TARYBOS SPRENDIMAS (BUSP) 2020/1127

2020 m. liepos 30 d.

kuriuo iš dalies keičiamas Sprendimas (BUSP) 2019/797 dėl ribojamųjų priemonių, skirtų kovai su Sąjungai ar jos valstybėms narėms gresiančiais kibernetiniais išpuoliais

EUROPOS SĄJUNGOS TARYBA,

atsižvelgdama į Europos Sąjungos sutartį, ypač į jos 29 straipsnį,

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

kadangi:

(1) 2019 m. gegužės 17 d. Taryba priėmė Sprendimą (BUSP) 2019/797 ([1]);

(2) tikslinės ribojamosios priemonės, nukreiptos prieš didelį poveikį turinčius kibernetinius išpuolius, kurie kelia išorės grėsmę Sąjungai ar jos valstybėms narėms, yra viena iš priemonių, įtrauktų į Sąjungos bendro diplomatinio atsako į kibernetinę kenkimo veiklą sistemą (Kibernetinio saugumo diplomatijos priemonių rinkinį) ir yra gyvybiškai svarbi priemonė siekiant atgrasyti nuo tokios veiklos ir į ją reaguoti. Ribojamosios priemonės taip pat gali būti taikomos reaguojant į kibernetinius išpuolius, turinčius didelį poveikį trečiosioms valstybėms ar tarptautinėms organizacijoms, kai manoma, kad tai būtina siekiant bendrų užsienio ir saugumo politikos tikslų, nustatytų atitinkamose Europos Sąjungos sutarties 21 straipsnio nuostatose;

(3) 2018 m. balandžio 16 d. Taryba priėmė išvadas, kuriose ji griežtai pasmerkė piktavališką informacinių ir ryšių technologijų (IRT), įskaitant „WannaCry“ ir „NotPetya“, padariusių didelę žalą ir ekonominių nuostolių Sąjungoje ir už jos ribų, naudojimą. 2018 m. spalio 4 d. Europos Vadovų Tarybos ir Europos Komisijos pirmininkai ir Sąjungos vyriausiasis įgaliotinis užsienio reikalams ir saugumo politikai (vyriausiasis įgaliotinis) bendrame pareiškime išreiškė didelį susirūpinimą dėl mėginimo įvykdyti kibernetinį išpuolį siekiant pakenkti Cheminio ginklo uždraudimo organizacijos (OPCW) Nyderlanduose vientisumui – tai buvo agresyvus aktas, demonstruojantis nepagarbą kilniam OPCW tikslui. Vyriausiasis įgaliotinis 2019 m. balandžio 12 d. deklaracijoje Sąjungos vardu paragino subjektus liautis vykdžius kibernetinę kenkimo veiklą, kuria siekiama pakenkti Sąjungos vientisumui, saugumui ir ekonominiam konkurencingumui, įskaitant intelektinės nuosavybės vagystes pasinaudojant kibernetine erdve. Tokios vagystės pasinaudojant kibernetine erdve apima vagystes, kurias vykdo subjektas, viešai žinomas kaip „APT10“ („Advanced Persistent Threat 10“);

(4) atsižvelgiant į tai ir siekiant užkirsti kelią besitęsiančiam ir aktyvėjančiam piktavališkam elgesiui kibernetinėje erdvėje, neskatinti jo, atgrasyti nuo jo ir reaguoti į jį, į Sprendimo (BUSP) 2019/797 priede pateiktą fizinių ir juridinių asmenų, subjektų ir organizacijų, kuriems taikomos ribojamosios priemonės, sąrašą turėtų būti įtraukti šeši fiziniai asmenys ir trys subjektai arba organizacijos. Tie asmenys arba subjektai yra atsakingi už kibernetinius išpuolius arba mėginimus įvykdyti kibernetinius išpuolius, įskaitant mėginimus įvykdyti kibernetinį išpuolį prieš OPCW, ir kibernetinius išpuolius, viešai žinomus kaip „WannaCry“ ir „NotPetya“, taip pat „Operation Cloud Hopper“, arba teikė paramą, dalyvavo ar sudarė palankias sąlygas juos vykdant;

(5) todėl Sprendimas (BUSP) 2019/797 turėtų būti atitinkamai iš dalies pakeistas,

PRIĖMĖ ŠĮ SPRENDIMĄ:

1 straipsnis

Sprendimo (BUSP) 2019/797 priedas iš dalies keičiamas taip, kaip išdėstyta šio sprendimo priede.

([1]) 2019 m. gegužės 17 d. Tarybos sprendimas (BUSP) 2019/797 dėl ribojamųjų priemonių, skirtų kovai su Sąjungai ar jos valstybėms narėms gresiančiais kibernetiniais išpuoliais (OL L 129 I, 2019 5 17, p. 13).

2 straipsnis

Šis sprendimas įsigalioja jo paskelbimo *Europos Sąjungos oficialiajame leidinyje* dieną.

Priimta Briuselyje 2020 m. liepos 30 d.

Tarybos vardu
Pirmininkas
M. ROTH

PRIEDAS

Į Sprendimo (BUSP) 2019/797 priede pateiktą fizinių ir juridinių asmenų, subjektų ir organizacijų sąrašą įtraukiami toliau nurodyti asmenys ir subjektai arba organizacijos:

„A. Fiziniai asmenys

	Vardas, pavardė	Identifikuojamoji informacija	Įtraukimo į sąrašą priežastys	Įtraukimo į sąrašą data
1.	GAO Qiang	Gimimo vieta: Shandong provincija, Kinija Adresas: Room 1102, Guanfu Mansion, 46 Xinkai Road, Hedong District, Tianjin, China Pilietybė: Kinijos Lytis: vyras	Gao Qiang dalyvauja vykdant operaciją „Operation Cloud Hopper“ – eilę kibernetinių išpuolių, kurie turi didelį poveikį, kurių kilmė – už Sąjungos ribų ir kurie kelia išorinę grėsmę Sąjungai ar jos valstybėms narėms, taip pat kibernetinių išpuolių, kurie turi didelį poveikį trečiosioms valstybėms. „Operation Cloud Hopper“ buvo nukreipta prieš tarptautinių bendrovių šešiuose žemynuose, įskaitant Sąjungoje esančias bendroves, informacines sistemas ir ją įvykdžius buvo įgyta neteisėta prieiga prie neskelbtinų komercinių duomenų ir dėl to buvo sukelta didelių ekonominių nuostolių. „Operation Cloud Hopper“ įvykdė subjektas, viešai žinomas kaip „APT10“ („Advanced Persistent Threat 10“) (*alias*: „Red Apollo“, CVNX, „Stone Panda“, „MenuPass“ ir „Potassium“). Gao Qiang gali būti susietas su APT10, įskaitant per jo sąsajas su APT10 valdymo ir kontrolės infrastruktūra. Be to, Gao Qiang buvo įdarbintas subjekte „Huaying Haitai“, kuris yra įtrauktas į sąrašą už paramos teikimą ir palankių sąlygų sudarymą vykdant „Operation Cloud Hopper“. Jis turi sąsajų su Zhang Shilong, kuris taip pat yra įtrauktas į sąrašą dėl sąsajų su „Operation Cloud Hopper“. Todėl Gao Qiang yra siejamas tiek su „Huaying Haitai“, tiek su Zhang Shilong.	2020 7 30
2.	ZHANG Shilong	Adresas: Hedong, Yuyang Road No 121, Tianjin, China Pilietybė: Kinijos Lytis: vyras	Zhang Shilong dalyvauja vykdant „Operation Cloud Hopper“ – eilę kibernetinių išpuolių, kurie turi didelį poveikį, kurių kilmė – už Sąjungos ribų ir kurie kelia išorinę grėsmę Sąjungai ar jos valstybėms narėms, taip pat kibernetinių išpuolių, kurie turi didelį poveikį trečiosioms valstybėms. „Operation Cloud Hopper“ buvo nukreipta prieš tarptautinių bendrovių šešiuose žemynuose, įskaitant Sąjungoje esančias bendroves, informacines sistemas ir ją įvykdžius buvo įgyta neteisėta prieiga prie neskelbtinų komercinių duomenų ir dėl to buvo sukelta didelių ekonominių nuostolių. „Operation Cloud Hopper“ įvykdė subjektas, viešai žinomas kaip „APT10“ („Advanced Persistent Threat 10“) (*alias*: „Red Apollo“, CVNX, „Stone Panda“, „MenuPass“ ir „Potassium“).	2020 7 30

			Zhang Shilong gali būti siejamas su APT10, be kita ko, dėl kenkimo programinės įrangos, kurią jis sukūrė ir testavo APT10 vykdytų kibernetinių išpuolių kontekste. Be to, Zhang Shilong buvo įdarbintas subjekte „Huaying Haitai“, kuris yra įtrauktas į sąrašą už paramos teikimą ir palankių sąlygų sudarymą vykdant „Operation Cloud Hopper“. Jis turi sąsajų su Gao Qiang, kuris taip pat yra įtrauktas į sąrašą dėl sąsajų su „Operation Cloud Hopper“. Todėl Zhang Shilong yra siejamas tiek su „Huaying Haitai“, tiek su Gao Qiang.	
3.	Alexey Valeryevich MININ	Алексей Валерьевич МИНИН Gimimo data: 1972 m. gegužės 27 d. Gimimo vieta: Permės apskritis, Rusijos TFSR (dabar – Rusijos Federacija) Paso Nr.: 120017582 Išduotas: Rusijos Federacijos užsienio reikalų ministerijos Galioja: nuo 2017 m. balandžio 17 d. iki 2022 m. balandžio 17 d. Vieta: Maskva, Rusijos Federacija Pilietybė: Rusijos Lytis: vyras	Alexey Minin dalyvavo mėginant įvykdyti kibernetinį išpuolį, kuris galėjo turėti didelį poveikį, prieš Cheminio ginklo uždraudimo organizaciją (OPCW) Nyderlanduose. 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. Jeigu šis mėginimas būtų buvęs sėkmingai įvykdytas, būtų kilusi grėsmė tinklo saugumui ir OPCW vykdomam tiriamajam darbui. Nyderlandų gynybos žvalgybos ir saugumo tarnyba (DISS) (*Militaire Inlichtingen- en Veiligheidsdienst* – MIVD) sužlugdė mėginimą įvykdyti kibernetinį išpuolį ir tokiu būdu užkirto kelią padaryti didelę žalą OPCW.	2020 7 30
4.	Aleksei Sergeyvich MORENETS	Алексей Сергеевич МОРЕНЕЦ Gimimo data: 1977 m. liepos 31 d. Gimimo vieta: Murmansko apskritis, Rusijos TFSR (dabar – Rusijos Federacija) Paso Nr.: 100135556 Išduotas: Rusijos Federacijos užsienio reikalų ministerijos Galioja: nuo 2017 m. balandžio 17 d. iki 2022 m. balandžio 17 d. Vieta: Maskva, Rusijos Federacija Pilietybė: Rusijos Lytis: vyras	Aleksei Morenets dalyvavo mėginant įvykdyti kibernetinį išpuolį, kuris galėjo turėti didelį poveikį, prieš Cheminio ginklo uždraudimo organizaciją (OPCW) Nyderlanduose. Rusijos Federacijos ginkluotųjų pajėgų generalinio štabo vyriausiosios valdybos (GU/GRU) kibernetinis 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. Jeigu šis mėginimas būtų buvęs sėkmingai įvykdytas, būtų kilusi grėsmė tinklo saugumui ir OPCW vykdomam tiriamajam darbui. Nyderlandų gynybos žvalgybos ir saugumo tarnyba (DISS) (*Militaire Inlichtingen- en Veiligheidsdienst* – MIVD) sužlugdė mėginimą įvykdyti kibernetinį išpuolį ir tokiu būdu užkirto kelią galimybei padaryti didelę žalą OPCW.	2020 7 30

5.	Evgenii Mikhaylovich SEREBRIAKOV	Евгений Михайлович СЕРЕБРЯКОВ Gimimo data: 1981 m. liepos 26 d. Gimimo vieta: Kurskas, Rusijos TFSR (dabar – Rusijos Federacija) Paso Nr.: 100135555 Išduotas: Rusijos Federacijos užsienio reikalų ministerijos Galioja: nuo 2017 m. balandžio 17 d. iki 2022 m. balandžio 17 d. Vieta: Maskva, Rusijos Federacija Pilietybė: Rusijos Lytis: vyras	Evgenii Serebriakov dalyvavo mėginant įvykdyti kibernetinį išpuolį, kuris galėjo turėti didelį poveikį, prieš Cheminio ginklo uždraudimo organizaciją (OPCW) Nyderlanduose. Rusijos Federacijos ginkluotųjų pajėgų generalinio štabo vyriausiosios valdybos (GU/GRU) kibernetinis 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. Jeigu šis mėginimas būtų buvęs sėkmingai įvykdytas, būtų kilusi grėsmė tinklo saugumui ir OPCW vykdomam tiriamajam darbui. Nyderlandų gynybos žvalgybos ir saugumo tarnyba (DISS) (*Militaire Inlichtingen- en Veiligheidsdienst* – MIVD) sužlugdė mėginimą įvykdyti kibernetinį išpuolį ir tokiu būdu užkirto kelią galimybei padaryti didelę žalą OPCW.	2020 7 30
6.	Oleg Mikhaylovich SOTNIKOV	Олег Михайлович СОТНИКОВ Gimimo data: 1972 m. rugpjūčio 24 d. Gimimo vieta: Uljanovskas, Rusijos TFSR (dabar – Rusijos Federacija) Paso Nr.: 120018866 Išduotas: Rusijos Federacijos užsienio reikalų ministerijos Galioja nuo 2017 m. balandžio 17 d. iki 2022 m. balandžio 17 d. Vieta: Maskva, Rusijos Federacija Pilietybė: Rusijos Lytis: vyras	Oleg Sotnikov dalyvavo mėginant įvykdyti kibernetinį išpuolį, kuris galėjo turėti didelį poveikį, prieš Cheminio ginklo uždraudimo organizaciją (OPCW) Nyderlanduose. 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. Jeigu šis mėginimas būtų buvęs sėkmingai įvykdytas, būtų kilusi grėsmė tinklo saugumui ir OPCW vykdomam tiriamajam darbui. Nyderlandų gynybos žvalgybos ir saugumo tarnyba (DISS) (*Militaire Inlichtingen- en Veiligheidsdienst* – MIVD) sužlugdė mėginimą įvykdyti kibernetinį išpuolį ir tokiu būdu užkirto kelią galimybei padaryti didelę žalą OPCW.	2020 7 30

B. Juridiniai asmenys, subjektai ir organizacijos

	Pavadinimas	Identifikuojamoji informacija	Įtraukimo į sąrašą priežastys	Įtraukimo į sąrašą data
1.	Tianjin Huaying Haitai Science and Technology Development Co. Ltd (Huaying Haitai)	*Alias*: Haitai Technology Development Co. Ltd Vieta: Tianjin, Kinija	„Huaying Haitai“ teikė finansinę, techninę arba materialinę paramą ir sudarė palankias sąlygas vykdant operaciją „Operation Cloud Hopper“ – eilę kibernetinių išpuolių, kurie turi didelį poveikį, kurių kilmė – už Sąjungos ribų ir kurie kelia išorinę grėsmę Sąjungai ar jos valstybėms narėms, taip pat kibernetinių išpuolių, kurie turi didelį poveikį trečiosioms valstybėms.	2020 7 30

			„Operation Cloud Hopper“ buvo nukreipta prieš tarptautinių bendrovių šešiuose žemynuose, įskaitant Sąjungoje esančias bendroves, informacines sistemas ir ją įvykdžius buvo įgyta neteisėta prieiga prie neskelbtinų komercinių duomenų ir dėl to buvo sukelta didelių ekonominių nuostolių. „Operation Cloud Hopper“ įvykdė subjektas, viešai žinomas kaip „APT10“ („Advanced Persistent Threat 10“) (*alias*: „Red Apollo“, CVNX, „Stone Panda“, „MenuPass“ ir „Potassium“). „Huaying Haitai“ gali būti siejamas su APT10. Be to, subjekte „Huaying Haitai“ buvo įdarbinti Gao Qiang ir Zhang Shilong, kurie abu yra įtraukti į sąrašą dėl sąsajų su „Operation Cloud Hopper“. Todėl „Huaying Haitai“ siejamas su Gao Qiang ir Zhang Shilong.	
2.	Chosun Expo	*Alias*: Chosen Expo; Korėjos eksporto bendroji įmonė Vieta: KLDR	„Chosun Expo“ teikė finansinę, techninę arba materialinę paramą ir sudarė palankias sąlygas vykdant eilę kibernetinių išpuolių, kurie turi didelį poveikį, kurių kilmė – už Sąjungos ribų ir kurie kelia išorinę grėsmę Sąjungai ar jos valstybėms narėms, taip pat kibernetinių išpuolių, kurie turi didelį poveikį trečiosioms valstybėms. Tarp šių kibernetinių išpuolių – išpuolis, viešai žinomas kaip „WannaCry“, ir kibernetiniai išpuoliai prieš Lenkijos finansų priežiūros instituciją ir „Sony Pictures Entertainment“, taip pat kibernetinė vagystė iš Bangladešo banko ir bandymas įvykdyti kibernetinę vagystę iš Vietnamo „Tien Phong“ banko. „WannaCry“ sutrikdė informacines sistemas visame pasaulyje, nes pasinaudojant išpirkos reikalavimo programine įranga buvo įsibrauta į informacines sistemas ir užblokuota prieiga prie duomenų. Šis kibernetinis išpuolis paveikė Sąjungoje esančių bendrovių informacines sistemas, be kita ko, informacines sistemas, susijusias su paslaugomis, kurios yra reikalingos esminėms paslaugoms ir ekonominei veiklai valstybėse narėse palaikyti. „WannaCry“ įvykdė subjektas, viešai žinomas kaip „APT38“ („Advanced persistent Threat 38“) arba „Lazarus Group“. „Chosun Expo“ gali būti siejama su APT38 ir „Lazarus Group“, be kita ko, dėl sąskaitų, naudotų vykdant kibernetinius išpuolius.	2020 7 30
3.	Rusijos Federacijos ginkluotųjų pajėgų generalinio štabo vyriausiosios valdybos (GU/GRU) pagrindinis specialiųjų technologijų centras (GTsST)	Adresas: Kirovo gatvė 22, Maskva, Rusijos Federacija	Rusijos Federacijos ginkluotųjų pajėgų generalinio štabo vyriausiosios valdybos (GU/GRU) pagrindinis specialiųjų technologijų centras (GTsST), taip pat žinomas pagal vietos pašto numerį 74455, yra atsakingas už kibernetinius išpuolius, kurie turi didelį poveikį, kurių kilmė – už Sąjungos ribų ir kurie kelia išorinę grėsmę Sąjungai ar jos valstybėms narėms, taip pat kibernetinius išpuolius, kurie turi 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.	2020 7 30“

			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. „NotPetya“ arba „EternalPetya“ įvykdė subjektas, viešai žinomas kaip „Sandworm“ (alias: „Sandworm Team“, „BlackEnergy Group“, „Voodoo Bear“, „Quedagh“, „Olympic Destroyer“ ir „Telebots“), kuris taip pat yra susijęs su išpuoliu prieš Ukrainos elektros tinklą. 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“.	