SKLEPI

SKLEP SVETA (SZVP) 2019/797

z dne 17. maja 2019

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

SVET EVROPSKE UNIJE JE –

ob upoštevanju Pogodbe o Evropski uniji in zlasti člena 29 Pogodbe,

ob upoštevanju predloga visokega predstavnika Unije za zunanje zadeve in varnostno politiko,

ob upoštevanju naslednjega:

(1) Svet je 19. junija 2017 sprejel sklepe o okviru za skupen diplomatski odziv EU na zlonamerne kibernetske dejavnosti (v nadaljnjem besedilu: zbirka orodij za kibernetsko diplomacijo), v katerih je izrazil zaskrbljenost zaradi vedno večje sposobnosti in pripravljenosti državnih in nedržavnih akterjev, da svoje cilje dosegajo z zlonamernimi kibernetskimi dejavnostmi, ter potrdil vse večjo potrebo po zaščiti celovitosti in varnosti Unije, njenih držav članic in državljanov pred kibernetskimi grožnjami in zlonamernimi kibernetskimi dejavnostmi.

(2) Svet je poudaril, da jasno opozarjanje na verjetne posledice skupnega diplomatskega odziva Unije na takšne zlonamerne kibernetske dejavnosti vpliva na ravnanje potencialnih storilcev v kibernetskem prostoru in tako krepi varnost Unije in njenih držav članic. Svet je prav tako potrdil, da so ukrepi v okviru skupne zunanje in varnostne politike (SZVP), po potrebi pa tudi omejevalni ukrepi, sprejeti na podlagi ustreznih določb iz Pogodb, primerni za okvir za skupen diplomatski odziv Unije na zlonamerne kibernetske dejavnosti ter da je njihov namen spodbujati sodelovanje, prispevati k zmanjšanju takojšnjih in dolgoročnih groženj in vplivati na ravnanje potencialnih napadalcev na dolgi rok.

(3) Politični in varnostni odbor je 11. oktobra 2017 odobril izvedbene smernice za zbirko orodij za kibernetsko diplomacijo. Izvedbene smernice se navezujejo na pet kategorij ukrepov iz zbirke orodij za kibernetsko diplomacijo, tudi na omejevalne ukrepe, in na postopek za uporabo teh ukrepov.

(4) Svet je v sklepih z dne 16. aprila 2018 o zlonamernih kibernetskih dejavnostih ostro obsodil zlonamerno uporabo informacijskih in komunikacijskih tehnologij (IKT) ter poudaril, da je zlonamerna uporaba IKT nesprejemljiva, saj ogroža stabilnost in varnost ter spodkopava prednosti interneta in uporabe IKT. Poleg tega je opozoril, da zbirka orodij za kibernetsko diplomacijo prispeva k preprečevanju konfliktov, sodelovanju in stabilnosti v kibernetskem prostoru, saj v okviru SZVP opredeljuje ukrepe, tudi omejevalne, ki jih je mogoče uporabiti za preprečevanje zlonamernih kibernetskih dejavnosti in v odziv nanje. Navedel je, da bo Unija še naprej odločno zastopala stališče, da obstoječe mednarodno pravo velja tudi za kibernetski prostor, in poudaril, da je spoštovanje mednarodnega prava, zlasti Ustanovne listine Združenih narodov, bistveno za ohranjanje miru in stabilnosti. Svet je poleg tega posebej poudaril, da države ne smejo uporabljati posredniških strežnikov za izvajanje mednarodnih kršitev z uporabo IKT in da bi si morale prizadevati zagotoviti, da nedržavni akterji za takšna dejanja ne bodo uporabljali njihovega ozemlja, kot je navedeno v poročilu skupin vladnih strokovnjakov v okviru Združenih narodov za razvoj na področju informacij in telekomunikacij v kontekstu mednarodne varnosti za leto 2015.

(5) Evropski svet je 28. junija 2018 sprejel sklepe, v katerih je poudaril, da je treba okrepiti zmogljivosti za zaščito pred kibernetskimi grožnjami iz držav zunaj Unije. Institucije in države članice je pozval, naj izvedejo ukrepe iz skupnega sporočila Komisije in visoke predstavnice Evropskemu parlamentu, Evropskemu svetu in Svetu z dne 13. junija 2018 z naslovom „Povečanje odpornosti in krepitev zmogljivosti za obravnavanje hibridnih groženj“, vključno s praktično uporabo zbirke orodij za kibernetsko diplomacijo.

(6) Evropski svet je 18. oktobra 2018 sprejel sklepe, v katerih je pozval k vzpostavitvi zmogljivosti za odzivanje na kibernetske napade in odvračanje od njih, in sicer z omejevalnimi ukrepi Unije, ki se sprejmejo na podlagi sklepov Sveta z dne 19. junija 2017.

(7) Zato ta sklep vzpostavlja okvir za ciljno usmerjene omejevalne ukrepe za odvračanje od kibernetskih napadov s pomembnim učinkom in odzivanje nanje, ki pomenijo zunanjo grožnjo Uniji ali njenim državam članicam. Kadar se to zdi potrebno za doseganje ciljev SZVP iz ustreznih določb člena 21 Pogodbe o Evropski uniji, ta sklep omogoča, da se lahko omejevalni ukrepi uporabljajo kot odziv na kibernetske napade, ki imajo pomemben učinek na tretje države ali mednarodne organizacije.

(8) Da bi ciljno usmerjeni omejevalni ukrepi bili svarilo in bi imeli odvračilni učinek, bi morali biti usmerjeni na namerno izpeljane kibernetske napade, ki spadajo v področje uporabe tega sklepa.

(9) Ciljno usmerjene omejevalne ukrepe bi bilo treba razlikovati od pripisovanja odgovornosti tretji državi za kibernetske napade. Pri uporabi ciljno usmerjenih omejevalnih ukrepov ne gre za pripisovanje takšne odgovornosti, ker gre v slednjem primeru za suvereno politično odločitev, ki se sprejme za vsak primer posebej. Vsaka država članica lahko sama odloča glede pripisovanja odgovornosti za kibernetski napad tretji državi.

(10) Za izvajanje nekaterih ukrepov je potrebno nadaljnje ukrepanje Unije –

SPREJEL NASLEDNJI SKLEP:

Člen 1

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

2. Med kibernetske 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 tem sklepu so kibernetski 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 kibernetske napade, ki pomenijo grožnjo za državo članico, spadajo napadi z vplivom na informacijske sisteme, ki so med drugim povezani z naslednjim:

(a) ključno infrastrukturo, vključno s podvodnimi kabli 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, zlati 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;

(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 kibernetske 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 SZVP iz ustreznih določb člena 21 Pogodbe o Evropski uniji, se lahko omejevalni ukrepi iz tega sklepa uporabljajo tudi kot odziv na kibernetske napade, ki imajo znaten učinek na tretje države ali mednarodne organizacije.

Člen 2

V tem sklepu 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.

Člen 3

Dejavniki, ki odločajo o tem, ali ima kibernetski 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 fizičnh 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 4

1. Države članice sprejmejo potrebne ukrepe, da preprečijo vstop na svoja ozemlja ali tranzit preko njega:

(a) fizičnim osebam, ki so odgovorne za kibernetske napade ali poskuse kibernetskih napadov;

(b) fizičnim osebam, ki zagotavljajo finančno, tehnično ali materialno podporo ali so kako drugače vpletene v kibernetske napade ali poskuse kibernetskih 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) fizičnim osebam, povezanim z osebami iz točk (a) in (b);

kot so navedene v Prilogi.

2. Odstavek 1 držav članic ne zavezuje k temu, da bi lastnim državljanom zavrnile vstop na svoje ozemlje.

3. Odstavek 1 ne posega v primere, v katerih posamezno državo članico zavezuje mednarodnopravna obveznost, in sicer:

(a) kot državo gostiteljico mednarodne medvladne organizacije;

(b) kot državo gostiteljico mednarodne konference, ki jo skliče OZN ali katere pokroviteljica je OZN;

(c) v skladu z večstranskim sporazumom o dodeljenih privilegijih in imunitetah, ali

(d) v okviru Lateranske pogodbe, ki sta jo leta 1929 sklenila Sveti sedež (Vatikanska mestna država) in Italija.

4. Za odstavek 3 se šteje, da se uporablja tudi, kadar je država članica gostiteljica Organizacije za varnost in sodelovanje v Evropi (OVSE).

5. Svet je ustrezno obveščen vsakič, ko posamezna država članica odobri izjemo v skladu z odstavkom 3 ali 4.

6. Države članice lahko odobrijo izjeme od ukrepov, uvedenih na podlagi odstavka 1, kadar je potovanje upravičeno zaradi nujnih humanitarnih potreb ali udeležbe na medvladnih srečanjih ali srečanjih, ki jih podpira ali gosti Unija ali ki jih gosti država članica, ki predseduje OVSE, in na katerih poteka politični dialog za neposredno spodbujanje uresničevanja ciljev politike omejevalnih ukrepov, vključno z varnostjo in stabilnostjo v kibernetskem prostoru.

7. Države članice lahko odobrijo izjeme od ukrepov, uvedenih na podlagi odstavka 1, kadar je vstop ali tranzit potreben zaradi izvedbe sodnega postopka.

8. Država članica, ki želi odobriti izvzetje iz odstavka 6 ali 7, o tem pisno uradno obvesti Svet. Izvzetje se šteje za odobreno, razen če eden ali več članov Sveta vloži pisni ugovor v dveh delovnih dneh po prejemu uradnega obvestila o predlaganem izvzetju. Če en ali več članov Sveta vloži ugovor, lahko Svet s kvalificirano večino odloči, da se predlagano izvzetje odobri.

9. Kadar država članica na podlagi odstavkov 3, 4, 6, 7 ali 8 osebam s seznama iz Priloge odobri vstop na svoje ozemlje ali tranzit preko njega, je odobritev strogo omejena na namen, za katerega je bila podeljena, in na osebe, na katere se neposredno nanaša.

Člen 5

1. Zamrznejo se vsa sredstva in gospodarski viri, ki pripadajo, so v lasti ali pod nadzorom:

(a) fizičnih ali pravnih oseb, subjektov ali organov, ki so odgovorni za kibernetske napade ali poskuse kibernetskih napadov;

(b) fizičnih ali pravnih oseb, subjektov ali organov, ki zagotavljajo finančno, tehnično ali materialno podporo ali so kako drugače vpletene v kibernetske napade ali poskuse kibernetskih 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) fizičnih ali pravnih oseb, subjektov ali organov, ki so povezani s fizičnimi ali pravnimi osebami, subjekti ali organi iz točk (a) in (b),

kot so navedeni v Prilogi.

2. Fizičnim ali pravnim osebam, subjektom ali organom s seznama iz Priloge ne smejo biti neposredno ali posredno dana na razpolago ali v njihovo korist nikakršna sredstva ali gospodarski viri.

3. Z odstopanjem od odstavkov 1 in 2 lahko pristojni organi držav članic pod takšnimi pogoji, za katere menijo, da so primerni, odobrijo sprostitev določenih zamrznjenih sredstev ali gospodarskih virov ali razpolaganje z njimi, potem ko so ugotovili, da so sredstva ali gospodarski viri:

(a) nujni za osnovne potrebe fizičnih oseb s seznama iz Priloge in vzdrževanih družinskih članov takih fizičnih oseb, vključno s plačili za živila, najemnine ali hipoteke, zdravila in zdravljenje, davke, zavarovalne premije in pristojbine za storitve javne komunale;

(b) namenjeni izključno za plačilo razumnih honorarjev ali nadomestil nastalih izdatkov, povezanih z zagotavljanjem pravnih storitev;

(c) namenjeni izključno za plačilo honorarjev ali stroškov storitev za redno hranjenje ali vzdrževanje zamrznjenih sredstev ali gospodarskih virov;

(d) potrebni za kritje izrednih izdatkov, če ustrezni pristojni organ vsaj dva tedna pred odobritvijo pristojnim organom drugih držav članic in Komisiji uradno sporoči razloge, 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 taka plačila namenjena za uradne naloge diplomatske ali konzularne misije ali mednarodne organizacije.

Zadevna država članica obvesti druge države članice in Komisijo o vseh odobritvah, izdanih na podlagi tega odstavka.

4. Z odstopanjem od odstavka 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 uvrstitve fizične ali pravne osebe, subjekta ali organa iz odstavka 1 na seznam iz Priloge, 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 fizične ali pravne osebe, subjekta ali organa s seznama iz Priloge ter

(d) priznanje odločbe ni v nasprotju z javnim redom zadevne države članice.

Zadevna država članica obvesti druge države članice in Komisijo o vseh odobritvah, izdanih na podlagi tega odstavka.

5. Odstavek 1 fizični ali pravni osebi, subjektu ali organu s seznama iz Priloge ne preprečuje, da bi izvedel plačilo, zapadlo po pogodbi, ki je bila sklenjena pred datumom uvrstitve navedene fizične ali pravne osebe, subjekta ali organa na seznam v navedeni prilogi, pod pogojem, da je zadevna država članica ugotovila, da plačila neposredno ali posredno ne prejme fizična ali pravna oseba, subjekt ali organ iz odstavka 1.

6. Odstavek 2 se ne uporablja za prilive na zamrznjene račune, ki so:

(a) obresti ali drugi dohodki na navedenih računih;

(b) zapadla plačila po pogodbah, sporazumih ali obveznostih, sklenjenih ali nastalih pred datumom, ko so za te račune začeli veljati ukrepi iz odstavkov 1 in 2, ali

(c) zapadla plačila po sodnih, upravnih ali arbitražnih odločbah, izdanih v Uniji ali izvršljivih v zadevni državi članici,

pod pogojem, da za vse takšne obresti, druge dohodke in plačila še naprej veljajo ukrepi iz odstavka 1.

Člen 6

1. Svet na predlog države članice ali visokega predstavnika Unije za zunanje zadeve in varnostno politiko soglasno pripravi oziroma spremeni seznam iz Priloge.

2. Svet o sklepu 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 obvestila, s čimer da navedeni fizični ali pravni osebi, subjektu ali organu možnost, da predloži pripombe.

3. Kadar so predložene pripombe ali so predstavljeni novi tehtni dokazi, Svet pregleda sklep iz odstavka 1 in o tem ustrezno obvesti zadevno fizično ali pravno osebo, subjekt ali organ.

Člen 7

1. Priloga vključuje razloge za uvrstitev na seznam fizičnih in pravnih oseb, subjektov in organov iz členov 4 in 5.

2. Priloga 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 lahko te informacije vključujejo imena, kraj in datum registracije, matično številko in sedež podjetja.

Člen 8

V zvezi s kakršno koli pogodbo ali transakcijo, katere izvedba je bila neposredno ali posredno v celoti ali deloma ovirana zaradi ukrepov, uvedenih v skladu s tem sklepom, vključno z zahtevki za nadomestilo škode ali kakršnimi koli drugimi zahtevki te vrste, kot je odškodninski zahtevek ali zahtevek za uveljavljanje garancije, zlasti zahtevek za podaljšanje dospelosti ali za plačilo obveznice, garancije ali nadomestilo škode, zlasti finančne garancije ali finančnega jamstva v kakršni koli obliki, se ne ugodi nobenemu zahtevku, če ga vložijo:

(a) fizične ali pravne osebe, subjekti ali organi, uvrščeni na seznam iz Priloge,

(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.

Člen 9

Da bi bili ukrepi, določeni v tem sklepu, čim bolj učinkoviti, Unija spodbuja tretje države k sprejetju omejevalnih ukrepov, podobnih tistim, ki so določeni v tem sklepu.

Člen 10

Ta sklep se uporablja do 18. maja 2020 in se redno pregleduje. Če Svet meni, da njegovi cilji niso bili doseženi, ga po potrebi obnovi ali spremeni.

Člen 11

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

V Bruslju, 17. maja 2019

Za Svet

Predsednik

E.O. TEODOROVICI

PRILOGA

Seznam fizičnih in pravih oseb, subjektov in organov iz členov 4 in 5

[…]