AFGØRELSER

RÅDETS AFGØRELSE (FUSP) 2019/797

af 17. maj 2019

om restriktive foranstaltninger til bekæmpelse af cyberangreb, der truer Unionen eller dens medlemsstater

RÅDET FOR DEN EUROPÆISKE UNION HAR —

under henvisning til traktaten om Den Europæiske Union, særlig artikel 29,

under henvisning til forslag fra Unionens højtstående repræsentant for udenrigsanliggender og sikkerhedspolitik, og

ud fra følgende betragtninger:

(1) Den 19. juni 2017 vedtog Rådet konklusioner om en ramme for fælles diplomatiske reaktion på ondsindede cyberaktiviteter (»cyberdiplomatisk værktøjskasse«), hvori Rådet gav udtryk for sin bekymring over statslige og ikkestatslige aktørers øgede evne og vilje til at forfølge deres mål ved at foretage ondsindede cyberaktiviteter og bekræftede det stigende behov for at beskytte integriteten og sikkerheden for Unionen og dens medlemsstater og deres borgere mod cybertrusler og ondsindede cyberaktiviteter.

(2) Rådet understregede, at et klart signal om de sandsynlige konsekvenser af Unionens fælles diplomatiske reaktion på sådanne ondsindede cyberaktiviteter påvirker adfærden hos potentielle udøvere af ondsindede cyberaktiviteter og derfor styrker sikkerheden for Unionen og dens medlemsstater. Det bekræftede også, at foranstaltninger inden for den fælles udenrigs- og sikkerhedspolitik (FUSP), herunder om nødvendigt restriktive foranstaltninger vedtaget i henhold til de relevante bestemmelser i traktaterne, kan anvendes til en ramme for Unionens fælles diplomatiske reaktion på ondsindede cyberaktiviteter med det formål at fremme samarbejde, lette afværgelse af umiddelbare og langsigtede trusler og påvirke adfærden hos potentielle udøvere af ondsindede cyberaktiviteter på lang sigt.

(3) Den 11. oktober 2017 blev retningslinjerne for gennemførelse af den cyberdiplomatiske værktøjskasse godkendt af Den Udenrigs- og Sikkerhedspolitiske Komité. Retningslinjerne for gennemførelse vedrører fem kategorier af foranstaltninger, herunder restriktive foranstaltninger, i den cyberdiplomatiske værktøjskasse og processen til at bringe disse foranstaltninger i anvendelse.

(4) Rådets konklusioner vedtaget den 16. april 2018 om ondsindede cyberaktiviteter fordømte kraftigt den ondsindede brug af informations- og kommunikationsteknologier (IKT'er) og understregede, at brug af IKT'er til ondsindede formål er uacceptabel, idet det undergraver den stabilitet og sikkerhed samt de fordele, som internettet og brugen af IKT'er giver. Rådet mindede om, at den cyberdiplomatiske værktøjskasse bidrager til forebyggelse af konflikter og til samarbejde og stabilitet i cyberspace ved at anføre foranstaltninger inden for FUSP, herunder restriktive foranstaltninger, der kan anvendes til at forebygge og imødegå ondsindede cyberaktiviteter. Det erklærede, at Unionen fortsat bestemt vil fastholde, at den eksisterende folkeret er gældende for cyberspace, og understregede, at respekten for folkeretten, navnlig FN-pagten, er afgørende for at opretholde fred og stabilitet. Rådet understregede også, at stater ikke må bruge stedfortrædere til at begå internationalt retsstridige handlinger ved hjælp af IKT'er og bør søge at sikre, at deres område ikke anvendes af ikkestatslige aktører til at begå sådanne handlinger som udtrykt i rapporten fra 2015 fra FN's grupper af regeringseksperter inden for information og telekommunikation i forbindelse med international sikkerhed.

(5) Den 28. juni 2018 vedtog Det Europæiske Råd konklusioner, der understregede behovet for at styrke kapaciteter mod cybersikkerhedstrusler fra områder uden for Unionen. Det Europæiske Råd anmodede institutionerne og medlemsstaterne om at gennemføre foranstaltningerne i den fælles meddelelse fra Kommissionen og Unionens højtstående repræsentant for udenrigsanliggender og sikkerhedspolitik af 13. juni 2018 med titlen »Øget modstandsdygtighed og bedre kapacitet til at imødegå hybride trusler«, herunder anvendelsen af den cyberdiplomatiske værktøjskasse, i praksis.

(6) Den 18. oktober 2018 vedtog Det Europæiske Råd konklusioner, hvori det opfordrede til at fremme arbejdet med kapaciteten til at reagere på og afskrække fra cyberangreb gennem Unionens restriktive foranstaltninger i forlængelse af Rådets konklusioner af 19. juni 2017.

(7) I den forbindelse etablerer denne afgørelse en ramme for målrettede restriktive foranstaltninger til at afværge og reagere på cyberangreb med betydelige konsekvenser, der udgør en ekstern trussel mod Unionen eller dens medlemsstater. Hvis det skønnes nødvendigt for at nå FUSP-målene i de relevante bestemmelser i artikel 21 i traktaten om Den Europæiske Union, kan restriktive foranstaltninger også anvendes som reaktion på cyberangreb med betydelige konsekvenser over for tredjelande eller internationale organisationer.

(8) For at få en præventiv og afskrækkende virkning bør de målrettede restriktive foranstaltninger fokusere på de cyberangreb, der er omfattet af denne afgørelse, og som er foretaget forsætligt.

(9) Der bør skelnes mellem målrettede restriktive foranstaltninger og henregnelsen af ansvaret for cyberangreb til et tredjeland. Anvendelsen af målrettede restriktive foranstaltninger udgør ikke en sådan henregnelse af ansvar, som er en suveræn politisk afgørelse, der træffes fra sag til sag. Hver medlemsstat kan frit træffe sin egen beslutning med hensyn til henregning af ansvaret hos et tredjeland.

(10) Der er behov for yderligere handling fra Unionens side for at iværksætte visse foranstaltninger —

VEDTAGET DENNE AFGØRELSE

Artikel 1

1. Denne afgørelse finder anvendelse på cyberangreb med betydelige konsekvenser, herunder forsøg på cyberangreb med potentielt betydelige konsekvenser, der udgør en ekstern trussel mod Unionen eller dens medlemsstater.

2. Cyberangreb, der udgør en ekstern trussel, omfatter dem, der:

a) hidrører eller udføres fra områder uden for Unionen

b) anvender infrastruktur uden for Unionen

c) udføres af fysiske eller juridiske personer, enheder eller organer, der er etableret eller opererer uden for Unionen, eller

d) udføres med støtte fra, under ledelse af eller under kontrol af fysiske eller juridiske personer, enheder eller organer, der opererer uden for Unionen.

3. Med henblik herpå er cyberangreb handlinger, der omfatter et af følgende elementer:

a) adgang til informationssystemer

b) indgreb i informationssystemer

c) indgreb i data, eller

d) opfangelse af data,

når ejeren eller en anden rettighedsindehaver af systemet eller dataene eller en del heraf ikke har givet behørig tilladelse til sådanne handlinger, eller de ikke er tilladt i henhold til EU-retten eller den berørte medlemsstats ret.

4. Cyberangreb, der udgør en trussel mod medlemsstaterne, omfatter dem, der påvirker informationssystemer med tilknytning til bl.a.:

a) kritisk infrastruktur, herunder undervandskabler og genstande, der sendes ud i det ydre rum, som er væsentlig for opretholdelsen af vitale funktioner i samfundet eller menneskers sundhed, sikkerhed og økonomiske eller sociale velfærd

b) tjenester, der er nødvendige for opretholdelsen af væsentlige sociale og/eller økonomiske aktiviteter, navnlig i sektorerne energi (elektricitet, olie og gas), transport (luft-, jernbane-, vand- og vejtransport), bankvæsen, finansielle markedsinfrastrukturer, sundhed (sundhedstjenesteyder, hospitaler og private klinikker), forsyning med og distribution af drikkevand, digital infrastruktur og andre sektorer, der er væsentlige for den berørte medlemsstat

c) kritiske statslige funktioner, navnlig inden for forsvar, regeringsførelse og institutioners funktion, herunder i forbindelse med offentlige valg eller afstemningsprocessen, økonomisk og civil infrastrukturs funktion, intern sikkerhed og eksterne forbindelser, herunder gennem diplomatiske missioner

d) lagring eller behandling af fortrolige oplysninger, eller

e) statslige beredskabsenheder.

5. Cyberangreb, der udgør en ekstern trussel mod Unionen, omfatter dem, der udføres mod dens institutioner, organer, kontorer og agenturer, dens delegationer i tredjelande eller internationale organisationer, operationer og missioner som led i dens fælles sikkerheds- og forsvarspolitik (FSFP) og dens særlige repræsentanter.

6. Hvis det skønnes nødvendigt for at nå FUSP-målene i de relevante bestemmelser i artikel 21 i traktaten om Den Europæiske Union, kan restriktive foranstaltninger i henhold til denne afgørelse også anvendes som reaktion på cyberangreb med betydelige konsekvenser over for tredjelande eller internationale organisationer.

Artikel 2

I denne afgørelse forstås ved:

a) »informationssystemer«: en anordning eller gruppe af indbyrdes forbundne eller beslægtede anordninger, hvoraf en eller flere ved hjælp af et program automatisk behandler digitale data, samt digitale data, som lagres, behandles, fremfindes eller overføres af denne anordning eller gruppe af anordninger med henblik på drift, brug, beskyttelse og vedligeholdelse af samme

b) »indgreb i informationssystemer«: hindring eller afbrydelse af et informationssystems drift ved indlæsning af digitale data, ved overførsel, beskadigelse, sletning, forvanskning, ændring eller tilbageholdelse af sådanne data eller ved utilgængeliggørelse af sådanne data

c) »indgreb i data«: sletning, beskadigelse, forvanskning, ændring eller tilbageholdelse af digitale data i et informationssystem eller utilgængeliggørelse af sådanne data; det omfatter også tyveri af data, pengemidler, økonomiske ressourcer eller intellektuel ejendom

d) »opfangelse af data«: opfangelse via tekniske midler af ikkeoffentlige overførsler af digitale data til, fra eller inden for et informationssystem, herunder elektromagnetiske emissioner fra et informationssystem, der indeholder sådanne digitale data.

Artikel 3

Til de faktorer, der bestemmer, om et cyberangreb har betydelige konsekvenser, jf. artikel 1, stk. 1, hører følgende:

a) omfanget, størrelsen, virkningerne eller alvoren af de forstyrrelser, der forårsages, herunder for økonomiske og samfundsmæssige aktiviteter, væsentlige tjenester, kritiske statslige funktioner, den offentlige orden eller den offentlige sikkerhed

b) antallet af berørte fysiske eller juridiske personer, enheder eller organer

c) antallet af berørte medlemsstater

d) værdien af det økonomiske tab, der er forårsaget af f.eks. omfattende tyveri af pengemidler, økonomiske ressourcer eller intellektuel ejendom

e) den økonomiske fordel, som gerningsmanden har opnået for sig selv eller andre

f) mængden eller arten af stjålne data eller omfanget af brud på datasikkerheden, eller

g) arten af kommercielt følsomme data, der er opnået adgang til.

Artikel 4

1. Medlemsstaterne træffer de nødvendige foranstaltninger for at hindre indrejse i eller transit gennem deres områder af:

a) fysiske personer, der er ansvarlige for cyberangreb eller forsøg på cyberangreb

b) fysiske personer, der yder finansiel, teknisk eller materiel støtte til eller på anden vis er involveret i cyberangreb eller forsøg på cyberangreb, herunder gennem planlægning af, forberedelse af, deltagelse i, ledelse af, medvirken til eller tilskyndelse til sådanne angreb eller formidling af dem ved enten handling eller undladelse

c) fysiske personer med tilknytning til de personer, der er omfattet af litra a) og b),

jf. bilaget.

2. Stk. 1 forpligter ikke en medlemsstat til at nægte sine egne statsborgere indrejse på sit område.

3. Stk. 1 berører ikke tilfælde, hvor en medlemsstat er bundet af en folkeretlig forpligtelse, dvs.:

a) som værtsland for en international mellemstatslig organisation

b) som værtsland for en international konference, som er indkaldt af FN eller afholdes i FN's regi

c) i henhold til en multilateral aftale, hvorved der tilkendes privilegier og immuniteter, eller

d) i henhold til Lateranforliget fra 1929 mellem Pavestolen (Vatikanstaten) og Italien.

4. Stk. 3 anses ligeledes for at finde anvendelse i tilfælde, hvor en medlemsstat er værtsland for Organisationen for Sikkerhed og Samarbejde i Europa (OSCE).

5. Rådet underrettes behørigt, hver gang en medlemsstat indrømmer en fritagelse i henhold til stk. 3 eller 4.

6. Medlemsstaterne kan indrømme fritagelser fra foranstaltningerne i stk. 1, hvis rejsen er berettiget af tvingende humanitære hensyn eller af hensyn til muligheden for at kunne deltage i mellemstatslige møder eller møder, som Unionen tager initiativ til eller er vært for, eller møder, hvor en medlemsstat, der varetager formandskabet for OSCE, er vært, og hvor der føres en politisk dialog, som direkte fremmer de politiske mål med restriktive foranstaltninger, herunder sikkerhed og stabilitet i cyberspace.

7. Medlemsstaterne kan også indrømme fritagelser fra foranstaltningerne i stk. 1, hvis indrejse eller transit er nødvendig med henblik på gennemførelsen af en retslig procedure.

8. En medlemsstat, der ønsker at indrømme fritagelser, jf. stk. 6 eller 7, giver Rådet skriftlig meddelelse herom. Fritagelsen anses for at være indrømmet, medmindre et eller flere rådsmedlemmer skriftligt gør indsigelse inden for to arbejdsdage efter at have modtaget meddelelsen om den foreslåede fritagelse. Hvis et eller flere af medlemmerne af Rådet gør indsigelse, kan Rådet med kvalificeret flertal beslutte at indrømme den foreslåede fritagelse.

9. I tilfælde, hvor en medlemsstat i medfør af stk. 3, 4, 6, 7 eller 8 tillader indrejse i eller transit gennem sit område for de personer, der er opført på listen i bilaget, gælder tilladelsen udelukkende det formål, til hvilket den er udstedt, og de direkte berørte personer.

Artikel 5

1. Alle pengemidler og økonomiske ressourcer, som tilhører eller ejes, besiddes eller kontrolleres af:

a) fysiske eller juridiske personer, enheder eller organer, der er ansvarlige for cyberangreb eller forsøg på cyberangreb

b) fysiske eller juridiske personer, enheder eller organer, der yder finansiel, teknisk eller materiel støtte til eller på anden vis er involveret i cyberangreb eller forsøg på cyberangreb, herunder gennem planlægning af, forberedelse af, deltagelse i, ledelse af, medvirken til eller tilskyndelse til sådanne angreb eller formidling af dem ved enten handling eller undladelse

c) fysiske eller juridiske personer, enheder eller organer med tilknytning til de fysiske eller juridiske personer, enheder eller organer, der er omfattet af litra a) og b),

som opført på listen i bilaget, indefryses.

2. Ingen pengemidler eller økonomiske ressourcer må direkte eller indirekte stilles til rådighed for eller være til fordel for de fysiske eller juridiske personer, enheder eller organer, der er opført på listen i bilaget.

3. Uanset stk. 1 og 2 kan medlemsstaternes kompetente myndigheder på sådanne vilkår, som de skønner hensigtsmæssige, give tilladelse til frigivelse af visse indefrosne pengemidler eller økonomiske ressourcer eller til, at visse pengemidler eller økonomiske ressourcer stilles til rådighed, efter at have konstateret, at de pågældende pengemidler eller økonomiske ressourcer:

a) er nødvendige til at dække basale behov hos de fysiske personer, der er opført på listen i bilag I, og de familiemedlemmer, som disse fysiske personer har forsørgerpligt over for, herunder betaling af fødevarer, husleje eller renter og afdrag på boliglån, medicin og lægebehandling, skatter, forsikringspræmier og offentlige forbrugsafgifter

b) alene er bestemt til betaling af rimelige honorarer eller godtgørelse af udgifter i forbindelse med juridisk bistand

c) alene er bestemt til betaling af afgifter eller gebyrer til rutinemæssig opbevaring eller forvaltning af indefrosne pengemidler eller økonomiske ressourcer

d) er nødvendige til afholdelse af ekstraordinære udgifter, forudsat at den relevante kompetente myndighed mindst to uger før meddelelsen af tilladelsen har meddelt de øvrige medlemsstaters kompetente myndigheder og Kommissionen, hvorfor den skønner, at der bør gives særlig tilladelse, eller

e) skal betales til eller fra en konto, der indehaves af en diplomatisk eller konsulær repræsentation eller en international organisation, der nyder immunitet i overensstemmelse med folkeretten, for så vidt de pågældende betalinger skal anvendes til den diplomatiske eller konsulære repræsentations eller internationale organisations officielle formål.

Den berørte medlemsstat underretter de øvrige medlemsstater og Kommissionen om enhver tilladelse, der måtte være meddelt i medfør af dette stykke.

4. Uanset stk. 1 kan medlemsstaternes kompetente myndigheder give tilladelse til frigivelse af visse indefrosne pengemidler eller økonomiske ressourcer, hvis følgende betingelser er opfyldt:

a) pengemidlerne eller de økonomiske ressourcer er omfattet af en voldgiftsmæssig afgørelse, der er truffet inden den dato, hvor den fysiske eller juridiske person, enheden eller organet som omhandlet i stk. 1 blev optaget på listen i bilaget, eller af en retslig eller administrativ afgørelse, der er truffet i Unionen, eller en retslig afgørelse, der kan fuldbyrdes i den pågældende medlemsstat, forud for eller efter denne dato

b) pengemidlerne eller de økonomiske ressourcer skal udelukkende anvendes til at opfylde fordringer, der er sikret ved en sådan afgørelse eller er anerkendt som gyldige ved en sådan afgørelse, inden for de grænser, som er fastsat ved gældende lovgivning og administrative bestemmelser om sådanne fordringshaveres rettigheder

c) afgørelsen er ikke til fordel for en fysisk eller juridisk person, en enhed eller et organ, der er opført på listen i bilaget, og

d) anerkendelsen af afgørelsen er ikke i strid med de almindelige retsprincipper i den pågældende medlemsstat.

Den berørte medlemsstat underretter de øvrige medlemsstater og Kommissionen om enhver tilladelse, der meddeles i medfør af dette stykke.

5. Stk. 1 er ikke til hinder for, at en fysisk eller juridisk person, en enhed eller et organ, der er opført på listen i bilaget, foretager en betaling i henhold til en kontrakt, der er indgået før den dato, hvor denne fysiske eller juridiske person eller enhed eller dette organ blev opført herpå, såfremt den pågældende medlemsstat har fastslået, at betalingen ikke, hverken direkte eller indirekte, modtages af en fysisk eller juridisk person, en enhed eller et organ, der er omhandlet i stk. 1.

6. Stk. 2 gælder ikke beløb, der tilføres indefrosne konti i form af:

a) renter eller anden form for afkast fra disse konti

b) forfaldne betalinger i henhold til kontrakter, aftaler eller forpligtelser, som er indgået eller opstået forud for den dato, hvor disse konti blev omfattet af foranstaltningerne i stk. 1 og 2, eller

c) forfaldne betalinger i henhold til retslige, administrative eller voldgiftsmæssige afgørelser, der er truffet i Unionen, eller som kan fuldbyrdes i den pågældende medlemsstat,

forudsat at sådanne renter, andre afkast og betalinger forbliver omfattet af de foranstaltninger, der er fastsat i stk. 1.

Artikel 6

1. Rådet, der træffer afgørelse med enstemmighed på forslag af en medlemsstat eller Unionens højtstående repræsentant for udenrigsanliggender og sikkerhedspolitik, udarbejder og ændrer listen i bilaget.

2. Rådet underretter den pågældende fysiske eller juridiske person, den pågældende enhed eller det pågældende organ om den afgørelse, der er omhandlet i stk. 1, herunder om begrundelsen for opførelsen på listen, enten direkte, hvis adressen er kendt, eller ved offentliggørelse af en bekendtgørelse, og giver den pågældende fysiske eller juridiske person, den pågældende enhed eller det pågældende organ mulighed for at fremsætte bemærkninger.

3. Når der fremsættes bemærkninger eller forelægges væsentlig ny dokumentation, tager Rådet den i stk. 1 omhandlede afgørelse op til fornyet vurdering og underretter den pågældende fysiske eller juridiske person, den pågældende enhed eller det pågældende organ herom.

Artikel 7

1. Bilaget skal indeholde grundene til at opføre de i artikel 4 og 5 omhandlede fysiske eller juridiske personer, enheder og organer på listen.

2. Bilaget skal, hvis de er tilgængelige, indeholde de oplysninger, som er nødvendige for at identificere de pågældende fysiske eller juridiske personer, enheder eller organer. For så vidt angår fysiske personer kan sådanne oplysninger omfatte navne og aliasser, fødselsdato og fødested, nationalitet, pas- og identitetskortnumre, køn, adresse, hvis denne er kendt, og funktion eller erhverv. For så vidt angår juridiske personer, enheder eller organer kan sådanne oplysninger omfatte navne, registreringssted og -dato, registreringsnummer og forretningssted.

Artikel 8

Ingen fordringer må indfries i forbindelse med kontrakter eller transaktioner, hvis opfyldelse eller gennemførelse direkte eller indirekte er blevet påvirket helt eller delvis af foranstaltninger i denne afgørelse, herunder erstatningskrav og andre tilsvarende fordringer, såsom krav om modregning og erstatning i henhold til garanti, navnlig fordringer, som tager sigte på forlængelse eller indfrielse af garantier eller modgarantier, navnlig finansielle garantier eller modgarantier, uanset form, såfremt disse fordringer gøres gældende af:

a) fysiske eller juridiske personer, enheder eller organer, der er opført på listen i bilaget

b) andre fysiske eller juridiske personer, enheder eller organer, som handler gennem eller på vegne af en eller et af de i litra a) omhandlede fysiske eller juridiske personer, enheder eller organer.

Artikel 9

For at give foranstaltningerne i denne afgørelse størst mulig virkning tilskynder Unionen tredjelande til at vedtage restriktive foranstaltninger svarende til dem, der er indeholdt i denne afgørelse.

Artikel 10

Denne afgørelse finder anvendelse indtil den 18. maj 2020 og overvåges løbende. Den forlænges eller ændres, alt efter hvad der er relevant, hvis Rådet skønner, at dens mål ikke er nået.

Artikel 11

Denne afgørelse træder i kraft dagen efter offentliggørelsen i *Den Europæiske Unions Tidende*.

Udfærdiget i Bruxelles, den 17. maj 2019.

På Rådets vegne
E.O. TEODOROVICI
Formand

BILAG

Liste over fysiske og juridiske personer, enheder og organer som omhandlet i artikel 4 og 5

[…]