2025/887

13.5.2025

RÅDETS BESLUT (Gusp) 2025/887

av den 12 maj 2025

om ändring av beslut (Gusp) 2019/797 om restriktiva åtgärder mot cyberattacker som hotar unionen eller dess medlemsstater

EUROPEISKA UNIONENS RÅD HAR ANTAGIT DETTA BESLUT

med beaktande av fördraget om Europeiska unionen, särskilt artikel 29,

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

av följande skäl:

(1) Den 17 maj 2019 antog rådet beslut (Gusp) 2019/797 ([1]).

(2) Beslut (Gusp) 2019/797 är tillämpligt till och med den 18 maj 2025. På grundval av en översyn av det beslutet anser rådet att dess tillämpning bör förlängas till och med den 18 maj 2028.

(3) På grundval av en översyn av bilagan till beslut (Gusp) 2019/797 bör tillämpningen av de åtgärder som anges i artiklarna 4 och 5 i det beslutet vad gäller de fysiska och juridiska personer, enheter och organ som förtecknas i den bilagan förlängas till och med den 18 maj 2026. Dessutom bör skälen för att inkludera sex personer i förteckningen över fysiska och juridiska personer, enheter och organ som omfattas av restriktiva åtgärder uppdateras.

(4) Beslut (Gusp) 2019/797 bör därför ändras i enlighet med detta.

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

Artikel 1

Beslut (Gusp) 2019/797 ska ändras på följande sätt:

1. Artikel 10 ska ersättas med följande:

”*Artikel 10*

Detta beslut ska tillämpas till och med den 18 maj 2028 och ska ses över fortlöpande. De åtgärder som anges i artiklarna 4 och 5 ska, avseende de fysiska och juridiska personer, enheter och organ som förtecknas i bilagan, tillämpas till och med den 18 maj 2026.”

2. Bilagan ska ändras i enlighet med bilagan till det här beslutet.

Artikel 2

Detta beslut träder i kraft dagen efter det att det har offentliggjorts i *Europeiska unionens officiella tidning*.

Utfärdat i Bryssel den 12 maj 2025.

På rådets vägnar

B. NOWACKA

Ordförande

([1]) Rådets beslut (Gusp) 2019/797 av den 17 maj 2019 om restriktiva åtgärder mot cyberattacker som hotar unionen eller dess medlemsstater (EUT L 129 I, 17.5.2019, s. 13, ELI: http://data.europa.eu/eli/dec/2019/797/oj).

BILAGA

I bilagan till beslut (Gusp) 2019/797 under rubriken ”A. Fysiska personer” ska posterna 3–8 ersättas med följande:

	Namn	Identifieringsuppgifter	Skäl	Datum för uppförande
”3.	Alexey Valeryevich MININ	Алексей Валерьевич МИНИН Födelsedatum: 27.5.1972 Födelseort: Perm Oblast (länet Perm), Ryska SFSR (numera Ryska federationen) Passnummer: 120017582 Utfärdat av: Ryska federationens utrikesministerium Giltighet: 17.4.2017–17.4.2022 Plats: Moskva, Ryska federationen Nationalitet: rysk Kön: man	Alexey Minin deltog i ett försök till cyberattack med en potentiellt betydande effekt på Organisationen för förbud mot kemiska vapen (OPCW) i Nederländerna och i cyberattacker med en betydande effekt mot tredjeländer. I egenskap av officer inom personbaserad inhämtning vid huvuddirektoratet vid generalstaben inom Ryska federationens försvarsmakt (GU/GRU), ingick Alexey Minin i en grupp bestående av fyra ryska militära underrättelseofficerare som utan tillstånd försökte få tillträde till OPCW:s trådlösa nätverk i Haag i Nederländerna i april 2018. Syftet med försöket till cyberattack var att man skulle hacka sig in i OPCW:s trådlösa nätverk. Om detta hade lyckats skulle det ha äventyrat säkerheten i nätverket och OPCW:s pågående utredningsarbete. Nederländernas Defence Intelligence and Security Service (Militaire Inlichtingen- en Veiligheidsdienst) avbröt försöket till cyberattack och förhindrade därmed allvarlig skada för OPCW. En åtalsjury i Pennsylvanias västra distrikt (Amerikas förenta stater) har åtalat Alexey Minin i egenskap av officer vid GRU, för hackning, nätbedrägeri, grov identitetsstöld och penningtvätt. GRU fortsätter att aktivt utföra cyberattacker mot unionen eller dess medlemsstater. I egenskap av medlem i GRU är Alexey Minin därför inblandad i cyberattacker med en betydande effekt, inbegripet försök till cyberattacker med en potentiellt betydande effekt, som utgör ett externt hot för unionen eller dess medlemsstater.	30.7.2020

	Namn	Identifieringsuppgifter	Skäl	Datum för uppförande
4.	Aleksei Sergeyvich MORENETS	Алексей Сергеевич МОРЕНЕЦ Födelsedatum: 31.7.1977 Födelseort: Murmanskaya Oblast (länet Murmansk), Ryska SFSR (numera Ryska federationen) Passnummer: 100135556 Utfärdat av: Ryska federationens utrikesministerium Giltighet: 17.4.2017–17.4.2022 Plats: Moskva, Ryska federationen Nationalitet: rysk Kön: man	Aleksei Morenets deltog i ett försök till cyberattack med en potentiellt betydande effekt på Organisationen för förbud mot kemiska vapen (OPCW) i Nederländerna och i cyberattacker med en betydande effekt mot tredjeländer. I egenskap av it-operatör vid huvuddirektoratet vid generalstaben inom Ryska federationens försvarsmakt (GU/GRU), ingick Aleksei Morenets i en grupp bestående av fyra ryska militära underrättelseofficerare som utan tillstånd försökte få tillträde till OPCW:s trådlösa nätverk i Haag i Nederländerna i april 2018. Syftet med försöket till cyberattack var att man skulle hacka sig in i OPCW:s trådlösa nätverk. Om detta hade lyckats skulle det ha äventyrat säkerheten i nätverket och OPCW:s pågående utredningsarbete. Nederländernas Defence Intelligence and Security Service (Militaire Inlichtingen- en Veiligheidsdienst) avbröt försöket till cyberattack och förhindrade därmed allvarlig skada för OPCW. En åtalsjury i Pennsylvanias västra distrikt (Amerikas förenta stater) har åtalat Aleksei Morenets i egenskap av medlem av militärenhet 26165, för hackning, nätbedrägeri, grov identitetsstöld och penningtvätt GRU fortsätter att aktivt utföra cyberattacker mot unionen eller dess medlemsstater. I egenskap av medlem i GRU är Aleksei Morenets därför inblandad i cyberattacker med en betydande effekt, inbegripet försök till cyberattacker med en potentiellt betydande effekt, som utgör ett externt hot för unionen eller dess medlemsstater.	30.7.2020

	Namn	Identifieringsuppgifter	Skäl	Datum för uppförande
5.	Evgenii Mikhaylovich SEREBRIAKOV	Евгений Михайлович СЕРЕБРЯКОВ Födelsedatum: 26.7.1981 Födelseort: Kursk, Ryska SFSR (numera Ryska federationen) Passnummer: 100135555 Utfärdat av: Ryska federationens utrikesministerium Giltighet: 17.4.2017–17.4.2022 Plats: Moskva, Ryska federationen Nationalitet: rysk Kön: man	Evgenii Serebriakov deltog i ett försök till cyberattack med en potentiellt betydande effekt på Organisationen för förbud mot kemiska vapen (OPCW) i Nederländerna och i cyberattacker med en betydande effekt mot tredjeländer. I egenskap av it-operatör vid huvuddirektoratet vid generalstaben inom Ryska federationens försvarsmakt (GU/GRU) ingick Evgenii Serebriakov i en grupp bestående av fyra ryska militära underrättelseofficerare som utan tillstånd försökte få tillträde till OPCW:s trådlösa nätverk i Haag i Nederländerna i april 2018. Syftet med försöket till cyberattack var att man skulle hacka sig in i OPCW:s trådlösa nätverk. Om detta hade lyckats skulle det ha äventyrat säkerheten i nätverket och OPCW:s pågående utredningsarbete. Nederländernas Defence Intelligence and Security Service (Militaire Inlichtingen- en Veiligheidsdienst) avbröt försöket till cyberattack och förhindrade därmed allvarlig skada för OPCW. Sedan våren 2022 leder Evgenii Serebriakov 'Sandworm' (även kallad 'Sandworm Team', 'BlackEnergy Group', 'Voodoo Bear', 'Quedagh', 'Olympic Destroyer' och 'Telebots'), en aktör och hackergrupp knuten till enhet 74455 vid Rysslands centrala underrättelsedirektorat. Sandworm har utfört cyberattacker mot Ukraina, inbegripet ukrainska statliga myndigheter, till följd av Rysslands anfallskrig mot Ukraina. GRU fortsätter att aktivt utföra cyberattacker mot unionen eller dess medlemsstater. I egenskap av medlem i GRU är Evgenii Serebriakov därför inblandad i cyberattacker med en betydande effekt, inbegripet försök till cyberattacker med en potentiellt betydande effekt, som utgör ett externt hot för unionen eller dess medlemsstater.	30.7.2020

	Namn	Identifieringsuppgifter	Skäl	Datum för uppförande
6.	Oleg Mikhaylovich SOTNIKOV	Олег Михайлович СОТНИКОВ Födelsedatum: 24.8.1972 Födelseort: Uljanovsk, Ryska SFSR (numera Ryska federationen) Passnummer: 120018866 Utfärdat av: Ryska federationens utrikesministerium Giltighet: 17.4.2017–17.4.2022 Plats: Moskva, Ryska federationen Nationalitet: rysk Kön: man	Oleg Sotnikov deltog i ett försök till cyberattack med en potentiellt betydande effekt på Organisationen för förbud mot kemiska vapen (OPCW) i Nederländerna och i cyberattacker med en betydande effekt mot tredjeländer. I egenskap av officer inom personbaserad inhämtning vid huvuddirektoratet vid generalstaben inom Ryska federationens försvarsmakt (GU/GRU) ingick Oleg Sotnikov i en grupp bestående av fyra ryska underrättelseofficerare som utan tillstånd försökte få tillträde till OPCW:s trådlösa nätverk i Haag i Nederländerna i april 2018. Syftet med försöket till cyberattack var att man skulle hacka sig in i OPCW:s trådlösa nätverk. Om detta hade lyckats skulle det ha äventyrat säkerheten i nätverket och OPCW:s pågående utredningsarbete. Nederländernas Defence Intelligence and Security Service (Militaire Inlichtingen- en Veiligheidsdienst) avbröt försöket till cyberattack och förhindrade därmed allvarlig skada för OPCW. En åtalsjury i Pennsylvanias västra distrikt (Amerikas förenta stater) har åtalat Oleg Sotnikov i egenskap av officer vid GRU, för hackning, nätbedrägeri, grov identitetsstöld och penningtvätt. GRU fortsätter att aktivt utföra cyberattacker mot unionen eller dess medlemsstater. I egenskap av medlem i GRU är Oleg Sotnikov därför inblandad i cyberattacker med en betydande effekt, inbegripet försök till cyberattacker med en potentiellt betydande effekt, som utgör ett externt hot för unionen eller dess medlemsstater.	30.7.2020

	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 en betydande effekt mot Tysklands förbundsdag (Deutscher Bundestag) och i cyberattacker med en betydande effekt mot tredjeländer. I egenskap av militär underrättelseofficer vid 85th Main Centre for Special Services (GTsSS) 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 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 tidigare förbundskansler Angela Merkels e-postkonton påverkades. En åtalsjury i Pennsylvanias västra distrikt (Amerikas förenta stater) har åtalat Dmitry Badin i egenskap av medlem av militärenhet 26165 för hackning, nätbedrägeri, grov identitetsstöld och penningtvätt. GRU fortsätter att aktivt utföra cyberattacker mot unionen eller dess medlemsstater. I egenskap av medlem i GRU är Dmitry Badin därför inblandad i cyberattacker med en betydande effekt, inbegripet försök till cyberattacker med en potentiellt betydande effekt, som utgör ett externt hot för unionen eller dess medlemsstater.	22.10.2020

	Namn	Identifieringsuppgifter	Skäl	Datum för uppförande
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) (även kallad 'militär enhet 26165', 'APT28', 'Fancy Bear', 'Sofacy Group', 'Pawn Storm' och 'Strontium'). I denna egenskap är Igor Kostyukov ansvarig för cyberattacker som genomförts av GTsSS, även cyberattacker med en betydande effekt som utgör ett externt hot för unionen eller dess medlemsstater. I synnerhet deltog militära underrättelseofficerare vid GTsSS i cyberattacken mot Tysklands förbundsdag (Deutscher Bundestag) i april och maj 2015 och försöket till cyberattack då man skulle hacka sig in i Organisationen för förbud mot kemiska vapens (OPCW) 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 tidigare förbundskansler Angela Merkels e-postkonton påverkades. GRU fortsätter att aktivt utföra cyberattacker mot unionen eller dess medlemsstater. I egenskap av medlem i GRU är Igor Kostyukov därför inblandad i cyberattacker med en betydande effekt, inbegripet försök till cyberattacker med en potentiellt betydande effekt, som utgör ett externt hot för unionen eller dess medlemsstater.	22.10.2020".