2025/887

13.5.2025

RÅDETS AFGØRELSE (FUSP) 2025/887

af 12. maj 2025

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) Afgørelse (FUSP) 2019/797 finder anvendelse indtil den 18. maj 2025. På grundlag af en gennemgang af nævnte afgørelse vurderer Rådet, at anvendelsen heraf bør forlænges indtil den 18. maj 2028.

(3) På grundlag af en fornyet gennemgang af bilaget til afgørelse (FUSP) 2019/797 bør anvendelsen af foranstaltningerne i nævnte afgørelses artikel 4 og 5 på de fysiske og juridiske personer, enheder og organer, der er opført på listen i nævnte bilag, forlænges indtil den 18. maj 2026. Desuden bør begrundelserne for opførelsen af seks personer på listen over fysiske og juridiske personer, enheder og organer, der er omfattet af restriktive foranstaltninger, ajourføres.

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

VEDTAGET DENNE AFGØRELSE:

Artikel 1

I afgørelse (FUSP) 2019/797 foretages følgende ændringer:

1) Artikel 10 affattes således:

»*Artikel 10*

Denne afgørelse finder anvendelse indtil den 18. maj 2028 og overvåges løbende. Foranstaltningerne fastsat i artikel 4 og 5 finder anvendelse på de fysiske og juridiske personer, enheder og organer, der er opført på listen i bilaget, indtil den 18. maj 2026.«

2) Bilaget ændres som angivet i bilaget til nærværende afgørelse.

Artikel 2

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

Udfærdiget i Bruxelles, den 12. maj 2025.

På Rådets vegne

B. NOWACKA

Formand

([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, ELI: http://data.europa.eu/eli/dec/2019/797/oj).

BILAG

I bilaget til afgørelse (FUSP) 2019/797 under overskriften »A. Fysiske personer« affattes punkt 3-8 således:

	Navn	Identificerende oplysninger	Begrundelse	Dato for opførelse
»3.	Alexey Valeryevich MININ	Алексей Валерьевич МИНИН Fødselsdato: 27.5.1972 Fødested: Perm Oblast, Russiske SFSR (nu Den Russiske Føderation) Pasnummer: 120017582 Udstedt af: Den Russiske Føderations udenrigsministerium Gyldighed: fra den 17.4.2017 til den 17.4.2022 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 og i cyberangreb med betydelige konsekvenser for tredjelande. 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 kompromitteret nettets sikkerhed og OPCW's igangværende undersøgelser. Den nederlandske militære efterretningstjeneste (Militaire Inlichtingen- en Veiligheidsdienst) forpurrede forsøget på cyberangreb og forhindrede derved, at OPCW led alvorlig overlast. En storjury i Pennsylvanias vestlige kreds (Western District of Pennsylvania) (USA) har rejst tiltale mod Alexey Minin som officer i GRU for computerhacking, elektronisk bedrageri, groft identitetstyveri og hvidvask af penge. GRU udfører fortsat aktivt cyberangreb mod Unionen eller dens medlemsstater. Som medlem af GRU er Alexey Minin derfor involveret i cyberangreb med betydelige konsekvenser, herunder forsøg på cyberangreb med potentielt betydelige konsekvenser, der udgør en ekstern trussel mod Unionen eller dens medlemsstater.	30.7.2020

	Navn	Identificerende oplysninger	Begrundelse	Dato for opførelse
4.	Aleksei Sergeyvich MORENETS	Алексей Сергеевич МОРЕНЕЦ Fødselsdato: 31.7.1977 Fødested: Murmanskaya Oblast, Russiske SFSR (nu Den Russiske Føderation) Pasnummer: 100135556 Udstedt af: Den Russiske Føderations udenrigsministerium Gyldighed: fra den 17.4.2017 til den 17.4.2022 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 og i cyberangreb med betydelige konsekvenser for tredjelande. 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 (Militaire Inlichtingen- en Veiligheidsdienst) forpurrede forsøget på cyberangreb og forhindrede derved, at OPCW led alvorlig overlast. En storjury i Pennsylvanias vestlige kreds (Western District of Pennsylvania) (USA) har rejst tiltale mod Aleksei Morenets som tilknyttet militærenhed 26165 for computerhacking, elektronisk bedrageri, groft identitetstyveri og hvidvask af penge. GRU udfører fortsat aktivt cyberangreb mod Unionen eller dens medlemsstater. Som medlem af GRU er Aleksei Morenets derfor involveret i cyberangreb med betydelige konsekvenser, herunder forsøg på cyberangreb med potentielt betydelige konsekvenser, der udgør en ekstern trussel mod Unionen eller dens medlemsstater.	30.7.2020

	Navn	Identificerende oplysninger	Begrundelse	Dato for opførelse
5.	Evgenii Mikhaylovich SEREBRIAKOV	Евгений Михайлович СЕРЕБРЯКОВ Fødselsdato: 26.7.1981 Fødested: Kursk, Russiske SFSR (nu Den Russiske Føderation) Pasnummer: 100135555 Udstedt af: Den Russiske Føderations udenrigsministerium Gyldighed: fra den 17.4.2017 til den 17.4.2022 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 og i cyberangreb med betydelige konsekvenser for tredjelande. 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 (Militaire Inlichtingen- en Veiligheidsdienst) forpurrede forsøget på cyberangreb og forhindrede derved, at OPCW led alvorlig overlast. Siden foråret 2022 har Evgenii Serebriakov ledet »Sandworm« (alias »Sandworm Team«, »BlackEnergy Group«, »Voodoo Bear«, »Quedagh«, »Olympic Destroyer« og »Telebots«), en aktør og hackinggruppe, der er tilknyttet enhed 74455 i Ruslands øverste efterretningsdirektorat. Sandworm har foretaget cyberangreb på Ukraine, herunder ukrainske regeringsorganer, efter Ruslands angrebskrig mod Ukraine. GRU udfører fortsat aktivt cyberangreb mod Unionen eller dens medlemsstater. Som medlem af GRU er Evgenii Serebriakov derfor involveret i cyberangreb med betydelige konsekvenser, herunder forsøg på cyberangreb med potentielt betydelige konsekvenser, der udgør en ekstern trussel mod Unionen eller dens medlemsstater.	30.7.2020

	Navn	Identificerende oplysninger	Begrundelse	Dato for opførelse
6.	Oleg Mikhaylovich SOTNIKOV	Олег Михайлович СОТНИКОВ Fødselsdato: 24.8.1972 Fødested: Ulyanovsk, Russiske SFSR (nu Den Russiske Føderation) Pasnummer: 120018866 Udstedt af: Den Russiske Føderations udenrigsministerium Gyldighed: fra den 17.4.2017 til den 17.4.2022 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 og i cyberangreb med betydelige konsekvenser for tredjelande. 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 (Militaire Inlichtingen- en Veiligheidsdienst) forpurrede forsøget på cyberangreb og forhindrede derved, at OPCW led alvorlig overlast. En storjury i Pennsylvanias vestlige kreds (Amerikas Forenede Stater) har rejst tiltale mod Oleg Sotnikov som officer i GRU for computerhacking, elektronisk bedrageri, groft identitetstyveri og hvidvask af penge. GRU udfører fortsat aktivt cyberangreb mod Unionen eller dens medlemsstater. Som medlem af GRU er Oleg Sotnikov derfor involveret i cyberangreb med betydelige konsekvenser, herunder forsøg på cyberangreb med potentielt betydelige konsekvenser, der udgør en ekstern trussel mod Unionen eller dens medlemsstater.	30.7.2020

	Navn	Identificerende oplysninger	Begrundelse	Dato for opførelse
7.	Dmitry Sergeyevich BADIN	Дмитрий Сергеевич БАДИН Fødselsdato: 15.11.1990 Fødested: Kursk, Russiske SFSR (nu Den Russiske Føderation) Nationalitet: russisk Køn: mand	Dmitry Badin deltog i et cyberangreb med betydelige konsekvenser mod den tyske Forbundsdag (Deutscher Bundestag) og i cyberangreb med betydelige konsekvenser for tredjelande. Som militær efterretningsofficer i 85. hovedcenter for særlige tjenester (85th Main Centre for Special Services (GTsSS)) ved hoveddirektoratet for Den Russiske Føderations væbnede styrkers generalstab (GU/GRU) var Dmitry Badin en del af et hold bestående af russiske militære efterretningsofficerer, som udførte et cyberangreb mod den tyske Forbundsdag i april og maj 2015. Dette cyberangreb havde parlamentets informationssystem som sit mål og påvirkede dets drift i flere dage. Der blev stjålet en betydelig mængde data, og flere parlamentsmedlemmers e-mailkonti samt forhenværende kansler Angela Merkels e-mailkonto blev berørt. En storjury i Pennsylvanias vestlige kreds (Western District of Pennsylvania) (USA) har rejst tiltale mod Dmitry Badin som tilknyttet militærenhed 26165 for computerhacking, elektronisk bedrageri, groft identitetstyveri og hvidvask af penge. GRU udfører fortsat aktivt cyberangreb mod Unionen eller dens medlemsstater. Som medlem af GRU er Dmitry Badin derfor involveret i cyberangreb med betydelige konsekvenser, herunder forsøg på cyberangreb med potentielt betydelige konsekvenser, der udgør en ekstern trussel mod Unionen eller dens medlemsstater.	22.10.2020

	Navn	Identificerende oplysninger	Begrundelse	Dato for opførelse
8.	Igor Olegovich KOSTYUKOV	Игорь Олегович КОСТЮКОВ Fødselsdato: 21.2.1961 Nationalitet: russisk Køn: mand	Igor Kostyukov er den nuværende chef for hoveddirektoratet for Den Russiske Føderations væbnede styrkers generalstab (GU/GRU), hvor han tidligere var første vicechef. En af enhederne under hans kommando er 85. hovedcenter for særlige tjenester (85th Main Centre for Special Services (GTsSS)) (alias »militærenhed 26165«, »APT28«, »Fancy Bear«, »Sofacy Group«, »Pawn Storm« og »Strontium«). I denne egenskab er Igor Kostyukov ansvarlig for cyberangreb, der blev udført af GTsSS, herunder angreb med betydelige konsekvenser, der udgør en ekstern trussel mod Unionen eller dens medlemsstater. Navnlig deltog militære efterretningsofficerer i GTsSS i cyberangrebet på den tyske Forbundsdag (Deutscher Bundestag) i april og maj 2015 og forsøget på cyberangreb, hvis formål var at hacke sig ind i Organisationen for Forbud mod Kemiske Våbens (OPCW's) wi-fi-net i Nederlandene i april 2018. Cyberangrebet mod den tyske Forbundsdag havde parlamentets informationssystem som sit mål og påvirkede dets drift i flere dage. Der blev stjålet en betydelig mængde data, og flere parlamentsmedlemmers e-mailkonti samt forhenværende kansler Angela Merkels e-mailkonto blev berørt. GRU udfører fortsat aktivt cyberangreb mod Unionen eller dens medlemsstater. Som medlem af GRU er Igor Kostyukov derfor involveret i cyberangreb med betydelige konsekvenser, herunder forsøg på cyberangreb med potentielt betydelige konsekvenser, der udgør en ekstern trussel mod Unionen eller dens medlemsstater.	22.10.2020«.