RÅDETS BESLUT (Gusp) 2020/1127

av den 30 juli 2020

om ändring av beslut (Gusp) 2019/797 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 17 maj 2019 antog rådet beslut (Gusp) 2019/797 ([1]).

(2) Riktade restriktiva åtgärder mot cyberattacker med en betydande effekt, som utgör ett externt hot för unionen eller dess medlemsstater är bland de åtgärder som ingår i unionens ram för en gemensam diplomatisk respons mot skadlig it-verksamhet (verktygslådan för cyberdiplomati) och är ett viktigt instrument för att avskräcka och reagera på sådan verksamhet. Restriktiva åtgärder kan också tillämpas som svar på cyberattacker med betydande effekt på tredjeländer eller internationella organisationer, om det anses nödvändigt för att uppnå målen för den gemensamma utrikes- och säkerhetspolitiken som anges i de relevanta bestämmelserna i artikel 21 i fördraget om Europeiska unionen.

(3) Den 16 april 2018 antog rådet slutsatser där man fördömde skadlig användning av informations- och kommunikationsteknik, inbegripet de cyberattacker som allmänt kallas *WannaCry* och *NotPetya*, som har orsakat stor skada och betydande ekonomiska förluster både i och utanför EU. Den 4 oktober 2018 uttryckte Europeiska rådets ordförande, Europeiska kommissionens ordförande och unionens höga representant för utrikes frågor och säkerhetspolitik (den höga representanten) allvarliga farhågor i ett gemensamt uttalande om ett försök till cyberattack som syftade till att undergräva integriteten för Organisationen för förbud mot kemiska vapen (OPCW) i Nederländerna, en aggressiv handling som visade förakt för det allvarliga syftet med OPCW. I ett uttalande som gjordes på unionens vägnar av den 12 april 2019 uppmanade den höga representanten aktörerna att sluta ägna sig åt skadlig it-verksamhet som syftar till att undergräva unionens integritet, säkerhet och ekonomiska konkurrenskraft, inbegripet stölder av immateriella rättigheter, som möjliggörs av informationsteknik. Till sådana stölder räknas stölder som utförs av den aktör som allmänt är känd som *APT10* (*Advance Persistent Threat 10*).

(4) I detta sammanhang och för att förebygga, avskräcka, motverka och bemöta fortsatta och ökande skadliga ageranden i cyberrymden bör sex fysiska personer och tre enheter eller organ föras upp på förteckningen över fysiska och juridiska personer, enheter och organ som är föremål för restriktiva åtgärder som anges i bilagan till beslut (Gusp) 2019/797. Dessa personer och enheter eller organ är ansvariga för, tillhandahållit stöd för eller har varit involverade i, eller underlättat cyberattacker eller försök till cyberattacker, inbegripet försöket till cyberattack mot OPCW och de cyberattacker som allmänt är kända som *WannaCry* och *NotPetya* samt *Operation Cloud Hoppers*.

(5) Beslut (Gusp) 2019/797 bör därför ändras i enlighet med detta.

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

Artikel 1

Bilagan till beslut (Gusp) 2019/797 ska ändras i enlighet med bilagan till det här beslutet.

([1]) 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).

Artikel 2

Detta beslut träder i kraft samma dag som det offentliggörs i *Europeiska unionens officiella tidning*.

Utfärdat i Bryssel den 30 juli 2020.

På rådets vägnar
M. ROTH
Ordförande

BILAGA

Följande personer och enheter eller organ ska läggas till i förteckningen över fysiska och juridiska personer, enheter och organ i bilagan till beslut (Gusp) 2019/797:

”A. Fysiska personer

	Namn	Identifieringsuppgifter	Skäl	Datum för uppförande
1.	GAO Qiang	Födelseort: Shandongprovinsen, Kina Adress: Room 1102, Guanfu Mansion, 46 Xinkai Road, Hedong District, Tianjin, Kina 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 and Zhang Shilong.	30.7.2020
2.	ZHANG Shilong	Adress: Hedong, Yuyang Road No 121, Tianjin, Kina 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. 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*.	30.7.2020

			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.	
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

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

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

			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
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.	30.7.2020”

			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 *Sandworm Team*, *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.	