

To besedilo je zgolj informativne narave in nima pravnega učinka. Institucije Unije za njegovo vsebino ne prevzemajo nobene odgovornosti. Verodostojne različice zadevnih aktov, vključno z uvodnimi izjavami, so objavljene v Uradnem listu Evropske unije. Na voljo so na portalu EUR-Lex. Uradna besedila so neposredno dostopna prek povezav v tem dokumentu

► **B****UREDBA SVETA (EU) 2019/796**

z dne 17. maja 2019

o omejevalnih ukrepih proti kibernetским napadom, ki ogrožajo Unijo ali njene države članice

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

spremenjena z:

Uradni list

		št.	stran	datum
► <u>M1</u>	Izvedbena uredba Sveta (EU) 2020/1125 z dne 30. julija 2020	L 246	4	30.7.2020
► <u>M2</u>	Izvedbena uredba Sveta (EU) 2020/1536 z dne 22. oktobra 2020	L 351 I	1	22.10.2020
► <u>M3</u>	Izvedbena uredba Sveta (EU) 2020/1744 z dne 20. novembra 2020	L 393	1	23.11.2020

popravljen z:

- **C1** Popravek, UL L 230, 17.7.2020, str. 37 (2019/796)



UREDBA SVETA (EU) 2019/796

z dne 17. maja 2019

**o omejevalnih ukrepih proti kibernetским napadom, ki ogrožajo
Unijo ali njene države članice**

Člen 1

1. Ta uredba se uporablja za kibernetiske napade s pomembnim učinkom in na poskuse kibernetiskih napadov s potencialno pomembnim učinkom, ki pomenijo zunanjo grožnjo Uniji ali njenim državam članicam.

2. Med kibernetiske napade, ki pomenijo zunanjo grožnjo, spadajo napadi:

- (a) ki izvirajo ali so bili izvedeni iz držav zunaj Unije;
- (b) pri katerih se uporablja infrastruktura zunaj Unije;
- (c) ki jih je izvedla katera koli fizična ali pravna oseba, subjekt ali organ, ki ima sedež zunaj Unije ali ki deluje od tam ali
- (d) ki so bili izvedeni s podporo, vodenjem ali pod nadzorom katere koli fizične ali pravne osebe, subjekta ali organa, ki deluje zunaj Unije.

3. V ta namen so kibernetiski napadi dejanja, ki vključujejo kar koli od naslednjega:

- (a) dostop do informacijskih sistemov;
- (b) motnje informacijskega sistema;
- (c) poseganje v podatke ali
- (d) prestrezanje podatkov,

kadar teh dejanj ni ustrezno odobril lastnik ali drugi imetnik pravice do sistema ali podatkov oziroma do dela sistema ali podatkov ali ki jih ne dovoljuje pravo Unije ali zadevne države članice.

4. Med kibernetiskimi napadi, ki pomenijo grožnjo za državo članico, so napadi z vplivom na informacijske sisteme, ki so med drugim povezani z naslednjim:

- (a) ključno infrastrukturo, vključno s podvodnimi kablji in objekti, izstreljenimi v vesolje, ki je bistvena za ohranjanje ključnih funkcij v družbi ali zdravja, varnosti, zaščite, ekonomske ali socialne blaginje ljudi;
- (b) storitvami, potrebnimi za ohranjanje bistvenih družbenih in/ali gospodarskih dejavnosti, zlasti v sektorjih: energije (elektrika, nafta in plin); prevoza (zračni, železniški, vodni in cestni); bančništva; infrastrukture finančnega trga; zdravstva (izvajalci zdravstvene dejavnosti, bolnišnice in zasebne klinike); oskrbe s pitno vodo in njeno distribucijo; digitalne infrastrukture; in v katerem koli drugem sektorju, bistvenem za zadevno državo članico;

▼B

(c) kritičnimi državnimi funkcijami, zlasti na področjih obrambe, vodenja in delovanja institucij, vključno z javnimi volitvami in postopki glasovanja volitev, delovanja gospodarske in civilne infrastrukture, notranje varnosti in zunanjih odnosov, vključno z diplomatskimi misijami;

(d) s shranjevanjem ali obdelavo tajnih podatkov ali

(e) vladnimi skupinami za ukrepanje v izrednih razmerah.

5. Med kibernetске napade, ki pomenijo grožnjo za Unijo, spadajo napadi, izvedeni proti njenim institucijam, organom, uradom in agencijam, njenim delegacijam v tretjih državah ali mednarodnih organizacijah, operacijam in misijam v okviru skupne vojaške in obrambne politike (SVOP) in njenim posebnim predstavnikom.

6. Kadar se to zdi potrebno za doseganje ciljev v okviru skupne zunanje in varnostne politike (SZVP) iz ustreznih določb člena 21 Pogodbe o Evropski uniji, se lahko omejevalni ukrepi iz te uredbe uporabljajo tudi kot odziv na kibernetске napade, ki imajo znaten učinek na tretje države ali mednarodne organizacije.

7. V tej uredbi se uporabljajo naslednje opredelitve pojmov:

(a) „informacijski sistemi“ pomeni napravo ali skupino med seboj povezanih ali sorodnih naprav, od katerih ena ali več v skladu s programom samodejno obdeluje digitalne podatke, kakor tudi digitalne podatke, ki so shranjeni, obdelani, pridobljeni ali se po tej napravi ali skupini naprav prenašajo zaradi njenega ali njihovega delovanja, uporabe, varovanja in vzdrževanja;

(b) „motnje informacijskega sistema“ pomeni oviranje ali prekinitev delovanja informacijskega sistema z vnašanjem digitalnih podatkov, prenašanjem, poškodovanjem, brisanjem, poslabšanjem, spreminjanjem ali odstranitvijo takih podatkov ali povzročitvijo nedostopnosti takšnih podatkov;

(c) „poseganje v podatke“ pomeni brisanje, poškodovanje, poslabšanje, spreminjanje ali odstranitev digitalnih podatkov v informacijskem sistemu ali povzročitev nedostopnosti takšnih podatkov; vključuje tudi krajo podatkov, sredstev, gospodarskih virov ali intelektualne lastnine;

(d) „prestrezanje podatkov“ pomeni prestrezanje nejavnega prenosa digitalnih podatkov v informacijski sistem, iz ali znotraj njega s tehničnimi sredstvi, vključno z elektromagnetnimi emisijami iz informacijskega sistema, ki prenašajo takšne digitalne podatke.

8. V tej uredbi se uporabljajo naslednje dodatne opredelitve:

(a) „zahtevek“ pomeni vsak zahtevek, ne glede na to, ali se uveljavlja v pravnem postopku ali ne, vložen pred dnevom začetka veljavnosti te uredbe ali po njem, ki izhaja iz pogodbe ali transakcije ali je povezan s pogodbo ali transakcijo, in vključuje zlasti:

(i) zahtevek za izpolnitev katere koli obveznosti, ki izhaja iz pogodbe ali transakcije ali je v zvezi s pogodbo ali transakcijo;

(ii) zahtevek za podaljšanje dospelosti ali za plačilo obveznice, finančne garancije ali jamstva v kakršni koli obliki;

(iii) zahtevek za nadomestilo škode v zvezi s pogodbo ali transakcijo;

(iv) nasprotni zahtevek;

▼B

- (v) zahtev po priznanju ali izvršitvi, vključno s postopkom eksekvuturne, sodbe, arbitražne odločbe ali enakovredne odločitve, kjer koli je bila oblikovana ali izdana;
- (b) „pogodba ali transakcija“ pomeni vsako transakcijo v kakršni koli obliki in v okviru katere koli veljavne zakonodaje, ki vsebuje eno ali več pogodb ali podobnih obveznosti, sklenjenih med istimi ali različnimi strankami; v ta namen „pogodba“ vključuje obveznice, garancije ali jamstva, zlasti finančne garancije ali jamstva, ter kredite, ki so lahko pravno samostojni, in vse pripadajoče določbe, ki izhajajo iz transakcije ali so z njo v zvezi;
- (c) „pristojni organi“ pomeni pristojne organe držav članic, kot so opredeljeni na spletnih mestih iz Priloge II;
- (d) „gospodarski viri“ pomeni vse vrste premoženja, opredmetenega ali neopredmetenega, premičnega ali nepremičnega, ki sicer niso sredstva, se pa lahko uporabijo za pridobitev sredstev, blaga ali storitev;
- (e) „zamrznitev gospodarskih virov“ pomeni preprečitev njihove uporabe za pridobivanje sredstev, blaga ali storitev na kakršen koli način, kar vključuje njihovo prodajo, najem ali zastavo, ni pa na to omejeno;
- (f) „zamrznitev sredstev“ pomeni preprečitev vsakršnega premika, prenosa, spremembe ali uporabe sredstev, dostopa do njih ali kakršnega koli ravnanja z njimi, ki bi imelo za posledico spremembe v njihovi količini, znesku, lokaciji, lastništvu, posedovanju, vrsti ali namembnosti ali druge spremembe, ki bi omogočile uporabo sredstev, vključno z upravljanjem portfeljev;
- (g) „sredstva“ pomeni vse vrste finančnih sredstev in koristi, kar vključuje, vendar ni omejeno na:
 - (i) gotovino, čeke, denarne terjatve, menice, denarna nakazila in druge plačilne instrumente;
 - (ii) vloge pri finančnih institucijah ali drugih subjektih, stanja na računih, dolgove in dolžniške obveznosti;
 - (iii) vrednostne papirje in dolžniške instrumente, s katerimi se trguje javno ali zasebno, vključno z delnicami in deleži, certifikati vrednostnih papirjev, obveznicami, dolžniškimi vrednostnimi papirji, nakupnimi boni, zadolžnicami in pogodbami na izvedene finančne instrumente;
 - (iv) obresti, dividende ali druge dohodke iz sredstev ali vrednost, ustvarjeno s sredstvi;
 - (v) kredit, pravico do pobota, garancije, garancije za dobro izvedbo posla ali druge finančne obveznosti;
 - (vi) kreditna pisma, konosamente in kupoprodajne listine; ter
 - (vii) dokumente, ki izkazujejo upravičenost do sredstev ali finančnih virov;

▼B

- (h) „ozemlje Unije“ pomeni ozemlja držav članic, kjer se uporablja Pogodba, pod pogoji, določenimi v Pogodbi, vključno z njihovim zračnim prostorom.

Člen 2

Dejavniki, ki odločajo o tem, ali ima kibernetški napad pomemben učinek iz člena 1(1), vključujejo kar koli od naslednjega:

- (a) obseg, razsežnost, učinek ali resnost motnje, ki jih ta povzroči, vključno z gospodarskimi in družbenimi dejavnostmi, bistvenimi storitvami, kritičnimi državnimi funkcijami, javnim redom ali javno varnostjo;
- (b) število prizadetih fizičnih ali pravnih oseb, subjektov ali organov;
- (c) število zadevnih držav članic;
- (d) znesek ekonomske izgube, povzročene na primer z obsežno krajo sredstev, gospodarskih virov ali intelektualne lastnine;
- (e) gospodarska korist, ki jo pridobi storilec zase ali za druge;
- (f) količina ali značaj ukradenih podatkov ali obseg kršitev varnosti podatkov ali
- (g) značaj pridobljenih poslovno občutljivih podatkov.

Člen 3

1. Vsa sredstva in gospodarski viri, ki pripadajo, so v lasti, posesti ali pod nadzorom katere koli fizične ali pravne osebe, subjekta ali organa iz Priloge I, se zamrznejo.

2. Fizičnim ali pravnim osebam, subjektom ali organom iz Priloge I je prepovedano neposredno ali posredno dajati na razpolago ali v njihovo korist kakršna koli sredstva ali gospodarske vire.

3. Priloga I zajema, kot je določil Svet v skladu s členom 5(1) Sklepa (SZVP) 2019/797:

- (a) fizične ali pravne osebe, subjekte ali organe, ki so odgovorni za kibernetške napade ali poskuse kibernetških napadov;
- (b) fizičnih oseb ali pravnih oseb, subjektov ali organov, ki zagotavljajo finančno, tehnično ali materialno podporo ali so kako drugače vpletene v kibernetške napade ali poskuse kibernetških napadov, na primer z njihovim načrtovanjem, pripravljanjem, sodelovanjem pri njih, njihovim vodenjem, pomočjo ali spodbujanjem takih napadov ali z njihovim omogočanjem bodisi z dejanji ali opustitvijo dejanj;
- (c) fizične ali pravne osebe, subjekte ali organe, ki so povezani s fizičnimi ali pravnimi osebami, subjekti in organi, zajetimi v točkah (a) in (b) tega odstavka.

▼B

Člen 4

1. Z odstopanjem od člena 3 lahko pristojni organi držav članic odobrijo sprostitev nekaterih zamrznjenih sredstev ali gospodarskih virov ali razpolaganje z določenimi sredstvi ali gospodarskimi viri pod pogoji, ki se jim zdijo primerni, potem ko so ugotovili, da so sredstva ali gospodarski viri:

- (a) ►C1 potrebni za zadovoljitev osnovnih potreb fizičnih in pravnih oseb, subjektov ali organov s seznama iz Priloge I ◄ in vzdrževanih družinskih članov takih fizičnih oseb, vključno s plačili za živila, najemnine ali hipoteke, zdravila in zdravstveno oskrbo, davke, zavarovalne premije in za storitve javnih služb;
- (b) namenjeni izključno za plačilo razumnih honorarjev in povračilo nastalih izdatkov, povezanih z zagotavljanjem pravnih storitev;
- (c) namenjeni izključno za plačilo pristojbin ali stroškov za redno hrambo ali vzdrževanje zamrznjenih sredstev ali gospodarskih virov,
- (d) potrebni za kritje izrednih izdatkov, pod pogojem, da ustrezni pristojni organ vsaj dva tedna pred odobritvijo pristojne organe drugih držav članic in Komisijo uradno obvesti o razlogih, na podlagi katerih meni, da je treba izdati posamezno odobritev, ali
- (e) nakazani na račun ali z računa diplomatske ali konzularne misije ali mednarodne organizacije, ki ima imuniteto v skladu z mednarodnim pravom, če so takšna plačila namenjena za uradne naloge diplomatske ali konzularne misije ali mednarodne organizacije.

2. Zadevna država članica v roku dveh tednov po odobritvi obvesti druge države članice in Komisijo o vseh odobritvah, izdanih na podlagi odstavka 1.

Člen 5

1. Z odstopanjem od člena 3(1) lahko pristojni organi držav članic odobrijo sprostitev določenih zamrznjenih sredstev ali gospodarskih virov, če so izpolnjeni naslednji pogoji:

- (a) sredstva ali gospodarski viri so predmet arbitražne odločbe, izdane pred datumom, ko so bili fizična ali pravna oseba, subjekt ali organ iz člena 3 uvrščeni na seznam iz Prilogo I, ali sodne ali upravne odločbe, izdane v Uniji, ali sodne odločbe, izvršljive v zadevni državi članici, pred navedenim datumom ali po njem;
- (b) sredstva ali gospodarski viri se bodo uporabljali izključno za poravnavo terjatev, ki so zavarovane s tako odločbo ali so v taki odločbi priznane kot veljavne, v mejah, določenih z veljavno zakonodajo in predpisi, ki urejajo pravice oseb s takimi terjatvami;
- (c) odločba ni v korist fizični ali pravni osebi, subjektu ali organu iz Priloge I ter
- (d) priznanje odločbe ni v nasprotju z javnim redom zadevne države članice.

▼B

2. Zadevna država članica v roku dveh tednov po odobritvi obvesti druge države članice in Komisijo o vseh odobritvah, izdanih na podlagi odstavka 1.

Člen 6

1. Z odstopanjem od člena 3(1) in pod pogojem, da mora fizična ali pravna oseba, subjekt ali organ s seznama iz Priloge I poravnati plačilo na podlagi pogodbe ali sporazuma, ki ga je sklenila zadevna fizična ali pravna oseba, subjekt ali organ, ali obveznosti, ki je nastala za zadevno fizično ali pravno osebo, subjekt ali organ, pred dnem, ko je bila ta fizična ali pravna oseba, subjekt ali organ vključen v Prilogo I, lahko pristojni organi držav članic, pod pogoji, ki se jim zdijo primerni,odobrijo sprostitev določenih zamrznjenih sredstev ali gospodarskih virov, pod pogojem, da je zadevni pristojni organ ugotovil, da:

- (a) se sredstva ali gospodarski viri uporabijo za plačilo s strani fizične ali pravne osebe, subjekta ali organa s seznama v Prilogi I ter
- (b) plačilo ne pomeni kršitve člena 3(2).

2. Zadevna država članica v roku dveh tednov po odobritvi obvesti druge države članice in Komisijo o vseh odobritvah, izdanih na podlagi odstavka 1.

Člen 7

1. Člen 2(2) finančnim ali kreditnim institucijam, ki prejemajo finančna sredstva, ki jih tretje strani prenesejo na račune fizičnih ali pravnih oseb, subjektov ali organov s seznama, ne preprečuje kreditiranja zamrznjenih računov, pod pogojem, da se vsak priliv na tak račun tudi zamrzne. Finančne ali kreditne institucije o kakršnih koli takih transakcijah nemudoma obvestijo pristojne organe.

2. Člen 3(2) se ne uporablja za prilive na zamrznjenih računih za:

- (a) obresti ali druge dohodke na navedenih računih;
- (b) zapadla plačila po pogodbah, sporazumih ali obveznostih, ki so bili sklenjeni ali so nastali pred datumom, ko je bila fizična ali pravna oseba, subjekt ali organ iz člena 3(1) vključena v Prilogo I, ali
- (c) plačila, zapadla na podlagi sodnih, upravnih ali arbitražnih odločb, izdanih v državi članici ali izvršljivih v zadevni državi članici,

pod pogojem, da za takšne obresti, druge dohodke in plačila še naprej veljajo ukrepi iz člena 3(1).

Člen 8

1. Fizične in pravne osebe ter subjekti in organi brez poseganja v veljavna pravila glede poročanja, zaupnosti in poslovne skrivnosti:

▼B

- (a) pristojnemu organu države članice, kjer prebivajo ali imajo sedež, takoj predložijo vse informacije, ki bi olajšale skladnost s to uredbo, kot so informacije o računih in zneskih, zamrznjenih v skladu s členom 3(1), ter posredujejo take informacije Komisiji neposredno ali prek države članice ter
 - (b) sodelujejo s pristojnimi organi pri vsakršnem preverjanju informacij iz točke (a).
2. Vse dodatne informacije, ki jih Komisija prejme neposredno, se pošljejo državam članicam.
3. Vse informacije, poslane ali prejete v skladu s tem členom, se uporabljajo samo za namene, za katere so bile poslane ali prejete.

Člen 9

Prepovedano je zavestno in namerno sodelovati v dejavnostih, katerih namen ali učinek je izogibanje ukrepom iz člena 3.

Člen 10

1. Zamrznitev sredstev in gospodarskih virov ali odklonitev dajanja sredstev ali gospodarskih virov na razpolago, izvedena v dobri veri, da je tako dejanje v skladu s to uredbo, ne povzroči nikakršne odgovornosti fizične ali pravne osebe, subjekta ali organa, ki jo uveljavlja, ali njegovih predstojnikov ali uslužbencev, razen če se dokaže, da je bila zamrznitev ali zadržanje sredstev in gospodarskih virov posledica malomarnosti.
2. Če fizične ali pravne osebe, subjekti ali organi niso vedeli in niso imeli utemeljenega razloga za sum, da bi lahko s svojim ravnanjem kršili ukrepe iz te uredbe, za svoje ravnanje niso odgovorni.

Člen 11

1. V zvezi s pogodbami ali drugimi posli, katerih izvedba je bila posredno ali neposredno, v celoti ali deloma ovirana zaradi ukrepov, uvedenih v skladu s to uredbo, se ne ugotovi nobenemu zahtevku, vključno z zahtevki za nadomestilo škode ali podobnimi zahtevki te vrste, kot je odškodninski zahtevek ali zahtevek za uveljavljanje garancije, zlasti zahtevek za podaljšanje dospelosti obveznice, garancije ali jamstva, predvsem finančne garancije ali finančnega jamstva v kakršni koli obliki, ki ga zahtevajo:
- (a) fizična ali pravna oseba, subjekt ali organ s seznama iz Priloge I;
 - (b) katera koli fizična ali pravna oseba, subjekt ali organ, ki deluje prek fizičnih ali pravnih oseb, subjektov ali organov iz točke (a) ali v njihovem imenu.
2. V vseh postopkih za uveljavitev zahtevka dokazno breme, da izpolnitev zahtevka ni prepovedana z odstavkom 1, nosi fizična ali pravna oseba, subjekt ali organ, ki uveljavlja ta zahtevek.
3. Ta člen ne posega v pravico fizičnih ali pravnih oseb, subjektov in organov iz odstavka 1 do sodne presoje zakonitosti neizpolnjevanja pogodbenih obveznosti v skladu s to uredbo.

▼B*Člen 12*

1. Komisija in države članice se medsebojno obvestijo o ukrepih, sprejetih v skladu s to uredbo, in si izmenjajo vse druge relevantne informacije, ki so jim na voljo v zvezi s to uredbo, zlasti informacije o:

- (a) sredstvih, zamrznjenih v skladu s členom 3, in dovoljenjih, izdanih v skladu s členi 4, 5 in 6;
- (b) težavah v zvezi s kršitvami in pregonom ter o sodbah, ki jih izrečejo nacionalna sodišča.

2. Države članice takoj obvestijo druga drugo in Komisijo o vseh drugih relevantnih informacijah, s katerimi razpolagajo, ki bi lahko vplivale na učinkovito izvajanje te uredbe.

Člen 13

1. Če Svet odloči, da bodo za fizično ali pravno osebo, subjekt ali organ veljali ukrepi iz člena 3, ustrezno spremeni Prilogo I.

2. Svet o odločitvi iz odstavka 1, vključno z razlogi za uvrstitev na seznam, obvesti zadevno fizično ali pravno osebo, subjekt ali organ, bodisi neposredno, če je naslov znan, bodisi z objavo uradnega obvestila, s čimer da takšni fizični ali pravni osebi, subjektu ali organu možnost, da predloži pripombe.

3. Če so predložene pripombe ali tehtni novi dokazi, Svet preuči odločitev iz odstavka 1 in o tem ustrezno obvesti zadevno fizično ali pravno osebo, subjekt ali organ.

4. Seznam iz Priloge I se redno pregleduje, in sicer vsaj vsakih 12 mesecev.

5. Komisija je pooblaščenca, da spremeni Prilogo II na podlagi informacij, ki jih predložijo države članice.

Člen 14

1. Priloga I vključuje razloge za uvrstitev zadevnih fizičnih ali pravnih oseb, subjektov ali organov na seznam.

2. Priloga I vsebuje informacije, potrebne za identifikacijo zadevnih fizičnih ali pravnih oseb, subjektov ali organov, kadar so te informacije na voljo. Za fizične osebe lahko te informacije vključujejo: imena in vzdevke; datum in kraj rojstva; državljanstvo; številko potnega lista in osebne izkaznice; spol; naslov, če je znan; ter funkcijo ali poklic. Za pravne osebe, subjekte ali organe pa lahko te informacije vključujejo imena, kraj in datum vpisa, številko vpisa in sedež podjetja.

Člen 15

1. Države članice določijo pravila o kaznih za kršitve določb te uredbe in sprejmejo vse potrebne ukrepe za zagotovitev njihovega izvajanja. Te kazni morajo biti učinkovite, sorazmerne in odvračilne.

▼B

2. Države članice po začetku veljavnosti te uredbe brez odlašanja uradno obvestijo Komisijo o pravilih iz odstavka 1 in jo uradno obveščajo o vseh naknadnih spremembah.

Člen 16

1. Komisija obdeluje osebne podatke za namene opravljanja nalog, ki jih ima po tej uredbi. Te naloge zajemajo:

- (a) dodajanje vsebine Priloge I na elektronski konsolidirani seznam oseb, skupin in subjektov, za katere veljajo finančne sankcije Unije, ter na interaktivni zemljevid sankcij, ki sta javno dostopna;
- (b) obdelavo podatkov o učinku ukrepov iz te uredbe, kot so vrednost zamrznjenih sredstev in podatki o odobritvah, ki so jih izdali pristojni organi.

2. Za namene te uredbe je služba Komisije s seznama iz Priloge II določena za „upravljavca“ za Komisijo v smislu člena 3(8) Uredbe (EU) 2018/1725, da se zadevnim fizičnim osebam omogoči uveljavljanje pravic, ki jih imajo v skladu z navedeno uredbo.

Člen 17

1. Države članice imenujejo pristojne organe iz te uredbe in jih opredelijo na spletnih straneh iz Priloge II. Države članice Komisijo uradno obvestijo o vseh spremembah naslovov spletnih mest iz Priloge II.

2. Države članice po začetku veljavnosti te uredbe Komisijo brez odlašanja uradno obvestijo o svojih pristojnih organih, vključno s kontaktnimi podatki teh pristojnih organov, in jo uradno obveščajo o vseh naknadnih spremembah.

3. Kadar je v tej uredbi določena obveznost uradnega obveščanja Komisije, sporočanja ali kaknega drugega komuniciranja z njo, se za tako komunikacijo uporabljajo naslov in drugi kontaktni podatki, navedeni v Prilogi II.

Člen 18

Ta uredba se uporablja:

- (a) na ozemlju Unije, vključno z njenim zračnim prostorom;
- (b) na vsakem zrakoplovu ali plovilu, ki je v pristojnosti države članice;
- (c) za vse fizične osebe na ozemlju Unije ali zunaj njega, ki imajo državljanstvo države članice;
- (d) za vse pravne osebe, subjekte ali organe na ozemlju Unije ali zunaj njega, ki so registrirani ali ustanovljeni po pravu države članice;
- (e) za vse pravne osebe, subjekte ali organe v zvezi s katerim koli poslom, opravljenim v celoti ali delno znotraj Unije.



Člen 19

Ta uredba začne veljati dan po objavi v *Uradnem listu Evropske unije*.

Ta uredba je v celoti zavezujoča in se neposredno uporablja v vseh državah članicah.

▼ **B**

PRILOGA I

Seznam fizičnih in pravnih oseb, subjektov in organov iz člena 3

▼ **M1**

A. Fizične osebe

▼ **M3**

	Ime in priimek	Podatki za identifikacijo	Razlogi za uvrstitev na seznam	Datum uvrstitve na seznam
1.	GAO Qiang	Datum rojstva: 4. oktober 1983 Kraj rojstva: Provinca Shandong, Kitajska Naslov: Soba 1102, Guanfu Mansion, ulica Xinkai 46, okrožje Hedong, Tjandžin, Kitajska Državljanstvo: kitajsko Spol: moški	Gao Qiang je vpleten v „Operation Cloud Hopper“, vrsto kibernetских napadov s pomembnim učinkom, ki izvirajo iz držav zunaj Unije in pomenijo zunanjo grožnjo Uniji ali njenim državam članicam, ter kibernetских napadov, ki imajo pomemben učinek na tretje države. Tarča „Operation Cloud Hopper“ so bili informacijski sistemi multinacionalnih družb na šestih celinah, vključno z družbami v Uniji, pri čemer je bil pridobljen nepooblaščen dostop do komercialno občutljivih podatkov, kar je povzročilo precejšnjo ekonomsko izgubo. „Operation Cloud Hopper“ je izvedel akter, v javnosti znan kot „APT10“ („Advanced Persistent Threat 10“) (tudi „Red Apollo“, „CVNX“, „Stone Panda“, „MenuPass“ in „Potassium“). Gao Qianga je mogoče povezati z APT10, med drugim zaradi njegove povezave z infrastrukturo APT10 za poveljevanje in kontrolo. Poleg tega je bil Gao Qiang zaposlen pri Huaying Haitai, ki je subjekt, uvrščen na seznam zaradi zagotavljanja podpore in omogočanja „Operation Cloud Hopper“. Povezan je z Zhang Shilongom, ki je prav tako uvrščen na seznam v povezavi z „Operation Cloud Hopper“. Gao Qiang je torej povezan s Huaying Haitai in Zhang Shilongom.	30.7.2020
2.	ZHANG Shilong	Datum rojstva: 10. september 1981 Kraj rojstva: Kitajska Naslov: Hedong, ulica Yuyang 121, Tjandžin, Kitajska Državljanstvo: kitajsko Spol: moški	Zhang Shilong je vpleten v „Operation Cloud Hopper“, vrsto kibernetских napadov s pomembnim učinkom, ki izvirajo iz držav zunaj Unije in pomenijo zunanjo grožnjo Uniji ali njenim državam članicam, ter kibernetских napadov, ki imajo pomemben učinek na tretje države. Tarča „Operation Cloud Hopper“ so bili informacijski sistemi multinacionalnih družb na šestih celinah, vključno z družbami v Uniji, pri čemer je bil pridobljen nepooblaščen dostop do komercialno občutljivih podatkov, kar je povzročilo precejšnjo ekonomsko izgubo.	30.7.2020

▼ M3

	Ime in priimek	Podatki za identifikacijo	Razlogi za uvrstitev na seznam	Datum uvrstitve na seznam
			„Operation Cloud Hopper“ je izvedel akter, v javnosti znan kot „APT10“ („Advanced Persistent Threat 10“) (tudi „Red Apollo“, „CVNX“, „Stone Panda“, „MenuPass“ in „Potassium“). Zhang Shilong je mogoče povezati z APT10, med drugim zaradi zlonamerne programske opreme, ki jo je razvil in testiral v povezavi s kibernetскими napadi, ki jih je izvedel APT10. Poleg tega je bil Zhang Shilong zaposlen pri Huaying Haitai, ki je subjekt, uvrščen na seznam zaradi zagotavljanja podpore in omogočanja „Operation Cloud Hopper“. Povezan je z Gao Qiangom, ki je uvrščen na seznam v povezavi z „Operation Cloud Hopper“. Zhang Shilong je torej povezan s Huaying Haitai in Gao Qiangom.	

▼ M1

3.	Alexey Valeryevich MININ	Алексей Валерьевич МИНИН Datum rojstva: 27. maj 1972 Kraj rojstva: pokrajina Perm, Ruska SFSR (danes Ruska federacija) Številka potnega lista: 120017582 Izdajatelj: Ministrstvo za zunanje zadeve Ruske federacije Veljavnost: od 17. aprila 2017 do 17. aprila 2022 Lokacija: Moskva, Ruska federacija Državljanstvo: rusko Spol: moški	Alexej Minin je sodeloval pri poskusu kibernetnega napada s potencialno pomembnim učinkom na Organizacijo za prepoved kemičnega orožja (OPCW) na Nizozemskem. Kot pomožni uradnik za HUMINT (zbiranje obveščevalnih podatkov z osebnimi stiki) v Glavnem direktoratu generalštaba Oboroženih sil Ruske federacije (GU/GRU) je bil eden izmed štirih članov skupine ruskih vojaških obveščevalnih uradnikov, ki je aprila 2018 poskušala pridobiti nepooblaščen dostop do brezžičnega omrežja OPCW v Haagu (Nizozemska). Cilj poskusa kibernetnega napada je bil vdor v brezžično omrežje OPCW; če bi poskus uspel, bi to ogrozilo varnost omrežja in tekoče preiskovalno delo OPCW. Nizozemska varnostna služba za zaščito in varnost (DISS) (Militaire Inlichtingen- en Veiligheidsdienst – MIVD) je poskus kibernetnega napada ustavila in s tem preprečila resno škodo za OPCW.	30.7.2020
4.	Aleksei Sergeyvich MORENETS	Алексей Сергеевич МОРЕНЕЦ Datum rojstva: 31. julij 1977 Kraj rojstva: pokrajina Murmansk, Ruska SFSR (danes Ruska federacija) Številka potnega lista: 100135556 Izdajatelj: Ministrstvo za zunanje zadeve Ruske federacije Veljavnost: od 17. aprila 2017 do 17. aprila 2022 Lokacija: Moskva, Ruska federacija Državljanstvo: rusko Spol: moški	Aleksei Morenets je sodeloval pri poskusu kibernetnega napada s potencialno pomembnim učinkom na Organizacijo za prepoved kemičnega orožja (OPCW) na Nizozemskem. Kot kibernetni operater v Glavnem direktoratu generalštaba Oboroženih sil Ruske federacije (GU/GRU) je bil eden izmed štirih članov skupine ruskih vojaških obveščevalnih uradnikov, ki je aprila 2018 poskušala pridobiti nepooblaščen dostop do brezžičnega omrežja OPCW v Haagu (Nizozemska). Cilj poskusa kibernetnega napada je bil vdor v brezžično omrežje OPCW; če bi poskus uspel, bi to ogrozilo varnost omrežja in tekoče preiskovalno delo OPCW. Nizozemska varnostna služba za zaščito in varnost (DISS) (Militaire Inlichtingen- en Veiligheidsdienst – MIVD) je poskus kibernetnega napada ustavila in s tem preprečila resno škodo za OPCW.	30.7.2020

	Ime in priimek	Podatki za identifikacijo	Razlogi za uvrstitev na seznam	Datum uvrstitve na seznam
5.	Evgenii Mikhailovich SREBRIAKOV	Евгений Михайлович СЕРЕБРЯКОВ Datum rojstva: 26. julij 1981 Kraj rojstva: Kursk, Ruska SFSR (danes Ruska federacija) Številka potnega lista: 100135555 Izdajatelj: Ministrstvo za zunanje zadeve Ruske federacije Veljavnost: od 17. aprila 2017 do 17. aprila 2022 Lokacija: Moskva, Ruska federacija Državljanstvo: rusko Spol: moški	Evgenii Serebriakov je sodeloval pri poskusu kibernetkega napada s potencialno pomembnim učinkom na Organizacijo za prepoved kemičnega orožja (OPCW) na Nizozemskem. Kot kibernetki operater v Glavnem direktoratu generalštaba Oboroženih sil Ruske federacije (GU/GRU) je bil eden izmed štirih članov skupine ruskih vojaških obveščevalnih uradnikov, ki je aprila 2018 poskušala pridobiti nepooblaščen dostop do brezžičnega omrežja OPCW v Haagu (Nizozemska). Cilj poskusa kibernetkega napada je bil vdor v brezžično omrežje OPCW; če bi poskus uspel, bi to ogrozilo varnost omrežja in tekoče preiskovalno delo OPCW. Nizozemska varnostna služba za zaščito in varnost (DISS) (Militaire Inlichtingen- en Veiligheidsdienst – MIVD) je poskus kibernetkega napada ustavila in s tem preprečila resno škodo za OPCW.	30.7.2020
6.	Oleg Mikhailovich SOTNIKOV	Олег Михайлович СОТНИКОВ Datum rojstva: 24. avgust 1972 Kraj rojstva: Uljanovsk, Ruska SFSR (danes Ruska federacija) Številka potnega lista: 120018866 Izdajatelj: Ministrstvo za zunanje zadeve Ruske federacije Veljavnost: od 17. aprila 2017 do 17. aprila 2022 Lokacija: Moskva, Ruska federacija Državljanstvo: rusko Spol: moški	Oleg Sotnikov je sodeloval pri poskusu kibernetkega napada s potencialno pomembnim učinkom na Organizacijo za prepoved kemičnega orožja (OPCW) na Nizozemskem. Kot pomožni uradnik za HUMINT (zbiranje obveščevalnih podatkov z osebnimi stiki) v Glavnem direktoratu generalštaba Oboroženih sil Ruske federacije (GU/GRU) je bil eden izmed štirih članov skupine ruskih vojaških obveščevalnih uradnikov, ki je aprila 2018 poskušala pridobiti nepooblaščen dostop do brezžičnega omrežja OPCW v Haagu (Nizozemska). Cilj poskusa kibernetkega napada je bil vdor v brezžično omrežje OPCW; če bi poskus uspel, bi to ogrozilo varnost omrežja in tekoče preiskovalno delo OPCW. Nizozemska varnostna služba za zaščito in varnost (DISS) (Militaire Inlichtingen- en Veiligheidsdienst – MIVD) je poskus kibernetkega napada ustavila in s tem preprečila resno škodo za OPCW.	30.7.2020

▼ M1

▼ M2

	Ime in priimek	Podatki za identifikacijo	Razlogi za uvrstitev na seznam	Datum uvrstitve na seznam
7.	Dmitry Sergeyevich BADIN	Дмитрий Сергеевич Бадин Datum rojstva: 15. november 1990 Kraj rojstva: Kursk, Ruska SFSR (danes Ruska federacija) Državljanstvo: rusko Spol: moški	Dmitry Badin je sodeloval v kibernetnem napadu s pomembnim učinkom proti nemškemu zveznemu parlamentu (<i>Deutscher Bundestag</i>). Kot vojaški obveščevalni uradnik 85. glavnega centra za posebne storitve (GTsSS) Glavnega direktorata generalštaba Oboroženih sil Ruske federacije (GU/GRU) je bil Dmitry Badin član skupine ruskih vojaških obveščevalnih uradnikov, ki je aprila in maja 2015 izvedla kibernetni napad na nemški zvezni parlament (<i>Deutscher Bundestag</i>). Cilj tega kibernetnega napada je bil informacijski sistem parlamenta, katerega delovanje je bilo nato več dni prizadeto. Ukradena je bila znatna količina podatkov, prav tako pa so bili prizadeti e-poštni računi več poslancev, tudi kanclerke Angele Merkel.	22.10.2020
8.	Igor Olegovich KOSTYUKOV	Игорь Олегович Костюков Datum rojstva: 21. februar 1961 Državljanstvo: rusko Spol: moški	Igor Kostyukov je trenutno vodja Glavnega direktorata generalštaba Oboroženih sil Ruske federacije (GU/GRU), pred tem pa je bil prvi namestnik vodje. Ena od enot pod njegovim poveljstvom je 85. glavni center za posebne storitve (GTsSS), znan tudi kot „vojaška enota 26165“ (vzdevki v okviru panoge: „APT28“, „Fancy Bear“, „Sofacy Group“, „Pawn Storm“ in „Strontium“). V tej vlogi je Igor Kostyukov odgovoren za kibernetne napade, ki jih je izvedel GTsSS, tudi tiste s pomembnim učinkom, ki pomenijo zunanjo grožnjo Uniji ali njenim državam članicam. Vojaški obveščevalni uradniki GTsSS so sodelovali zlasti v kibernetnem napadu na nemški zvezni parlament (<i>Deutscher Bundestag</i>), izveden aprila in maja 2015, in v poskusu kibernetnega napada, katerega cilj je bil vdor v brezžično omrežje Organizacije za prepoved kemičnega orožja (OPCW) na Nizozemskem aprila 2018. Cilj kibernetnega napada na nemški zvezni parlament je bil informacijski sistem parlamenta, katerega delovanje je bilo nato več dni prizadeto. Ukradena je bila znatna količina podatkov, prav tako pa so bili prizadeti e-poštni računi več poslancev, tudi kanclerke Angele Merkel.	22.10.2020

▼ M1

B. Pravne osebe, subjekti in organi:

	Ime	Podatki za identifikacijo	Razlogi za uvrstitev na seznam	Datum uvrstitve na seznam
1.	Tianjin Huaying Haitai Science and Technology Development Co. Ltd (Huaying Haitai)	tudi: Haitai Technology Development Co. Ltd Lokacija: Tjandžin, Kitajska	Huaying Haitai je omogočil in zagotovil finančno, tehnično ali materialno podporo za „Operation Cloud Hopper“, vrsto kibernetских napadov s pomembnim učinkom, ki izvirajo iz držav zunaj Unije in pomenijo zunanjo grožnjo Uniji ali njenim državam članicam, ter kibernetских napadov, ki imajo pomemben učinek na tretje države. Tarča „Operation Cloud Hopper“ so bili informacijski sistemi multinacionalnih družb na šestih celinah, vključno z družbami v Uniji, pri čemer je bil pridobljen nepooblaščen dostop do komercialno občutljivih podatkov, kar je povzročilo precejšnjo ekonomsko izgubo. „Operation Cloud Hopper“ je izvedel akter, v javnosti znan kot „APT10“ („Advanced Persistent Threat 10“) (tudi „Red Apollo“, „CVNX“, „Stone Panda“, „MenuPass“ in „Potassium“). Huaying Haitai je mogoče povezati z APT10. Poleg tega sta bila pri Huaying Haitai zaposlena Gao Qiang in Zhang Shilong, ki sta oba uvrščena na seznam v povezavi z „Operation Cloud Hopper“. Huaying Haitai je torej povezan z Gao Qiangom in Zhang Shilongom.	30.7.2020
2.	Chosun Expo	tudi: Chosen Expo; Korea Export Joint Venture Lokacija: DLRK	Chosun Expo je omogočil in zagotovil finančno, tehnično ali materialno podporo za vrsto kibernetских napadov s pomembnim učinkom, ki izvirajo iz držav zunaj Unije in pomenijo zunanjo grožnjo Uniji ali njenim državam članicam, ter kibernetских napadov, ki imajo pomemben učinek na tretje države, vključno s kibernetскими napadi, v javnosti znanimi kot „WannaCry“, in kibernetскими napadi na poljski finančni nadzorni organ in Sony Pictures Entertainment, pa tudi kibernetisko krajo centralne banke Bangladeša in poskus kibernetiske kraje vietnamske banke Tien Phong. „WannaCry“ je z izsiljevalskim virusom in onemogočanjem dostopa do podatkov povzročil motnje v informacijskih sistemih po vsem svetu. Prizadel je informacijske sisteme družb v Uniji, tudi informacijske sisteme, povezane s storitvami, potrebnimi za vzdrževanje osnovnih storitev in gospodarskih dejavnosti v državah članicah.	30.7.2020

▼ M1

	Ime	Podatki za identifikacijo	Razlogi za uvrstitev na seznam	Datum uvrstitve na seznam
			„WannaCry“ je izvedel akter, v javnosti znan kot „APT38“ („Advanced persistent Threat 38“) ali „Lazarus Group“. Chosun Expo je mogoče povezati z APT38/Lazarus Group, tudi prek uporabniških računov, ki so bili uporabljeni za kibernetške napade.	
3.	Glavni center za posebne tehnologije (GTsST) Glavnega direktorata generalštaba Oboroženih sil Ruske federacije (GU/GRU)	Naslov: Kirova ulica 22, Moskva, Ruska federacija	Glavni center za posebne tehnologije (GTsST) Glavnega direktorata generalštaba Oboroženih sil Ruske federacije (GU/GRU), v javnosti znan tudi kot poštni predal 74455, je odgovoren za kibernetške napade s pomembnim učinkom, ki izvirajo iz držav zunaj Unije in pomenijo zunanjo grožnjo Uniji ali njenim državam članicam, ter kibernetške napade, ki imajo pomemben učinek na tretje države, vključno s kibernetiskima napadoma junija 2017, v javnosti znanima kot „NotPetya“ ali „EternalPetya“, in kibernetiskimi napadi na ukrajinsko električno omrežje pozimi leta 2015 in 2016. „NotPetya“ ali „EternalPetya“ sta z izsiljevalskim virusom in onemogočenjem dostopa do podatkov onemogočila dostop do podatkov v številnih družbah v Uniji, širši Evropi in po svetu, kar je med drugim povzročilo precejšnjo ekonomsko izgubo. Zaradi kibernetkega napada na ukrajinsko električno omrežje je pozimi prišlo do delnega izpada tega omrežja. „NotPetya“ ali „EternalPetya“ je izvedel akter, v javnosti znan kot „Sandworm“ (tudi „Sandworm Team“, „BlackEnergy Group“, „Voodoo Bear“, „Quedagh“, „Olympic Destroyer“ in „Telebots“), ki je odgovoren tudi za napad na ukrajinsko električno omrežje. Glavni center za posebne tehnologije pri Glavnem direktoratu generalštaba Oboroženih sil Ruske federacije dejavno sodeluje pri kibernetiskih dejavnostih, ki jih izvaja Sandworm, in ga je mogoče povezati s Sandwormom.	30.7.2020

▼ M1

	Ime	Podatki za identifikacijo	Razlogi za uvrstitev na seznam	Datum uvrstitve na seznam
▼ <u>M2</u>				
4.	85. glavni center za posebne storitve (GTsSS) Glavnega direktorata generalštaba Oboroženih sil Ruske federacije (GU/GRU)	Naslov: Komsomol'skiy Prospekt, 20, Moskva, 119146, Ruska federacija	85. glavni center za posebne storitve (GTsSS) Glavnega direktorata generalštaba Oboroženih sil Ruske federacije (GU/GRU), znan tudi kot „vojaška enota 26165“ (vzdevki v okviru panoge: „APT28“, „Fancy Bear“, „Sofacy Group“, „Pawn Storm“ in „Strontium“), je odgovoren za kibernetične napade s pomembnim učinkom, ki pomenijo zunanjo grožnjo Uniji ali njenim državam članicam. Vojaški obveščevalni uradniki GTsSS so sodelovali zlasti v kibernetičnem napadu na nemški zvezni parlament (<i>Deutscher Bundestag</i>), izveden aprila in maja 2015, in v poskusu kibernetičnega napada, katerega cilj je bil vdor v brezžično omrežje Organizacije za prepoved kemičnega orožja (OPCW) na Nizozemskem aprila 2018. Cilj kibernetičnega napada na nemški zvezni parlament je bil informacijski sistem parlamenta, katerega delovanje je bilo nato več dni prizadeto. Ukradena je bila znatna količina podatkov, prav tako pa so bili prizadeti e-poštni računi več poslancev, tudi kanclerke Angele Merkel.	22.10.2020



PRILOGA II

Spletna mesta za informacije o pristojnih organih in naslov za pošiljanje uradnih obvestil Komisiji

BELGIJA

https://diplomatie.belgium.be/nl/Beleid/beleidsthemas/vrede_en_veiligheid/sancties

https://diplomatie.belgium.be/fr/politique/themes_politiques/paix_et_securite/sanctions

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

BOLGARIJA

<https://www.mfa.bg/en/101>

ČEŠKA

www.financnianalytickurad.cz/mezinarodni-sankce.html

DANSKA

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

NEMČIJA

<http://www.bmwi.de/DE/Themen/Aussenwirtschaft/aussenwirtschaftsrecht,did=404888.html>

ESTONIJA

http://www.vm.ee/est/kat_622/

IRSKA

<http://www.dfa.ie/home/index.aspx?id=28519>

GRČIJA

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

ŠPANIJA

<http://www.exteriores.gob.es/Portal/en/PoliticaExteriorCooperacion/GlobalizacionOportunidadesRiesgos/Paginas/SancionesInternacionales.aspx>

FRANCIJA

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

HRVAŠKA

<http://www.mvep.hr/sankcije>

ITALIJA

https://www.esteri.it/mae/it/politica_estera/politica_europea/misure_deroghe

CIPER

http://www.mfa.gov.cy/mfa/mfa2016.nsf/mfa35_en/mfa35_en?OpenDocument

LATVIJA

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

LITVA

<http://www.urm.lt/sanctions>



LUKSEMBURG

<https://maec.gouvernement.lu/fr/directions-du-ministere/affaires-europeennes/mesures-restrictives.html>

MADŽARSKA

http://www.kormany.hu/download/9/2a/f0000/EU%20szankci%C3%B3s%20t%C3%A1j%C3%A9koztat%C3%B3_20170214_final.pdf

MALTA

<https://foreignaffairs.gov.mt/en/Government/SMB/Pages/Sanctions-Monitoring-Board.aspx>

NIZOZEMSKA

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

AVSTRIJA

http://www.bmeia.gv.at/view.php3?f_id=12750&LNG=en&version=

POLJSKA

<https://www.gov.pl/web/dyplomacja>

PORTUGALSKA

<http://www.portugal.gov.pt/pt/ministerios/mne/quero-saber-mais/sobre-o-ministerio/medidas-restritivas/medidas-restritivas.aspx>

ROMUNIJA

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

SLOVENIJA

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

SLOVAŠKA

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

FINSKA

<http://formin.finland.fi/kvyhteisty/pakotteet>

ŠVEDSKA

<http://www.ud.se/sanktioner>

ZDRUŽENO KRALJESTVO

<https://www.gov.uk/sanctions-embargoes-and-restrictions>

Naslov za pošiljanje uradnih obvestil Evropski komisiji:

European Commission
Service for Foreign Policy Instruments (FPI)
EEAS 07/99
1049 Bruxelles/Brussel, BELGIQUE/BELGIË
e-naslov: relex-sanctions@ec.europa.eu