Šis tekstas yra skirtas tik informacijai ir teisinės galios neturi. Europos Sąjungos institucijos nėra teisiškai atsakingos už jo turinį. Autentiškos atitinkamų teisės aktų, įskaitant jų preambules, versijos skelbiamos Europos Sąjungos oficialiajame leidinyje ir pateikiamos svetainėje „EUR-Lex“. Oficialūs tekstai tiesiogiai prieinami naudojantis šiame dokumente pateikiamomis nuorodomis

►B

TARYBOS SPRENDIMAS (BUSP) 2019/797

2019 m. gegužės 17 d.

dėl ribojamųjų priemonių, skirtų kovai su Sąjungai ar jos valstybėms narėms gresiančiais kibernetiniais išpuoliais

(OL L 129I, 2019 5 17, p. 13)

iš dalies keičiamas:

		Oficialusis leidinys		
		Nr.	puslapis	data
►M1	2020 m. gegužės 14 d. Tarybos sprendimas (BUSP) 2020/651	L 153	4	2020 5 15
►M2	2020 m. liepos 30 d. Tarybos sprendimas (BUSP) 2020/1127	L 246	12	2020 7 30
►M3	2020 m. spalio 22 d. Tarybos sprendimas (BUSP) 2020/1537	L 351 I	5	2020 10 22
►M4	2020 m. lapkričio 20 d. Tarybos sprendimas (BUSP) 2020/1748	L 393	19	2020 11 23

pataisytas:

►C1 Klaidų ištaisymas, OL L 230, 2020 7 17, p. 36 (2019/797)

▼B

TARYBOS SPRENDIMAS (BUSP) 2019/797

2019 m. gegužės 17 d.

dėl ribojamųjų priemonių, skirtų kovai su Sąjungai ar jos valstybėms narėms gresiančiais kibernetiniais išpuoliais

1 straipsnis

1. Šis sprendimas taikomas reikšmingą poveikį darantiems kibernetiniams išpuoliams (įskaitant pasikėsinimus įvykdyti reikšmingą poveikį darančius kibernetinius išpuolius), dėl kurių kyla išorinė grėsmė Sąjungos arba jos valstybių narių saugumui.

2. Kibernetiniai išpuoliai, dėl kurių kyla išorinė grėsmė, apima išpuolius:

a) kurių kilmė arba vykdymo vieta yra už Sąjungos ribų;

b) kurių metu naudojamasi infrastruktūra už Sąjungos ribų;

c) kuriuos vykdo fizinis ar juridinis asmuo, subjektas ar įstaiga, įsteigti arba veikiantys už Sąjungos ribų;

d) 'kurie yra vykdomi remiant, vadovaujant arba kontroliuojant fiziniam ar juridiniam asmeniui, subjektui ar įstaigai, įsteigtiems arba veikiantiems už Sąjungos ribų.

3. Šiuo tikslu kibernetiniai išpuoliai – tai veiksmai, susiję su vienu ar keliais iš šių aspektų:

a) prieiga prie informacinių sistemų;

b) įsikišimu į informacinę sistemą;

c) įsikišimu į duomenis, arba

d) duomenų perėmimu,

kai tokie veiksmai vykdomi neturint tinkamo sistemos arba duomenų arba jų dalies savininko arba kitų teisių turėtojo leidimo arba nėra leidžiami pagal Sąjungos arba atitinkamos valstybės narės teisę.

4. Kibernetiniai išpuoliai, dėl kurių kyla grėsmė valstybėms narėms, apima išpuolius, kuriais daromas poveikis informacinėms sistemoms, susijusioms, be kita ko, su:

a) ypatingos svarbos infrastruktūros objektais, įskaitant jūrinius kabelius ir objektus, paleistus į kosminę erdvę, kurie yra būtini siekiant palaikyti itin svarbias visuomenės funkcijas arba žmonių sveikatai, saugai, saugumui ir ekonominei arba socialinei gerovei;

b) paslaugomis, kurios būtinos siekiant palaikyti itin svarbią socialinę ir (arba) ekonominę veiklą, visų pirma energetikos (elektros, naftos ir dujų), transporto (oro susisiekimo, geležinkelių, vandens ir sausumos

▼B

kelių), bankininkystės, finansų rinkų infrastruktūros, sveikatos (sveikatos priežiūros paslaugų, ligoninių ir privačių klinikų), geriamojo vandens tiekimo ir paskirstymo, skaitmeninės infrastruktūros sektoriuose ir kituose sektoriuose, kurie yra itin svarbūs atitinkamai valstybei narei;

c) ypatingos svarbos valstybės funkcijomis, visų pirma gynybos, valdymo ir institucijų veikimo srityse, įskaitant rinkimus arba balsavimo procesą, ekonominės ir civilinės infrastruktūros veikimą, vidaus saugumą ir išorės santykius, įskaitant palaikomus per diplomatines misijas;

d) įslaptintos informacijos saugojimu arba tvarkymu, arba

e) vyriausybės reagavimo į nelaimes tarnybomis.

5. Kibernetiniai išpuoliai, dėl kurių kyla grėsmė Sąjungai, apima išpuolius prieš jos institucijas, įstaigas, organus ir agentūras, jos delegacijas trečiosiose valstybėse arba tarptautinėse organizacijose, jos bendrosios saugumo ir gynybos politikos (BSGP) operacijas ir misijas ir jos specialiuosius įgaliotinius.

6. Jei tai laikoma reikalinga, kad būtų pasiekti BUSP tikslai, išdėstyti atitinkamose Europos Sąjungos sutarties 21 straipsnio nuostatose, šiuo sprendimu taip pat leidžiama ribojamąsias priemones taikyti reaguojant į kibernetinius išpuolius, darančius reikšmingą poveikį trečiosioms valstybėms ar tarptautinėms organizacijoms.

2 straipsnis

Šiame sprendime vartojamų terminų apibrėžtys:

a) informacinės sistemos – prietaisas arba tarpusavyje sujungtų ar susijusių prietaisų grupė, iš kurių vienas arba daugiau pagal programą vykdo automatinį skaitmeninių duomenų tvarkymą, taip pat skaitmeniniai duomenys, saugomi, tvarkomi, išrenkami arba perduodami to prietaiso ar grupės prietaisų jo ar jų eksploatacijos, naudojimo, apsaugos ir priežiūros tikslais;

b) įsikišimas į informacinę sistemą – kliudymas informacinės sistemos veikimui arba jo pertraukimas įvedant skaitmeninius duomenis, perduodant, sugadinant, ištrinant tokius duomenis, pakenkiant jiems, juos pakeičiant ar pašalinant arba padarant tokius duomenis neprieinamais; tai taip pat apima duomenų, lėšų, ekonominių išteklių ar intelektinės nuosavybės vagystę;

c) įsikišimas į duomenis – informacinėje sistemoje esančių skaitmeninių duomenų ištrynimas, sugadinimas, pakenkimas jiems, pakeitimas ar pašalinimas arba tokių duomenų padarymas neprieinamais;

d) duomenų perėmimas – į informacinę sistemą, iš jos ar joje ne viešai perduodamų skaitmeninių duomenų, įskaitant informacinės sistemos elektromagnetinę spinduliuotę, kuria perduodami tokie duomenys, perėmimas techninėmis priemonėmis.

▼B

3 straipsnis

Veiksniai, lemiantys, ar kibernetinis išpuolis daro 1 straipsnio 1 dalyje nurodytą reikšmingą poveikį, apima:

a) kibernetinio išpuolio mastą, intensyvumą,, poveikį arba juo padaryto ardomojo poveikio sunkumą, be kita ko, ekonominei ir visuomeninei veiklai, esminėms paslaugoms, esminėms valstybės funkcijoms, viešajai tvarkai ar visuomenės saugumui;

b) poveikį pajutusių fizinių ar juridinių asmenų, subjektų ar įstaigų skaičių;

c) susijusių valstybių narių skaičių;

d) padarytą ekonominę žalą, pavyzdžiui, didelio masto lėšų, ekonominių išteklių arba intelektinės nuosavybės vagyste;

e) vykdytojo gautą ekonominę naudą sau arba kitiems;

f) pavogtų duomenų kiekį arba pobūdį arba duomenų pažeidimų mastą, arba

g) komerciškai jautrių duomenų, prie kurių gauta prieiga, pobūdį.

4 straipsnis

1. Valstybės narės imasi būtinų priemonių, kad į jų teritorijas atvykti arba vykti per jas tranzitu negalėtų fiziniai asmenys:

a) atsakingi už kibernetinius išpuolius arba mėginimus įvykdyti kibernetinius išpuolius;

b) teikiantys finansinę, techninę ar materialinę paramą arba kitaip susiję su kibernetiniais išpuoliais arba pasikėsinimais įvykdyti kibernetinius išpuolius, įskaitant planavimą, rengimą, dalyvavimą, vadovavimą, pagalbos teikimą, skatinimą, sąlygų sudarymą, veiksmais arba neveikimu;

c) susiję su a ir b punktuose nurodytais fiziniais asmenimis.

2. 1 dalis neįpareigoja valstybių narių neleisti jų pačių piliečiams atvykti į jų teritorijas.

3. 1 dalis nedaro poveikio tiems atvejams, kai valstybė narė privalo laikytis įsipareigojimo pagal tarptautinę teisę, būtent:

a) kaip tarptautinės tarpvyriausybinės organizacijos priimančioji šalis;

b) kaip Jungtinių Tautų rengiamos ar globojamos tarptautinės konferencijos priimančioji šalis;

c) pagal daugiašalį susitarimą dėl privilegijų ir imunitetų suteikimo, arba

d) pagal 1929 m. Šventojo Sosto (Vatikano Miesto Valstybės) ir Italijos Taikinimo sutartį (Laterano paktą).

▼B

4. Laikoma, kad 3 dalis taikoma ir tais atvejais, kai valstybė narė yra Europos saugumo ir bendradarbiavimo organizacijos (ESBO) priimančioji šalis.

5. Taryba tinkamai informuojama apie visus atvejus, kai valstybė narė leidžia taikyti išimtį pagal 3 arba 4 dalį.

6. Valstybės narės gali leisti taikyti 1 dalyje nustatytų priemonių išimtis, kai kelionė yra pateisinama dėl skubaus humanitarinio poreikio arba dėl dalyvavimo tarpvyriausybiniuose susitikimuose arba susitikimuose, kuriuos remia ar kurių priimančioji šalis yra Sąjunga arba kurių priimančioji šalis yra ESBO pirmininkaujanti valstybė narė, kuriuose vyksta politinis dialogas, kuriuo tiesiogiai padedama siekti ribojamųjų priemonių politikos tikslų, įskaitant saugumą ir stabilumą kibernetinėje erdvėje.

7. Valstybės narės taip pat gali leisti taikyti pagal 1 dalį nustatytų priemonių išimtis, kai atvykimas ar vykimas tranzitu yra būtinas teisminio proceso vykdymui.

8. Valstybė narė, ketinanti leisti taikyti 6 arba 7 dalyje nurodytas išimtis, apie tai raštu praneša Tarybai. Laikoma, kad išimtį taikyti leidžiama, jeigu per dvi darbo dienas nuo pranešimo apie siūlomą išimtį gavimo vienas ar keli Tarybos nariai raštu nepareiškia prieštaravimo. Jei vienas ar keli Tarybos nariai pareiškia prieštaravimą, Taryba kvalifikuota balsų dauguma gali nuspręsti leisti taikyti siūlomą išimtį.

9. Tais atvejais, kai pagal 3, 4, 6, 7 ar 8 dalį valstybė narė leidžia priede išvardytiems asmenims atvykti į savo teritoriją arba vykti per ją tranzitu, leidimas galioja griežtai tik tuo tikslu, kuriam jis buvo suteiktas, ir tik tiems asmenims, kurių atžvilgiu jis tiesiogiai suteiktas.

5 straipsnis

1. Įšaldomos visos lėšos ir ekonominiai ištekliai, kurie priklauso, kuriuos nuosavybės teise turi, valdo ar kontroliuoja fiziniai ar juridiniai asmenys, subjektai arba organizacijos:

a) atsakingi už kibernetinius išpuolius arba mėginimus įvykdyti kibernetinius išpuolius;

b) teikiantys finansinę, techninę ar materialinę paramą arba kitaip susiję su kibernetiniais išpuoliais arba pasikėsinimais įvykdyti kibernetinius išpuolius, įskaitant planavimą, rengimą, dalyvavimą, vadovavimą, pagalbos teikimą, skatinimą, sąlygų sudarymą, veiksmais arba neveikimu;

c) susiję su a ir b punktuose nurodytais fiziniais ar juridiniais asmenimis, subjektais arba organizacijomis.

▼B

2. Priede išvardytiems fiziniams arba juridiniams asmenims, subjektams ar organizacijoms arba jų naudai nei tiesiogiai, nei netiesiogiai nesudaroma galimybė naudotis jokiomis lėšomis ar ekonominiais ištekliais.

3. Nukrypstant nuo 1 ir 2 dalių, valstybių narių kompetentingos institucijos gali leisti nutraukti tam tikrų lėšų arba ekonominių išteklių įšaldymą arba leisti jais naudotis tokiomis sąlygomis, kurios, jų nuomone, yra tinkamos, nustačiusios, kad atitinkamos lėšos ar ekonominiai ištekliai yra:

a) ►C1 reikalingi priede išvardytų fizinių ar juridinių asmenų, subjektų arba organizacijų ir nuo tokių fizinių asmenų priklausomų šeimos narių pagrindiniams poreikiams ◄, įskaitant mokėjimus už maisto produktus, nuomą arba hipoteką, vaistus ir medicininį gydymą, mokesčius, draudimo įmokas ir komunalines paslaugas, tenkinti;

b) skirti tik pagrįstiems profesiniams mokesčiams sumokėti ar patirtoms išlaidoms, susijusioms su teisinių paslaugų teikimu, kompensuoti;

c) skirti tik mokesčiams arba aptarnavimo mokesčiams už kasdienį įšaldytų lėšų arba ekonominių išteklių laikymą ar tvarkymą sumokėti;

d) reikalingi ypatingoms išlaidoms, jei atitinkama kompetentinga institucija kitų valstybių narių kompetentingoms institucijoms ir Komisijai bent prieš dvi savaites iki leidimo suteikimo yra pranešusi priežastis, dėl kurių, jos nuomone, konkretus leidimas turėtų būti suteiktas, arba

e) mokėtini į diplomatinės ar konsulinės atstovybės arba tarptautinės organizacijos, kuri pagal tarptautinę teisę naudojasi imunitetais, sąskaitą arba iš jos, tiek, kiek tie mokėjimai skirti naudoti oficialiais diplomatinės arba konsulinės atstovybės arba tarptautinės organizacijos tikslais.

Atitinkama valstybė narė informuoja kitas valstybes nares ir Komisiją apie bet kokius pagal šią dalį suteiktus leidimus.

4. Nukrypstant nuo 1 dalies, valstybių narių kompetentingos institucijos gali leisti nutraukti tam tikrų lėšų ar ekonominių išteklių įšaldymą, jei laikomasi šių sąlygų:

a) lėšoms ar ekonominiams ištekliams taikomas arbitražo sprendimas, priimtas prieš tą dieną, kurią 1 dalyje nurodytas fizinis ar juridinis asmuo, subjektas ar organizacija buvo įtraukti į priede pateiktą sąrašą, arba Sąjungoje priimtas teisminės institucijos ar administracinis sprendimas, arba atitinkamoje valstybėje narėje vykdytinas teisminės institucijos sprendimas, priimtas iki tos dienos arba po jos;

▼B

b) lėšos ar ekonominiai ištekliai bus naudojami tik reikalavimams, kurių vykdymas užtikrintas tokiu sprendimu arba kurie pripažinti teisėtais tokiu sprendimu, tenkinti, laikantis taikomais įstatymais ir kitais teisės aktais, kuriais reglamentuojamos tokius reikalavimus turinčių asmenų teisės, nustatytų ribų;

c) sprendimas nėra į priede pateiktą sąrašą įtraukto fizinio ar juridinio asmens, subjekto ar organizacijos naudai, ir

d) sprendimo pripažinimas neprieštarauja atitinkamos valstybės narės viešajai tvarkai.

Atitinkama valstybė narė informuoja kitas valstybes nares ir Komisiją apie bet kokius pagal šią dalį suteiktus leidimus.

5. 1 dalis nekliudo tam, kad į priede pateiktą sąrašą įtrauktas fizinis ar juridinis asmuo, subjektas ar organizacija sumokėtų mokėtiną sumą pagal sutartį, sudarytą iki to fizinio ar juridinio asmens, subjekto ar organizacijos įtraukimo į tą sąrašą, jei atitinkama valstybė narė nustatė, kad mokėjimo tiesiogiai ar netiesiogiai negauna 1 dalyje nurodytas fizinis ar juridinis asmuo, subjektas ar organizacija.

6. 2 dalis netaikoma, kai įšaldytos sąskaitos papildomos:

a) palūkanomis arba kitomis dėl šių sąskaitų atsirandančiomis pajamomis;

b) mokėjimais pagal sutartis, susitarimus ar prievoles, kurios buvo sudarytos arba nustatyti anksčiau nei tą dieną, kurią toms sąskaitoms pradėtos taikyti 1 ir 2 dalyse numatytos priemonės, arba

c) mokėjimais pagal teisminių institucijų, administracinius arba arbitražo sprendimus, priimtus Sąjungoje arba vykdytinus atitinkamoje valstybėje narėje,

su sąlyga, kad tokioms palūkanoms, kitoms pajamoms ir mokėjimams yra toliau taikomos 1 dalyje numatytos priemonės.

6 straipsnis

1. Valstybės narės arba Sąjungos vyriausiojo įgaliotinio užsienio reikalams ir saugumo politikai pasiūlymu Taryba vienbalsiai sudaro priede pateikiamą sąrašą ir jį iš dalies keičia.

2. Taryba tiesiogiai, jei adresas žinomas, arba viešai paskelbdama pranešimą, atitinkamam fiziniam ar juridiniam asmeniui, subjektui ar organizacijai praneša 1 dalyje nurodytą sprendimą, įskaitant įtraukimo į sąrašą motyvus, suteikdama tam fiziniam ar juridiniam asmeniui, subjektui ar organizacijai galimybę pateikti pastabų.

3. Jeigu pateikiama pastabų arba naujų esminių įrodymų, Taryba peržiūri 1 dalyje nurodytą sprendimą ir atitinkamai informuoja atitinkamą fizinį ar juridinį asmenį, subjektą ar organizaciją.

▼B

7 straipsnis

1. Priede nurodomos 4 ir 5 straipsniuose nurodytų fizinių ir juridinių asmenų, subjektų ir organizacijų įtraukimo į sąrašą priežastys.

2. Priede pateikiama informacija, jei jos turima, būtina atitinkamų fizinių ar juridinių asmenų tapatybei nustatyti ir subjektams ar įstaigoms identifikuoti. Tokia apie fizinius asmenis teikiama informacija gali apimti: vardą ir pavardę ir slapyvardžius; gimimo datą ir vietą; pilietybę; paso bei asmens tapatybės kortelės numerius; lytį; adresą, jei žinomas; ir pareigas arba profesiją. Tokia apie juridinius asmenis, subjektus ar įstaigas teikiama informacija gali apimti pavadinimą, registracijos vietą ir datą, registracijos numerį ir veiklos vykdymo vietą.

8 straipsnis

Netenkinami jokie su sutartimi arba sandoriu, kurių vykdymui tiesioginį arba netiesioginį, visapusišką arba dalinį poveikį turėjo šiuo sprendimu nustatytos priemonės, susiję reikalavimai, įskaitant reikalavimus dėl žalos atlyginimo arba kitus šios rūšies reikalavimus, pavyzdžiui, reikalavimai dėl kompensacijos ar dėl garantijos suteikimo, visų pirma reikalavimai pratęsti arba apmokėti obligaciją, garantiją ar žalos atlyginimo įsipareigojimą, ypač finansinę garantiją ar finansinį žalos atlyginimo įsipareigojimą, nepriklausomai nuo jų formos, kuriuos pateikė:

a) į priede pateiktą sąrašą įtraukti fiziniai ar juridiniai asmenys, subjektai ar organizacijos;

b) fiziniai ar juridiniai asmenys, subjektai ar organizacijos, veikiantys per bet kurį a punkte nurodytą fizinį ar juridinį asmenį, subjektą ar organizaciją arba jų vardu.

9 straipsnis

Siekiant, kad šiame sprendime nustatytų priemonių poveikis būtų kuo didesnis, Sąjunga skatina trečiąsias valstybes patvirtinti ribojamąsias priemones, panašias į nustatytąsias šiame sprendime.

▼M1

10 straipsnis

Šis sprendimas taikomas iki 2021 m. gegužės 18 d. ir nuolat peržiūrimas. Jis atnaujinamas arba atitinkamai iš dalies keičiamas, jei Taryba mano, kad jo tikslai nepasiekti.

▼B

11 straipsnis

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

▼B

PRIEDAS

4 ir 5 straipsniuose nurodytų fizinių ir juridinių asmenų, subjektų ir organizacijų sąrašas

▼M2

A. Fiziniai asmenys

	Vardas, pavardė	Identifikuojamoji informacija	Įtraukimo į sąrašą priežastys	Įtraukimo į sąrašą data
▼M4				
1.	GAO Qiang	Gimimo data: 1983 m. spalio 4 d. 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“, t. y. didelį poveikį turinčių, iš už Sąjungos ribų vykdomų ir išorinę grėsmę Sąjungai ar jos valstybėms narėms keliančių kibernetinių išpuolių seka ir didelį poveikį trečiosioms valstybėms turinčių kibernetinių išpuolių seka. Operacija „Operation Cloud Hopper“ buvo nukreipta prieš tarptautinių bendrovių šešiuose žemynuose, įskaitant Sąjungoje esančias bendroves, informacines sistemas; ją vykdant buvo įgyta neteisėta prieiga prie neskelbtinų komercinių duomenų ir dėl to buvo sukelta didelių ekonominių nuostolių. Operaciją „Operation Cloud Hopper“ vykdė subjektas, viešai žinomas kaip „APT10“ („Advanced Persistent Threat 10“) (*alias*: „Red Apollo“, „CVNX“, „Stone Panda“, „MenuPass“ ir „Potassium“). Gao Qiang gali būti siejamas su APT10, be kita ko, per jo sąsajas su APT10 valdymo ir kontrolės infrastruktūra. Be to, Gao Qiang įdarbino subjektas „Huaying Haitai“, kuris yra įtrauktas į sąrašą už paramos teikimą ir palankesnių sąlygų sudarymą vykdant operaciją „Operation Cloud Hopper“. Jis turi sąsajų su Zhang Shilong, kuris taip pat yra įtrauktas į sąrašą dėl sąsajų su operacija „Operation Cloud Hopper“. Todėl Gao Qiang yra siejamas tiek su „Huaying Haitai“, tiek su Zhang Shilong.	2020 7 30
2.	ZHANG Shilong	Gimimo data: 1981 m. rugsėjo 10 d. Gimimo vieta: Kinija Adresas: Hedong, Yuyang Road No 121, Tianjin, China Pilietybė: Kinijos Lytis: vyras	Zhang Shilong dalyvauja vykdant operaciją „Operation Cloud Hopper“, t. y. didelį poveikį turinčių, iš už Sąjungos ribų vykdomų ir išorinę grėsmę Sąjungai ar jos valstybėms narėms keliančių kibernetinių išpuolių seka ir didelį poveikį trečiosioms valstybėms turinčių kibernetinių išpuolių seka.	2020 7 30

▼M4

	Vardas, pavardė	Identifikuojamoji informacija	Įtraukimo į sąrašą priežastys	Įtraukimo į sąrašą data
			Operacija „Operation Cloud Hopper“ buvo nukreipta prieš tarptautinių bendrovių šešiuose žemynuose, įskaitant Sąjungoje esančias bendroves, informacines sistemas; ją vykdant buvo įgyta neteisėta prieiga prie neskelbtinų komercinių duomenų ir dėl to buvo sukelta didelių ekonominių nuostolių. Operaciją „Operation Cloud Hopper“ vykdė subjektas, viešai žinomas kaip „APT10“ („Advanced Persistent Threat 10“) (*alias*: „Red Apollo“, „CVNX“, „Stone Panda“, „MenuPass“ ir „Potassium“). 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 įdarbino subjektas „Huaying Haitai“, kuris yra įtrauktas į sąrašą už paramos teikimą ir palankesnių sąlygų sudarymą vykdant operaciją „Operation Cloud Hopper“. Jis turi sąsajų su Gao Qiang, kuris taip pat yra įtrauktas į sąrašą dėl sąsajų su operacija „Operation Cloud Hopper“. Todėl Zhang Shilong yra siejamas tiek su „Huaying Haitai“, tiek su Gao Qiang.	

▼M2

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

▼M2

	Vardas, pavardė	Identifikuojamoji informacija	Įtraukimo į sąrašą priežastys	Įtraukimo į sąrašą data
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

▼M2

	Vardas, pavardė	Identifikuojamoji informacija	Įtraukimo į sąrašą priežastys	Įtraukimo į sąrašą data
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

▼M3

7.	Dmitry Sergeyevich BADIN	Дмитрий Сергеевич БАДИН Gimimo data: 1990 m. lapkričio 15 d. Gimimo vieta: Kurskas, Rusijos TFSR (dabar – Rusijos Federacija) Pilietybė: Rusijos Lytis: vyras	Dmitry Badin dalyvavo vykdant didelį poveikį turintį kibernetinį išpuolį prieš Vokietijos Federalinį Parlamentą (*Deutscher Bundestag*). 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 (*Deutscher Bundestag*), narys. Šis kibernetinis išpuolis buvo nukreiptas prieš Parlamento informacinę sistemą ir sutrikdė jos veikimą keletą dienų. Buvo pavogta daug duomenų ir padarytas poveikis kelių parlamento narių bei kanclerės Angelos Merkel el. pašto paskyroms.	2020 10 22

▼M3

	Vardas, pavardė	Identifikuojamoji informacija	Įtraukimo į sąrašą priežastys	Įtraukimo į sąrašą data
8.	Igor Olegovich KOSTYUKOV	Игорь Олегович КОСТЮКОВ Gimimo data: 1961 m. vasario 21 d. 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 26165 karinis padalinys (dar vadinamas: „APT28“, „Fancy Bear“, „Sofacy Group“, „Pawn Storm“ ir „Strontium“). Eidamas šias pareigas Igor Kostyukov yra atsakingas už GTsSS įvykdytus kibernetinius išpuolius, įskaitant didelį poveikį turinčius kibernetinius išpuolius, kurie kelia išorinę 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 keletą dienų. Buvo pavogta daug duomenų ir padarytas poveikis kelių parlamento narių bei kanclerės Angelos Merkel el. pašto paskyroms.	2020 10 22

▼M2

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

▼M2

	Pavadinimas	Identifikuojamoji informacija	Įtraukimo į sąrašą priežastys	Įtraukimo į sąrašą data
			„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

▼M2

	Pavadinimas	Identifikuojamoji informacija	Įtraukimo į sąrašą priežastys	Įtraukimo į sąrašą data
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. 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“.	2020 7 30

▼M3

4.	Rusijos Federacijos ginkluotųjų pajėgų generalinio štabo vyriausiosios valdybos (GU/GRU) 85-asis pagrindinis specialiųjų tarnybų centras (GTsSS)	Adresas: Komsomol'skiy Prospekt, 20, Maskva, 119146, Rusijos Federacija	Rusijos Federacijos ginkluotųjų pajėgų generalinio štabo vyriausiosios valdybos (GU/GRU) 85-asis pagrindinis specialiųjų tarnybų centras (GTsSS), dar žinomas kaip 26165 karinis padalinys (dar vadinamas: „APT28“, „Fancy Bear“, „Sofacy Group“, „Pawn Storm“ ir „Strontium“), yra atsakingas už didelį poveikį turinčius kibernetinius išpuolius, kurie kelia išorinę grėsmę Sąjungai ar jos valstybėms narėms.	2020 10 22

▼M3

	Pavadinimas	Identifikuojamoji informacija	Įtraukimo į sąrašą priežastys	Įtraukimo į sąrašą data
			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 keletą dienų. Buvo pavogta daug duomenų ir padarytas poveikis kelių parlamento narių bei kanclerės Angelos Merkel el. pašto paskyroms.	