►B

RÅDETS FÖRORDNING (EU) 2019/796

av den 17 maj 2019

om restriktiva åtgärder mot cyberattacker som hotar unionen eller dess medlemsstater

(EUT L 129I, 17.5.2019, s. 1)

Ändrad genom:

		Officiella tidningen		
		nr	sida	datum
►M1	Rådets genomförandeförordning (EU) 2020/1125 av den 30 juli 2020	L 246	4	30.7.2020
►M2	Rådets genomförandeförordning (EU) 2020/1536 av den 22 oktober 2020	L 351 I	1	22.10.2020
►M3	Rådets genomförandeförordning (EU) 2020/1744 av den 20 november 2020	L 393	1	23.11.2020
►M4	Kommissionens genomförandeförordning (EU) 2022/595 av den 11 april 2022	L 114	60	12.4.2022

Rättad genom:

►C1 Rättelse, EUT L 230, 17.7.2020, s. 37 (2019/796)

▼B

RÅDETS FÖRORDNING (EU) 2019/796

av den 17 maj 2019

om restriktiva åtgärder mot cyberattacker som hotar unionen eller dess medlemsstater

Artikel 1

1. Denna förordning är tillämplig 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

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,

▼B

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 målen för den gemensamma utrikes- och säkerhetspolitiken (Gusp) i de relevanta bestämmelserna i artikel 21 i fördraget om Europeiska unionen, får restriktiva åtgärder enligt denna förordning också tillämpas som svar på cyberattacker med betydande effekt på tredjeländer eller internationella organisationer.

7. I denna förordning 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.

8. I denna förordning gäller dessutom följande definitioner:

a) *krav*: alla krav, oavsett om de görs gällande genom rättsliga förfaranden eller ej och oavsett om de har framställts före eller efter dagen för denna förordnings ikraftträdande, genom eller i samband med ett avtal eller en transaktion, särskilt

   i) ett krav på fullgörande av varje slag av förpliktelse som uppstår genom eller i samband med ett avtal eller en transaktion,

   ii) ett krav på förlängning eller betalning av en obligation, en finansiell garanti eller gottgörelse, oavsett form,

   iii) ett krav på ersättning med avseende på ett avtal eller en transaktion,

   iv) ett motkrav,

▼B

v) ett krav på erkännande eller verkställighet, inbegripet genom exekvaturförfarande, av en dom, en skiljedom eller ett likvärdigt avgörande, oavsett var de meddelats.

b) *avtal eller transaktion*: alla transaktioner oavsett form eller tillämplig lagstiftning, och oavsett om de omfattar ett eller flera avtal eller liknande förpliktelser mellan samma eller olika parter; för detta ändamål ingår i begreppet *avtal* alla obligationer, garantier eller gottgörelser, särskilt varje finansiell garanti eller ekonomisk gottgörelse och varje kredit, oavsett om de är juridiskt fristående eller ej, samt varje därtill knuten bestämmelse som härrör från en sådan transaktion eller är knuten till denna.

c) *behöriga myndigheter*: de behöriga myndigheter i medlemsstaterna som anges på de webbplatser som förtecknas i bilaga II.

d) *ekonomiska resurser*: egendom av alla slag, materiell eller immateriell, lös eller fast, som inte utgör penningmedel, men som kan användas för att erhålla penningmedel, varor eller tjänster.

e) *frysning av ekonomiska resurser*: förhindrande av att ekonomiska resurser på något sätt används för att erhålla penningmedel, varor eller tjänster, inbegripet men inte begränsat till försäljning, uthyrning eller inteckning av dem.

f) *frysning av penningmedel*: förhindrande av varje flyttning, överföring, ändring, användning eller hantering av eller tillgång till penningmedel på ett sätt som skulle leda till en förändring av volym, belopp, belägenhet, ägandeförhållanden, innehav, art eller bestämmelse eller varje annan förändring som skulle göra det möjligt att utnyttja penningmedlen, inbegripet portföljförvaltning.

g) *penningmedel*: finansiella medel och ekonomiska förmåner av alla slag, inbegripet men inte begränsat till

i) kontanter, checkar, penningfordringar, växlar, betalningsorder och andra betalningsinstrument,

ii) inlåning hos finansinstitut eller andra enheter, kontotillgodohavanden, skuldebrev och skuldförbindelser,

iii) börsnoterade och onoterade värdepapper och skuldinstrument, inbegripet aktier och andelar, certifikat för värdepapper, obligationer, växlar, optioner, förlagsbevis och derivatkontrakt,

iv) räntor, utdelningar eller annan inkomst från, eller värde som härrör från eller skapas genom tillgångar,

v) krediter, kvittningsrätter, garantiförbindelser, fullgörandegarantier eller andra finansiella åtaganden,

vi) remburser, fraktsedlar och pantförskrivningar, och

vii) dokument som utgör bevis på andelar i penningmedel eller finansiella resurser.

▼B

h) *unionens territorium*: de medlemsstaters territorier på vilka fördraget är tillämpligt, enligt de villkor som fastställs i fördraget, inklusive medlemsstaternas luftrum.

Artikel 2

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 3

1. Alla penningmedel och ekonomiska resurser som tillhör, ägs, innehas eller kontrolleras av varje fysisk eller juridisk person, enhet eller organ som förtecknas i bilaga I 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 bilaga I.

3. Bilaga I ska omfatta följande, som fastställts av rådet i enlighet med artikel 5.1 i beslut (Gusp) 2019/797:

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 denna punkt.

▼B

Artikel 4

1. Genom undantag från artikel 3 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) ►C1 nödvändiga för att täcka grundläggande behov för de fysiska eller juridiska personer, enheter eller organ som förtecknas i bilaga I ◄ 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 relevanta behöriga myndigheten har meddelat de andra medlemsstaternas behöriga myndigheter och kommissionen av vilka skäl den anser att ett särskilt tillstånd bör beviljas senast två veckor före beviljandet av tillståndet, 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.

2. Den berörda medlemsstaten ska underrätta de andra medlemsstaterna och kommissionen om alla tillstånd som den beviljar enligt punkt 1 inom två veckor från beviljandet av tillståndet.

Artikel 5

1. Genom undantag från artikel 3.1 får de behöriga myndigheterna i medlemsstaterna ge tillstånd till att vissa frysta penningmedel eller ekonomiska resurser frigörs, förutsatt att 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 artikel 3 upptogs i bilaga I, 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 avgörande eller har erkänts som giltiga i ett sådant avgörande, 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 bilaga I.

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

▼B

2. Den berörda medlemsstaten ska underrätta de andra medlemsstaterna och kommissionen om alla tillstånd som den beviljar enligt punkt 1 inom två veckor från beviljandet av tillståndet.

Artikel 6

1. Genom undantag från artikel 3.1, och förutsatt att en betalning som ska göras av en fysisk eller juridisk person, en enhet eller ett organ som förtecknas i bilaga I har uppkommit inom ramen för ett avtal eller en överenskommelse som har ingåtts av, eller en förpliktelse som har uppkommit för, den fysiska eller juridiska personen, enheten eller organet i fråga före den dag då personen, enheten eller organet upptogs i förteckningen i bilaga I, får medlemsstaternas behöriga myndigheter, på de villkor de anser vara lämpliga, ge tillstånd till att vissa frysta penningmedel eller ekonomiska resurser frigörs, förutsatt att den berörda behöriga myndigheten har fastställt att

a) penningmedlen eller de ekonomiska resurserna kommer att användas för en betalning som görs av en fysisk eller juridisk person, en enhet eller ett organ som förtecknas i bilaga I, och

b) att betalningen inte innebär någon överträdelse av artikel 3.2.

2. Den berörda medlemsstaten ska underrätta de andra medlemsstaterna och kommissionen om alla tillstånd som den beviljar enligt punkt 1 inom två veckor från beviljandet av tillståndet.

Artikel 7

1. Artikel 3.2 ska inte hindra att finans- eller kreditinstitut, som tar emot penningmedel som överförs av tredje part till kontot för en fysisk eller juridisk person, en enhet eller ett organ som återfinns i förteckningen, krediterar frysta konton, under förutsättning att insättningar på sådana konton också fryses. Finans- eller kreditinstitutet ska utan dröjsmål underrätta den relevanta behöriga myndigheten om alla sådana transaktioner.

2. Artikel 3.2 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 den fysiska eller juridiska person, den enhet eller det organ som avses i artikel 3.1 upptogs i förteckningen i bilaga I, eller

c) betalningar enligt rättsliga eller administrativa beslut eller skiljedomsbeslut meddelade i en medlemsstat eller verkställbara i den berörda medlemsstaten,

under förutsättning att alla sådana räntor, intäkter och betalningar fortsätter att vara föremål för de åtgärder som föreskrivs i artikel 3.1.

Artikel 8

1. Utan att det påverkar tillämpningen av gällande regler om rapportering, konfidentialitet och tystnadsplikt ska fysiska och juridiska personer, enheter och organ

▼B

a) omedelbart lämna alla uppgifter som skulle underlätta efterlevnaden av denna förordning, till exempel uppgifter om konton och belopp som frysts i enlighet med artikel 3.1, till den behöriga myndigheten i den medlemsstat där de är bosatta eller etablerade samt sända dessa uppgifter till kommissionen, direkt eller genom medlemsstaten, och

b) samarbeta med den behöriga myndigheten vid alla kontroller av de uppgifter som avses i led a.

2. Alla ytterligare uppgifter som kommissionen tar emot direkt ska göras tillgängliga för medlemsstaterna.

3. Uppgifter som tillhandahålls eller mottas i enlighet med denna artikel får endast användas för de ändamål för vilka de tillhandahölls eller mottogs.

Artikel 9

Det ska vara förbjudet att medvetet och avsiktligt delta i verksamhet vars syfte eller verkan är att kringgå åtgärderna i artikel 3.

Artikel 10

1. Om någon fryser penningmedel och ekonomiska resurser eller vägrar att göra penningmedel eller ekonomiska resurser tillgängliga, och detta sker i god tro under antagandet att åtgärden är förenlig med denna förordning, ska detta inte medföra ansvar av något slag för den fysiska eller juridiska person eller den enhet eller det organ som genomför åtgärden, eller för dess ledning eller anställda, såvida det inte kan bevisas att penningmedlen och de ekonomiska resurserna frystes eller hölls inne till följd av vårdslöshet.

2. Handlingar som utförs av fysiska eller juridiska personer, enheter eller organ ska inte medföra ansvar av något slag för deras del, om de inte kände till och inte hade någon rimlig anledning att misstänka att deras handlande skulle strida mot de åtgärder som anges i denna förordning.

Artikel 11

1. 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 denna förordning, 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 bilaga I,

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.

2. I alla förfaranden som syftar till verkställighet av ett krav åligger det den fysiska eller juridiska person, den enhet eller det organ som begär att kravet ska verkställas att visa att detta inte strider mot punkt 1.

3. Denna artikel ska inte påverka den rätt som de fysiska och juridiska personer, enheter och organ som avses i punkt 1 har till domstolsprövning av lagligheten i att vissa avtalsförpliktelser inte uppfylls till följd av denna förordning.

▼B

Artikel 12

1. Kommissionen och medlemsstaterna ska underrätta varandra om de åtgärder som vidtas enligt denna förordning och utbyta alla övriga relevanta uppgifter som de förfogar över med anknytning till förordningen, särskilt uppgifter om

a) penningmedel som frysts enligt artikel 3 och tillstånd som beviljats enligt artiklarna 4, 5, och 6,

b) överträdelser, problem med efterlevnaden samt domar som meddelats i nationella domstolar.

2. Medlemsstaterna ska omedelbart underrätta varandra och kommissionen om andra relevanta uppgifter som de förfogar över och som kan hindra att denna förordning genomförs på ett effektivt sätt.

Artikel 13

1. Om rådet beslutar att tillämpa sådana åtgärder som avses i artikel 3 på en fysisk eller juridisk person, enhet eller organ, ska rådet ändra bilaga I i enlighet med detta.

2. Rådet ska meddela det beslut som avses i punkt 1, inbegripet skälen för upptagande i förteckningen, till den berörda fysiska eller juridiska personen, den berörda enheten eller det berörda organet, antingen direkt, om adressen är känd, eller genom att offentliggöra ett meddelande så att den fysiska eller juridiska personen, enheten eller organet har möjlighet att inkomma med synpunkter.

3. Om synpunkter lämnas, eller om väsentlig ny bevisning läggs fram, ska rådet se över det beslut som avses i punkt 1 och underrätta den berörda fysiska eller juridiska personen, den berörda enheten eller det berörda organet i enlighet med detta.

4. Förteckningen i bilaga I ska ses över regelbundet, och åtminstone var tolfte månad.

5. Kommissionen ska ha befogenhet att ändra bilaga II på grundval av information som lämnas av medlemsstaterna.

Artikel 14

1. Bilaga I ska innehålla skälen till att de berörda fysiska eller juridiska personerna, enheterna eller organen har förts upp på förteckningen.

2. Bilaga I 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 15

1. Medlemsstaterna ska fastställa regler om påföljder för överträdelser av bestämmelserna i denna förordning och vidta alla nödvändiga åtgärder för att säkerställa att reglerna tillämpas. Påföljderna ska vara effektiva, proportionella och avskräckande.

▼B

2. Medlemsstaterna ska anmäla de regler som avses i punkt 1 till kommissionen så snart denna förordning har trätt i kraft samt anmäla senare ändringar till kommissionen.

Artikel 16

1. Kommissionen ska behandla personuppgifter för att fullgöra sina uppgifter enligt denna förordning. I dessa uppgifter ingår att

a) tillföra innehållet i bilaga I i den elektroniska konsoliderade förteckningen över personer, grupper och enheter som är föremål för finansiella sanktioner från unionens sida samt på den interaktiva sanktionskartan, vilka båda finns offentligt tillgängliga,

b) behandla uppgifter om verkningarna av de åtgärder som föreskrivs i denna förordning, såsom uppgifter om värdet på de frysta penningmedlen och om tillstånd som beviljats av de behöriga myndigheterna.

2. För tillämpningen av denna förordning ska den avdelning inom kommissionen som anges i bilaga II utses till *personuppgiftsansvarig* för kommissionen i den mening som avses i artikel 3.8 i förordning (EU) 2018/1725, för att säkerställa att de berörda fysiska personerna kan utöva sina rättigheter enligt den förordningen.

Artikel 17

1. Medlemsstaterna ska utse de behöriga myndigheter som avses i denna förordning och ange dessa på de webbplatser som förtecknas i bilaga II. Medlemsstaterna ska underrätta kommissionen om varje ändring av adresserna till de webbplatser som förtecknas i bilaga II.

2. Medlemsstaterna ska anmäla namnen på sina behöriga myndigheter, inklusive kontaktuppgifter för dessa behöriga myndigheter, till kommissionen så snart denna förordning har trätt i kraft samt anmäla senare ändringar till kommissionen.

3. I de fall då denna förordning föreskriver anmälan, underrättelse eller annat meddelande till kommissionen, ska den adress och de andra kontaktuppgifter som anges i bilaga II användas.

Artikel 18

Denna förordning ska tillämpas

a) inom unionens territorium, inbegripet dess luftrum,

b) ombord på varje flygplan och varje fartyg under en medlemsstats jurisdiktion,

c) på varje fysisk person inom eller utanför unionens territorium som är medborgare i en medlemsstat,

d) på varje juridisk person, enhet eller organ, inom eller utom unionens territorium, som har bildats eller stiftats enligt en medlemsstats rätt,

e) på varje juridisk person, enhet eller organ med avseende på varje form av affärsverksamhet som helt eller delvis bedrivs i unionen.

▼B

Artikel 19

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

Denna förordning är till alla delar bindande och direkt tillämplig i alla medlemsstater.

▼B

BILAGA I

Förteckning över fysiska och juridiska personer, enheter och organ som avses i artikel 3

▼M1

A. Fysiska personer

	Namn	Identifieringsuppgifter	Skäl	Datum för uppförande
▼M3				
1.	GAO Qiang	Födelsedatum: 4 oktober 1983 Födelseort: Shandong Province, China (provinsen Shandong, Kina) Adress: Room 1102, Guanfu Mansion, 46 Xinkai Road, Hedong District, Tianjin, China Nationalitet: kinesisk Kön: man	Gao Qiang är involverad i *Operation Cloud Hopper*, en rad cyberattacker med betydande effekt och med ursprung utanför unionen, som utgör ett externt hot mot unionen eller dess medlemsstater, och cyberattacker som har en betydande effekt på tredjeländer. *Operation Cloud Hopper* har varit inriktad på multinationella företags informationssystem på sex kontinenter, inbegripet företag belägna i unionen, och har skaffat sig otillåten tillgång till kommersiellt känsliga uppgifter, vilket har medfört betydande ekonomiska förluster. Den aktör som är allmänt känd som *APT10* (*Advanced Persistent Threat 10*) (även kallad *Red Apollo*, *CVNX*, *Stone Panda*, *MenuPass* och *Potassium*) genomförde *Operation Cloud Hopper*. Gao Qiang kan kopplas till APT10, bl.a. genom sin koppling till APT10:s ledningsinfrastruktur. Dessutom har Gao Qiang varit anställd av Huaying Haitai, en enhet som förts upp på förteckningen för att ha gett stöd till och underlättat *Operation Cloud Hopper*. Han har kopplingar till Zhang Shilong, som också har förts upp på förteckningen i samband med *Operation Cloud Hopper*. Gao Qiang har därför kopplingar till både Huaying Haitai och Zhang Shilong.	30.7.2020
2.	ZHANG Shilong	Födelsedatum: 10 september 1981 Födelseort: China (Kina) Adress: Hedong, Yuyang Road No 121, Tianjin, China Nationalitet: kinesisk Kön: man	Zhang Shilong är involverad i *Operation Cloud Hopper*, en rad cyberattacker med betydande effekt och med ursprung utanför unionen, som utgör ett externt hot mot unionen eller dess medlemsstater, och cyberattacker som har en betydande effekt på tredjeländer. *Operation Cloud Hopper* har varit inriktad på multinationella företags informationssystem på sex kontinenter, inbegripet företag belägna i unionen, och har skaffat sig otillåten tillgång till kommersiellt känsliga uppgifter, vilket har medfört betydande ekonomiska förluster.	30.7.2020

▼M3

	Namn	Identifieringsuppgifter	Skäl	Datum för uppförande
			Den aktör som är allmänt känd som *APT10* (*Advanced Persistent Threat 10*) (även kallad *Red Apollo*, *CVNX*, *Stone Panda*, *MenuPass* och *Potassium*) genomförde *Operation Cloud Hopper*. Zhang Shilong kan kopplas till APT10, bl.a. genom sabotageprogram som han utvecklade och testade i samband med de cyberattacker som genomfördes av APT10. Dessutom har Zhang Shilong varit anställd av Huaying Haitai, en enhet som förts upp på förteckningen för att ha gett stöd till och underlättat *Operation Cloud Hopper*. Han har kopplingar till Gao Qiang, som också har förts upp på förteckningen i samband med *Operation Cloud Hopper*. Zhang Shilong har därför kopplingar till både Huaying Haitai och Gao Qiang.	

▼M1

3.	Alexey Valeryevich MININ	Алексей Валерьевич МИНИН Födelsedatum: 27 maj 1972 Födelseort: Perm Oblast, (Ryska SFSR) (numera Ryska federationen) Passnummer: 120017582, utfärdat av Ryska federationens utrikesministerium, giltigt 17 april 2017–17 april 2022. Plats: Moskva, Ryska federationen Nationalitet: rysk Kön: man	Alexey Minin deltog i ett försök till cyberattack med en potentiellt betydande effekt på Organisationen för förbud mot kemiska vapen (OPCW) i Nederländerna. I egenskap av officer inom personbaserad inhämtning vid huvuddirektoratet vid generalstaben inom Ryska federationens försvarsmakt (GU/GRU), ingick Aleksej Minin i en grupp bestående av fyra ryska militära underrättelseofficerare som utan tillstånd försökte få tillträde till OPCW:s trådlösa nätverk i Haag i Nederländerna i april 2018. Syftet med försöket till cyberattack var att man skulle hacka sig in i OPCW:s trådlösa nätverk. Om detta hade lyckats skulle det ha äventyrat säkerheten i nätverket och OPCW:s pågående utredningsarbete. Nederländernas *Defence Intelligence and Security Service* (DISS) (Militaire Inlichtingen- en Veiligheidsdienst – MIVD) (försvarets underrättelse- och säkerhetstjänst) avbröt försöket till cyberattack och förhindrade därmed allvarlig skada för OPCW.	30.7.2020
4.	Aleksei Sergeyvich MORENETS	Алексей Сергеевич МОРЕНЕЦ Födelsedatum: 31 juli 1977 Födelseort: Murmanskaya oblast (länet Murmansk), Ryska SFSR (numera Ryska federationen) Passnummer: 100135556, utfärdat av Ryska federationens utrikesministerium, giltigt 17 april 2017–17 april 2022 Plats: Moskva, Ryska federationen Nationalitet: rysk Kön: man	Aleksei Morenets deltog i ett försök till cyberattack med en potentiellt betydande effekt mot Organisationen för förbud mot kemiska vapen (OPCW) i Nederländerna. I egenskap av it-operatör vid huvuddirektoratet vid generalstaben inom Ryska federationens försvarsmakt (GU/GRU), ingick Aleksei Morenets i en grupp bestående av fyra ryska militära underrättelseofficerare som utan tillstånd försökte få tillträde till OPCW:s trådlösa nätverk i Haag i Nederländerna i april 2018. Syftet med försöket till cyberattack var att man skulle hacka sig in i OPCW:s trådlösa nätverk. Om detta hade lyckats skulle det ha äventyrat säkerheten i nätverket och OPCW:s pågående utredningsarbete. Nederländernas *Defence Intelligence and Security Service* (DISS) (Militaire Inlichtingen- en Veiligheidsdienst – MIVD) (försvarets underrättelse- och säkerhetstjänst) avbröt försöket till cyberattack och förhindrade därmed allvarlig skada för OPCW.	30.7.2020

▼M1

	Namn	Identifieringsuppgifter	Skäl	Datum för uppförande
5.	Evgenii Mikhaylovich SEREBRIAKOV	Евгений Михайлович СЕРЕБРЯКОВ Födelsedatum: 26 juli 1981 Födelseort: Kursk, Ryska SFSR (numera Ryska federationen) Passnummer: 100135555, utfärdat av Ryska federationens utrikesministerium, giltigt 17 april 2017–17 april 2022 Plats: Moskva, Ryska federationen Nationalitet: rysk Kön: man	Evgenii Serebriakov deltog i ett försök till cyberattack med en potentiellt betydande effekt mot Organisationen för förbud mot kemiska vapen (OPCW) i Nederländerna. I egenskap av it-operatör vid huvuddirektoratet vid generalstaben inom Ryska federationens försvarsmakt (GU/GRU) ingick Evgenii Serebriakov i en grupp bestående av fyra ryska militära underrättelseofficerare som utan tillstånd försökte få tillträde till OPCW:s trådlösa nätverk i Haag i Nederländerna i april 2018. Syftet med försöket till cyberattack var att man skulle hacka sig in i OPCW:s trådlösa nätverk. Om detta hade lyckats skulle det ha äventyrat säkerheten i nätverket och OPCW:s pågående utredningsarbete. Nederländernas *Defence Intelligence and Security Service* (DISS) (Militaire Inlichtingen- en Veiligheidsdienst – MIVD) (försvarets underrättelse- och säkerhetstjänst) avbröt försöket till cyberattack och förhindrade därmed allvarlig skada för OPCW.	30.7.2020
6.	Oleg Mikhaylovich SOTNIKOV (Oleg Michajlovitj SOTNIKOV)	Олег Михайлович СОТНИКОВ Födelsedatum: 24 augusti 1972 Födelseort: Ulyanovsk (Uljanovsk), Ryska SFSR (numera Ryska federationen) Passnummer: 120018866, utfärdat av Ryska federationens utrikesministerium, giltigt 17 april 2017–17 april 2022 Plats: Moskva, Ryska federationen Nationalitet: rysk Kön: man	Oleg Sotnikov deltog i ett försök till cyberattack med en potentiellt betydande effekt mot Organisationen för förbud mot kemiska vapen (OPCW) i Nederländerna. I egenskap av officer inom personbaserad inhämtning vid huvuddirektoratet vid generalstaben inom Ryska federationens försvarsmakt (GU/GRU) ingick Oleg Sotnikov i en grupp bestående av fyra ryska underrättelseofficerare som utan tillstånd försökte få tillträde till OPCW:s trådlösa nätverk i Haag i Nederländerna i april 2018. Syftet med försöket till cyberattack var att man skulle hacka sig in i OPCW:s trådlösa nätverk. Om detta hade lyckats skulle det ha äventyrat säkerheten i nätverket och OPCW:s pågående utredningsarbete. Nederländernas *Defence Intelligence and Security Service* (DISS) (Militaire Inlichtingen- en Veiligheidsdienst – MIVD) (försvarets underrättelse- och säkerhetstjänst) avbröt försöket till cyberattack och förhindrade därmed allvarlig skada för OPCW.	30.7.2020

▼M1

	Namn	Identifieringsuppgifter	Skäl	Datum för uppförande
▼M2				
7.	Dmitry Sergeyevich BADIN	Дмитрий Сергеевич Бадин Födelsedatum: 15.11.1990 Födelseort: Kursk, Ryska SFSR (numera Ryska federationen) Nationalitet: rysk Kön: man	Dmitry Badin deltog i en cyberattack med betydande effekt mot Tysklands förbundsdag (*Deutscher Bundestag*). I egenskap av militär underrättelseofficer vid *85th Main Centre for Special Services* (GTsSS) (huvudcentrum för specialtjänsten) vid huvuddirektoratet vid generalstaben inom Ryska federationens försvarsmakt (GU/GRU), ingick Dmitry Badin i en grupp bestående av ryska militära underrättelseofficerare som genomförde en cyberattack mot Tysklands förbundsdag (*Deutscher Bundestag*) i april och maj 2015. Denna cyberattack riktade sig mot förbundsdagens informationssystem och påverkade dess funktion under flera dagar. En stor mängd data stals och flera parlamentsledamöters liksom Tysklands förbundskansler Angela Merkels e-postkonton påverkades.	22.10.2020
8.	Igor Olegovich KOSTYUKOV	Игорь Олегович Костюков Födelsedatum: 21.2.1961 Nationalitet: rysk Kön: man	Igor Kostyukov är för närvarande chef för huvuddirektoratet vid generalstaben inom Ryska federationens försvarsmakt (GU/GRU), där han tidigare var förste biträdande chef. En enhet underställd honom är *85th Main Centre for Special Services* (GTsSS) (huvudcentrum för specialtjänsten), även kallad *militär enhet 26165* (inom branschen också kallad *APT28*, *Fancy Bear*, *Sofacy Group*, *Pawn Storm* och *Strontium*). I denna egenskap är Igor Kostyukov ansvarig för de cyberattacker som genomförts av GTsSS, även cyberattacker med betydande effekt som utgör ett externt hot mot unionen eller dess medlemsstater. I synnerhet deltog militära underrättelseofficerare vid GTsSS i cyberattacken mot Tysklands förbundsdag (*Deutscher Bundestag*) som ägde rum i april och maj 2015 och försöket till cyberattack då man skulle hacka sig in i OPCW:s (Organisationen för förbud mot kemiska vapen) trådlösa nätverk i Nederländerna i april 2018. Cyberattacken mot Tysklands förbundsdag riktade sig mot förbundsdagens informationssystem och påverkade dess funktion under flera dagar. En stor mängd data stals och flera parlamentsledamöters liksom Tysklands förbundskansler Angela Merkels e-postkonton påverkades.	22.10.2020

▼M1

B. Juridiska personer, enheter och organ

	Namn	Identifierings-uppgifter	Skäl	Datum för upp-förande
1.	Tianjin Huaying Haitai Science and Technology Development Co. Ltd (Huaying Haitai)	Även kallad: Haitai Technology Development Co. Ltd Plats: Tianjin, Kina	Huaying Haitai tillhandahöll finansiellt, tekniskt eller materiellt stöd till och underlättade *Operation Cloud Hopper*, en rad cyberattacker med betydande effekt och med ursprung utanför unionen, som utgör ett externt hot mot unionen eller dess medlemsstater, och cyberattacker som har en betydande effekt på tredjeländer. *Operation Cloud Hopper* har varit inriktad på multinationella företags informationssystem på sex kontinenter, inbegripet företag belägna i unionen, och har skaffat sig otillåten tillgång till kommersiellt känsliga uppgifter, vilket har medfört betydande ekonomiska förluster. Den aktör som är allmänt känd som *APT10* (*Advanced Persistent Threat 10*) (även kallad *Red Apollo*, *CVNX*, *Stone Panda*, *MenuPass* och *Potassium*) genomförde *Operation Cloud Hopper*. Huaying Haitai kan ha koppling till APT10. Dessutom Gao Qiang och Zhang Shilong, som båda har förts upp på förteckningen i samband med *Operation Cloud Hopper* varit anställda av Huaying Haitai. Huaying Haitai har därför samröre med Gao Qiang och Zhang Shilong.	30.7.2020
2.	Chosun Expo	Även kallad: Chosen Expo; Korea Export Joint Venture Plats: DPRK	Chosun Expo tillhandahöll finansiellt, tekniskt eller materiellt stöd till och underlättade en rad cyberattacker med betydande effekt och med ursprung utanför unionen, som utgör ett externt hot mot unionen eller dess medlemsstater, och cyberattacker som har en betydande effekt på tredjeländer, inbegripet de cyberattacker som allmänt kallas *WannaCry* och cyberattacker mot Polens *Financial Supervision Authority* (finansinspektion) och Sony Pictures Entertainment, samt cyberstöld från Bangladesh Bank och försök till cyberstöld från den vietnamesiska banken Tien Phong Bank. *WannaCry* störde informationssystem världen över genom att angripa informationssystem med utpressningsprogram och blockera åtkomsten till data. Detta påverkade informationssystem hos företag i unionen, inklusive informationssystem som rör tjänster som är nödvändiga för upprätthållande av grundläggande tjänster och ekonomisk verksamhet inom medlemsstaterna.	30.7.2020

▼M1

	Namn	Identifierings-uppgifter	Skäl	Datum för upp-förande
			Den aktör som är allmänt känd som *APT38* (*Advanced Persistent Threat 38*) eller *Lazarus Group* genomförde *WannaCry*. Chosun Expo kan kopplas till APT38/Lazarus Group, inbegripet via de konton som användes för cyberattackerna.	
3.	Main Centre for Special Technologies (GTsST) (huvudcentrum för specialteknik) vid huvuddirektoratet vid generalstaben inom Ryska federationens försvarsmakt (GU/GRU)	Adress: 22 Kirova Street, Moscow, Russian Federation	Huvudcentrumet för specialteknik vid huvuddirektoratet vid generalstaben inom Ryska federationens försvarsmakt, även känd som fältpostnummer 74455, är ansvarigt för cyberattacker med betydande effekt och med ursprung utanför unionen, som utgör ett externt hot mot unionen eller dess medlemsstater, och cyberattacker som har en betydande effekt på tredjeländer, inbegripet de cyberattacker som allmänt kallas *NotPetya* eller *EternalPetya* i juni 2017 och de cyberattacker som riktades mot ett ukrainskt kraftnät under vintern 2015/2016. *NotPetya* eller *EternalPetya* gjorde data oåtkomliga i ett antal företag i unionen, i Europa och världen över genom att angripa datorer med utpressningsprogram och blockera tillgången till data, vilket bland annat resulterade i betydande ekonomiska förluster. Cyberattacker på ett ukrainskt kraftnät ledde till att delar av nätet stängdes av under vintern.	30.7.2020
			Den aktör som är känd som *Sandworm* (även kallad *SandwormTeam*, *BlackEnergy Group*, *Voodoo Bear*, *Quedagh*, *Olympic Destroyer*, *Telebots*) ligger också bakom attacken på det ukrainska kraftnätet som utfördes av *NotPetya* eller *EternalPetya*. Huvudcentrumet för specialteknik vid huvuddirektoratet vid generalstaben vid Ryska federationens försvarsmakt har en aktiv roll i den cyberverksamhet som utförs av Sandworm och kan kopplas till Sandworm.	

▼M1

	Namn	Identifierings-uppgifter	Skäl	Datum för upp-förande
▼M2				
4.	85th Main Centre for Special Services (GTsSS) (huvudcentrum för specialtjänsten) vid huvuddirektoratet vid generalstaben inom Ryska federationens försvarsmakt (GU/GRU)	Adress: Komsomol'skiy Prospekt, 20, Moscow, 119146, Russian Federation	*85th Main Centre for Special Services* (GTsSS) (huvudcentrum för specialtjänsten) vid huvuddirektoratet vid generalstaben inom Ryska federationens försvarsmakt (GU/GRU), även kallad *militär enhet 26165* (inom branschen också kallad *APT28*, *Fancy Bear*, *Sofacy Group*, *Pawn Storm* och *Strontium*) är ansvarigt för cyberattacker med betydande effekt som utgör ett externt hot mot unionen eller dess medlemsstater. I synnerhet deltog militära underrättelseofficerare vid GTsSS i cyberattacken mot Tysklands förbundsdag (*Deutscher Bundestag*) som ägde rum i april och maj 2015 och försöket till cyberattack då man skulle hacka sig in i OPCW:s (Organisationen för förbud mot kemiska vapen) trådlösa nätverk i Nederländerna i april 2018. Cyberattacken mot Tysklands förbundsdag riktade sig mot förbundsdagens informationssystem och påverkade dess funktion under flera dagar. En stor mängd data stals och flera parlamentsledamöters liksom Tysklands förbundskansler Angela Merkels e-postkonton påverkades.	22.10.2020

▼B

BILAGA II

Webbplatser med uppgifter om de behöriga myndigheterna samt adress för anmälningar, meddelanden och underrättelser till kommissionen

▼M4

BELGIEN

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

BULGARIEN

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

TJECKIEN

www.financnianalytickyurad.cz/mezinarodni-sankce.html

DANMARK

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

TYSKLAND

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

ESTLAND

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

IRLAND

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

GREKLAND

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

SPANIEN

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

FRANKRIKE

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

KROATIEN

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

ITALIEN

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

CYPERN

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

LETTLAND

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

LITAUEN

http://www.urm.lt/sanctions

LUXEMBURG

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

UNGERN

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

▼**M4**

MALTA

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

NEDERLÄNDERNA

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

ÖSTERRIKE

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

POLEN

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

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

PORTUGAL

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

RUMÄNIEN

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

SLOVENIEN

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

SLOVAKIEN

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

FINLAND

https://um.fi/pakotteet

SVERIGE

https://www.regeringen.se/sanktioner

Adress för anmälan till Europeiska kommissionen:

Europeiska kommissionen

Generaldirektoratet för finansiell stabilitet, finansiella tjänster och kapitalmarknadsunionen (GD FISMA)

Rue de Spa/Spastraat 2

1049 Bruxelles/Brussel, BELGIEN

E-post: relex-sanctions@ec.europa.eu