Europeiska unionens råd

Bryssel den 14 maj 2019
(OR. en)

7299/19

LIMITE

CORLX 106
CFSP/PESC 191
RELEX 235
CYBER 81
JAI 264
FIN 216

RÄTTSAKTER OCH ANDRA INSTRUMENT

Ärende:	RÅDETS BESLUT om restriktiva åtgärder mot cyberattacker som hotar unionen eller dess medlemsstater

RÅDETS BESLUT (GUSP) 2019/…

av den

om restriktiva åtgärder
mot cyberattacker som hotar unionen eller dess medlemsstater

EUROPEISKA UNIONENS RÅD HAR ANTAGIT DETTA BESLUT

med beaktande av fördraget om Europeiska unionen, särskilt artikel 29,

med beaktande av förslaget från unionens höga representant för utrikes frågor och säkerhetspolitik, och

av följande skäl:

(1) Den 19 juni 2017 antog rådet slutsatser om en ram för en gemensam diplomatisk respons mot skadlig it-verksamhet (nedan kallad *verktygslådan för cyberdiplomati*), där rådet uttryckte oro över den ökade förmågan och viljan hos statliga och icke-statliga aktörer att försöka nå sina mål genom att ägna sig åt skadlig it-verksamhet och bekräftade det växande behovet av att skydda integriteten och säkerheten för unionen, medlemsstaterna och deras medborgare mot cyberhot och skadlig it-verksamhet.

(2) Rådet betonade att tydliga signaler avseende de troliga konsekvenserna av en gemensam diplomatisk respons från unionen mot skadlig it-verksamhet påverkar potentiella förövares agerande i cyberrymden och därigenom förstärker säkerheten för unionen och medlemsstaterna. Rådet bekräftade också att åtgärder inom den gemensamma utrikes- och säkerhetspolitiken (Gusp), om nödvändigt inbegripet restriktiva åtgärder, som antagits enligt relevanta bestämmelser i fördragen, är lämpade för en ram för en gemensam diplomatisk respons från unionen mot skadlig it-verksamhet som syftar till att uppmuntra samarbete, underlätta begränsning av omedelbara och långsiktiga hot samt påverka potentiella förövares agerande på lång sikt.

(3) Den 11 oktober 2017 godkände kommittén för utrikes- och säkerhetspolitik riktlinjer för genomförande för verktygslådan för cyberdiplomati. Riktlinjerna för genomförande avser fem kategorier av åtgärder, inbegripet restriktiva åtgärder, inom verktygslådan för cyberdiplomati, och processen för att åberopa dessa åtgärder.

(4) Rådets slutsatser om skadlig it-verksamhet av den 16 april 2018 fördömde med kraft skadlig användning av informations- och kommunikationsteknik (IKT) och framhöll att skadlig användning av IKT är oacceptabel eftersom den undergräver stabiliteten och säkerheten liksom de fördelar som internet och användningen av IKT ger. Rådet erinrade om att verktygslådan för cyberdiplomati bidrar till konfliktförebyggande, samarbete och stabilitet i cyberrymden genom att ange åtgärder inom ramen för Gusp, inbegripet restriktiva åtgärder, som kan användas för att förebygga och vidta åtgärder mot skadlig it-verksamhet. Rådet konstaterade att unionen även fortsättningsvis med kraft kommer att hävda att befintlig internationell rätt är tillämplig i cyberrymden och betonade att respekten för internationell rätt, särskilt Förenta nationernas stadga, är avgörande för upprätthållandet av fred och stabilitet. Rådet underströk också att stater inte får använda ombud för att begå internationella överträdelser med hjälp av IKT och bör sträva efter att säkerställa att deras territorium inte används av icke-statliga aktörer för att begå sådana handlingar, i enlighet med vad som anges i 2015 års rapport från FN:s grupp med myndighetsexperter på utveckling inom området för information och telekommunikation inom ramen för internationell säkerhet.

(5) Den 28 juni 2018 antog Europeiska rådet slutsatser i vilka man framhöll behovet att stärka förmågan att hantera cybersäkerhetshot från länder utanför unionen. Europeiska rådet uppmanade institutionerna och medlemsstaterna att genomföra de åtgärder som avses i det gemensamma meddelandet från kommissionen och unionens höga representant för utrikes frågor och säkerhetspolitik av den 13 juni 2018 med titeln *Att öka motståndskraften och stärka kapaciteten att hantera hybridhot*, inklusive den praktiska användningen av verktygslådan för cyberdiplomati.

(6) Den 18 oktober 2018 antog Europeiska rådet slutsatser där man uppmanade till fortsatt arbete med kapaciteten att reagera på och avskräcka från cyberattacker genom unionens restriktiva åtgärder, med hänvisning till rådets slutsatser av den 19 juni 2017.

(7) I detta sammanhang upprättas genom detta beslut en ram för riktade restriktiva åtgärder mot cyberattacker med betydande effekt som utgör ett externt hot för unionen eller dess medlemsstater. Om det anses nödvändigt för att uppnå Gusp-målen i de relevanta bestämmelserna i artikel 21 i fördraget om Europeiska unionen, får restriktiva åtgärder enligt detta beslut också tillämpas som svar på cyberattacker med betydande effekt på tredjeländer eller internationella organisationer.

(8) De riktade åtgärderna bör, för att få en preventiv och avskräckande verkan, inriktas på uppsåtliga cyberattacker som omfattas av detta beslut.

(9) Riktade restriktiva åtgärder bör inte likställas med att en tredjestat åläggs ansvar för cyberattacker. Tillämpningen av riktade restriktiva åtgärder innebär inte ett sådant ansvarsåläggande, vilket är ett suveränt politiskt beslut som fattas från fall till fall. Varje medlemsstat har rätt att göra sin egen bedömning i fråga om ansvarsåläggande av ett tredjeland för cyberattacker.

(10) Det krävs ytterligare insatser från unionen för att genomföra vissa åtgärder.

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

Artikel 1

1. Detta beslut är tillämpligt på cyberattacker med en betydande effekt, inbegripet försök till cyberattacker med en potentiellt betydande effekt, som utgör ett externt hot för unionen eller dess medlemsstater.

2. Cyberattacker som utgör ett externt hot omfattar sådana som

   a) har sitt ursprung eller utförs från platser utanför unionen,

   b) använder infrastruktur utanför unionen,

   c) utförs av fysiska eller juridiska personer, enheter eller organ som är etablerade eller som bedriver verksamhet utanför unionen, eller som

   d) utförs med stöd av, under ledning av eller under kontroll av fysiska eller juridiska personer, enheter eller organ som bedriver verksamhet utanför unionen.

3. Cyberattacker är därför handlingar som omfattar något av följande:

   a) Åtkomst till informationssystem.

   b) Störning av informationssystem.

   c) Datastörning.

   d) Dataavläsning.

Detta gäller om sådana handlingar inte vederbörligen har tillåtits av ägaren eller annan rättighetshavare till systemet eller uppgifterna eller del av detta, eller inte medges enligt lagstiftningen i unionen eller den berörda medlemsstaten.

4. Cyberattacker som utgör ett hot mot medlemsstaterna omfattar attacker som påverkar informationssystem som rör bland annat

a) kritisk infrastruktur, inbegripet undervattenskablar och föremål som har sänts ut i yttre rymden, som är nödvändig för att upprätthålla centrala samhällsfunktioner, eller människors hälsa, säkerhet, trygghet samt ekonomiska och sociala välfärd,

b) tjänster som är nödvändiga för att upprätthålla väsentliga sociala och/eller ekonomiska verksamheter, särskilt inom sektorerna energi (el, olja och gas), transport (lufttransport, järnvägstransport, vattentransport och vägtransport), banksektorn, finansmarknadsinfrastruktur, hälsa och sjukvård (vårdgivare, sjukhus och privata kliniker), leverans och distribution av dricksvatten, digital infrastruktur, och andra sektorer som är väsentliga för den berörda medlemsstaten,

c) kritiska statliga funktioner, särskilt på områdena försvar, institutioners förvaltning och funktion, inbegripet för allmänna val eller röstningsförfarandet, ekonomisk och civil infrastrukturs funktion, inre säkerhet och yttre förbindelser, inbegripet genom diplomatiska beskickningar,

d) lagring eller behandling av säkerhetsskyddsklassificerade uppgifter, eller

e) offentliga incidenthanteringsorganisationer.

5. Cyberattacker som utgör ett hot mot unionen inbegriper attacker som utförs mot unionens institutioner, organ och byråer, dess delegationer till tredjeländer eller internationella organisationer, dess uppdrag och insatser inom den gemensamma säkerhets- och försvarspolitiken (GSFP) samt dess särskilda representanter.

6. Om det anses nödvändigt för att uppnå Gusp-målen i de relevanta bestämmelserna i artikel 21 i fördraget om Europeiska unionen, får restriktiva åtgärder också tillämpas som svar på cyberattacker med betydande effekt på tredjeländer eller internationella organisationer.

Artikel 2

I detta beslut gäller följande definitioner:

a) *informationssystem*: en apparat eller en grupp av sammankopplade apparater eller apparater som hör samman med varandra, av vilka en eller flera genom ett program automatiskt behandlar digitala data, samt digitala data som lagras, behandlas, hämtas eller överförs med hjälp av denna apparat eller grupp av apparater för att den eller de ska kunna drivas, användas, skyddas och underhållas.

b) *störning av informationssystem*: förhindrande eller avbrott av driften av ett informationssystem genom att digitala data inmatas, överförs, skadas, raderas, försämras, ändras, undertrycks eller görs oåtkomliga.

c) *datastörning*: störning genom att digitala data i ett informationssystem raderas, skadas, försämras, ändras, undertrycks eller görs oåtkomliga; det inbegriper också stöld av data, penningmedel, ekonomiska resurser eller immateriella rättigheter.

d) *dataavläsning*: avläsning, genom tekniska medel, av icke offentlig överföring av digitala data till, från eller inom ett informationssystem, även elektromagnetisk emission från ett informationssystem som befordrar sådana digitala data.

Artikel 3

De faktorer som avgör huruvida en cyberattack har den betydande effekt som avses i artikel 1.1 inbegriper

a) hur omfattande, storskalig, effektfull eller allvarlig den störning som orsakas är, inbegripet dess inverkan på ekonomisk och samhällelig verksamhet, samhällsviktiga tjänster, kritiska statliga funktioner, allmän ordning eller allmän säkerhet,

b) det antal fysiska eller juridiska personer, enheter eller organ som berörs,

c) det antal medlemsstater som berörs,

d) omfattningen av den ekonomiska förlust som orsakas, såsom storskalig stöld av penningmedel, ekonomiska resurser eller immateriella rättigheter,

e) den ekonomiska fördel som gärningsmannen erhåller för sig själv eller andra,

f) omfattningen och typen av data som stjäls eller dataintrångens storskalighet, eller

g) typen av kommersiellt känsliga data till vilka åtkomst fås.

Artikel 4

1. Medlemsstaterna ska vidta nödvändiga åtgärder för att förhindra inresa till eller transitering genom sina territorier av

   a) fysiska personer som är ansvariga för cyberattacker eller försök till cyberattacker,

   b) fysiska personer som tillhandahåller finansiellt, tekniskt eller materiellt stöd till eller på annat sätt är inblandade i cyberattacker eller försök till cyberattacker, bland annat genom att planera, förbereda, delta i, styra, hjälpa till med eller uppmuntra sådana attacker, eller underlätta dem, antingen genom handling eller försummelse,

   c) fysiska personer som har samröre med de personer som omfattas av leden a och b,

   i enlighet med förteckningen i bilagan.

2. Punkt 1 ska inte innebära att en medlemsstat är skyldig att vägra sina egna medborgare inresa till det egna territoriet.

3. Punkt 1 ska inte påverka de fall då en medlemsstat är bunden av en skyldighet enligt internationell rätt, nämligen

   a) som värdland för en internationell mellanstatlig organisation,

   b) som värdland för en internationell konferens sammankallad av eller under överinseende av Förenta nationerna,

   c) enligt en multilateral överenskommelse som ger privilegier och immunitet, eller

   d) enligt 1929 års konkordat (Lateranfördraget) som ingåtts av Heliga stolen (Vatikanstaten) och Italien.

4. Punkt 3 ska anses tillämplig även i fall då en medlemsstat är värd för Organisationen för säkerhet och samarbete i Europa (OSSE).

5. Rådet ska vederbörligen informeras om alla fall då en medlemsstat beviljar undantag enligt punkt 3 eller 4.

6. Medlemsstaterna får bevilja undantag från de åtgärder som föreskrivs i punkt 1 om en resa är motiverad av brådskande humanitära skäl eller för deltagande i mellanstatliga möten eller möten som främjas eller anordnas av unionen eller anordnas av en medlemsstat som är ordförande i OSSE, där man för en politisk dialog som direkt främjar de restriktiva åtgärdernas politiska mål, inklusive säkerhet och stabilitet i cyberrymden.

7. Medlemsstaterna får bevilja undantag från de åtgärder som föreskrivs i punkt 1 om en inresa eller transitering är nödvändig för att genomföra en rättegång.

8. En medlemsstat som vill bevilja undantag som avses i punkt 6 eller 7 ska skriftligen anmäla detta till rådet. Undantaget ska anses beviljat såvida inte en eller flera av rådets medlemmar gör en skriftlig invändning inom två arbetsdagar efter det att de mottagit anmälan om det föreslagna undantaget. Om en eller flera av rådets medlemmar gör en invändning får rådet med kvalificerad majoritet besluta att bevilja det föreslagna undantaget.

9. Om en medlemsstat enligt punkterna 3, 4, 6, 7 eller 8 tillåter inresa till eller transitering genom sitt territorium av personer som förtecknas i bilagan, ska tillståndet strikt begränsas till det ändamål för vilket det ges och de personer som direkt berörs av detta.

Artikel 5

1. Alla penningmedel och ekonomiska resurser som ägs, innehas eller kontrolleras av

   a) fysiska eller juridiska personer, enheter eller organ som är ansvariga för cyberattacker eller försök till cyberattacker,

   b) fysiska eller juridiska personer, eller enheter eller organ som tillhandahåller finansiellt, tekniskt eller materiellt stöd till eller på annat sätt är inblandade i cyberattacker eller försök till cyberattacker, bland annat genom att planera, förbereda, delta i, styra, hjälpa till med eller uppmuntra sådana attacker, eller underlätta dem, antingen genom handling eller försummelse,

   c) fysiska eller juridiska personer, enheter eller organ som har samröre med de fysiska eller juridiska personer, enheter eller organ som omfattas av leden a och b,

   i enlighet med förteckningen i bilagan, ska frysas.

2. Inga penningmedel eller ekonomiska resurser får direkt eller indirekt ställas till förfogande för eller göras tillgängliga till förmån för någon av de fysiska eller juridiska personer, enheter eller organ som förtecknas i bilagan.

3. Genom undantag från punkterna 1 och 2 får de behöriga myndigheterna i medlemsstaterna ge tillstånd till att vissa frysta penningmedel eller ekonomiska resurser frigörs eller att vissa penningmedel eller ekonomiska resurser görs tillgängliga, på sådana villkor som de finner lämpliga, efter det att de har konstaterat att de berörda penningmedlen eller ekonomiska resurserna är

a) nödvändiga för att täcka grundläggande behov för de fysiska personer som förtecknas i bilagan och för sådana fysiska personers underhållsberättigade familjemedlemmar, inbegripet betalning av livsmedel, hyra eller amorteringar, mediciner och läkarvård, skatter, försäkringspremier och avgifter för samhällstjänster,

b) avsedda endast för betalning av rimliga arvoden eller ersättning av utgifter i samband med tillhandahållande av juridiska tjänster,

c) avsedda uteslutande för betalning av avgifter eller serviceavgifter för rutinmässig hantering eller förvaltning av frysta penningmedel eller ekonomiska resurser,

d) nödvändiga för att täcka extraordinära utgifter, under förutsättning att den berörda behöriga myndigheten senast två veckor före beviljandet av tillståndet har meddelat de andra medlemsstaternas behöriga myndigheter och kommissionen om skälen till att den anser att ett särskilt tillstånd bör beviljas, eller

e) avsedda att betalas in på eller från ett konto tillhörande en diplomatisk eller konsulär beskickning eller en internationell organisation som åtnjuter immunitet enligt internationell rätt, i den mån sådana betalningar är avsedda att användas för den diplomatiska eller konsulära beskickningens eller den internationella organisationens officiella ändamål.

Den berörda medlemsstaten ska underrätta övriga medlemsstater och kommissionen om alla tillstånd som den beviljar enligt denna punkt.

4. Genom undantag från punkt 1 får de behöriga myndigheterna i medlemsstaterna tillåta att vissa frysta penningmedel eller ekonomiska resurser frigörs, om följande villkor är uppfyllda:

a) Penningmedlen eller de ekonomiska resurserna är föremål för ett skiljedomsbeslut som meddelats före den dag då den fysiska eller juridiska person, den enhet eller det organ som avses i punkt 1 fördes upp på förteckningen i bilagan, eller för ett rättsligt eller administrativt beslut som meddelats i unionen, eller för ett rättsligt beslut som är verkställbart i den berörda medlemsstaten, före eller efter den dagen.

b) Penningmedlen eller de ekonomiska resurserna kommer att användas enbart för att tillgodose krav som har säkrats genom ett sådant beslut eller har erkänts som giltiga i ett sådant beslut, inom de gränser som fastställs i tillämpliga lagar och andra författningar som reglerar rättigheterna för personer med sådana krav.

c) Beslutet gynnar inte någon av de fysiska eller juridiska personer, enheter eller organ som förtecknas i bilagan.

d) Erkännandet av beslutet står inte i strid med den berörda medlemsstatens allmänna ordning.

Den berörda medlemsstaten ska underrätta övriga medlemsstater och kommissionen om alla tillstånd som den beviljar enligt denna punkt.

5. Punkt 1 ska inte hindra en fysisk eller juridisk person, en enhet eller ett organ som förtecknas i bilagan från att göra en betalning i samband med ett avtal som ingåtts före den dag då den fysiska eller juridiska personen, enheten eller organet förtecknades, under förutsättning att den berörda medlemsstaten har fastställt att betalningen inte direkt eller indirekt tas emot av en fysisk eller juridisk person, en enhet eller ett organ som avses i punkt 1.

6. Punkt 2 ska inte tillämpas på kreditering av frysta konton med

a) ränta eller andra intäkter på sådana konton,

b) betalningar enligt avtal, överenskommelser eller förpliktelser som ingåtts eller uppkommit före den dag då dessa konton blev föremål för de åtgärder som föreskrivs i punkterna 1 och 2, eller

c) betalningar enligt rättsliga eller administrativa beslut eller skiljedomsbeslut som meddelats i unionen eller som är verkställbara i den berörda medlemsstaten,

under förutsättning att alla sådana räntor, intäkter och betalningar fortsätter att vara föremål för de åtgärder som föreskrivs i punkt 1.

Artikel 6

1. Rådet ska, genom enhälligt beslut, på förslag av en medlemsstat eller unionens höga representant för utrikes frågor och säkerhetspolitik fastställa och ändra förteckningen i bilagan.

2. Rådet ska meddela den berörda fysiska eller juridiska personen, den berörda enheten eller det berörda organet det beslut som avses i punkt 1, inbegripet skälen för uppförandet på förteckningen, antingen direkt, om adressen är känd, eller genom att ett meddelande offentliggörs, så att den fysiska eller juridiska personen, enheten eller organet ges tillfälle att inkomma med synpunkter.

3. Om synpunkter lämnas eller om väsentlig ny bevisning läggs fram ska rådet ompröva de beslut som avses i punkt 1 och informera den berörda fysiska eller juridiska personen, den berörda enheten eller det berörda organet om detta.

Artikel 7

1. Bilagan ska innehålla skälen till att de fysiska eller juridiska personer, enheter och organ som avses i artiklarna 4 och 5 har förts upp på förteckningen.

2. Bilagan ska innehålla de uppgifter som krävs för att identifiera berörda fysiska eller juridiska personer, enheter eller organ, om sådana uppgifter finns att tillgå. När det gäller fysiska personer kan dessa uppgifter inbegripa namn och alias, födelsedatum och födelseort, medborgarskap, pass- och id-kortnummer, kön, adress (om känd) samt befattning eller yrke. När det gäller juridiska personer, enheter eller organ kan sådana uppgifter omfatta namn, plats och datum för registrering samt registreringsnummer och driftsställe.

Artikel 8

Inga krav får tillgodoses i samband med ett avtal eller en transaktion vars genomförande har påverkats direkt eller indirekt, helt eller delvis, av de åtgärder som införs genom detta beslut, inbegripet krav på gottgörelse eller andra krav av detta slag, t.ex. ett krav på ersättning eller krav enligt en garanti, särskilt krav på förlängning eller betalning av en obligation, garanti eller gottgörelse, i synnerhet en finansiell garanti eller ekonomisk gottgörelse, oavsett form, om kraven ställs av

a) fysiska eller juridiska personer, enheter eller organ som förtecknas i bilagan,

b) fysiska eller juridiska personer, enheter eller organ som agerar via någon av de fysiska eller juridiska personer, enheter eller organ som avses i led a eller för deras räkning.

Artikel 9

För att maximera verkan av de åtgärder som avses i detta beslut ska unionen uppmuntra tredjestater att anta restriktiva åtgärder av liknande typ som de åtgärder som föreskrivs i detta beslut.

Artikel 10

Detta beslut ska tillämpas till och med den … [ett år efter det att detta beslut har trätt ikraft] och ska ses över fortlöpande. Det ska förlängas, eller vid behov ändras, om rådet bedömer att dess mål inte har uppfyllts.

Artikel 11

Denna förordning träder i kraft dagen efter det att den har offentliggjorts i *Europeiska unionens officiella tidning*.

Utfärdat i

På rådets vägnar
Ordförande

BILAGA

Förteckning över fysiska och juridiska personer, enheter och organ som avses i artiklarna 4 och 5

[…]