinomas kaip Karinis dalinys 26165, „APT28“, „Fancy Bear“, „Sofacy Group“, „Pawn Storm“ ir „Strontium“). Eidamas šias pareigas Igor Kostyukov yra atsakingas už GTsSS įvykdytus kibernetinius išpuolius, įskaitant didelį poveikį darančius kibernetinius išpuolius, kurie kelia išorės grėsmę Sąjungai ar jos valstybėms narėms. Visų pirma, GTsSS karinės žvalgybos pareigūnai dalyvavo vykdant 2015 m. balandžio ir gegužės mėn. kibernetinį išpuolį prieš Vokietijos Federalinį Parlamentą (*Deutscher Bundestag*) ir 2018 m. balandžio mėn. Nyderlanduose mėginant įvykdyti kibernetinį išpuolį, kuriuo buvo siekiama įsilaužti į Cheminio ginklo uždraudimo organizacijos (OPCW) belaidį tinklą. Kibernetinis išpuolis prieš Vokietijos Federalinį Parlamentą buvo nukreiptas prieš Parlamento informacinę sistemą ir sutrikdė jos veikimą keletui dienų. Buvo pavogta daug duomenų ir padarytas poveikis kelių parlamento narių bei buvusios kanclerės Angelos Merkel el. pašto paskyroms.	2020 10 22;“

2) sąrašo su antrašte „B. Juridiniai asmenys, subjektai ir organizacijos“ 3 ir 4 įrašai pakeičiami taip:

	Pavadinimas	Identifikuojamoji informacija	Įtraukimo į sąrašą priežastys	Įtraukimo į sąrašą data
„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) (Rusijos Federacijos ginkluotųjų pajėgų generalinio štabo vyriausiosios valdybos (GU/GRU) pagrindinis specialiųjų technologijų centras (GTsST))	Adresas: 22 Kirova Street, Moscow, Russian Federation	Rusijos Federacijos ginkluotųjų pajėgų generalinio štabo vyriausiosios valdybos (GU/GRU) pagrindinis specialiųjų technologijų centras (GTsST), taip pat žinomas pagal vietos pašto numerį 74455, dalyvauja didelį poveikį darančiuose kibernetiniuose išpuoliuose, kurių kilmė – už Sąjungos ribų ir kurie kelia išorės grėsmę Sąjungai ar jos valstybėms narėms, taip pat kibernetiniuose išpuoliuose, darančiuose didelį poveikį trečiosioms valstybėms, įskaitant kibernetinius išpuolius, viešai žinomus kaip „NotPetya“ arba „EternalPetya“, įvykdytus 2017 m. birželio mėn., ir kibernetinius išpuolius prieš Ukrainos elektros tinklą, įvykdytus 2015–2016 m. žiemą. Dėl „NotPetya“ arba „EternalPetya“ ne vienoje bendrovėje, esančioje Sąjungoje, plačiau Europoje ir visame pasaulyje, duomenys tapo neprieinami, nes pasinaudojant išpirkos reikalavimo programine įranga buvo įsibrauta į kompiuterius ir užblokuota prieiga prie duomenų, ir dėl to, be kitų nuostolių, buvo sukelta didelių ekonominių nuostolių. Dėl kibernetinio išpuolio prieš Ukrainos elektros tinklą dalis tinklo buvo išjungta žiemos metu.	2020 7 30

	Pavadinimas	Identifikuojamoji informacija	Įtraukimo į sąrašą priežastys	Įtraukimo į sąrašą data
			Išpuolius „NotPetya“ arba „EternalPetya“ įvykdė subjektas, viešai žinomas kaip „Sandworm“ (dar žinomas kaip: „Sandworm Team“, „BlackEnergy Group“, „Voodoo Bear“, „Quedagh“, „Olympic Destroyer“ ir „Telebots“), kuris taip pat yra susijęs su išpuoliu prieš Ukrainos elektros tinklą. Nuo Rusijos agresijos karo prieš Ukrainą pradžios „Sandworm“ vykdo kibernetinius išpuolius prieš Ukrainą, įskaitant Ukrainos vyriausybines agentūras ir Ukrainos ypatingos svarbos infrastruktūrą. Tarp tų kibernetinių išpuolių – personalizuoto duomenų viliojimo kampanijos, išpuoliai naudojant kenkimo programinę įrangą ir išpirkos reikalavimo programinę įrangą. Rusijos Federacijos ginkluotųjų pajėgų generalinio štabo vyriausiosios valdybos pagrindinis specialiųjų technologijų centras atlieka aktyvų vaidmenį kibernetinėje veikloje, kurią vykdo „Sandworm“, ir gali būti siejamas su „Sandworm“.	

	Pavadinimas	Identifikuojamoji informacija	Įtraukimo į sąrašą priežastys	Įtraukimo į sąrašą data
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) (Rusijos Federacijos ginkluotųjų pajėgų generalinio štabo vyriausiosios valdybos (GU/GRU) 85-asis pagrindinis specialiųjų tarnybų centras (GTsSS))	Adresas: Komsomol'skiy Prospekt, 20, Moscow, 119146, Russian Federation	Rusijos Federacijos ginkluotųjų pajėgų generalinio štabo vyriausiosios valdybos (GU/GRU) 85-asis pagrindinis specialiųjų tarnybų centras (GTsSS) (dar žinomas kaip Karinis dalinys 26165, „APT28“, „Fancy Bear“, „Sofacy Group“, „Pawn Storm“ ir „Strontium“), dalyvauja vykdant didelį poveikį darančius kibernetinius išpuolius, kurie kelia išorės grėsmę Sąjungai ar jos valstybėms narėms, ir vykdant kibernetinius išpuolius, darančius didelį poveikį trečiosioms valstybėms. Visų pirma, GTsSS karinės žvalgybos pareigūnai dalyvavo vykdant 2015 m. balandžio ir gegužės mėn. kibernetinį išpuolį prieš Vokietijos Federalinį Parlamentą (*Deutscher Bundestag*) ir 2018 m. balandžio mėn. Nyderlanduose mėginant įvykdyti kibernetinį išpuolį, kuriuo buvo siekiama įsilaužti į Cheminio ginklo uždraudimo organizacijos (OPCW) belaidį tinklą. Kibernetinis išpuolis prieš Vokietijos Federalinį Parlamentą buvo nukreiptas prieš Parlamento informacinę sistemą ir sutrikdė jos veikimą keletui dienų. Buvo pavogta daug duomenų ir padarytas poveikis kelių parlamento narių bei buvusios kanclerės Angelos Merkel el. pašto paskyroms. Nuo Rusijos agresijos karo prieš Ukrainą pradžios GTsSS vykdo prieš Ukrainą nukreiptus kibernetinius išpuolius (personalizuoto duomenų viliojimo išpuolius ir išpuolius naudojant kenkimo programinę įrangą).	2020 10 22“.