SKLEP SVETA (SZVP) 2020/1127

z dne 30. julija 2020

o spremembi Sklepa Sveta (SZVP) 2019/797 o omejevalnih ukrepih proti kibernetskim napadom, ki ogrožajo Unijo ali njene države članice

SVET EVROPSKE UNIJE JE –

ob upoštevanju Pogodbe o Evropski uniji in zlasti člena 29 Pogodbe,

ob upoštevanju predloga visokega predstavnika Unije za zunanje zadeve in varnostno politiko,

ob upoštevanju naslednjega:

(1) Svet je 17. maja 2019 sprejel Sklep (SZVP) 2019/797 ([1]).

(2) Ciljno usmerjeni omejevalni ukrepi proti kibernetskim napadom s pomembnim učinkom, ki pomenijo zunanjo grožnjo Uniji ali njenim državam članicam, so med ukrepi, vključenimi v okvir Unije za skupen diplomatski odziv na zlonamerne kibernetske dejavnosti („zbirka orodij za kibernetsko diplomacijo“), in so bistven instrument za odvračanje od takšnih dejavnosti in odzivanje nanje. Omejevalni ukrepi se lahko uporabljajo tudi kot odziv na kibernetske napade, ki imajo pomemben učinek na tretje države ali mednarodne organizacije, kadar se to zdi potrebno za doseganje ciljev skupne zunanje in varnostne politike iz ustreznih določb člena 21 Pogodbe o Evropski uniji.

(3) Svet je 16. aprila 2018 sprejel sklepe, v katerih je ostro obsodil zlonamerno uporabo informacijskih in komunikacijskih tehnologij, tudi v kibernetskih napadih, v javnosti znanih kot „WannaCry“ in „NotPetya“, ki sta povzročila precejšnjo škodo in ekonomsko izgubo v Uniji in širše. Predsednika Evropskega sveta in Evropske komisije ter visoki predstavnik Unije za zunanje zadeve in varnostno politiko (v nadaljnjem besedilu: visoki predstavnik) so 4. oktobra 2018 v skupni izjavi izrazili resno zaskrbljenost zaradi poskusa kibernetskega napada, ki naj bi spodkopal integriteto Organizacije za prepoved kemičnega orožja (OPCW) na Nizozemskem; označili so ga za dejanje agresije, ki kaže prezir do plemenitega namena OPCW. V izjavi, podani v imenu Unije dne 12. aprila 2019 je visoki predstavnik pozval akterje, naj prenehajo z zlonamernimi kibernetskimi dejavnostmi, namenjenimi spodkopavanju integritete, varnosti in gospodarske konkurenčnosti Unije, vključno s krajami intelektualne lastnine v kibernetskem prostoru. Med takšne kraje v kibernetskem prostoru spadajo tudi kraje, ki jih izvaja akter, v javnosti znan kot „APT10“ („Advanced Persistent Threat 10“).

(4) V zvezi s tem in zato, da se prepreči nadaljevanje in širjenje zlonamernega ravnanja, odvrne od njega in nanj odzove, bi bilo treba na seznam fizičnih in pravnih oseb, subjektov in organov, za katere veljajo omejevalni ukrepi iz Priloge k Sklepu (SZVP) 2019/797, uvrstiti šest fizičnih oseb in tri subjekte ali organe. Te osebe in subjekti ali organi so odgovorni za kibernetske napade ali poskuse kibernetskih napadov, so jim zagotovili podporo oziroma so bili vpleteni vanje ali so jih omogočili, vključno s poskusom kibernetskega napada na OPCW in kibernetskimi napadi, v javnosti znanimi kot „WannaCry“ in „NotPetya“ ter „Operation Cloud Hopper“.

(5) Sklep (SZVP) 2019/797 bi bilo treba zato ustrezno spremeniti –

SPREJEL NASLEDNJI SKLEP:

Člen 1

Priloga k Sklepu (SZVP) 2019/797 se spremeni v skladu s Prilogo k temu sklepu.

([1]) Sklep Sveta (SZVP) 2019/797 z dne 17. maja 2019 o omejevalnih ukrepih proti kibernetskim napadom, ki ogrožajo Unijo ali njene države članice (UL L 129 I, 17.5.2019, str. 13).

Člen 2

Ta sklep začne veljati na dan objave v *Uradnem listu Evropske unije*.

V Bruslju, 30. julija 2020

Za Svet
Predsednik
M. ROTH

PRILOGA

Na seznam fizičnih in pravnih oseb, subjektov in organov iz Priloge k Sklepu (SZVP) 2019/797 se dodajo naslednje osebe in subjekti ali organi:

„A. Fizične osebe

	Ime in priimek	Podatki za identifikacijo	Razlogi za uvrstitev na seznam	Datum uvrstitve na seznam
1.	GAO Qiang	Kraj rojstva: provinca Shandong, Kitajska Naslov: Soba 1102, Guanfu Mansion, ulica Xinkai 46, okrožje Hedong, Tjandžin, Kitajska Državljanstvo: kitajsko Spol: moški	Gao Qiang je vpleten v ‚Operation Cloud Hopper', vrsto kibernetskih napadov s pomembnim učinkom, ki izvirajo iz držav zunaj Unije in pomenijo zunanjo grožnjo Uniji ali njenim državam članicam, ter kibernetskih napadov, ki imajo pomemben učinek na tretje države. Tarča ‚Operation Cloud Hopper' so bili informacijski sistemi multinacionalnih družb na šestih celinah, vključno z družbami v Uniji, pri čemer je bil pridobljen nepooblaščen dostop do komercialno občutljivih podatkov, kar je povzročilo precejšnjo ekonomsko izgubo. ‚Operation Cloud Hopper' je izvedel akter, v javnosti znan kot ‚APT10' (‚Advanced Persistent Threat 10') (tudi ‚Red Apollo', ‚CVNX', ‚Stone Panda', ‚MenuPass' in ‚Potassium'). Gao Qianga je mogoče povezati z APT10, med drugim zaradi njegove povezave z infrastrukturo APT10 za poveljevanje in kontrolo. Poleg tega je bil Gao Qiang zaposlen pri Huaying Haitai, ki je subjekt, uvrščen na seznam zaradi zagotavljanja podpore in omogočanja ‚Operation Cloud Hopper'. Povezan je z Zhang Shilongom, ki je prav tako uvrščen na seznam v povezavi z ‚Operation Cloud Hopper'. Gao Qiang je torej povezan s Huaying Haitai in Zhang Shilongom.	30.7.2020
2.	ZHANG Shilong	Naslov: Hedong, ulica Yuyang 121, Tjandžin, Kitajska Državljanstvo: kitajsko Spol: moški	Zhang Shilong je vpleten v ‚Operation Cloud Hopper', vrsto kibernetskih napadov s pomembnim učinkom, ki izvirajo iz držav zunaj Unije in pomenijo zunanjo grožnjo Uniji ali njenim državam članicam, ter kibernetskih napadov, ki imajo pomemben učinek na tretje države. Tarča ‚Operation Cloud Hopper' so bili informacijski sistemi multinacionalnih družb na šestih celinah, vključno z družbami v Uniji, pri čemer je bil pridobljen nepooblaščen dostop do komercialno občutljivih podatkov, kar je povzročilo precejšnjo ekonomsko izgubo. ‚Operation Cloud Hopper' je izvedel akter, v javnosti znan kot ‚APT10' (‚Advanced Persistent Threat 10') (tudi ‚Red Apollo', ‚CVNX', ‚Stone Panda', ‚MenuPass' in ‚Potassium').	30.7.2020

			Zhang Shilonga je mogoče povezati z APT10, med drugim zaradi zlonamerne programske opreme, ki jo je razvil in testiral v povezavi s kibernetskimi napadi, ki jih je izvedel APT10. Poleg tega je bil Zhang Shilong zaposlen pri Huaying Haitai, ki je subjekt, uvrščen na seznam zaradi zagotavljanja podpore in omogočanja ‚Operation Cloud Hopper'. Povezan je z Gao Qiangom, ki je uvrščen na seznam v povezavi z ‚Operation Cloud Hopper'. Zhang Shilong je torej povezan s Huaying Haitai in Gao Qiangom.	
3.	Alexey Valeryevich MININ	Алексей Валерьевич МИНИН Datum rojstva: 27. maj 1972 Kraj rojstva: pokrajina Perm, Ruska SFSR (danes Ruska federacija) Številka potnega lista: 120017582 Izdajatelj: Ministrstvo za zunanje zadeve Ruske federacije Veljavnost: od 17. aprila 2017 do 17. aprila 2022 Lokacija: Moskva, Ruska federacija Državljanstvo: rusko Spol: moški	Alexej Minin je sodeloval pri poskusu kibernetskega napada s potencialno pomembnim učinkom na Organizacijo za prepoved kemičnega orožja (OPCW) na Nizozemskem. Kot pomožni uradnik za HUMINT (zbiranje obveščevalnih podatkov z osebnimi stiki) v Glavnem direktoratu generalštaba Oboroženih sil Ruske federacije (GU/GRU) je bil eden izmed štirih članov skupine ruskih vojaških obveščevalnih uradnikov, ki je aprila 2018 poskušala pridobiti nepooblaščen dostop do brezžičnega omrežja OPCW v Haagu (Nizozemska). Cilj poskusa kibernetskega napada je bil vdor v brezžično omrežje OPCW; če bi poskus uspel, bi to ogrozilo varnost omrežja in tekoče preiskovalno delo OPCW. Nizozemska varnostna služba za zaščito in varnost (DISS) (Militaire Inlichtingen- en Veiligheidsdienst – MIVD) je poskus kibernetskega napada ustavila in s tem preprečila resno škodo za OPCW.	30.7.2020
4.	Aleksei Sergeyvich MORENETS	Алексей Сергеевич МОРЕНЕЦ Datum rojstva: 31. julij 1977 Kraj rojstva: pokrajina Murmansk, Ruska SFSR (danes Ruska federacija) Številka potnega lista: 100135556 Izdajatelj: Ministrstvo za zunanje zadeve Ruske federacije Veljavnost: od 17. aprila 2017 do 17. aprila 2022 Lokacija: Moskva, Ruska federacija Državljanstvo: rusko Spol: moški	Aleksei Morenets je sodeloval pri poskusu kibernetskega napada s potencialno pomembnim učinkom na Organizacijo za prepoved kemičnega orožja (OPCW) na Nizozemskem. Kot kibernetski operater v Glavnem direktoratu generalštaba Oboroženih sil Ruske federacije (GU/GRU) je bil eden izmed štirih članov skupine ruskih vojaških obveščevalnih uradnikov, ki je aprila 2018 poskušala pridobiti nepooblaščen dostop do brezžičnega omrežja OPCW v Haagu (Nizozemska). Cilj poskusa kibernetskega napada je bil vdor v brezžično omrežje OPCW; če bi poskus uspel, bi to ogrozilo varnost omrežja in tekoče preiskovalno delo OPCW. Nizozemska varnostna služba za zaščito in varnost (DISS) (Militaire Inlichtingen- en Veiligheidsdienst – MIVD) je poskus kibernetskega napada ustavila in s tem preprečila resno škodo za OPCW.	30.7.2020

5.	Evgenii Mikhaylovich SEREBRIAKOV	Евгений Михайлович СЕРЕБРЯКОВ Datum rojstva: 26. julij 1981 Kraj rojstva: Kursk, Ruska SFSR (danes Ruska federacija) Številka potnega lista: 100135555 Izdajatelj: Ministrstvo za zunanje zadeve Ruske federacije Veljavnost: od 17. aprila 2017 do 17. aprila 2022 Lokacija: Moskva, Ruska federacija Državljanstvo: rusko Spol: moški	Evgenii Serebriakov je sodeloval pri poskusu kibernetskega napada s potencialno pomembnim učinkom na Organizacijo za prepoved kemičnega orožja (OPCW) na Nizozemskem. Kot kibernetski operater v Glavnem direktoratu generalštaba Oboroženih sil Ruske federacije (GU/GRU) je bil eden izmed štirih članov skupine ruskih vojaških obveščevalnih uradnikov, ki je aprila 2018 poskušala pridobiti nepooblaščen dostop do brezžičnega omrežja OPCW v Haagu (Nizozemska). Cilj poskusa kibernetskega napada je bil vdor v brezžično omrežje OPCW; če bi poskus uspel, bi to ogrozilo varnost omrežja in tekoče preiskovalno delo OPCW. Nizozemska varnostna služba za zaščito in varnost (DISS) (Militaire Inlichtingen- en Veiligheidsdienst – MIVD) je poskus kibernetskega napada ustavila in s tem preprečila resno škodo za OPCW.	30.7.2020
6.	Oleg Mikhaylovich SOTNIKOV	Олег Михайлович СОТНИКОВ Datum rojstva: 24. avgust 1972 Kraj rojstva: Uljanovsk, Ruska SFSR (danes Ruska federacija) Številka potnega lista: 120018866 Izdajatelj: Ministrstvo za zunanje zadeve Ruske federacije Veljavnost: od 17. aprila 2017 do 17. aprila 2022 Lokacija: Moskva, Ruska federacija Državljanstvo: rusko Spol: moški	Oleg Sotnikov je sodeloval pri poskusu kibernetskega napada s potencialno pomembnim učinkom na Organizacijo za prepoved kemičnega orožja (OPCW) na Nizozemskem. Kot pomožni uradnik za HUMINT (zbiranje obveščevalnih podatkov z osebnimi stiki) v Glavnem direktoratu generalštaba Oboroženih sil Ruske federacije (GU/GRU) je bil eden izmed štirih članov skupine ruskih vojaških obveščevalnih uradnikov, ki je aprila 2018 poskušala pridobiti nepooblaščen dostop do brezžičnega omrežja OPCW v Haagu (Nizozemska). Cilj poskusa kibernetskega napada je bil vdor v brezžično omrežje OPCW; če bi poskus uspel, bi to ogrozilo varnost omrežja in tekoče preiskovalno delo OPCW. Nizozemska varnostna služba za zaščito in varnost (DISS) (Militaire Inlichtingen- en Veiligheidsdienst – MIVD) je poskus kibernetskega napada ustavila in s tem preprečila resno škodo za OPCW.	30.7.2020

B. Pravne osebe, subjekti in organi:

	Ime	Podatki za identifikacijo	Razlogi za uvrstitev na seznam	Datum uvrstitve na seznam
1.	Tianjin Huaying Haitai Science and Technology Development Co. Ltd (Huaying Haitai)	tudi: Haitai Technology Development Co. Ltd Lokacija: Tjandžin, Kitajska	Huaying Haitai je omogočil in zagotovil finančno, tehnično ali materialno podporo za ‚Operation Cloud Hopper', vrsto kibernetskih napadov s pomembnim učinkom, ki izvirajo iz držav zunaj Unije in pomenijo zunanjo grožnjo Uniji ali njenim državam članicam, ter kibernetskih napadov, ki imajo pomemben učinek na tretje države.	30.7.2020

			Tarča ‚Operation Cloud Hopper' so bili informacijski sistemi multinacionalnih družb na šestih celinah, vključno z družbami v Uniji, pri čemer je bil pridobljen nepooblaščen dostop do komercialno občutljivih podatkov, kar je povzročilo precejšnjo ekonomsko izgubo. ‚Operation Cloud Hopper' je izvedel akter, v javnosti znan kot ‚APT10' (‚Advanced Persistent Threat 10') (tudi ‚Red Apollo', ‚CVNX', ‚Stone Panda', ‚MenuPass' in ‚Potassium'). Huaying Haitai je mogoče povezati z APT10. Poleg tega sta bila pri Huaying Haitai zaposlena Gao Qiang in Zhang Shilong, ki sta oba uvrščena na seznam v povezavi z ‚Operation Cloud Hopper'. Huaying Haitai je torej povezan z Gao Qiangom in Zhang Shilongom.	
2.	Chosun Expo	tudi: Chosen Expo; Korea Export Joint Venture Lokacija: DLRK	Chosun Expo je omogočil in zagotovil finančno, tehnično ali materialno podporo za vrsto kibernetskih napadov s pomembnim učinkom, ki izvirajo iz držav zunaj Unije in pomenijo zunanjo grožnjo Uniji ali njenim državam članicam, ter kibernetskih napadov, ki imajo pomemben učinek na tretje države, vključno s kibernetskimi napadi, v javnosti znanimi kot ‚WannaCry', in kibernetskimi napadi na poljski finančni nadzorni organ in Sony Pictures Entertainment, pa tudi kibernetsko krajo centralne banke Bangladeša in poskus kibernetske kraje vietnamske banke Tien Phong. ‚WannaCry' je z izsiljevalskim virusom in onemogočanjem dostopa do podatkov povzročil motnje v informacijskih sistemih po vsem svetu. Prizadel je informacijske sisteme družb v Uniji, tudi informacijske sisteme, povezane s storitvami, potrebnimi za vzdrževanje osnovnih storitev in gospodarskih dejavnosti v državah članicah. ‚WannaCry' je izvedel akter, v javnosti znan kot ‚APT38' (‚Advanced persistent Threat 38') ali ‚Lazarus Group'. Chosun Expo je mogoče povezati z APT38/Lazarus Group, tudi prek uporabniških računov, ki so bili uporabljeni za kibernetske napade.	30.7.2020
3.	Glavni center za posebne tehnologije (GTsST) Glavnega direktorata generalštaba Oboroženih sil Ruske federacije (GU/GRU)	Naslov: Kirova ulica 22, Moskva, Ruska federacija	Glavni center za posebne tehnologije (GTsST) Glavnega direktorata generalštaba Oboroženih sil Ruske federacije (GU/GRU), v javnosti znan tudi kot poštni predal 74455, je odgovoren za kibernetske napade s pomembnim učinkom, ki izvirajo iz držav zunaj Unije in pomenijo zunanjo grožnjo Uniji ali njenim državam članicam, ter kibernetske napade, ki imajo pomemben učinek na tretje države, vključno s kibernetskima napadoma junija 2017, v javnosti znanima kot ‚NotPetya' ali ‚EternalPetya', in kibernetskimi napadi na ukrajinsko električno omrežje pozimi leta 2015 in 2016.	30.7.2020“

			‚NotPetya‘ ali ‚EternalPetya‘ sta z izsiljevalskim virusom in onemogočenjem dostopa do podatkov onemogočila dostop do podatkov v številnih družbah v Uniji, širši Evropi in po svetu, kar je med drugim povzročilo precejšnjo ekonomsko izgubo. Zaradi kibernetskega napada na ukrajinsko električno omrežje je pozimi prišlo do delnega izpada tega omrežja. ‚NotPetya‘ ali ‚EternalPetya‘ je izvedel akter, v javnosti znan kot ‚Sandworm‘ (tudi ‚Sandworm Team‘, ‚BlackEnergy Group‘, ‚Voodoo Bear‘, ‚Quedagh‘, ‚Olympic Destroyer‘ in ‚Telebots‘), ki je odgovoren tudi za napad na ukrajinsko električno omrežje. Glavni center za posebne tehnologije pri Glavnem direktoratu generalštaba Oboroženih sil Ruske federacije dejavno sodeluje pri kibernetskih dejavnostih, ki jih izvaja Sandworm, in ga je mogoče povezati s Sandwormom.	