►**B**

RÅDETS BESLUT (GUSP) 2019/797

av den 17 maj 2019

om restriktiva åtgärder mot cyberattacker som hotar unionen eller dess medlemsstater

(EUT L 129I, 17.5.2019, s. 13)

Ändrad genom:

		Officiella tidningen		
		nr	sida	datum
►**M1**	Rådets beslut (Gusp) 2020/651 av den 14 maj 2020	L 153	4	15.5.2020
►**M2**	Rådets beslut (Gusp) 2020/1127 av den 30 juli 2020	L 246	12	30.7.2020
►**M3**	Rådets beslut (Gusp) 2020/1537 av den 22 oktober 2020	L 351 I	5	22.10.2020
►**M4**	Rådets beslut (Gusp) 2020/1748 av den 20 november 2020	L 393	19	23.11.2020
►**M5**	Rådets beslut (Gusp) 2021/796 av den 17 maj 2021	L 174 I	1	18.5.2021
►**M6**	Rådets beslut (Gusp) 2022/754 av den 16 maj 2022	L 138	16	17.5.2022

Rättad genom:

►**C1** Rättelse, EUT L 230, 17.7.2020, s. 36 (2019/797)

▼B

RÅDETS BESLUT (GUSP) 2019/797

av den 17 maj 2019

om restriktiva åtgärder mot cyberattacker som hotar unionen eller dess medlemsstater

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),

▼B

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.

▼B

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.

▼B

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.

▼B

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) ►C1 nödvändiga för att täcka grundläggande behov för de fysiska eller juridiska personer, enheter eller organ 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

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.

▼B

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.

▼M6

Artikel 10

Detta beslut ska tillämpas till och med den 18 maj 2025 och ska ses över fortlöpande. De åtgärder som anges i artiklarna 4 och 5 ska vad gäller fysiska och juridiska personer, enheter och organ som förtecknas i bilagan tillämpas till och med den 18 maj 2023.

▼B

Artikel 11

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

▼B

BILAGA

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

▼M2

A. Fysiska personer

▼M4

	Namn	Identifieringsuppgifter	Skäl	Datum för uppförande
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.	30.7.2020

▼M4

	Namn	Identifieringsuppgifter	Skäl	Datum för uppförande
			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*. 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.	

▼M2

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

▼M2

	Namn	Identifieringsuppgifter	Skäl	Datum för uppförande
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
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

▼M2

	Namn	Identifieringsuppgifter	Skäl	Datum för uppförande
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
▼M3 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

▼M3

	Namn	Identifieringsuppgifter	Skäl	Datum för uppförande
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

▼M2

B. Juridiska personer, enheter och organ

	Namn	Identifierings-uppgifter	Skäl	Datum för uppförande
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.	30.7.2020

▼M2

	Namn	Identifierings-uppgifter	Skäl	Datum för uppförande
			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.	
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. 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.	30.7.2020

▼M2

	Namn	Identifierings-uppgifter	Skäl	Datum för uppförande
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. 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.	30.7.2020

▼M3

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.	22.10.2020

▼M3

	Namn	Identifierings-uppgifter	Skäl	Datum för uppförande
			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.	