RÅDETS AFGØRELSE (FUSP) 2020/1127

af 30. juli 2020

om ændring af afgørelse (FUSP) 2019/797 om restriktive foranstaltninger til bekæmpelse af cyberangreb, der truer Unionen eller dens medlemsstater

RÅDET FOR DEN EUROPÆISKE UNION HAR —

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

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

ud fra følgende betragtninger:

(1) Rådet vedtog den 17. maj 2019 afgørelse (FUSP) 2019/797 ([1]).

(2) Målrettede restriktive foranstaltninger til bekæmpelse af cyberangreb med betydelige konsekvenser, der udgør en ekstern trussel mod Unionen eller dens medlemsstater, er blandt foranstaltningerne i Unionens ramme for en fælles diplomatisk reaktion på ondsindede cyberaktiviteter (»cyberdiplomatisk værktøjskasse«) og er et afgørende instrument til at afskrække fra og reagere på sådanne aktiviteter. Restriktive foranstaltninger kan også anvendes som reaktion på cyberangreb med betydelige konsekvenser for tredjelande eller internationale organisationer, hvis det skønnes nødvendigt for at nå målene inden for den fælles udenrigs- og sikkerhedspolitik i de relevante bestemmelser i artikel 21 i traktaten for Den Europæiske Union.

(3) Rådet vedtog den 16. april 2018 konklusioner, hvori det kraftigt fordømte den ondsindede brug af informations- og kommunikationsteknologier, herunder i de cyberangreb, der offentligt er kendt som »WannaCry« og »NotPetya«, og som har forårsaget væsentlig skade og økonomiske tab i og uden for Unionen. Den 4. oktober 2018 gav formændene for Det Europæiske Råd og Europa-Kommissionen og Unionens højtstående repræsentant for udenrigsanliggender og sikkerhedspolitik (»den højtstående repræsentant«) udtryk for alvorlige betænkeligheder i en fælles erklæring om et forsøg på cyberangreb for at underminere integriteten i Organisationen for Forbud mod Kemiske Våben (OPCW) i Nederlandene, en aggressiv handling, der udviser foragt for det højtidelige formål med OPCW. I en erklæring på vegne af Unionen den 12. april 2019 opfordrede den højtstående repræsentant aktørerne til at ophøre med at udføre ondsindede cyberaktiviteter med det formål at undergrave Unionens integritet, sikkerhed og økonomiske konkurrenceevne, herunder tilfælde af cyberbaseret tyveri af intellektuel ejendom. Sådanne cyberbaserede tyverier omfatter tyverier, der udføres af den aktør, som offentlig er kendt som »APT10« (»Advanced Persistent Threat 10«).

(4) I den forbindelse og for at forhindre, modvirke, afskrække fra og reagere på fortsat og øget ondsindet adfærd i cyberspace bør seks fysiske personer og tre enheder eller organer opføres på listen over fysiske og juridiske personer, enheder og organer, der er omfattet af restriktive foranstaltninger, i bilaget til afgørelse (FUSP) 2019/797. Disse personer og enheder eller organer er ansvarlige for, har ydet støtte til eller været involveret i eller har lettet cyberangreb eller forsøg på cyberangreb, herunder forsøget på cyberangreb mod OPCW og de cyberangreb, der offentligt er kendt som »WannaCry« og »NotPetya«, samt »Operation Cloud Hopper«.

(5) Afgørelse (FUSP) 2019/797 bør derfor ændres i overensstemmelse hermed —

VEDTAGET DENNE AFGØRELSE:

Artikel 1

Bilaget til afgørelse (FUSP) 2019/797 ændres i overensstemmelse med bilaget til nærværende afgørelse.

([1]) Rådets afgørelse (FUSP) 2019/797 af 17. maj 2019 om restriktive foranstaltninger til bekæmpelse af cyberangreb, der truer Unionen eller dens medlemsstater (EUT L 129 I af 17.5.2019, s. 13).

Artikel 2

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

Udfærdiget i Bruxelles, den 30. juli 2020.

På Rådets vegne
M. ROTH
Formand

BILAG

Følgende personer og enheder eller organer tilføjes på listen over fysiske og juridiske personer, enheder og organer, som findes i bilaget til afgørelse (FUSP) 2019/797:

»A. Fysiske personer

	Navn	Identificerende oplysninger	Begrundelse	Dato for opførelse
1.	GAO Qiang	Fødested: Shandongprovinsen, Kina Adresse: Room 1102, Guanfu Mansion, 46 Xinkai Road, Hedong District, Tianjin, China Nationalitet: kinesisk Køn: mand	Gao Qiang er involveret i »Operation Cloud Hopper«, en række cyberangreb med betydelige konsekvenser og med oprindelse uden for Unionen, som udgør en ekstern trussel mod Unionen eller dets medlemsstater, og i cyberangreb, som har betydelige konsekvenser for tredjelande. »Operation Cloud Hopper« har været rettet mod multinationale selskabers informationssystemer på seks kontinenter, herunder virksomheder i Unionen, og har opnået uautoriseret adgang til kommercielt følsomme data, hvilket har medført et betydeligt økonomisk tab. Den aktør, der offentligt er kendt som »APT10« (»Advanced Persistent Threat 10«) (alias »Red Apollo«, »CVNX«, »Stone Panda«, »MenuPass« og »Potassium«), gennemførte »Operation Cloud Hopper«. Gao Qiang kan sættes i forbindelse med APT10, bl.a. gennem sin tilknytning til APT10's kommando- og kontrolinfrastruktur. Desuden ansatte Huaying Haitai, en enhed, der er opført på listen for at have ydet støtte til og lettet »Operation Cloud Hopper«, Gao Qiang. Han har forbindelser til Zhang Shilong, som også er opført på listen i forbindelse med »Operation Cloud Hopper«. Gao Qiang har således tilknytning til både Huaying Haitai og Zhang Shilong.	30.7.2020
2.	ZHANG Shilong	Adresse: Hehong, Yuyang Road nr. 121, Tianjin, Kina Nationalitet: kinesisk Køn: mand	Zhang Shilong er involveret i »Operation Cloud Hopper«, en række cyberangreb med betydelige konsekvenser og med oprindelse uden for Unionen, som udgør en ekstern trussel mod Unionen eller dets medlemsstater, og i cyberangreb, som har betydelige konsekvenser for tredjelande. »Operation Cloud Hopper« har været rettet mod multinationale selskabers informationssystemer på seks kontinenter, herunder virksomheder i Unionen, og har opnået uautoriseret adgang til kommercielt følsomme data, hvilket har medført et betydeligt økonomisk tab. Den aktør, der offentligt er kendt som »APT10« (»Advanced Persistent Threat 10«) (alias »Red Apollo«, »CVNX«, »Stone Panda«, »MenuPass« og »Potassium«), gennemførte »Operation Cloud Hopper«.	30.7.2020

			Zhang Shilong kan sættes i forbindelse med APT10, herunder den malware, han har udviklet og testet i forbindelse med de cyberangreb, der er blevet udført af APT10. Desuden ansatte Huaying Haitai, en enhed, der er opført på listen for at have ydet støtte til og lettet »Operation Cloud Hopper«, Zhang Shilong. Han har forbindelser til Gao Qiang, som også er opført på listen i forbindelse med »Operation Cloud Hopper«. Zhang Shilong har således tilknytning til både Huaying Haitai og Gao Qiang.	
3.	Alexey Valeryevich MININ	Алексей Валерьевич МИНИН Fødselsdato: 27. maj 1972 Fødested: Perm Oblast, russiske SFSR (nu Den Russiske Føderation) Pasnummer: 120017582, udstedt af Den Russiske Føderations udenrigsministerium Gyldighed: fra den 17. april 2017 til den 17. april 2022 Sted: Moskva, Den Russiske Føderation Nationalitet: russisk Køn: mand	Alexey Minin deltog i et forsøg på cyberangreb med potentielt betydelige konsekvenser for Organisationen for Forbud mod Kemiske Våben (OPCW) i Nederlandene. Som støtteofficer for menneskelige efterretninger ved hoveddirektoratet for Den Russiske Føderations væbnede styrkers generalstab (GU/GRU) var Alexey Minin en del af et hold bestående af fire russiske militære efterretningsofficerer, der forsøgte at få uautoriseret adgang til OPCW's wi-fi-net i Haag, Nederlandene, i april 2018. Formålet med forsøget på cyberangreb var at hacke sig ind i OPCW's wi-fi-net, hvilket, hvis det var lykkedes, ville have undergravet nettets sikkerhed og OPCW's igangværende undersøgelser. Den nederlandske forsvars- og sikkerhedstjeneste (DISS) (Militaire Inlichtingen- en Veiligheidsdienst — MIVD) forpurrede forsøget på cyberangreb og forhindrede derved, at OPCW led alvorlig overlast.	30.7.2020
4.	Aleksei Sergeyvich MORENETS	Алексей Сергеевич МОРЕНЕЦ Fødselsdato: 31. juli 1977 Fødested: Murmanskaya Oblast, russiske SFSR (nu Den Russiske Føderation) Pasnummer: 100135556, udstedt af Den Russiske Føderations udenrigsministerium Gydighed: fra den 17. april 2017 til den 17. april 2022 Sted: Moskva, Den Russiske Føderation Nationalitet: russisk Køn: mand	Aleksei Morenets deltog i et forsøg på cyberangreb med potentielt betydelige konsekvenser for Organisationen for Forbud mod Kemiske Våben (OPCW) i Nederlandene. Som cyberoperatør ved hoveddirektoratet for Den Russiske Føderations væbnede styrkers generalstab (GU/GRU) var Aleksei Morenets en del af et hold bestående af fire russiske militære efterretningsofficerer, der forsøgte at få uautoriseret adgang til OPCW's wi-fi-net i Haag, Nederlandene, i april 2018. Formålet med forsøget på cyberangreb var at hacke sig ind i OPCW's wi-fi-net, hvilket, hvis det var lykkedes, ville have kompromitteret nettets sikkerhed og OPCW's igangværende undersøgelser. Den nederlandske militære efterretningstjeneste (DISS) (Militaire Inlichtingen- en Veiligheidsdienst — MIVD) forpurrede forsøget på cyberangreb og forhindrede derved, at OPCW led alvorlig overlast.	30.7.2020

5.	Evgenii Mikhaylovich SEREBRIAKOV	Евгений Михайлович СЕРЕБРЯКОВ Fødselsdato: 26. juli 1981 Fødested: Kursk, russiske SFSR (nu Den Russiske Føderation) Pasnummer: 100135555, udstedt af Den Russiske Føderations udenrigsministerium Gyldighed: fra den 17. april 2017 til den 17. april 2022 Sted: Moskva, Den Russiske Føderation Nationalitet: russisk Køn: mand	Evgenii Serebriakov deltog i et forsøg på cyberangreb med potentielt betydelige konsekvenser for Organisationen for Forbud mod Kemiske Våben (OPCW) i Nederlandene. Som cyberoperatør ved hoveddirektoratet for Den Russiske Føderations væbnede styrkers generalstab (GU/GRU) var Evgenii Serebriakov en del af et hold bestående af fire russiske militære efterretningsofficerer, der forsøgte at få uautoriseret adgang til OPCW's wi-fi-net i Haag, Nederlandene, i april 2018. Formålet med forsøget på cyberangreb var at hacke sig ind i OPCW's wi-fi-net, hvilket, hvis det var lykkedes, ville have kompromitteret nettets sikkerhed og OPCW's igangværende undersøgelser. Den nederlandske militære efterretningstjeneste (DISS) (Militaire Inlichtingen- en Veiligheidsdienst — MIVD) forpurrede forsøget på cyberangreb og forhindrede derved, at OPCW led alvorlig overlast.	30.7.2020
6.	Oleg Mikhaylovich SOTNIKOV	Олег Михайлович СОТНИКОВ Fødselsdato: 24. august 1972 Fødested: Ulyanovsk, russiske SFSR (nu Den Russiske Føderation) Pasnummer: 120018866, udstedt af Den Russiske Føderations udenrigsministerium Gyldighed: fra den 17. april 2017 til den 17. april 2022 Sted: Moskva, Den Russiske Føderation Nationalitet: russisk Køn: mand	Oleg Sotnikov deltog i et forsøg på cyberangreb med potentielt betydelige konsekvenser for Organisationen for Forbud mod Kemiske Våben (OPCW) i Nederlandene. Som støtteofficer for menneskelige efterretninger ved hoveddirektoratet for Den Russiske Føderations væbnede styrkers generalstab (GU/GRU) var Oleg Sotnikov en del af et hold bestående af fire russiske militære efterretningsofficerer, der forsøgte at få uautoriseret adgang til OPCW's wi-fi-net i Haag, Nederlandene, i april 2018. Formålet med forsøget på cyberangreb var at hacke sig ind i OPCW's wi-fi-net, hvilket, hvis det var lykkedes, ville have kompromitteret nettets sikkerhed og OPCW's igangværende undersøgelser. Den nederlandske militære efterretningstjeneste (DISS) (Militaire Inlichtingen- en Veiligheidsdienst — MIVD) forpurrede forsøget på cyberangreb og forhindrede derved, at OPCW led alvorlig overlast.	30.7.2020

B. Juridiske personer, enheder og organer

	Navn	Identificerende oplysninger	Begrundelse	Dato for opførelse
1.	Tianjin Huaying Haitai Science and Technology Development Co Ltd (Huaying Haitai)	Alias Haitai Technology Development Co. Ltd Sted: Tianjin, Kina	Huaying Haitai har ydet finansiel, teknisk eller materiel støtte til og lettet »Operation Cloud Hopper«, en række cyberangreb med betydelige konsekvenser og med oprindelse uden for Unionen, som udgør en ekstern trussel mod Unionen eller dets medlemsstater, og i cyberangreb, som har betydelige konsekvenser for tredjelande.	30.7.2020

			»Operation Cloud Hopper« har været rettet mod multinationale selskabers informationssystemer på seks kontinenter, herunder virksomheder i Unionen, og har opnået uautoriseret adgang til kommercielt følsomme data, hvilket har medført et betydeligt økonomisk tab. Den aktør, der offentligt er kendt som »APT10« (»Advanced Persistent Threat 10«) (alias »Red Apollo«, »CVNX«, »Stone Panda«, »MenuPass« og »Potassium«), gennemførte »Operation Cloud Hopper«. Huaying Haitai kan sættes i forbindelse med APT10. Desuden har Huaying Haitai ansat Gao Qiang og Zhang Shilong, som begge er opført på listen i forbindelse med »Operation Cloud Hopper«. Huaying Haitai har således tilknytning til både Gao Qiang og Zhang Shilong.	
2.	Chosun Expo	Alias Chosen Expo; Korea Export Joint Venture Sted: DPRK	Chosun Expo har ydet finansiel, teknisk eller materiel støtte til og lettet en række cyberangreb med betydelige konsekvenser og med oprindelse uden for Unionen, og som udgør en ekstern trussel mod Unionen eller dets medlemsstater, og i cyberangreb med betydelige konsekvenser for tredjelande, herunder de cyberangreb, der offentligt er kendt som »WannaCry«, samt angrebene mod det polske finanstilsyn og Sony Pictures Entertainment samt cybertyveri fra Bangladesh Bank og forsøg på cybertyveri fra Vietnam Tien Phong Bank. »WannaCry« forstyrrede informationssystemerne rundt om i verden ved at ramme informationssystemerne med ransomware og blokere adgangen til data. Det påvirkede informationssystemer i virksomheder i Unionen, herunder informationssystemer vedrørende tjenesteydelser, der er nødvendige for at opretholde væsentlige tjenester og økonomiske aktiviteter i medlemsstaterne. Den aktør, der offentligt er kendt som »APT38« (»Advanced Persistent Threat 38«), eller »Lazarusgruppen« gennemførte »WannaCry«. Chosun Expo kan forbindes med APT38/Lazarusgruppen, herunder gennem de konti, der blev anvendt til cyberangrebene.	30.7.2020
3.	Main Centre for Special Technologies (GTsST) of the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GU/GRU)	Adresse: 22 Kirova Street, Moskva, Den Russiske Føderation	Hovedcentret for særlige teknologier (Main Centre for Special Technologies (GTsST)) ved hoveddirektoratet for Den Russiske Føderations væbnede styrkers generalstab (GU/GGRU), også kendt med sit feltnummer 74455, er ansvarligt for cyberangreb med betydelige konsekvenser og med oprindelse uden for Unionen, som udgør en ekstern trussel mod Unionen eller dets medlemsstater, og for cyberangreb, som har betydelige konsekvenser for tredjelande, herunder de cyberangreb, der offentligt er kendt som »NotPetya« eller »EternalPetya« i juni 2017, og de cyberangreb, der var rettet mod et ukrainsk elnet i vinteren 2015 og 2016.	30.7.2020«

			»NotPetya« eller »EternalPetya« blokerede adgangen til data i en række virksomheder i Unionen, i det øvrige Europa og i resten af verden, ved at ramme computere med ransomware og blokere adgangen til data, hvilket bl.a. medførte betydelige økonomiske tab. Cyberangrebet på et ukrainsk elnet førte til, at dele af det blev afbrudt om vinteren. Den aktør, der offentligt er kendt som »Sandworm« (alias »Sandworm Team«, »BlackEnergy Group«, »Voodoo Bear«, »Quedagh«, »Olympic Destroyer« og »Telebots«), og som også stod bag angrebet på det ukrainske elnet, gennemførte »NotPetya« eller »EternalPetya«. Hovedcentret for særlige teknologier i hoveddirektoratet for Den Russiske Føderations væbnede styrkers generalstab spiller en aktiv rolle i de cyberaktiviteter, der er udført af Sandworm, og kan sættes i forbindelse med Sandworm.	