AFGØRELSER

RÅDETS AFGØRELSE (FUSP) 2020/1537

af 22. oktober 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.

(3) For at forhindre, modvirke, afskrække fra og reagere på fortsat og øget ondsindet adfærd i cyberspace bør to fysiske personer og et organ 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 det organ er ansvarlige for eller har været involveret i cyberangreb med betydelige konsekvenser, der udgør en ekstern trussel mod Unionen eller dens medlemsstater, navnlig cyberangrebet mod den tyske Forbundsdag (Deutscher Bundestag), som fandt sted i april og maj 2015.

(4) 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.

Artikel 2

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

Udfærdiget i Bruxelles, den 22. oktober 2020.

På Rådets vegne
M. ROTH
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 129I af 17.5.2019, s. 13).

BILAG

Følgende punkter 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
»7.	Dmitry Sergeyevich BADIN	Дмитрий Сергеевич БАДИН Fødselsdato: 15. november 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). Som militær efterretningsofficer i 85th Main Centre for Special Services (GTsSS) of the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GU/GRU) var Dmitry Badin en del af et hold bestående af russiske militære efterretningsofficerer, som udførte et cyberangreb mod den tyske Forbundsdag (Deutscher Bundestag) 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 kansler Angela Merkels e-mailkonto blev berørt.	22.10.2020
8.	Igor Olegovich KOSTYUKOV	Игорь Олегович КОСТЮКОВ Fødselsdato: 21. februar 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 85th Main Centre for Special Services (GTsSS), der også er kendt som »militærenhed 26165« (branchetilnavne: »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), som fandt sted 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 kansler Angela Merkels e-mailkonto blev berørt.	22.10.2020«

B. Juridiske personer, enheder og organer

	Navn	Identificerende oplysninger	Begrundelse	Dato for opførelse
»4.	85th Main Centre for Special Services (GTsSS) of the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GU/GRU)	Adresse: Komsomol'skiy Prospekt, 20, Moscow, 119146, Russian Federation	85th Main Centre for Special Services (GTsSS) of the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GU/GRU), der også er kendt som »militærenhed 26165« (branchetilnavne: »APT28«, »Fancy Bear«, »Sofacy Group«, »Pawn Storm« og »Strontium«), er ansvarlig for cyberangreb 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), som fandt sted 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 kansler Angela Merkels e-mailkonto blev berørt.	22.10.2020«