II

(Icke-lagstiftningsakter)

FÖRORDNINGAR

RÅDETS GENOMFÖRANDEFÖRORDNING (EU) 2020/1536

av den 22 oktober 2020

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 betydande effekt, som utgör ett externt hot mot unionen eller dess medlemsstater är bland de åtgärder som ingår i unionens ram för en gemensam diplomatisk respons mot skadlig it-verksamhet (verktygslådan för cyberdiplomati) och är ett viktigt instrument för att avskräcka och reagera på sådan verksamhet.

(3) För att förebygga, avskräcka, motverka och bemöta fortsatta och ökande skadliga ageranden i cyberrymden bör två fysiska personer och ett organ 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 och detta organ är ansvariga för eller har varit involverade i cyberattacker med betydande effekt som utgör ett externt hot mot unionen eller dess medlemsstater, särskilt cyberattacken mot Tysklands förbundsdag (*Deutscher Bundestag*) som ägde rum i april och maj 2015.

(4) 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.

([1]) EUT L 129 I, 17.5.2019, s. 1.

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 22 oktober 2020.

På rådets vägnar
M. ROTH
Ordförande

BILAGA

Följande poster ska läggas till i förteckningen över fysiska och juridiska personer, enheter och organ i bilaga I till förordning (EU) 2019/796:

A. Fysiska personer

	Namn	Identifieringsuppgifter	Skäl	Datum för uppförande
”7.	Dmitry Sergeyevich BADIN	Дмитрий Сергеевич Бадин Födelsedatum: 15.11.1990 Födelseort: Kursk, Ryska SFSR (numera Ryska federationen) Nationalitet: rysk Kön: man	Dmitry Badin deltog i en cyberattack med betydande effekt mot Tysklands förbundsdag (*Deutscher Bundestag*). I egenskap av militär underrättelseofficer vid *85th Main Centre for Special Services* (GTsSS) (huvudcentrum för specialtjänsten) vid huvuddirektoratet vid generalstaben inom Ryska federationens försvarsmakt (GU/GRU), ingick Dmitry Badin i en grupp bestående av ryska militära underrättelseofficerare som genomförde en cyberattack mot Tysklands förbundsdag (*Deutscher Bundestag*) i april och maj 2015. Denna cyberattack riktade sig mot förbundsdagens informationssystem och påverkade dess funktion under flera dagar. En stor mängd data stals och flera parlamentsledamöters liksom Tysklands förbundskansler Angela Merkels e-postkonton påverkades.	22.10.2020
8.	Igor Olegovich KOSTYUKOV	Игорь Олегович Костюков Födelsedatum: 21.2.1961 Nationalitet: rysk Kön: man	Igor Kostyukov är för närvarande chef för huvuddirektoratet vid generalstaben inom Ryska federationens försvarsmakt (GU/GRU), där han tidigare var förste biträdande chef. En enhet underställd honom är *85th Main Centre for Special Services* (GTsSS) (huvudcentrum för specialtjänsten), även kallad *militär enhet 26165* (inom branschen också kallad *APT28*, *Fancy Bear*, *Sofacy Group*, *Pawn Storm* och *Strontium*). I denna egenskap är Igor Kostyukov ansvarig för de cyberattacker som genomförts av GTsSS, även cyberattacker med betydande effekt som utgör ett externt hot mot unionen eller dess medlemsstater. I synnerhet deltog militära underrättelseofficerare vid GTsSS i cyberattacken mot Tysklands förbundsdag (*Deutscher Bundestag*) som ägde rum i april och maj 2015 och försöket till cyberattack då man skulle hacka sig in i OPCW:s (Organisationen för förbud mot kemiska vapen) trådlösa nätverk i Nederländerna i april 2018. Cyberattacken mot Tysklands förbundsdag riktade sig mot förbundsdagens informationssystem och påverkade dess funktion under flera dagar. En stor mängd data stals och flera parlamentsledamöters liksom Tysklands förbundskansler Angela Merkels e-postkonton påverkades.”	22.10.2020

B. Juridiska personer, enheter och organ

	Namn	Identifieringsuppgifter	Skäl	Datum för uppförande
”4.	85th Main Centre for Special Services (GTsSS) (huvudcentrum för specialtjänsten) vid huvuddirektoratet vid generalstaben inom Ryska federationens försvarsmakt (GU/GRU)	Adress: Komsomol'skiy Prospekt, 20, Moscow, 119146, Russian Federation	*85th Main Centre for Special Services* (GTsSS) (huvudcentrum för specialtjänsten) vid huvuddirektoratet vid generalstaben inom Ryska federationens försvarsmakt (GU/GRU), även kallad *militär enhet 26165* (inom branschen också kallad *APT28*, *Fancy Bear*, *Sofacy Group*, *Pawn Storm* och *Strontium*) är ansvarigt för cyberattacker med betydande effekt som utgör ett externt hot mot unionen eller dess medlemsstater. I synnerhet deltog militära underrättelseofficerare vid GTsSS i cyberattacken mot Tysklands förbundsdag (*Deutscher Bundestag*) som ägde rum i april och maj 2015 och försöket till cyberattack då man skulle hacka sig in i OPCW:s (Organisationen för förbud mot kemiska vapen) trådlösa nätverk i Nederländerna i april 2018. Cyberattacken mot Tysklands förbundsdag riktade sig mot förbundsdagens informationssystem och påverkade dess funktion under flera dagar. En stor mängd data stals och flera parlamentsledamöters liksom Tysklands förbundskansler Angela Merkels e-postkonton påverkades.	22.10.2020”