2025/173

27.1.2025

RÅDETS GENNEMFØRELSESFORORDNING (EU) 2025/173

af 27. januar 2025

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

(2) Målrettede restriktive foranstaltninger til bekæmpelse af cyberangreb med betydelige konsekvenser, der udgør en ekstern trussel mod Unionen eller dens medlemsstater, er en af de foranstaltninger, der indgår i Unionens ramme for en fælles diplomatisk reaktion på ondsindede cyberaktiviteter, nemlig den cyberdiplomatiske værktøjskasse, og er et afgørende instrument til at forebygge, afskrække fra, modvirke og reagere på sådanne aktiviteter.

(3) Ondsindede cyberaktiviteter mod kritisk infrastruktur eller væsentlige tjenester, herunder gennem brug af ransomware og wipere, målretning mod forsyningskæder og cyberspionage, herunder tyveri af intellektuelle ejendomsrettigheder, er stigende for så vidt angår antal, hyppighed og sofistikeringsgrad. Med deres skadelige og ødelæggende virkninger udgør disse aktiviteter en systemisk trussel mod Unionens sikkerhed, økonomi og demokrati og samfundet som helhed.

(4) I 2020 blev der gennemført cyberangreb med betydelige konsekvenser mod Estland. Der blev gennemført cyberangreb rettet mod adskillige institutioners computersystemer med det formål at anvende dataene til at true Estlands sikkerhed. Disse angreb vedrørte opbevaring af klassificerede informationer.

(5) Som led i den fortsatte skræddersyede og koordinerede EU-indsats over for persistente cybertrusselsaktører bør tre fysiske personer opføres på listen over fysiske og juridiske personer, enheder og organer, der er omfattet af restriktive foranstaltninger, i bilag I til forordning (EU) 2019/796. Disse personer er ansvarlige for eller er involveret i cyberangreb med betydelige konsekvenser, der udgør en ekstern trussel mod Unionen eller dens medlemsstater.

(6) 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 på dagen for offentliggørelsen i *Den Europæiske Unions Tidende*.

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

Udfærdiget i Bruxelles, den 27. januar 2025.

På Rådets vegne

K. KALLAS

Formand

([1]) EUT L 129 I af 17.5.2019, s. 1 ELI: http://data.europa.eu/eli/reg/2019/796/oj.

BILAG

Følgende punkter tilføjes under overskriften »A. Fysiske personer« i bilag I til forordning (EU) 2019/796:

	Navn	Identificerende oplysninger	Begrundelse	Dato for opførelse
»15.	Nikolay Alexandrovich KORCHAGIN	Николай Александрович Корчагин Fødselsdato: 16.9.1997 Nationalitet: russisk Køn: mand Tilknyttet enhed: hoveddirektoratet for Den Russiske Føderations væbnede styrkers generalstab	Nikolay Korchagin er involveret i og ansvarlig for cyberangreb med betydelige konsekvenser ved gennemførelse af efterretningsaktiviteter rettet mod Estland og ulovlig opnåelse af adgang til et computersystem. Nikolay Korchagin er officer i militær enhed 29155 i hoveddirektoratet for Den Russiske Føderations væbnede styrkers generalstab (GRU). I denne rolle er han involveret i og ansvarlig for cyberangreb mod computersystemer, som har til formål at indsamle data fra flere institutioners datasystemer, som uafhængigt eller i kombination giver et overblik over Estlands cybersikkerhedspolitik, statens cyberkapacitet, følsomme personoplysninger og andre følsomme oplysninger, med det formål at anvende dataene til at true Estlands sikkerhed. Angrebene vedrører derfor lagring af klassificerede informationer. Angrebene vedrørte Estlands allierede og partnere. Nikolay Korchagin er derfor involveret i og ansvarlig for cyberangreb med betydelige konsekvenser, der udgør en ekstern trussel mod en medlemsstat.	27.1.2025
16.	Vitaly SHEVCHENKO	Виталий Шевченко Fødselsdato: 1.9.1997 Nationalitet: russisk Køn: mand Tilknyttet enhed: hoveddirektoratet for Den Russiske Føderations væbnede styrkers generalstab	Vitaly Shevchenko er involveret i og ansvarlig for cyberangreb med betydelige konsekvenser ved gennemførelse af efterretningsaktiviteter rettet mod Estland og ulovlig opnåelse af adgang til et computersystem. Vitaly Shevchenko er officer i militær enhed 29155 i hoveddirektoratet for Den Russiske Føderations væbnede styrkers generalstab (GRU). I denne rolle er han involveret i og ansvarlig for cyberangreb mod computersystemer, som har til formål at indsamle data fra flere institutioners datasystemer, som uafhængigt eller i kombination giver et overblik over Estlands cybersikkerhedspolitik, statens cyberkapacitet, følsomme personoplysninger og andre følsomme oplysninger, med det formål at anvende dataene til at true Estlands sikkerhed. Angrebene vedrører derfor lagring af klassificerede informationer. Angrebene vedrørte Estlands allierede og partnere. Vitaly Shevchenko er derfor involveret i og ansvarlig for cyberangreb med betydelige konsekvenser, der udgør en ekstern trussel mod en medlemsstat.	27.1.2025

ELI: http://data.europa.eu/eli/reg_impl/2025/173/oj

	Navn	Identificerende oplysninger	Begrundelse	Dato for opførelse
17.	Yuriy Fedorovich DENISOV	Юрий Федорович Денисов Fødselsdato: 17.6.1980 Nationalitet: russisk Køn: mand Tilknyttet enhed: hoveddirektoratet for Den Russiske Føderations væbnede styrkers generalstab	Yuriy Denisov er involveret i og ansvarlig for cyberangreb med betydelige konsekvenser ved gennemførelse af efterretningsaktiviteter rettet mod Estland og ulovlig opnåelse af adgang til et computersystem. Yuriy Denisov er officer i militær enhed 29155 i hoveddirektoratet for Den Russiske Føderations væbnede styrkers generalstab (GRU). I denne rolle er han involveret i og ansvarlig for cyberangreb mod computersystemer, som har til formål at indsamle data fra flere institutioners datasystemer, som uafhængigt eller i kombination giver et overblik over Estlands cybersikkerhedspolitik, statens cyberkapacitet, følsomme personoplysninger og andre følsomme oplysninger, med det formål at anvende dataene til at true Estlands sikkerhed. Angrebene vedrører derfor lagring af klassificerede informationer. Angrebene vedrørte Estlands allierede og partnere. Yuriy Denisov er derfor involveret i og ansvarlig for cyberangreb med betydelige konsekvenser, der udgør en ekstern trussel mod en medlemsstat.	27.1.2025«.