2025/173

27.1.2025

RÅDETS GENOMFÖRANDEFÖRORDNING (EU) 2025/173

av den 27 januari 2025

om genomförande av förordning (EU) 2019/796 om restriktiva åtgärder mot cyberattacker som hotar unionen eller dess medlemsstater

EUROPEISKA UNIONENS RÅD HAR ANTAGIT DENNA FÖRORDNING

med beaktande av fördraget om Europeiska unionens funktionssätt,

med beaktande av rådets förordning (EU) 2019/796 av den 17 maj 2019 om restriktiva åtgärder mot cyberattacker som hotar unionen eller dess medlemsstater ([1]), särskilt artikel 13.1,

med beaktande av förslaget från unionens höga representant för utrikes frågor och säkerhetspolitik, och

av följande skäl:

(1) Den 17 maj 2019 antog rådet förordning (EU) 2019/796.

(2) Riktade restriktiva åtgärder mot cyberattacker med en betydande effekt, som utgör ett externt hot för unionen eller dess medlemsstater, är en av de åtgärder som ingår i unionens ram för en gemensam diplomatisk respons mot skadlig cyberverksamhet, nämligen verktygslådan för cyberdiplomati, och är ett viktigt instrument för att förebygga, motverka, avskräcka, och bemöta sådan verksamhet.

(3) Skadlig cyberverksamhet mot kritisk infrastruktur eller grundläggande tjänster, bland annat genom användning av utpressningsprogram och wipers, inriktning på leveranskedjor och cyberspionage, inbegripet stöld av immateriella rättigheter, blir allt vanligare, mer frekvent och sofistikerad. Med sina omvälvande och destruktiva effekter utgör sådan verksamhet ett systemhot mot unionens säkerhet, ekonomi och demokrati och samhället i stort.

(4) Under 2020 genomfördes cyberattacker med en betydande effekt mot Estland. Cyberattacker mot flera institutioners datorsystem genomfördes i syfte att använda uppgifterna för att hota Estlands säkerhet. Dessa cyberattacker rörde sig om lagring av säkerhetsskyddsklassificerade uppgifter.

(5) Som en del i de kontinuerliga, skräddarsydda och samordnade unionsinsatserna mot aktörer som utgör ett ihållande cyberhot bör tre fysiska personer föras upp på förteckningen över fysiska och juridiska personer, enheter och organ som är föremål för restriktiva åtgärder som anges i bilaga I till förordning (EU) 2019/796. Dessa personer är ansvariga för eller inblandade i cyberattacker med en betydande effekt som utgör ett externt hot mot unionen eller dess medlemsstater.

(6) Bilaga I till förordning (EU) 2019/796 bör därför ändras i enlighet med detta.

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

Artikel 1

Bilaga I till förordning (EU) 2019/796 ska ändras i enlighet med bilagan till den här förordningen.

Artikel 2

Denna förordning träder i kraft samma dag som den offentliggörs i *Europeiska unionens officiella tidning*.

Denna förordning är till alla delar bindande och direkt tillämplig i alla medlemsstater.

Utfärdad i Bryssel den 27 januari 2025.

På rådets vägnar

K. KALLAS

Ordförande

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

BILAGA

I bilaga I till förordning (EU) 2019/796 ska följande poster läggas till i avsnitt ”A. Fysiska personer”:

	Namn	Identifieringsuppgifter	Skäl	Datum för uppförande
”15.	Nikolay Alexandrovich KORCHAGIN	Николай Александрович Корчагин Födelsedatum: 16.9.1997 Nationalitet: rysk Kön: man Associerad enhet: huvuddirektoratet vid generalstaben inom Ryska federationens försvarsmakt	Nikolay Korchagin är inblandad i och ansvarig för cyberattacker med en betydande effekt genom att bedriva underrättelseverksamhet riktad mot Estland och genom att olagligen skaffa sig tillgång till ett datorsystem. Nikolay Korchagin är officer vid militärenhet 29155 vid huvuddirektoratet vid generalstaben inom Ryska federationens försvarsmakt (GRU). I denna roll är han inblandad i och ansvarig för cyberattacker mot datorsystem i syfte att samla in uppgifter från flera institutioners datasystem, som var för sig eller tillsammans ger en överblick över Estlands cybersäkerhetspolitik, statens cyberkapacitet, känsliga personuppgifter och andra känsliga uppgifter, i syfte att använda uppgifterna för att hota Estlands säkerhet. Attackerna rör därför lagring av säkerhetsskyddsklassificerade uppgifter. Attackerna berörde allierade och partner till Estland. Nikolay Korchagin är därför inblandad i och ansvarig för cyberattacker med en betydande effekt som utgör ett externt hot mot en medlemsstat.	27.1.2025
16.	Vitaly SHEVCHENKO	Виталий Шевченко Födelsedatum: 1.9.1997 Nationalitet: rysk Kön: man Associerad enhet: huvuddirektoratet vid generalstaben inom Ryska federationens försvarsmakt	Vitaly Shevchenko är inblandad i och ansvarig för cyberattacker med en betydande effekt genom att bedriva underrättelseverksamhet riktad mot Estland och genom att olagligen skaffa sig tillgång till ett datorsystem. Vitaly Shevchenko är officer vid militärenhet 29155 vid huvuddirektoratet vid generalstaben inom Ryska federationens försvarsmakt (GRU). I denna roll är han inblandad i och ansvarig för cyberattacker mot datorsystem i syfte att samla in uppgifter från flera institutioners datasystem, som var för sig eller tillsammans ger en överblick över Estlands cybersäkerhetspolitik, statens cyberkapacitet, känsliga personuppgifter och andra känsliga uppgifter, i syfte att använda uppgifterna för att hota Estlands säkerhet. Attackerna rör därför lagring av säkerhetsskyddsklassificerade uppgifter. Attackerna berörde allierade och partner till Estland. Vitaly Shevchenko är därför inblandad i och ansvarig för cyberattacker med en betydande effekt som utgör ett externt hot mot en medlemsstat.	27.1.2025

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

	Namn	Identifieringsuppgifter	Skäl	Datum för uppförande
17.	Yuriy Fedorovich DENISOV	Юрий Федорович Денисов Födelsedatum: 17.6.1980 Nationalitet: rysk Kön: man Associerad enhet: huvuddirektoratet vid generalstaben inom Ryska federationens försvarsmakt	Yuriy Denisov är inblandad i och ansvarig för cyberattacker med en betydande effekt genom att bedriva underrättelseverksamhet riktad mot Estland och genom att olagligen skaffa sig tillgång till ett datorsystem. Yuriy Denisov är officer vid militärenhet 29155 vid huvuddirektoratet vid generalstaben inom Ryska federationens försvarsmakt (GRU). I denna roll är han inblandad i och ansvarig för cyberattacker mot datorsystem i syfte att samla in uppgifter från flera institutioners datasystem, som var för sig eller tillsammans ger en överblick över Estlands cybersäkerhetspolitik, statens cyberkapacitet, känsliga personuppgifter och andra känsliga uppgifter, i syfte att använda uppgifterna för att hota Estlands säkerhet. Attackerna rör därför lagring av säkerhetsskyddsklassificerade uppgifter. Attackerna berörde allierade och partner till Estland. Yuriy Denisov är därför inblandad i och ansvarig för cyberattacker med en betydande effekt som utgör ett externt hot mot en medlemsstat.	27.1.2025”.