►B ►C1 **UREDBA VIJEĆA (EU) 2019/796**

od 17. svibnja 2019.

o mjerama ograničavanja protiv kibernapada koji predstavljaju prijetnju Uniji ili njezinim državama članicama ◄

(SL L 129I, 17.5.2019., str. 1.)

Koju je izmijenila:

		Službeni list		
		br.	stranica	datum
►M1	Provedbena uredba Vijeća (EU) 2020/1125 od 30. srpnja 2020.	L 246	4	30.7.2020.
►M2	Provedbena uredba Vijeća (EU) 2020/1536 od 22. listopada 2020.	L 351 I	1	22.10.2020.
►M3	Provedbena uredba Vijeća (EU) 2020/1744 od 20. studenoga 2020.	L 393	1	23.11.2020.
►M4	Provedbena uredba Komisije (EU) 2022/595 od 11. travnja 2022.	L 114	60	12.4.2022.
►M5	Uredba Vijeća (EU) 2023/2694 od 27. studenoga 2023.	L 2694	1	28.11.2023.
►M6	Provedbena uredba Vijeća (EU) 2024/1390 od 17. svibnja 2024.	L 1390	1	17.5.2024.

Koju je ispravio:

►C1 Ispravak, SL L 176, 5.6.2020, str. 16 (2019/796)
►C2 Ispravak, SL L 230, 17.7.2020, str. 37 (2019/796)

▼B
▼C1

UREDBA VIJEĆA (EU) 2019/796

od 17. svibnja 2019.

o mjerama ograničavanja protiv kibernapada koji predstavljaju prijetnju Uniji ili njezinim državama članicama

▼B

Članak 1.

1. Ova Uredba primjenjuje se na kibernapade sa znatnim učinkom, uključujući pokušaje kibernapada s potencijalno znatnim učinkom, koji predstavljaju vanjsku prijetnju Uniji ili njezinim državama članicama.

2. Kibernapadi koji predstavljaju vanjsku prijetnju obuhvaćaju kibernapade:

(a) koji potječu ili su izvedeni iz područja izvan Unije;

(b) za koje se upotrebljava infrastruktura izvan Unije;

(c) koje izvede bilo koja fizička ili pravna osoba, subjekt ili tijelo koje ima poslovni nastan ili djeluje izvan Unije; ili

(d) koji se izvedu uz potporu, prema nalogu ili pod kontrolom bilo koje fizičke ili pravne osobe, subjekta ili tijela koji djeluju izvan Unije.

3. U tu svrhu kibernapadi su djelovanja koja obuhvaćaju bilo koje od sljedećeg:

(a) pristup informacijskim sustavima;

(b) ometanje informacijskih sustava;

(c) ometanje podataka; ili

(d) presretanje podataka,

ako takva djelovanja nije propisno ovlastio vlasnik ili drugi nositelj prava u vezi sa sustavom ili podacima ili njihovim dijelom, ili ako nisu dopuštena u skladu s pravom Unije ili dotične države članice.

4. Kibernapadi koji predstavljaju prijetnju državama članicama obuhvaćaju kibernapade koji pogađaju informacijske sustave povezane s, među ostalim:

(a) kritičnom infrastrukturom, uključujući podmorske kabele i predmete poslane u svemir, koja je ključna za održavanje vitalnih funkcija društva ili za zdravlje, sigurnost, zaštitu i gospodarsku ili društvenu dobrobit ljudi;

(b) službama nužnima za održavanje ključnih društvenih i/ili gospodarskih aktivnosti, posebno u sektorima energetike (električna energija, nafta i plin); prijevoza (zračnog, željezničkog, vodnog i cestovnog); bankarstva; infrastruktura financijskog tržišta; zdravstvenog sektora (pružatelji zdravstvene zaštite, bolnice i privatne klinike); opskrbe pitkom vodom i njezine distribucije; digitalne infrastrukture; i bilo kojeg drugog sektora koji je ključan za dotičnu državu članicu;

▼B

(c) ključnim državnim funkcijama, posebno u područjima obrane, upravljanja i funkcioniranja institucija, među ostalim za javne izbore ili postupak glasovanja, funkcioniranja gospodarske i civilne infrastrukture, unutarnje sigurnosti te vanjskih odnosa, među ostalim putem diplomatskih misija;

(d) pohranom ili obradom klasificiranih podataka; ili

(e) vladinim timovima za hitne intervencije.

5. Kibernapadi koji predstavljaju prijetnju Uniji obuhvaćaju kibernapade na njezine institucije, tijela, urede i agencije, njezine delegacije u trećim zemljama ili međunarodne organizacije, njezine operacije ili misije zajedničke vanjske i obrambene politike (ZSOP) i njezine posebne predstavnike.

6. Ako se to smatra potrebnim kako bi se ostvarili ciljevi zajedničke vanjske i sigurnosne politike (ZVSP) iz odgovarajućih odredaba članka 21. Ugovora o Europskoj uniji, mjere ograničavanja u skladu s ovom Uredbom mogu se primijeniti i kao odgovor na kibernapade sa znatnim učinkom protiv trećih država ili međunarodnih organizacija.

7. Za potrebe ove Uredbe primjenjuju se sljedeće definicije:

(a) „informacijski sustavi” znači uređaj ili skupina međupovezanih ili srodnih uređaja, od kojih jedan ili više njih, sukladno programu, provodi automatsku obradu digitalnih podataka, te digitalni podaci koji su pohranjeni, obrađeni, pronađeni ili preneseni tim uređajem ili skupinom uređaja za potrebe njegova ili njihova funkcioniranja, upotrebe, zaštite i održavanja;

(b) „ometanje informacijskog sustava” znači sprečavanje ili prekidanje funkcioniranja informacijskog sustava unosom, prijenosom, oštećivanjem, brisanjem, degradacijom, mijenjanjem ili prikrivanjem digitalnih podataka, ili onemogućavanjem pristupa takvim podacima;

(c) „ometanje podataka” znači brisanje, oštećivanje, degradacija, mijenjanje ili prikrivanje digitalnih podataka u informacijskom sustavu, ili onemogućavanje pristupa takvim podacima; to uključuje i krađu podataka, financijskih sredstava, gospodarskih resursa ili intelektualnog vlasništva;

(d) „presretanje podataka” znači presretanje, s pomoću tehničkih sredstava, nejavnih prijenosa digitalnih podataka u informacijski sustav, iz ili unutar njega, uključujući elektromagnetske emisije iz informacijskog sustava kojima se prenose takvi digitalni podaci.

8. Za potrebe ove Uredbe primjenjuju se sljedeće dodatne definicije:

(a) „zahtjev” znači svaki zahtjev neovisno o tome je li istaknut u pravnom postupku, koji je podnesen prije ili nakon dana stupanja na snagu ove Uredbe, a temelji se na ugovoru ili transakciji ili je povezan s ugovorom ili transakcijom te posebice uključuje:

i. zahtjev za ispunjenje bilo koje obveze koja proizlazi iz ugovora ili transakcije ili je povezana s ugovorom ili transakcijom;

ii. zahtjev za produljenje ili plaćanje obveznice, financijskog jamstva ili odštete u bilo kojem obliku;

iii. zahtjev za naknadu štete povezane s ugovorom ili transakcijom;

iv. protuzahtjev;

▼B

v. zahtjev za priznanje ili izvršenje, među ostalim postupkom egzekvature, presude, arbitražnog pravorijeka ili jednakovrijedne odluke, neovisno o tome gdje su doneseni;

(b) „ugovor ili transakcija” znači svaka transakcija u bilo kojem obliku i u okviru bilo kojeg primjenjivog prava, neovisno o tome obuhvaća li jedan ili više ugovora, odnosno sličnih obveza sklopljenih, odnosno preuzetih između istih ili različitih stranaka; za te potrebe „ugovor” uključuje obveznicu, jamstvo ili odštetu, posebice financijsko jamstvo ili financijsku odštetu, i kredite, neovisno o tome jesu li pravno neovisni, te sve povezane odredbe koje proizlaze iz transakcije ili su s njom povezane;

(c) „nadležna tijela” odnosi se na nadležna tijela država članica kako su navedena na internetskim stranicama popisanima u Prilogu II.;

(d) „gospodarski resursi” znači imovina bilo koje vrste, materijalna ili nematerijalna, pokretna ili nepokretna, izuzev financijskih sredstava, koja se može upotrijebiti za stjecanje financijskih sredstava, robe ili usluga;

(e) „zamrzavanje gospodarskih resursa” znači sprječavanje upotrebe gospodarskih resursa za stjecanje financijskih sredstava, robe ili usluga na bilo koji način, uključujući, ali ne ograničujući se na, njihovu prodaju, unajmljivanje ili stavljanje pod hipoteku;

(f) „zamrzavanje financijskih sredstava” znači sprječavanje svakog kretanja, prijenosa, izmjene, upotrebe, pristupa ili svakog raspolaganja financijskim sredstvima koje bi dovelo do bilo kakve promjene u njihovu obujmu, iznosu, lokaciji, vlasništvu, naravi ili odredištu, ili do bilo kojih drugih promjena koje bi omogućile korištenje tih financijskih sredstava, uključujući upravljanje portfeljem;

(g) „financijska sredstva” znači financijska imovina i koristi bilo koje vrste, uključujući, ali ne ograničujući se na:

i. gotovina, čekovi, novčana potraživanja, mjenice, novčane doznake i druga sredstva plaćanja;

ii. depoziti u financijskim institucijama ili drugim subjektima, stanja na računima, dugovanja i dužničke obveze;

iii. vrijednosni papiri i dužnički instrumenti kojima se trguje javno ili privatno, uključujući dionice i udjele, potvrde o vrijednosnim papirima, obveznice, mjenice, jamstva, zadužnice i ugovore o financijskim izvedenicama;

iv. kamate, dividende ili drugi prihodi od imovine ili vrijednost koja se akumulira iz imovine ili je proizvod imovine;

v. krediti, prava prijeboja, jamstva, jamstva da će ugovor biti izvršen prema ugovorenim uvjetima ili druge financijske obveze;

vi. akreditivi, teretnice, kupoprodajni ugovori; i

vii. dokumenti kojima se dokazuje udio u financijskim sredstvima ili financijskim resursima;

▼B

(h) „područje Unije” znači državna područja država članica na koja se primjenjuje Ugovor, u skladu s uvjetima utvrđenima u Ugovoru, uključujući njihov zračni prostor.

Članak 2.

Čimbenici s pomoću kojih se utvrđuje ima li kibernapad znatan učinak kako je navedeno u članku 1. stavku 1. obuhvaćaju bilo koje od sljedećeg:

(a) opseg, razinu, učinak ili ozbiljnost uzrokovanog poremećaja, među ostalim u pogledu gospodarskih i društvenih aktivnosti, ključnih usluga, ključnih državnih funkcija, javnog reda ili javne sigurnosti;

(b) broj fizičkih ili pravnih osoba, subjekata ili tijela na koje utječe;

(c) broj dotičnih država članica;

(d) opseg gospodarskih gubitaka uzrokovanih primjerice velikom krađom financijskih sredstava, gospodarskih resursa ili intelektualnog vlasništva;

(e) gospodarsku korist koju je počinitelj ostvario za sebe ili druge;

(f) količinu ili prirodu ukradenih podataka ili razmjer povreda podataka ili

(g) prirodu komercijalno osjetljivih podataka kojima se pristupilo.

Članak 3.

1. Zamrzavaju se sva financijska sredstva i gospodarski resursi koji pripadaju odnosno koji su u vlasništvu, posjedu ili pod kontrolom bilo koje fizičke ili pravne osobe, subjekta ili tijela navedenih u Prilogu I.

2. Nikakva financijska sredstva ni gospodarski resursi ne stavljaju se na raspolaganje ni izravno ni neizravno fizičkim ni pravnim osobama, subjektima ni tijelima navedenima u Prilogu I. niti u njihovu korist.

3. Prilog I. uključuje, kako je utvrdilo Vijeće u skladu s člankom 5. stavkom 1. Odluke Vijeća (ZVSP) 2019/797:

(a) fizičke ili pravne osobe, subjekte ili tijela odgovorne za kibernapade ili pokušaje kibernapada;

(b) fizičke ili pravne osobe, subjekte ili tijela koji pružaju financijsku, tehničku ili materijalnu potporu ili su na neki drugi način svjesno umiješani u kibernapade ili pokušaje kibernapada, među ostalim planiranjem, pripremanjem, usmjeravanjem, pomaganjem ili poticanjem takvih napada ili sudjelovanjem u takvim napadima, ili olakšavanjem takvih napada ili djelovanjem ili nedjelovanjem;

(c) fizičke ili pravne osobe, subjekte ili tijela povezane s fizičkim ili pravnim osobama, subjektima ili tijelima obuhvaćenima točkama (a) i (b) ovog stavka.

▼B

Članak 4.

1. Odstupajući od članka 3., nadležna tijela država članica mogu odobriti oslobađanje određenih zamrznutih financijskih sredstava ili gospodarskih resursa odnosno stavljanje na raspolaganje određenih sredstava ili gospodarskih resursa pod uvjetima koje smatraju primjerenima, nakon što utvrde da su financijska sredstva ili gospodarski resursi:

(a) ►C2 potrebni za zadovoljavanje osnovnih potreba fizičkih ili pravnih osoba, subjekata ili tijela navedenih u Prilogu I. ◄ te uzdržavanih članova obitelji tih fizičkih osoba, uključujući plaćanja za prehrambene proizvode, najamninu ili otplatu hipoteke, lijekove i liječenje, poreze, premije osiguranja i naknade za javne komunalne usluge;

(b) namijenjeni isključivo za plaćanje opravdanih honorara i naknadu nastalih troškova povezanih s pružanjem pravnih usluga;

(c) namijenjeni isključivo za plaćanje pristojbi ili naknada za usluge redovitog čuvanja zamrznutih financijskih sredstava ili gospodarskih resursa ili upravljanja njima;

(d) potrebni za izvanredne troškove, pod uvjetom da je relevantno nadležno tijelo najmanje dva tjedna prije dodjele odobrenja priopćilo nadležnim tijelima ostalih država članica i Komisiji razloge zbog kojih smatra da bi trebalo dodijeliti posebno odobrenje ili

(e) namijenjeni uplati na račun ili isplati s računa diplomatske ili konzularne misije ili međunarodne organizacije koje uživaju imunitet u skladu s međunarodnim pravom, pod uvjetom da su ta plaćanja namijenjena za službene potrebe diplomatske ili konzularne misije ili međunarodne organizacije.

2. Dotična država članica obavješćuje druge države članice i Komisiju o svim odobrenjima izdanima na temelju stavka 1. u roku od dva tjedna od odobrenja.

▼M5

Članak 4.a

1. Članak 3. stavci 1. i 2. ne primjenjuju se na stavljanje na raspolaganje financijskih sredstava ili gospodarskih izvora potrebnih za osiguravanje pravodobne isporuke humanitarne pomoći ili za potporu drugim aktivnostima kojima se podupiru osnovne ljudske potrebe ako tu isporuku pomoći i druge aktivnosti provode:

(a) Ujedinjeni narodi (UN), uključujući njihove programe, fondove i druge subjekte i tijela, te njihove specijalizirane agencije i povezane organizacije;

(b) međunarodne organizacije;

(c) humanitarne organizacije sa statusom promatrača u Općoj skupštini UN-a i članovi tih humanitarnih organizacija;

(d) bilateralno ili multilateralno financirane nevladine organizacije koje sudjeluju u planovima UN-a za humanitarni odgovor, planovima UN-a za odgovor na izbjeglice, drugim apelima UN-a ili humanitarnim klasterima koje koordinira Ured UN-a za koordinaciju humanitarnih poslova;

▼M5

(e) organizacije i agencije kojima je Unija izdala certifikat o humanitarnom partnerstvu ili koje je država članica certificirala ili priznala u skladu s nacionalnim postupcima;

(f) specijalizirane agencije država članica; ili

(g) zaposlenici, korisnici bespovratnih sredstava, podružnice ili provedbeni partneri subjekata iz točaka od (a) do (f) dok i ako djeluju u tom svojstvu.

2. Ne dovodeći u pitanje stavak 1. i odstupajući od članka 3. stavaka 1. i 2., nadležna tijela država članica mogu odobriti oslobađanje određenih zamrznutih financijskih sredstava ili gospodarskih izvora ili stavljanje na raspolaganje određenih financijskih sredstava ili gospodarskih izvora, pod uvjetima koje smatraju primjerenima, nakon što utvrde da je pružanje takvih financijskih sredstava ili gospodarskih izvora potrebno radi osiguravanja pravodobne isporuke humanitarne pomoći ili pružanja potpore drugim aktivnostima kojima se podupiru osnovne ljudske potrebe.

3. Ako u roku od pet radnih dana od datuma primitka zahtjeva za odobrenje na temelju stavka 2. relevantno nadležno tijelo ne donese negativnu odluku, ne zatraži informacije niti izda obavijest o dodatnom vremenu, smatra se da je to odobrenje izdano.

4. Dotična država članica obavješćuje ostale države članice i Komisiju o svakom odobrenju izdanom na temelju stavaka 2. i 3. u roku od četiri tjedna od izdavanja takvog odobrenja.

▼B

Članak 5.

1. Odstupajući od članka 3. stavka 1. nadležna tijela država članica mogu odobriti oslobađanje određenih zamrznutih financijskih sredstava ili gospodarskih resursa ako su ispunjeni sljedeći uvjeti:

(a) financijska sredstva ili gospodarski resursi predmet su arbitražne odluke donesene prije datuma na koji su fizička ili pravna osoba, subjekt ili tijelo iz članka 3. uvršteni na popis iz Priloga I., ili su predmet su sudske ili upravne odluke donesene u Uniji ili sudske odluke izvršive u dotičnoj državi članici, prije ili nakon tog datuma;

(b) financijska sredstva ili gospodarski resursi upotrebljavat će se isključivo za namirenje potraživanja osiguranih takvom odlukom ili priznatih kao valjanih takvom odlukom, u okvirima određenima važećim zakonima i propisima kojima se uređuju prava osoba s takvim potraživanjima;

(c) odluka nije u korist fizičke ili pravne osobe, subjekta ili tijela uvrštenih na popis iz Priloga I.; i

(d) priznavanje odluke nije protivno javnom poretku dotične države članice.

▼B

2. Dotična država članica obavješćuje ostale države članice i Komisiju o svim odobrenjima izdanima na temelju stavka 1. u roku od dva tjedna od odobrenja.

Članak 6.

1. Odstupajući od članka 3. stavka 1., pod uvjetom da je uplata fizičke ili pravne osobe, subjekta ili tijela uvrštenih na popis iz Priloga I. dospjela na temelju ugovora ili sporazuma, odnosno obveze koju je dotična fizička ili pravna osoba, subjekt ili tijelo sklopilo, odnosno preuzelo prije datuma na koji su ta fizička ili pravna osoba, subjekt ili tijelo uvršteni na popis iz Priloga I., nadležna tijela država članica mogu, pod uvjetima koje smatraju primjerenima, odobriti oslobađanje određenih zamrznutih sredstava ili gospodarskih resursa, pod uvjetom da je dotično nadležno tijelo utvrdilo sljedeće:

(a) da će ta financijska sredstva ili te gospodarske resurse za plaćanje upotrijebiti fizička ili pravna osoba, subjekt ili tijelo uvršteno u Prilog I.; i

(b) da se plaćanjem ne krši članak 3. stavak 2.

2. Dotična država članica obavješćuje druge države članice i Komisiju o svim odobrenjima izdanima na temelju stavka 1. u roku od dva tjedna od odobrenja.

Članak 7.

1. Člankom 3. stavkom 2. ne sprječava se financijske ni kreditne institucije da na zamrznute račune pripisuju financijska sredstva koja treće osobe doznače u korist fizičke ili pravne osobe, subjekta ili tijela uvrštenog na popis, pod uvjetom da se svaki takav priljev na te račune zamrzne. Financijska ili kreditna institucija bez odgode obavješćuje relevantno nadležno tijelo o svim takvim transakcijama.

2. Članak 3. stavak 2. ne primjenjuje se na sljedeće priljeve na zamrznute račune:

▼C1

(a) kamate ili druge prihode od tih računa;

(b) plaćanja koja su dospjela na temelju ugovora, sporazuma ili obveza sklopljenih ili preuzetih prije datuma na koji je fizička ili pravna osoba, subjekt ili tijelo iz članka 3. stavka 1. uvršteno na popis iz Priloga I.; ili

(c) plaćanja koja su dospjela na temelju sudske, upravne ili arbitražne odluke koja je donesena u državi članici ili je izvršiva u dotičnoj državi članici,

▼B

pod uvjetom da takve kamate, drugi prinosi i plaćanja i dalje podliježu mjerama predviđenima člankom 3. stavkom 1.

Članak 8.

1. Ne dovodeći u pitanje primjenjiva pravila o izvješćivanju, povjerljivosti i profesionalnoj tajni, fizičke, odnosno pravne osobe, subjekti i tijela:

▼B

(a) nadležnom tijelu države članice u kojoj borave ili imaju sjedište odmah dostavljaju sve informacije koje bi mogle olakšati poštovanje ove Uredbe, kao što su informacije o računima i iznosima zamrznutima u skladu s člankom 3. stavkom 1., te takve informacije prosljeđuju Komisiji, izravno ili preko države članice; i

(b) surađuju s nadležnim tijelom u svakoj provjeri informacija iz točke (a).

2. Sve dodatne informacije koje Komisija izravno primi stavljaju se na raspolaganje državama članicama.

3. Sve informacije dostavljene ili primljene u skladu s ovim člankom koriste se samo za potrebe za koje su dostavljene ili primljene.

Članak 9.

Zabranjuje se svjesno i namjerno sudjelovanje u aktivnostima čiji je cilj ili učinak izbjegavanje mjera iz članka 3.

Članak 10.

1. Zamrzavanjem financijskih sredstava i gospodarskih resursa ili odbijanjem njihova stavljanja na raspolaganje, koje je provedeno u dobroj vjeri na osnovi toga da je takvo djelovanje u skladu s ovom Uredbom, ne nastaje nikakva odgovornost fizičke ni pravne osobe, subjekta ni tijela koje ga provodi, kao ni njegovih direktora ni zaposlenika, osim ako se dokaže je zamrzavanje ili zadržavanje tih financijskih sredstava i gospodarskih resursa posljedica nemara.

2. Fizičke i pravne osobe, subjekti i tijela za svoja postupanja ne snose nikakvu odgovornost ako nisu znali niti su imali opravdan razlog sumnjati da svojim postupanjem krše mjere navedene u ovoj Uredbi.

Članak 11.

1. Ne udovoljava se nijednom zahtjevu u vezi s bilo kojim ugovorom ili transakcijom na čije su izvršenje izravno ili neizravno, u cijelosti ili djelomično, utjecale mjere određene na temelju ove Uredbe, uključujući zahtjeve za odštetu ili bilo koje druge zahtjeve te vrste, primjerice zahtjev za naknadu štete ili zahtjev na temelju jamstva, posebno zahtjev za produljenje ili plaćanje obveznice, jamstva ili odštete, osobito financijskog jamstva ili financijske odštete, u bilo kojem obliku, ako ga podnesu:

(a) fizičke ili pravne osobe, subjekti ili tijela uvršteni na popis iz Priloga I.;

(b) bilo koje fizičke ili pravne osobe, subjekti ili tijela koji djeluju putem jedne od fizičkih ili pravnih osoba, subjekata ili tijela iz točke (a) ili u njihovo ime.

2. U svim postupcima za izvršenje zahtjeva teret dokazivanja da ispunjenje zahtjeva nije zabranjeno stavkom 1. na fizičkoj je ili pravnoj osobi, subjektu ili tijelu koje traži izvršenje tog zahtjeva.

3. Ovim se člankom ne dovodi u pitanje pravo fizičkih ili pravnih osoba, subjekata i tijela iz stavka 1. na sudsko preispitivanje zakonitosti neizvršenja ugovornih obveza u skladu s ovom Uredbom.

▼B

Članak 12.

1. Komisija i države članice međusobno se obavješćuju o mjerama poduzetima u skladu s ovom Uredbom te razmjenjuju sve ostale relevantne informacije koje su im na raspolaganju u vezi s ovom Uredbom, a posebice informacije o:

(a) sredstvima zamrznutima u skladu s člankom 3. i odobrenjima izdanima u skladu s člancima 4., 5. i 6.;

(b) poteškoćama u vezi s kršenjem i izvršenjem te o presudama koje su donijeli nacionalni sudovi.

2. Države članice odmah obavješćuju jedna drugu i Komisiju o svim ostalim relevantnim informacijama koje su im na raspolaganju, a koje bi mogle utjecati na djelotvornu provedbu ove Uredbe.

Članak 13.

1. Ako Vijeće odluči fizičku ili pravnu osobu, subjekt ili tijelo podvrgnuti mjerama iz članka 3., ono u skladu s tim mijenja Prilog I.

2. Vijeće odluku iz stavka 1., kao i razloge za uvrštavanje na popis, priopćuje dotičnoj fizičkoj ili pravnoj osobi, subjektu ili tijelu izravno, ako je adresa poznata, ili objavom obavijesti, pružajući toj fizičkoj ili pravnoj osobi, subjektu ili tijelu mogućnost očitovanja.

3. Ako su podnesena očitovanja ili su izneseni važni novi dokazi, Vijeće preispituje odluku iz stavka 1. i o tome obavješćuje dotičnu fizičku ili pravnu osobu, subjekt ili tijelo.

4. Popis iz Priloga I. redovito se preispituje, a najmanje svakih 12 mjeseci.

▼C1

5. Komisija je ovlaštena izmijeniti Prilog II. na temelju informacija koje dostave države članice.

▼B

Članak 14.

1. U Prilogu I. navode se razlozi za uvrštavanje na popis dotičnih fizičkih ili pravnih osoba, subjekata ili tijela.

2. ►C1 Prilog I. sadržava, ako su dostupne, informacije potrebne za utvrđivanje identiteta dotičnih fizičkih ili pravnih osoba, subjekata ili tijela. ◄ U pogledu fizičkih osoba takvi podaci mogu uključivati: imena i druga imena; datum i mjesto rođenja; državljanstvo; broj putovnice i osobne iskaznice; spol; adresu ako je poznata; te funkciju ili zanimanje. U pogledu pravnih osoba, subjekata ili tijela, takvi podaci mogu uključivati nazive, mjesto i datum upisa u registar, broj upisa u registar i mjesto obavljanja djelatnosti.

Članak 15.

1. Države članice utvrđuju pravila o sankcijama koje se primjenjuju na kršenja odredaba ove Uredbe i poduzimaju sve potrebne mjere radi osiguravanja njihove provedbe. Predviđene sankcije moraju biti učinkovite, proporcionalne i odvraćajuće.

▼B

2. Države članice nakon stupanja na snagu ove Uredbe bez odgode obavješćuju Komisiju o pravilima iz stavka 1.i svim njihovim naknadnim izmjenama.

Članak 16.

1. Komisija obrađuje osobne podatke kako bi ispunila svoje zadaće na temelju ove Uredbe. Te zadaće uključuju:

(a) dodavanje sadržaja Priloga I. u elektronički, konsolidirani popis osoba, skupina i subjekata koji podliježu financijskim sankcijama Unije i u interaktivnu kartu sankcija, koji su oboje dostupni javnosti;

(b) obradu informacija o učinku mjera iz ove Uredbe, na primjer podataka o vrijednosti zamrznutih financijskih sredstava i podataka o odobrenjima koja su izdala nadležna tijela.

2. Za potrebe ove Uredbe služba Komisije iz Priloga II. određuje se kao „voditelj obrade” za Komisiju u smislu članka 3. stavka 8. Uredbe (EU) 2018/1725 kako bi se osiguralo da dotične fizičke osobe mogu ostvarivati svoja prava na temelju te uredbe.

Članak 17.

1. Države članice imenuju nadležna tijela iz ove Uredbe i to navode na internetskim stranicama s popisa u Prilogu II. Države članice obavješćuju Komisiju o svakoj promjeni adrese internetskih stranica navedenih u Prilogu II.

2. Države članice nakon stupanja na snagu ove Uredbe bez odgode obavješćuju Komisiju o svojim nadležnim tijelima, među ostalim o njihovim podacima za kontakt, te o svim naknadnim izmjenama.

3. Ako se ovom Uredbom određuje obveza priopćavanja Komisiji, njezina obavješćivanja ili drugog načina komuniciranja s njom, za tu se komunikaciju upotrebljavaju adresa i drugi podaci za kontakt navedeni u Prilogu II.

Članak 18.

Ova se Uredba primjenjuje:

(a) unutar područja Unije, uključujući njezin zračni prostor;

(b) u svim zrakoplovima i plovilima koji su pod jurisdikcijom neke države članice;

(c) na sve fizičke osobe na području Unije ili izvan njega koje su državljani neke države članice;

(d) na sve pravne osobe, subjekte ili tijela na području Unije ili izvan njega koji su osnovani ili registrirani u skladu s pravom države članice;

(e) na sve pravne osobe, subjekte ili tijela u vezi s bilo kojim poslom u cijelosti ili djelomično obavljenim u Uniji.

▼B

Članak 19.

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

Ova je Uredba u cijelosti obvezujuća i izravno se primjenjuje u svim državama članicama.

▼B

PRILOG I.

Popis fizičkih i pravnih osoba, subjekata i tijela iz članka 3.

▼M1

A. Fizičke osobe

	Ime	Identifikacijski podaci	Obrazloženje	Datum uvrštenja na popis
▼M3				
1.	GAO Qiang	Datum rođenja: 4. listopada 1983. Mjesto rođenja: Provincija Shandong, Kina Adresa: Room 1102, Guanfu Mansion, 46 Xinkai Road, Hedong District, Tianjin, Kina Državljanstvo: kinesko Spol: muški	Gao Qiang sudjeluje u operaciji „Operation Cloud Hopper”, nizu kibernapada sa znatnim učinkom koji potječu iz područja izvan Unije i predstavljaju vanjsku prijetnju Uniji ili njezinim državama članicama te kibernapada sa znatnim učinkom protiv trećih država. Meta operacije „Operation Cloud Hopper” informacijski su sustavi multinacionalnih društava na šest kontinenata, uključujući društva sa sjedištem u Uniji, te je u okviru te operacije ostvaren neovlašten pristup komercijalno osjetljivim podacima, što je dovelo do znatnog gospodarskog gubitka. Subjekt javnosti poznat kao „APT10” („Advanced Persistent Threat 10”) (također poznat kao „Red Apollo”, „CVNX”, „Stone Panda”, „MenuPass” i „Potassium”) izvršio je operaciju „Operation Cloud Hopper”. Gaoa Qianga može se povezati sa subjektom „APT10”, među ostalim zbog njegove povezanosti s kontrolno-upravljačkom infrastrukturom subjekta „APT10”. Nadalje, Huaying Haitai, subjekt uvršten na popis zbog pružanja potpore operaciji „Operation Cloud Hopper” i njezina olakšavanja, angažirao je Gaoa Qianga. Povezan je sa Zhangom Shilongom, koji je također uvršten na popis u vezi s operacijom „Operation Cloud Hopper”. Gao Qiang stoga je povezan i sa subjektom Huaying Haitai i sa Zhangom Shilongom.	30.7.2020.
2.	ZHANG Shilong	Datum rođenja: 10. rujna 1981. Mjesto rođenja: Kina Adresa: Hedong, Yuyang Road No 121, Tianjin, Kina Državljanstvo: kinesko Spol: muški	Zhang Shilong sudjeluje u operaciji „Operation Cloud Hopper”, niz kibernapada sa znatnim učinkom koji potječu iz područja izvan Unije i predstavljaju vanjsku prijetnju Uniji ili njezinim državama članicama te kibernapada sa znatnim učinkom protiv trećih država. Meta operacije „Operation Cloud Hopper” informacijski su sustavi multinacionalnih društava na šest kontinenata, uključujući društva sa sjedištem u Uniji, te je u okviru te operacije ostvaren neovlašten pristup komercijalno osjetljivim podacima, što je dovelo do znatnog gospodarskog gubitka.	30.7.2020.

▼M3

	Ime	Identifikacijski podaci	Obrazloženje	Datum uvrštenja na popis
			Subjekt javnosti poznat kao „APT10” („Advanced Persistent Threat 10”) (također poznat kao „Red Apollo”, „CVNX”, „Stone Panda”, „MenuPass” i „Potassium”) izvršio je operaciju „Operation Cloud Hopper”. Zhanga Shilonga može se povezati sa subjektom „APT10”, među ostalim s pomoću štetnog softvera koji je razvio i ispitao u vezi s kibernapadima koje je izvršio subjekt „APT10”. Nadalje, Huaying Haitai, subjekt uvršten na popis zbog pružanja potpore operaciji „Operation Cloud Hopper” i njezina olakšavanja, angažirao je Zhanga Shilonga. Povezan je s Gaom Qiangom, koji je također uvršten na popis u vezi s operacijom „Operation Cloud Hopper”. Zhang Shilong stoga je povezan i sa subjektom Huaying Haitai i s Gaom Qiangom.	

▼M6

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.

▼M6

	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.
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.

▼M6

	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.
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.

▼M6

	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.

▼M1

B. Pravne osobe, subjekti i tijela

	Ime	Identifikacijski podaci	Obrazloženje	Datum uvrštenja na popis
1.	Tianjin Huaying Haitai Science and Technology Development Co. Ltd (Huaying Haitai)	Također poznat kao: Haitai Technology Development Co. Ltd Lokacija: Tianjin, Kina	Huaying Haitai pružio je financijsku, tehničku ili materijalnu potporu za operaciju ‚Operation Cloud Hopper' te ju je olakšao, a radi se o nizu kibernapada sa znatnim učinkom koji potječu iz područja izvan Unije i predstavljaju vanjsku prijetnju Uniji ili njezinim državama članicama te kibernapada sa znatnim učinkom na treće države. Meta operacije ‚Operation Cloud Hopper' bili su informacijski sustavi multinacionalnih društava na šest kontinenata, uključujući društva sa sjedištem u Uniji, te je u okviru te operacije ostvaren neovlašten pristup komercijalno osjetljivim podacima, što je dovelo do znatnog gospodarskog gubitka. Subjekt javnosti poznat kao ‚APT10' (‚Advanced Persistent Threat 10') (također poznat kao ‚Red Apollo', ‚CVNX', ‚Stone Panda', ‚MenuPass' i ‚Potassium') izvršio je operaciju ‚Operation Cloud Hopper'. Huaying Haitai može se povezati sa subjektom ‚APT10'. Nadalje, Huaying Haitai angažirao je Gaoa Qianga i Zhanga Shilonga, koji su uvršteni na popis u vezi s operacijom ‚Operation Cloud Hopper'. Huaying Haitai stoga je povezan s Gaom Qiangom i Zhangom Shilongom.	30.7.2020.
2.	Chosun Expo	Također poznat kao: Chosen Expo; Korea Export Joint Venture Lokacija: DNRK	Chosun Expo pružio je financijsku, tehničku ili materijalnu potporu za i olakšao niz kibernapada sa znatnim učinkom koji potječu iz područja izvan Unije i predstavljaju vanjsku prijetnju Uniji ili njezinim državama članicama te kibernapada sa znatnim učinkom na treće države, uključujući kibernapade koji su javnosti poznati kao ‚WannaCry' i kibernapade na poljsko tijelo za financijski nadzor i poduzeće Sony Pictures Entertainment, kao i kiberkrađu u banci Bangladesh Bank te pokušaj kiberkrađe u vijetnamskoj banci Tien Phong Bank. ‚WannaCry' je uzrokovao poremećaje u informacijskim sustavima diljem svijeta tako što ih je napao ucjenjivačkim softverom (engl. *ransomware*) i blokirao pristup podacima. Utjecao je na informacijske sustave društava u Uniji, uključujući informacijske sustave povezane s uslugama potrebnim za održavanje ključnih usluga i gospodarskih aktivnosti u državama članicama.	30.7.2020.

▼M1

	Ime	Identifikacijski podaci	Obrazloženje	Datum uvrštenja na popis
			Subjekt javnosti poznat pod nazivom ‚APT38' (‚Advanced persistent Threat 38') i skupina ‚Lazarus Group' izvršili su napad ‚WannaCry'. Chosun Expo može se povezati sa subjektom ‚APT38' / skupinom ‚Lazarus Group', među ostalim s pomoću računa koji su upotrijebljeni za kibernapade.	

▼M6

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. 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.	30.7.2020.

▼M6

	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.

▼B

PRILOG II.

Internetske stranice s informacijama o nadležnim tijelima i adresa za slanje obavijesti Komisiji

▼M4

BELGIJA

https://diplomatie.belgium.be/en/policy/policy_areas/peace_and_security/sanctions

BUGARSKA

https://www.mfa.bg/en/EU-sanctions

ČEŠKA

www.financnianalytickyurad.cz/mezinarodni-sankce.html

DANSKA

http://um.dk/da/Udenrigspolitik/folkeretten/sanktioner/

NJEMAČKA

https://www.bmwi.de/Redaktion/DE/Artikel/Aussenwirtschaft/embargos-aussenwirtschaftsrecht.html

ESTONIJA

https://vm.ee/et/rahvusvahelised-sanktsioonid

IRSKA

https://www.dfa.ie/our-role-policies/ireland-in-the-eu/eu-restrictive-measures/

GRČKA

http://www.mfa.gr/en/foreign-policy/global-issues/international-sanctions.html

ŠPANJOLSKA

https://www.exteriores.gob.es/es/PoliticaExterior/Paginas/SancionesInternacionales.aspx

FRANCUSKA

http://www.diplomatie.gouv.fr/fr/autorites-sanctions/

HRVATSKA

https://mvep.gov.hr/vanjska-politika/medjunarodne-mjere-ogranicavanja/22955

ITALIJA

https://www.esteri.it/it/politica-estera-e-cooperazione-allo-sviluppo/politica_europea/misure_deroghe/

CIPAR

https://mfa.gov.cy/themes/

LATVIJA

http://www.mfa.gov.lv/en/security/4539

LITVA

http://www.urm.lt/sanctions

LUKSEMBURG

https://maee.gouvernement.lu/fr/directions-du-ministere/affaires-europeennes/organisations-economiques-int/mesures-restrictives.html

MAĐARSKA

https://kormany.hu/kulgazdasagi-es-kulugyminiszterium/ensz-eu-szankcios-tajekoztato

▼**M4**

MALTA

https://foreignandeu.gov.mt/en/Government/SMB/Pages/SMB-Home.aspx

NIZOZEMSKA

https://www.rijksoverheid.nl/onderwerpen/internationale-sancties

AUSTRIJA

https://www.bmeia.gv.at/themen/aussenpolitik/europa/eu-sanktionen-nationale-behoerden/

POLJSKA

https://www.gov.pl/web/dyplomacja/sankcje-miedzynarodowe

https://www.gov.pl/web/diplomacy/international-sanctions

PORTUGAL

https://www.portaldiplomatico.mne.gov.pt/politica-externa/medidas-restritivas

RUMUNJSKA

http://www.mae.ro/node/1548

SLOVENIJA

http://www.mzz.gov.si/si/omejevalni_ukrepi

SLOVAČKA

https://www.mzv.sk/europske_zalezitosti/europske_politiky-sankcie_eu

FINSKA

https://um.fi/pakotteet

ŠVEDSKA

https://www.regeringen.se/sanktioner

Adresa za slanje obavijesti Europskoj komisiji:

Europska komisija

Glavna uprava za financijsku stabilnost, financijske usluge i uniju tržišta kapitala (GU FISMA)

Rue de Spa 2

1048 Bruxelles/Brussel Belgique/België

E-pošta: relex-sanctions@ec.europa.eu