ODLUKA VIJEĆA (ZVSP) 2020/1127

od 30. srpnja 2020.

o izmjeni Odluke (ZVSP) 2019/797 o mjerama ograničavanja protiv kibernapada koji predstavljaju prijetnju Uniji ili njezinim državama članicama

VIJEĆE EUROPSKE UNIJE,

uzimajući u obzir Ugovor o Europskoj uniji, a posebno njegov članak 29.,

uzimajući u obzir prijedlog Visokog predstavnika Unije za vanjske poslove i sigurnosnu politiku,

budući da:

(1) Vijeće je 17. svibnja 2019. donijelo Odluku (ZVSP) 2019/797 ([1]).

(2) Ciljane mjere ograničavanja protiv kibernapada sa znatnim učinkom koji predstavljaju vanjsku prijetnju Uniji ili njezinim državama članicama neke su od mjera uključenih u okvir Unije za zajednički diplomatski odgovor na zlonamjerne kiberaktivnosti (alati za kiberdiplomaciju) te su ključan instrument za suzbijanje takvih aktivnosti te za odgovor na njih. Mjere ograničavanja mogu se primijeniti i kao odgovor na kibernapade sa znatnim učinkom protiv trećih država ili međunarodnih organizacija ako se to smatra potrebnim za postizanje zajedničkih ciljeva vanjske i sigurnosne politike iz relevantnih odredaba članka 21. Ugovora o Europskoj uniji.

(3) Vijeće je 16. travnja 2018. usvojilo zaključke u kojima je oštro osudilo zlonamjernu uporabu informacijskih i komunikacijskih tehnologija, među ostalim u okviru kibernapada koji su javnosti poznati kao „WannaCry" i „NotPetya", koji su prouzročili znatnu štetu i gospodarski gubitak u Uniji i izvan nje. Predsjednik Europskog vijeća i predsjednik Europske komisije te Visoki predstavnik Unije za vanjske poslove i sigurnosnu politiku („Visoki predstavnik") 4. listopada 2018. u zajedničkoj su izjavi izrazili ozbiljnu zabrinutost zbog pokušaja kibernapada s ciljem podrivanja integriteta Organizacije za zabranu kemijskog oružja (OPCW) u Nizozemskoj, agresivnom činu koji je pokazao nepoštovanje prema plemenitoj svrsi OPCW-a. U izjavi u ime Unije od 12. travnja 2019. Visoki predstavnik pozvao je aktere da prestanu poduzimati zlonamjerne kiberaktivnosti čiji je cilj podrivanje integriteta, sigurnosti i gospodarske konkurentnosti Unije, uključujući krađe intelektualnog vlasništva omogućenih kibertehnologijama. Takve krađe omogućene kibertehnologijama uključuju i krađe koje je izvršio subjekt javnosti poznat pod nazivom „APT10" („Advanced Persistent Threat 10").

(4) U tom kontekstu te u svrhu sprečavanja i suzbijanja kontinuiranog i sve prisutnijeg zlonamjernog ponašanja u kiberprostoru te odvraćanja od takvog ponašanja i odgovora na njega, šest fizičkih osoba i tri subjekta ili tijela trebalo bi uvrstiti na popis fizičkih i pravnih osoba, subjekata i tijela koji podliježu mjerama ograničavanja naveden u Prilogu Odluci (ZVSP) 2019/797. Te osobe i subjekti ili tijela odgovorni su za kibernapade ili pokušaje kibernapada, uključujući pokušaj kibernapada na OPCW i kibernapade javnosti poznate kao „WannaCry" i „NotPetya" te „Operation Cloud Hopper", ili su im pružili potporu, u njima sudjelovali ili olakšali njihovo izvršenje.

(5) Odluku (ZVSP) 2019/797 trebalo bi stoga na odgovarajući način izmijeniti,

DONIJELO JE OVU ODLUKU:

Članak 1.

Prilog Odluci (ZVSP) 2019/797 mijenja se u skladu s Prilogom ovoj Odluci.

([1]) Odluka Vijeća (ZVSP) 2019/797 od 17. svibnja 2019. o mjerama ograničavanja protiv kibernapada koji predstavljaju prijetnju Uniji ili njezinim državama članicama (SL L 129 I, 17.5.2019., str. 13).

Članak 2.

Ova Odluka stupa na snagu na dan objave u *Službenom listu Europske unije*.

Sastavljeno u Bruxellesu 30. srpnja 2020.

Za Vijeće
Predsjednik
M. ROTH

PRILOG

Sljedeće osobe i subjekti ili tijela dodaju se na popis fizičkih i pravnih osoba, subjekata i tijela naveden u Prilogu Odluci (ZVSP) 2019/797:

„A. Fizičke osobe

	Ime	Identifikacijski podaci	Obrazloženje	Datum uvrštenja na popis
1.	GAO Qiang	Mjesto rođenja: pokrajina Shandong, Kina Adresa: Room 1102, Guanfu Mansion, 46 Xinkai Road, Hedong District, Tianjin, Kina Državljanstvo: kinesko Spol: muški	Gao Qiang uključen je u operaciju ‚Operation Cloud Hopper', niz kibernapada sa znatnim učinkom koji potječu iz područja izvan Unije i predstavljaju vanjsku prijetnju Uniji ili njezinim državama članicama te kibernapada sa znatnim učinkom na treće države. Meta operacije ‚Operation Cloud Hopper' bili su informacijski sustavi multinacionalnih društava na šest kontinenata, uključujući društva sa sjedištem u Uniji, te je u okviru te operacije ostvaren neovlašten pristup komercijalno osjetljivim podacima, što je dovelo do znatnog gospodarskog gubitka. Subjekt javnosti poznat kao ‚APT10' („Advanced Persistent Threat 10') (također poznat kao ‚Red Apollo', ‚CVNX', ‚Stone Panda', ‚MenuPass' i ‚Potassium') izvršio je operaciju ‚Operation Cloud Hopper'. Gao Qiang može se povezati sa subjektom ‚APT10', među ostalim zbog njegove povezanosti s kontrolno-upravljačkom infrastrukturom subjekta ‚APT10'. Nadalje, Huaying Haitai, subjekt uvršten na popis zbog podupiranja i olakšavanja operacije ‚Operation Cloud Hopper', angažirao je Gaoa Qianga. Povezan je sa Zhangom Shilongom, koji je također uvršten na popis u vezi s operacijom ‚Operation Cloud Hopper'. Gao Qiang stoga je povezan i sa subjektom Huaying Haitai i sa Zhangom Shilongom.	30.7.2020.
2.	ZHANG Shilong	Adresa: Hedong, Yuyang Road No 121, Tianjin, Kina Državljanstvo: kinesko Spol: muški	Zhang Shilong uključen je u operaciju ‚Operation Cloud Hopper', niz kibernapada sa znatnim učinkom koji potječu iz područja izvan Unije i predstavljaju vanjsku prijetnju Uniji ili njezinim državama članicama te kibernapada sa znatnim učinkom na treće države. Meta operacije ‚Operation Cloud Hopper' bili su informacijski sustavi multinacionalnih društava na šest kontinenata, uključujući društva sa sjedištem u Uniji, te je u okviru te operacije ostvaren neovlašten pristup komercijalno osjetljivim podacima, što je dovelo do znatnog gospodarskog gubitka. Subjekt javnosti poznat kao ‚APT10' („Advanced Persistent Threat 10') (također poznat kao ‚Red Apollo', ‚CVNX', ‚Stone Panda', ‚MenuPass' i ‚Potassium') izvršio je operaciju ‚Operation Cloud Hopper'.	30.7.2020.

			Zhang Shilong može se povezati sa subjektom ‚APT10', među ostalim s pomoću štetnog softvera koji je razvio i ispitao u vezi s kibernapadima koje je izvršio subjekt ‚APT10'. Nadalje, Huaying Haitai, subjekt uvršten na popis zbog pružanja potpore operaciji ‚Operation Cloud Hopper' i njezina olakšavanja, angažirao je Zhanga Shilonga. Povezan je s Gaom Qiangom, koji je također uvršten na popis u vezi s operacijom ‚Operation Cloud Hopper'. Zhang Shilong stoga je povezan i sa subjektom Huaying Haitai i s Gaom Qiangom.	
3.	Alexey Valeryevich MININ	Алексей Валерьевич МИНИН Datum rođenja: 27. svibnja 1972. Mjesto rođenja: Permska oblast, Ruski SFSR (sada Ruska Federacija) Broj putovnice: 120017582 Izdalo: Ministarstvo vanjskih poslova Ruske Federacije Vrijedi: od 17. travnja 2017. do 17. travnja 2022. Lokacija: Moskva, Ruska Federacija Državljanstvo: rusko Spol: muški	Alexey Minin sudjelovao je u pokušaju kibernapada s potencijalno znatnim učinkom na Organizaciju za zabranu kemijskog oružja (OPCW) u Nizozemskoj. Kao službenik za prikupljanje obavještajnih podataka osobnim kontaktima u okviru glavne uprave glavnog stožera oružanih snaga Ruske Federacije (GU/GRU), Alexey Minin bio je dio tima od četiriju ruskih vojnih obavještajnih službenika koji su pokušali neovlašteno pristupiti bežičnoj mreži OPCW-a u Haagu u Nizozemskoj u travnju 2018. Pokušaj kibernapada bio je usmjeren na hakiranje bežične mreže OPCW-a, što bi, da je bilo uspješno, ugrozilo sigurnost mreže i tekuće istražne radove OPCW-a. Nizozemska obrambena obavještajna i sigurnosna služba (DISS) (Militaire Inlichtingen- en Veiligheidsdienst – MIVD) spriječila je pokušaj kibernapada i time izbjegla ozbiljnu štetu za OPCW.	30.7.2020.
4.	Aleksei Sergeyvich MORENETS	Алексей Сергеевич МОРЕНЕЦ Datum rođenja: 31. srpnja 1977. Mjesto rođenja: Murmanska oblast, Ruski SFSR (sada Ruska Federacija) Broj putovnice: 100135556 Izdalo: Ministarstvo vanjskih poslova Ruske Federacije Vrijedi: od 17. travnja 2017. do 17. travnja 2022. Lokacija: Moskva, Ruska Federacija Državljanstvo: rusko Spol: muški	Aleksei Morenets sudjelovao je u pokušaju kibernapada s potencijalno znatnim učinkom na Organizaciju za zabranu kemijskog oružja (OPCW) u Nizozemskoj. Kao kiberoperater glavne uprave glavnog stožera oružanih snaga Ruske Federacije (GU/GRU), Aleksei Morenets bio je dio tima od četiriju ruskih vojnih obavještajnih službenika koji su pokušali neovlašteno pristupiti bežičnoj mreži OPCW-a u Haagu u Nizozemskoj u travnju 2018. Pokušaj kibernapada bio je usmjeren na hakiranje bežične mreže OPCW-a, što bi, da je bilo uspješno, ugrozilo sigurnost mreže i tekuće istražne radove OPCW-a. Nizozemska obrambena obavještajna i sigurnosna služba (DISS) (Militaire Inlichtingen- en Veiligheidsdienst – MIVD) spriječila je pokušaj kibernapada i time izbjegla ozbiljnu štetu za OPCW.	30.7.2020.

5.	Evgenii Mikhaylovich SEREBRIAKOV	Евгений Михайлович СЕРЕБРЯКОВ Datum rođenja: 26. srpnja 1981. Mjesto rođenja: Kursk, Ruski SFSR (sada Ruska Federacija) Broj putovnice: 100135555 Izdalo: Ministarstvo vanjskih poslova Ruske Federacije Vrijedi: od 17. travnja 2017. do 17. travnja 2022. Lokacija: Moskva, Ruska Federacija Državljanstvo: rusko Spol: muški	Evgenii Serebriakov sudjelovao je u pokušaju kibernapada s potencijalno znatnim učinkom na Organizaciju za zabranu kemijskog oružja (OPCW) u Nizozemskoj. Kao kiberoperater glavne uprave glavnog stožera oružanih snaga Ruske Federacije (GU/GRU), Evgenii Serebriakov bio je dio tima od četiriju ruskih vojnih obavještajnih službenika koji su pokušali neovlašteno pristupiti bežičnoj mreži OPCW-a u Haagu u Nizozemskoj u travnju 2018. Pokušaj kibernapada bio je usmjeren na hakiranje bežične mreže OPCW-a, što bi, da je bilo uspješno, ugrozilo sigurnost mreže i tekuće istražne radove OPCW-a. Nizozemska obrambena obavještajna i sigurnosna služba (DISS) (Militaire Inlichtingen- en Veiligheidsdienst – MIVD) spriječila je pokušaj kibernapada i time izbjegla ozbiljnu štetu za OPCW.	30.7.2020.
6.	Oleg Mikhaylovich SOTNIKOV	Олег Михайлович СОТНИКОВ Datum rođenja: 24. kolovoza 1972. Mjesto rođenja: Uljanovsk, Ruski SFSR (sada Ruska Federacija) Broj putovnice: 120018866 Izdalo: Ministarstvo vanjskih poslova Ruske Federacije Vrijedi: od 17. travnja 2017. do 17. travnja 2022. Lokacija: Moskva, Ruska Federacija Državljanstvo: rusko Spol: muški	Oleg Sotnikov sudjelovao je u pokušaju kibernapada s potencijalno znatnim učinkom na Organizaciju za zabranu kemijskog oružja (OPCW) u Nizozemskoj. Kao službenik za prikupljanje obavještajnih podataka osobnim kontaktima u okviru glavne uprave glavnog stožera oružanih snaga Ruske Federacije (GU/GRU), Oleg Sotnikov bio je dio tima od četiriju ruskih vojnih obavještajnih službenika koji su pokušali neovlašteno pristupiti bežičnoj mreži OPCW-a u Haagu u Nizozemskoj u travnju 2018. Pokušaj kibernapada bio je usmjeren na hakiranje bežične mreže OPCW-a, što bi, da je bilo uspješno, ugrozilo sigurnost mreže i tekuće istražne radove OPCW-a. Nizozemska obrambena obavještajna i sigurnosna služba (DISS) (Militaire Inlichtingen- en Veiligheidsdienst – MIVD spriječila je pokušaj kibernapada i time izbjegla ozbiljnu štetu za OPCW.	30.7.2020.

B. Pravne osobe, subjekti i tijela

	Ime	Identifikacijski podaci	Obrazloženje	Datum uvrštenja na popis
1.	Tianjin Huaying Haitai Science and Technology Development Co. Ltd (Huaying Haitai)	Također poznat kao: Haitai Technology Development Co. Ltd Lokacija: Tianjin, Kina	Huaying Haitai pružio je financijsku, tehničku ili materijalnu potporu za operaciju ‚Operation Cloud Hopper' te ju je olakšao, a radi se o nizu kibernapada sa znatnim učinkom koji potječu iz područja izvan Unije i predstavljaju vanjsku prijetnju Uniji ili njezinim državama članicama te kibernapada sa znatnim učinkom na treće države.	30.7.2020.

			Meta operacije ‚Operation Cloud Hopper' bili su informacijski sustavi multinacionalnih društava na šest kontinenata, uključujući društva sa sjedištem u Uniji, te je u okviru te operacije ostvaren neovlašten pristup komercijalno osjetljivim podacima, što je dovelo do znatnog gospodarskog gubitka. Subjekt javnosti poznat kao ‚APT10' („Advanced Persistent Threat 10') (također poznat kao ‚Red Apollo', ‚CVNX', ‚Stone Panda', ‚MenuPass' i ‚Potassium') izvršio je operaciju ‚Operation Cloud Hopper'. Huaying Haitai može se povezati sa subjektom ‚APT10'. Nadalje, Huaying Haitai angažirao je Gaoa Qianga i Zhanga Shilonga, koji su uvršteni na popis u vezi s operacijom ‚Operation Cloud Hopper'. Huaying Haitai stoga je povezan s Gaom Qiangom i Zhangom Shilongom.	
2.	Chosun Expo	Također poznat kao: Chosen Expo; Korea Export Joint Venture Lokacija: DNRK	Chosun Expo pružio je financijsku, tehničku ili materijalnu potporu za i olakšao niz kibernapada sa znatnim učinkom koji potječu iz područja izvan Unije i predstavljaju vanjsku prijetnju Uniji ili njezinim državama članicama te kibernapada sa znatnim učinkom na treće države, uključujući kibernapade koji su javnosti poznati kao ‚WannaCry' i kibernapade na poljsko tijelo za financijski nadzor i poduzeće Sony Pictures Entertainment, kao i kiberkrađu u banci Bangladesh Bank te pokušaj kiberkrađe u vijetnamskoj banci Tien Phong Bank. ‚WannaCry' je uzrokovao poremećaje u informacijskim sustavima diljem svijeta tako što ih je napao ucjenjivačkim softverom (engl. *ransomware*) i blokirao pristup podacima. Utjecao je na informacijske sustave društava u Uniji, uključujući informacijske sustave povezane s uslugama potrebnim za održavanje ključnih usluga i gospodarskih aktivnosti u državama članicama. Subjekt javnosti poznat pod nazivom ‚APT38' („Advanced persistent Threat 38') i skupina ‚Lazarus Group' izvršili su napad ‚WannaCry'. Chosun Expo može se povezati sa subjektom ‚APT38'/skupinom ‚Lazarus Group', među ostalim s pomoću računa koji su upotrijebljeni za kibernapade.	30.7.2020.
3.	Glavni centar za posebne tehnologije (GTsST) glavne uprave glavnog stožera oružanih snaga Ruske Federacije (GU/GRU)	Adresa: 22 Kirova Street, Moskva, Ruska Federacija	Glavni centar za posebne tehnologije (GTsST) Glavne uprave Glavnog stožera oružanih snaga Ruske Federacije (GU/GRU), poznat i pod brojem vojne pošte 74455, odgovoran je za kibernapade sa znatnim učinkom koji potječu iz područja izvan Unije i predstavljaju vanjsku prijetnju Uniji ili njezinim državama članicama te kibernapade sa znatnim učinkom na treće države, uključujući kibernapade u lipnju 2017. koji su javnosti poznati kao ‚NotPetya' ili ‚EternalPetya' i kibernapade na ukrajinsku energetsku mrežu tijekom zima 2015. i 2016.	30.7.2020."

			‚NotPetya' ili ‚EternalPetya' onemogućili su pristup podacima u nizu društava u Uniji, široj Europi i svijetu tako što su računala napali ucjenjivačkim softverom i blokirali pristup podacima, što je, među ostalim, dovelo do znatnog gospodarskog gubitka. Kibernapad na ukrajinsku energetsku mrežu rezultirao je gašenjem dijelova te mreže tijekom zime. Subjekt javnosti poznat pod nazivom ‚Sandworm' (također poznat kao ‚Sandworm Team', ‚BlackEnergy Group', ‚Voodoo Bear', ‚Quedagh', ‚Olympic Destroyer', i ‚Telebots'), koji također stoji iza napada na ukrajinsku energetsku mrežu, izvršio je napade ‚NotPetya' ili ‚EternalPetya'. Glavni centar za posebne tehnologije glavne uprave glavnog stožera oružanih snaga Ruske Federacije ima aktivnu ulogu u kiberaktivnostima koje provodi ‚Sandworm' i može se povezati sa subjektom ‚Sandworm'.	