Rådet for
Den Europæiske Union

Bruxelles, den 13. maj 2024
(OR. en)

8502/24

LIMITE

CORLX 356
CFSP/PESC 512
RELEX 467
CYBER 110
JAI 572
FIN 341

LOVGIVNINGSMÆSSIGE RETSAKTER OG ANDRE INSTRUMENTER

Vedr.:	RÅDETS GENNEMFØRELSESFORORDNING om gennemførelse af forordning (EU) 2019/796 om restriktive foranstaltninger til bekæmpelse af cyberangreb, der truer Unionen eller dens medlemsstater

RÅDETS GENNEMFØRELSESFORORDNING (EU) 2024/…

af …

om gennemførelse af forordning (EU) 2019/796 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 Unions funktionsmåde,

under henvisning til Rådets forordning (EU) 2019/796 af 17. maj 2019 om restriktive foranstaltninger til bekæmpelse af cyberangreb, der truer Unionen eller dens medlemsstater[1], særlig artikel 13, stk. 1,

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

ud fra følgende betragtninger:

[1] EUT L 129 I af 17.5.2019, s. 1.

(1) Rådet vedtog den 17. maj 2019 forordning (EU) 2019/796.

(2) I lyset af den fortsatte og stigende ondsindede adfærd i cyberspace, herunder adfærd rettet mod tredjelande, bør begrundelserne for at tilføje seks personer og to enheder på listen over fysiske og juridiske personer, enheder og organer, der er omfattet af restriktive foranstaltninger som fastsat i bilag I til forordning (EU) 2019/796, ajourføres.

(3) Bilag I til forordning (EU) 2019/796 bør derfor ændres i overensstemmelse hermed —

VEDTAGET DENNE FORORDNING:

Artikel 1

Bilag I til forordning (EU) 2019/796 ændres som angivet i bilaget til nærværende forordning.

Artikel 2

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

Denne forordning er bindende i alle enkeltheder og gælder umiddelbart i hver medlemsstat.

Udfærdiget i …, den …

På Rådets vegne
Formand

BILAG

I bilag I til forordning (EU) 2019/796 ("Liste over fysiske og juridiske personer, enheder og organer som omhandlet i artikel 3") foretages følgende ændringer:

1) I listen med 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 Ruslands øverste efterretningsdirektorat (GRU) for computerhacking, elektronisk bedrageri, groft identitetstyveri og hvidvask af penge.	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.	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.	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 (Western District of Pennsylvania) har rejst tiltale mod Oleg Sotnikov som officer i Ruslands øverste efterretningsdirektorat (GRU) for computerhacking, elektronisk bedrageri, groft identitetstyveri og hvidvask af penge.	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.	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.	22.10.2020".

2) I listen med overskriften "B. Juridiske personer, enheder og organer" affattes punkt 3 og 4 således:

	Navn	Identificerende oplysninger	Begrundelse	Dato for opførelse
"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, Moscow, Russian Federation	Hovedcentret for særlige teknologier (Main Centre for Special Technologies (GTsST)) ved hoveddirektoratet for Den Russiske Føderations væbnede styrkers generalstab (GU/GRU), også kendt med sit feltnummer 74455, er involveret i cyberangreb med betydelige konsekvenser og med oprindelse uden for Unionen, som udgør en ekstern trussel mod Unionen eller dens medlemsstater, og i 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. "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.	30.7.2020

	Navn	Identificerende oplysninger	Begrundelse	Dato for opførelse
			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". Sandworm har foretaget cyberangreb på Ukraine, herunder ukrainske regeringsorganer og ukrainsk kritisk infrastruktur, efter indledningen af Ruslands angrebskrig mod Ukraine. Disse cyberangreb omfatter spearphishing-kampagner og malware- og ransomwareangreb. 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.	

	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	85. hovedcenter for særlige tjenester (85th Main Centre for Special Services (GTsSS)) ved hoveddirektoratet for Den Russiske Føderations væbnede styrkers generalstab (GU/GRU) (alias "militærenhed 26165", "APT28", "Fancy Bear", "Sofacy Group", "Pawn Storm" og "Strontium"), er involveret i cyberangreb med betydelige konsekvenser, der udgør en ekstern trussel mod Unionen eller dens medlemsstater, og i cyberangreb med betydelige konsekvenser for tredjelande. 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. Efter indledningen af Ruslands angrebskrig mod Ukraine blev der foretaget cyberangreb af GTsSS (spearphishing og malwarebaserede angreb) på Ukraine.	22.10.2020".