Europeiska unionens råd

Bryssel den 13 maj 2024
(OR. en)

8500/24

LIMITE

CORLX 354
CFSP/PESC 510
CYBER 108
JAI 570
FIN 339

LAGSTIFTNINGSAKTER OCH ANDRA INSTRUMENT

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

RÅDETS BESLUT (Gusp) 2024/…

av den …

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 tillämpas till och med den 18 maj 2025. På grundval av en översyn av det beslutet bör giltigheten för de restriktiva åtgärder som fastställs däri förlängas till och med detta datum.

(3) Mot bakgrund av fortsatta och ökande skadliga ageranden i cyberrymden, inbegripet ageranden riktade mot tredjeländer, bör skälen för att inkludera sex personer och två enheter i förteckningen över fysiska och juridiska personer, enheter och organ som är föremål för de restriktiva åtgärder som anges i bilagan till beslut (Gusp) 2019/797 uppdateras.

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

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

[1] Rådets beslut (Gusp) 2019/797 av den 17 maj 2019 om restriktiva åtgärder mot cyberattacker som hotar unionen eller dess medlemsstater (EUT L 129I 17.5.2019, s. 13).

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 2025 och ska ses över fortlöpande.”.

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 … den …

På rådets vägnar
[…]
Ordförande

BILAGA

Bilagan till beslut (Gusp) 2019/797 (”Förteckning över fysiska och juridiska personer, enheter och organ som avses i artiklarna 4 och 5”) ska ändras på följande sätt:

1. I förteckningen med rubriken ”A. Fysiska personer” ska posterna 3–8 ersättas med följande:

	Namn	Identifieringsuppgifter	Skäl	Datum för uppförande
”3.	Alexey Valeryevich MININ (Aleksej Valerjevitj MININ)	Алексей Валерьевич МИНИН Födelsedatum: 27.5.1972 Födelseort: Perm Oblast, (Ryska SFSR) (numera Ryska federationen) Passnummer: 120017582 utfärdat av Ryska federationens utrikesministerium, giltigt 17.4. 2017–17.4.2022. Plats: Moskva, Ryska federationen Nationalitet: rysk Kön: man	Aleksej 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 betydande effekt mot tredjeländer. I egenskap av officer inom personbaserad inhämtning vid huvuddirektoratet vid generalstaben inom Ryska federationens försvarsmakt (GU/GRU), ingick Aleksej 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) (försvarets underrättelse- och säkerhetstjänst) avbröt försöket till cyberattack och förhindrade därmed allvarlig skada för OPCW. En åtalsjury i Pennsylvanias västra distrikt (Förenta staterna) har åtalat Aleksej Minin i egenskap av officer vid Rysslands centrala underrättelsedirektorat (GRU), för hackning, nätbedrägeri, grov identitetsstöld och penningtvätt.	30.7.2020

	Namn	Identifieringsuppgifter	Skäl	Datum för uppförande
4.	Aleksei Sergeyvich MORENETS (Aleksej Sergejevitj 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, giltigt 17.4.2017–17.4.2022. Plats: Moskva, Ryska federationen Nationalitet: rysk Kön: man	Aleksej 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 betydande effekt mot tredjeländer. I egenskap av it-operatör vid huvuddirektoratet vid generalstaben inom Ryska federationens försvarsmakt (GU/GRU), ingick Aleksej 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) (försvarets underrättelse- och säkerhetstjänst) avbröt försöket till cyberattack och förhindrade därmed allvarlig skada för OPCW. En åtalsjury i Pennsylvanias västra distrikt (Förenta staterna) har åtalat Aleksej Morenets i egenskap av medlem av militärenhet 26165, för hackning, nätbedrägeri, grov identitetsstöld och penningtvätt	30.7.2020

	Namn	Identifieringsuppgifter	Skäl	Datum för uppförande
5.	Evgenii Mikhaylovich SEREBRIAKOV (Jevgenij Michajlovitj SEREBRJAKOV)	Евгений Михайлович СЕРЕБРЯКОВ Födelsedatum: 26.7.1981 Födelseort: Kursk, Ryska SFSR (numera Ryska federationen) Passnummer: 100135555 utfärdat av Ryska federationens utrikesministerium, giltigt 17.4.2017–17.4.2022. Plats: Moskva, Ryska federationen Nationalitet: rysk Kön: man	Jevgenij Serebrjakov 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 betydande effekt mot tredjeländer. I egenskap av it-operatör vid huvuddirektoratet vid generalstaben inom Ryska federationens försvarsmakt (GU/GRU) ingick Jevgenij Serebrjakov 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) (försvarets underrättelse- och säkerhetstjänst) avbröt försöket till cyberattack och förhindrade därmed allvarlig skada för OPCW. Sedan våren 2022 leder Jevgenij Serebrjakov Sandworm (även kallad Sandworm Team, BlackEnergy Group, Voodoo Bear, Quedagh, Olympic Destroyer och Telebots), en aktör och hackergrupp knuten till enhet 74455 vid det ryska centrala underrättelsedirektoratet. Sandworm har utfört cyberattacker mot Ukraina, inbegripet ukrainska statliga myndigheter, till följd av Rysslands anfallskrig mot Ukraina.	30.7.2020

	Namn	Identifieringsuppgifter	Skäl	Datum för uppförande
6.	Oleg Mikhaylovich SOTNIKOV (Oleg Michajlovitj SOTNIKOV)	Олег Михайлович СОТНИКОВ Födelsedatum: 24.8.1972 Födelseort: Ulyanovsk (Uljanovsk), Ryska SFSR (numera Ryska federationen) Passnummer: 120018866 utfärdat av Ryska federationens utrikesministerium, giltigt 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 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 –) (försvarets underrättelse- och säkerhetstjänst) avbröt försöket till cyberattack och förhindrade därmed allvarlig skada för OPCW. En åtalsjury i Pennsylvanias västra distrikt (Förenta staterna) har åtalat Oleg Sotnikov i egenskap av officer vid Rysslands centrala underrättelsedirektorat (GRU), för hackning, nätbedrägeri, grov identitetsstöld och penningtvätt.	30.7.2020

	Namn	Identifieringsuppgifter	Skäl	Datum för uppförande
7.	Dmitry Sergeyevich BADIN (Dmitrij Sergejevitj BADIN)	Дмитрий Сергеевич БАДИН Födelsedatum: 15.11.1990 Födelseort: Kursk, Ryska SFSR (numera Ryska federationen) Nationalitet: rysk Kön: man	Dmitrij Badin deltog i en cyberattack med betydande effekt mot Tysklands förbundsdag (Deutscher Bundestag) och i cyberattacker med betydande effekt mot tredjeländer. 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 Dmitrij 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 (Förenta staterna) har åtalat Dmitrij Badin i egenskap av medlem av militärenhet 26165 för hackning, nätbedrägeri, grov identitetsstöld och penningtvätt.	22.10.2020

	Namn	Identifieringsuppgifter	Skäl	Datum för uppförande
8.	Igor Olegovich KOSTYUKOV (Igor Olegovitj KOSTJUKOV)	Игорь Олегович КОСТЮКОВ Födelsedatum: 21.2.1961 Nationalitet: rysk Kön: man	Igor Kostjukov 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, APT28, Fancy Bear, Sofacy Group, Pawn Storm och Strontium). I denna egenskap är Igor Kostjukov 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) 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 tidigare förbundskansler Angela Merkels e-postkonton påverkades.	22.10.2020”

2. I förteckningen med rubriken ”B. Juridiska personer, enheter och organ” ska posterna 3 och 4 ersättas med följande:

	Namn	Identifieringsuppgifter	Skäl	Datum för uppförande
”3.	Main Centre for Special Technologies (GTsST) (huvudcentrum för specialteknik) vid huvuddirektoratet vid generalstaben inom Ryska federationens försvarsmakt (GU/GRU)	Adress: 22 Kirova Street, Moscow, Russian Federation	Huvudcentrumet för specialteknik vid huvuddirektoratet vid generalstaben inom Ryska federationens försvarsmakt, även känd som fältpostnummer 74455, är inblandat i cyberattacker med betydande effekt och med ursprung utanför unionen, som utgör ett externt hot mot unionen eller dess medlemsstater, och cyberattacker som har en betydande effekt på tredjeländer, inbegripet de cyberattacker som allmänt kallas NotPetya eller EternalPetya i juni 2017 och de cyberattacker som riktades mot ett ukrainskt kraftnät under vintern 2015/2016. NotPetya eller EternalPetya gjorde data oåtkomliga i ett antal företag i unionen, i Europa och världen över genom att angripa datorer med utpressningsprogram och blockera tillgången till data, vilket bland annat resulterade i betydande ekonomiska förluster. Cyberattacker på ett ukrainskt kraftnät ledde till att delar av nätet stängdes av under vintern.	30.7.2020

	Namn	Identifieringsuppgifter	Skäl	Datum för uppförande
			Den aktör som är känd som Sandworm (även kallad SandwormTeam, BlackEnergy Group, Voodoo Bear, Quedagh, Olympic Destroyer, Telebots) ligger också bakom attacken på det ukrainska kraftnätet som utfördes av NotPetya eller EternalPetya. Sandworm har utfört cyberattacker mot Ukraina, inbegripet ukrainska statliga myndigheter och ukrainsk kritisk infrastruktur, efter Rysslands anfallskrig mot Ukraina. Dessa cyberattacker inbegriper harpunfiske, sabotageprogram och angrepp med utpressningsprogram. Huvudcentrumet för specialteknik vid huvuddirektoratet vid generalstaben vid Ryska federationens försvarsmakt har en aktiv roll i den cyberverksamhet som utförs av Sandworm och kan kopplas till Sandworm.	

	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, APT28, Fancy Bear, Sofacy Group, Pawn Storm och Strontium) är inblandat i cyberattacker med betydande effekt som utgör ett externt hot mot unionen eller dess medlemsstater och i cyberattacker med betydande effekt mot tredjeländer. 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. Efter Rysslands anfallskrig mot Ukraina utfördes it-attacker av GTsSS (harpunfiske och angrepp med sabotageprogram) mot Ukraina.	22.10.2020"