269.

Na osnovu člana 8 Zakona o međunarodnim restriktivnim mjerama („Službeni list CG", br. 56/18 i 72/19), Vlada Crne Gore, na sjednici od 20. januara 2023. godine, donijela je

ODLUKU
O UVOĐENjU MEĐUNARODNIH RESTRIKTIVNIH MJERA UTVRĐENIH ODLUKAMA SAVJETA EVROPSKE UNIJE ZBOG SAJBER NAPADA KOJI PREDSTAVLjAJU PRIJETNjU EVROPSKOJ UNIJI I NJENIM DRŽAVAMA ČLANICAMA

Član 1

Ovom odlukom uvode se međunarodne restriktivne mjere zbog sajber napada koji predstavljaju prijetnju Evropskoj uniji i njenim državama članicama, utvrđene odlukama Savjeta Evropske unije 2019/797/ZVBP od 17. maja 2019. godine, 2020/651/ZVBP od 14. maja 2020. godine, 2020/1127/ZVBP od 30. jula 2020. godine, 2020/1537/ZVBP od 22. oktobra 2020. godine, 2020/1748/ZVBP od 20. novembra 2020. godine, 2021/796/ZVBP od 17. maja 2021. godine i 2022/754/ZVBP od 16. maja 2022. godine kojima se Crna Gora pridružila, u skladu sa vanjskopolitičkim prioritetom usaglašavanja sa Evropskom unijom u oblasti zajedničke vanjske i bezbjednosne politike.

Član 2

Ova odluka se primjenjuje na sajber napade sa značajnim posljedicama, uključujući pokušaje sajber napada sa potencijalno značajnim posljedicama, koji predstavljaju vanjsku prijetnju Evropskoj uniji ili njenim državama članicama.

Sajber napadi koji predstavljaju vanjsku prijetnju obuhvataju sajber napade:

- koji potiču ili su izvedeni sa područja van Evropske unije;
- za koje se upotrebljava infrastruktura van Evropske unije;
- koje izvede fizičko ili pravno lice, subjekt ili organ koje ima poslovno sjedište ili djeluje van Evropske unije; ili
- koji se izvedu uz podršku, po nalogu ili pod kontrolom bilo kog fizičkog ili pravnog lica, subjekta ili organa koji djeluje van Evropske unije.

Sajber napadi iz stava 2 ovog člana su djelovanja koja obuhvataju pristup informacionim sistemima, ometanje informacionih sistema, ometanje podataka ili presretanje podataka, ako takva djelovanja nije odobrio vlasnik ili drugi imalac prava u vezi sa informacionim sistemom, podacima ili njihovim dijelom ili ako nijesu dopuštena u skladu sa pravom Evropske unije ili države članice.

Sajber napadi koji predstavljaju prijetnju državama članicama Evropske unije obuhvataju sajber napade koji pogađaju informacione sisteme povezane sa:

- kritičnom infrastrukturom, uključujući podvodne kablove i predmete poslate u svemir, koja je ključna za održavanje vitalnih funkcija u društvu ili za zdravlje, bezbjednost, zaštitu i ekonomsku ili društvenu dobrobit ljudi;

- službama neophodnim za održavanje ključnih društvenih i ekonomskih aktivnosti, posebno u sektorima energetike (električna energija, nafta i plin), transporta (vazdušnog, željezničkog, vodnog i drumskog), bankarstva, infrastrukture finansijskog tržišta, sistema zdravstva (pružaoci zdravstvene zaštite, bolnice i privatne klinike), snabdijevanja pitkom vodom i njenom distribucijom, digitalne infrastrukture i drugim sektorima koji su ključni za državu članicu Evropske unije;

- ključnim državnim funkcijama, posebno u oblasti bezbjednosti, upravljanja i funkcionisanja institucija ili privredne i civilne infrastrukture, unutrašnje bezbjednosti i vanjskih odnosa;

- skladištenjem ili obradom tajnih podataka;

- vladinim tijelima za preduzimanje aktivnosti u vanrednim situacijama.

Sajber napadi koji predstavljaju prijetnju Evropskoj uniji obuhvataju sajber napade na njene institucije, organe, službe i agencije, njene delegacije u trećim državama ili međunarodnim organizacijama, operacije ili misije zajedničke vanjske i bezbjednosne politike i njene specijalne predstavnike.

Ako se to smatra potrebnim kako bi se ostvarili ciljevi zajedničke vanjske i bezbjednosne politike iz odgovarajućih odredbi člana 21 Ugovora o Evropskoj uniji, restriktivne mjere u skladu sa ovom odlukom mogu se primijeniti i kao odgovor na sajber napade sa značajnim posljedicama protiv trećih država ili međunarodnih organizacija.

Član 3

Izrazi upotrijebljeni u ovoj odluci imaju sljedeća značenja:

1) **informacioni sistem** podrazumijeva uređaj ili skup međusobno povezanih ili srodnih uređaja, od kojih jedan ili više njih, u skladu sa programom, sprovodi automatsku obradu digitalnih podataka, kao i digitalne podatke koji su uskladišteni, obrađeni, pronađeni ili preneseni tim uređajem ili skupom uređaja za potrebe njegovog ili njihovog funkcionisanja, upotrebe, zaštite i održavanja;
2) **ometanje informacionog sistema** podrazumijeva sprečavanje ili prekidanje funkcionisanja informacionog sistema unosom, prenosom, oštećenjem, brisanjem, degradacijom, mijenjanjem ili prikrivanjem digitalnih podataka ili onemogućavanjem pristupa tim podacima;
3) **ometanje podataka** podrazumijeva brisanje, oštećenje, degradaciju, mijenjanje i prikrivanje digitalnih podataka u informacionom sistemu ili onemogućavanje pristupa tim podacima, kao i krađu podataka, finansijskih sredstava, ekonomskih resursa ili intelektualne svojine;
4) **presretanje podataka** je presretanje nejavnog prenosa digitalnih podataka iz ili unutar informacionog sistema uz pomoć tehničkih sredstava, uključujući elektromagnetske emisije iz informacionog sistema kojima se prenose digitalni podaci.

Član 4

Elementi na osnovu kojih se utvrđuje ima li sajber napad značajne posljedice u smislu člana 2 stav 1 ove odluke, obuhvataju :

- obim, razmjere, učinak ili ozbiljnost uzrokovanog poremećaja, pored ostalog u pogledu ekonomskih i društvenih aktivnosti, ključnih usluga i državnih funkcija, javnog reda i bezbjednosti;
- broj fizičkih ili pravnih lica, subjekata ili organa na koje utiču sajber napadi;
- broj država članica Evropske unije koje su pogođene sajber napadom;
- razmjere ekonomskih gubitaka uzrokovanih velikom krađom finansijskih sredstava, ekonomskih resursa ili intelektualne svojine;
- ekonomsku korist koju je učinilac sajber napada ostvario za sebe ili druge;
- količinu ili prirodu ukradenih podataka ili razmjeru povreda podataka; ili
- prirodu poslovno osjetljivih podataka kojima se pristupilo.

Član 5

Ograničava se ulazak u Crnu Goru ili prelazak preko njene teritorije fizičkim licima:

- odgovornim za sajber napade ili pokušaje sajber napada;

- koja pružaju finansijsku, tehničku ili materijalnu podršku ili su na neki drugi način svjesno umiješana u sajber napad ili pokušaj sajber napada, pored ostalog, planiranjem, pripremanjem, usmjeravanjem, pomaganjem ili podsticanjem takvih napada ili učestovanjem u takvim napadima ili olakšavanjem takvih napada činjenjem ili nečinjenjem;

- povezanim sa licima iz al. 1 i 2 ovog stava.

Ograničenje iz stava 1 ovog člana ne obavezuje Crnu Goru da crnogorskim državljanima zabrani ulazak na svoju teritoriju.

Ograničenje iz stava 1 ovog člana ne utiče na slučajeve u kojima Crnu Goru obavezuje međunarodno pravo, i to:

- kao državu domaćina međunarodne međuvladine organizacije;

- kao državu domaćina međunarodne konferencije sazvane od Ujedinjenih nacija ili pod njihovim pokroviteljstvom;

- na osnovu multilateralnog sporazuma kojim se dodjeljuju povlastice i imuniteti;

- kao državu domaćina Organizacije za evropsku bezbjednost i saradnju (OEBS).

Organi iz člana 9 ove odluke, u okviru svojih nadležnosti, mogu odobriti ulazak na teritoriju Crne Gore ili prelazak preko nje ako je to opravdano zbog hitne humanitarne potrebe ili zbog učestvovanja na međuvladinim sastancima ili sastancima koje promoviše ili koje organizuje Evropska unija ili koje organizuje država članica Evropske unije ili Crna Gora kad predsjedava OEBS-om, na kojima se odvija politički dijalog kojim se direktno promovišu politički ciljevi restriktivnih mjera, uključujući bezbjednost i stabilnost u sajber prostoru, kao i ako je ulazak ili prelazak potreban zbog sprovođenja sudskog postupka.

U slučaju da organ iz člana 9 ove odluke, u okviru svojih nadležnosti, u skladu sa st. 3 i 4 ovog člana odobri ulazak ili prelazak preko teritorije Crne Gore licima iz stava 1 ovog člana, odobrenje se ograničava u skladu sa svrhom zbog koje je izdato.

Član 6

Ograničava se raspolaganje finansijskim sredstvima i imovinom koja su u vlasništvu, državini ili pod kontrolom fizičkog ili pravnog lica, subjekta ili organa:

- koji je odgovoran za sajber napade ili pokušaje sajber napada;

- koji pruža finansijsku, tehničku ili materijalnu podršku ili je na neki drugi način svjesno umiješan u sajber napade ili pokušaje sajber napada, pored ostalog planiranjem, pripremanjem, usmjeravanjem, pomaganjem ili podsticanjem takvih napada ili učestovanjem u takvim napadima ili olakšavanjem takvih napada činjenjem ili nečinjenjem;

- povezanog sa fizičkim ili pravnim licima, subjektima ili organima iz al. 1 i 2 ovog stava.

Fizička ili pravna lica, subjekti ili organi iz stava 1 ovog člana ne mogu, direktno ili indirektno, raspolagati nikakvim finansijskim sredstvima ni imovinom.

Organ državne uprave nadležan za unutrašnje poslove može odobriti oslobađanje dijela finansijskih sredstava i odobriti korišćenje dijela imovine čije je raspolaganje, odnosno korišćenje ograničeno primjenom restriktivne mjere kad utvrdi da je taj dio finansijskih sredstava ili imovine:

- neophodan za ispunjavanje osnovnih potreba fizičkih ili pravnih lica, subjekata ili organa iz stava 1 ovog člana i članova porodice fizičkih lica, uključujući troškove za prehrambene proizvode, zakupninu, hipotekarni kredit, ljekove i liječenje, poreze, premije osiguranja i naknade za javne komunalne usluge;

- namijenjen isključivo plaćanju opravdanih honorara i naknadi troškova povezanih sa pružanjem pravnih usluga;

- namijenjen isključivo za plaćanje troškova ili naknada za uobičajeno čuvanje zamrznutih finansijskih sredstava i imovine i upravljanja njima;

- potreban za vanredne troškove;

- namijenjen uplati na račun ili isplati sa računa diplomatske ili konzularne misije ili međunarodne organizacije koje uživaju imunitet u skladu sa međunarodnom pravom, pod uslovom da su ta plaćanja namijenjena za službene potrebe diplomatske ili konzularne misije ili međunarodne organizacije.

Organ državne uprave nadležan za unutrašnje poslove može odobriti oslobađanje dijela finansijskih sredstava i odobriti korišćenje dijela imovine čije je raspolaganje, odnosno korišćenje ograničeno primjenom restriktivne mjere kad utvrdi da:

- su ta finansijska sredstva ili imovina predmet arbitražne odluke donesene prije datuma utvrđivanja restriktivne mjere prema fizičkom ili pravnom licu, subjektu ili organu iz stava 1 ovog člana ili sudske ili upravne odluke donesene u državi članici Evropske unije ili Crnoj Gori ili sudske odluke koja je izvršna u državi članici Evropske unije ili Crnoj Gori, prije ili nakon tog datuma;

- će se ta finansijska sredstva ili imovina upotrebljavati kako bi se podmirila potraživanja osigurana odlukom iz alineje 1 ovog stava ili potraživanja koja su priznata kao valjana na osnovu odluke iz alineje 1 ovog stava u granicama utvrđenim zakonima i drugim propisima kojima se uređuju prava lica koja imaju takva potraživanja;

- ta odluka nije u korist fizičkog ili pravnog lica, subjekta ili organa iz stava 1 ovog člana, a to priznavanje odluke nije u suprotnosti sa javnim poretkom države članice Evropske unije ili Crne Gore.

Ograničenje iz stava 1 ovog člana ne sprečava fizičko ili pravno lice, subjekt ili organ iz stava 1 ovog člana da izvrši dospjela plaćanja prema ugovoru zaključenom prije datuma utvrđivanja restriktivnih mjera, pod uslovom da organ iz člana 9 ove odluke, u okviru svojih nadležnosti, utvrdi da plaćanje ne primaju, direktno ili indirektno, fizička ili pravna lica, subjekti ili organi prema kojima se primjenjuju restriktivne mjere utvrđene ovom odlukom.

Ograničenje iz stava 2 ovog člana ne primjenjuje se na prilive na zamrznute račune, i to na kamate ili druga primanja na tim računima, plaćanja dospijela na osnovu ugovora, sporazuma ili obaveza koji su zaključeni ili su nastupili prije datuma utvrđivanja restriktivnih mjera iz st. 1 i 2 ovog člana, plaćanja dospjela na osnovu sudskih, upravnih ili arbitražnih odluka donesenih ili izvršivih u Evropskoj uniji ili Crnoj Gori, pod uslovom da sve te kamate, druga primanja i plaćanja podliježu mjerama iz stava 1 ovog člana.

Član 7

Fizička lica iz člana 5 stav 1 i člana 6 stav 1 ove odluke, odnosno pravna lica, subjekti i organi iz člana 6 stav 1 ove odluke navedeni su u Prilogu 1, odnosno Prilogu 2 koji su sastavni dio ove odluke.

Informacije neophodne za identifikaciju fizičkog lica iz člana 5 stav 1 i člana 6 stav 1 ove odluke, odnosno pravnog lica, subjekta i organa iz člana 6 stav 1 ove odluke sadržane su u Prilogu 1, odnosno Prilogu 2.

Informacije iz stava 2 ovog člana su:

- ime i prezime, uključujući pseudonim ako je poznat, datum i mjesto rođenja, adresa ili prebivalište ako su poznati, državljanstvo, broj pasoša ili lične karte ako su poznati, pol, kao i zanimanje ili funkciju - za fizička lica;

- naziv, adresa, mjesto, sjedište, datum i broj registracije ako su poznati – za pravna lica, subjekte i organe.

Član 8

Neće se udovoljavati zahtjevima u vezi sa ugovorom ili transakcijom na čije su izvršenje, direktno ili indirektno, u cjelini ili djelimično, uticale mjere uvedene ovom

odlukom, uključujući zahtjeve za odštetu ili bilo koje druge zahtjeve te vrste kao što su zahtjev za naknadu štete ili zahtjev na osnovu jemstva, a posebno zahtjev za produženje ili plaćanje obveznice, jemstva ili odštete, posebno finansijskog jemstva ili odštete, u bilo kojem obliku, ako ga podnesu:

- fizička ili pravna lica, subjekti ili organi iz člana 7 stav 1 ove odluke;
- fizička ili pravna lica, subjekti ili organi koji djeluju preko ili za račun jednog od fizičkih ili pravnih lica, subjekata ili organa iz člana 7 stav 1 ove odluke.

Član 9

Ministarstvo ekonomskog razvoja, Ministarstvo finansija, Ministarstvo unutrašnjih poslova, Ministarstvo kapitalnih investicija, Centralna banka Crne Gore, Agencija za nacionalnu bezbjednost, kao i drugi organi i pravna lica nadležni za primjenu restriktivnih mjera uvedenih ovom odlukom, dužni su da, u okviru svojih nadležnosti obezbijede primjenu ove odluke, kao i da o preduzetim aktivnostima obavijeste Ministarstvo vanjskih poslova.

Član 10

Ova odluka će se primjenjivati do 18. maja 2025. godine.

Član 11

Ova odluka objaviće se u „Službenom listu Crne Gore“.

Broj: 07-011/23-104
Podgorica, 12. januara 2023. godine

Vlada Crne Gore
Predsjednik,
dr **Dritan Abazović**, s.r.

Prilog 1

	Ime i prezime fizičkog lica	Lični podaci fizičkog lica	Obrazloženje	Datum utvrđivanja restriktivne mjere
1.	GAO Qiang	Datum rođenja: 9. oktobar 1983. godine Mjesto rođenja: Provincija Šandong, Kina Shandong, China Adresa: Soba 1102, Guanfu palata, 46 Xinkai Road (Šinkai ulica), Hedong distrikt, Tianjin, Kina Državljanstvo: kinesko Pol: muški	Gao Qiang učestvuje u operaciji "Operation Cloud Hopper", nizu sajber napada sa značajnim posljedicama koji potiču sa područja van Crne Gore i Evropske unije i predstavljaju vanjsku prijetnju Crnoj Gori i Evropskoj uniji i njenim državama članicama, kao i sajber napadima sa značajnim posledicama protiv trećih država. Meta operacije "Operation Cloud Hopper" su informacioni sistemi multinacionalnih društava na šest kontinenata, uključujući društva sa sjedištem u Crnoj Gori i Evropskoj uniji, a u okviru te operacije ostvaren je neovlašćen pristup komercijalno osjetljivim podacima, što je dovelo do značajnih ekonomskih gubitaka. Javni subjekt poznat kao "APT10" ("Advanced persistent Threat 10") (Takođe poznat kao "Red Apollo", "CVNX", "Stone Panda", "MenuPass" i "Potassium") izvršio je operaciju "Operation Cloud Hopper". Gao Qiang se može povezati sa subjektom "APT10", između ostalog i zbog njegove povezanosti sa kontrolno-upravljačkom infrastrukturom subjekta "APT10". Dalje, Huaying Haitai, subjekt uvršten u prilogu ove odluke zbog pružanja podrške operaciji "Operation Cloud Hopper" i njenog olakšavanja, angažovao je Gao-a Qiang-a. Povezan je sa Zhang-om Shilong-om koji je takođe uvršten u prilog ove odluke zbog veza sa operacijom "Operation Cloud Hopper". Gao Quiang stoga je povezan i sa subjektom Huaying Haitai i sa Zhang-om Shilong-om.	30.7.2020.

2.	Zhang Shilong	Datum rođenja: 10. oktobar 1981. godine Mjesto rođenja: Kina Adresa: Hedong, Yuyang Road No 121, (Džudžang ulica br 121) Tianjin, Kina Državljanstvo: kinesko Pol: muški	Zhang Shilong učestvuje u operaciji "Operation Cloud Hopper", nizu sajber napada sa značajnim posljedicama koji potiču sa područja van Crne Gore i Evropske unije i predstavljaju vanjsku prijetnju Crnoj Gori i Evropskoj uniji i njenim državama članicama, kao i sajber napadima sa značajnim posledicama protiv trećih država. Meta operacije "Operation Cloud Hopper" su informacioni sistemi multinacionalnih društava na šest kontinenata, uključujući društva sa sjedištem u Crnoj Gori i Evropskoj uniji, a u okviru te operacije ostvaren je neovlašćen pristup komercijalno osjetljivim podacima, što je dovelo do značajnih ekonomskih gubitaka. Javni subjekt poznat kao "APT10" ("Advanced persistent Threat 10") (Takođe poznat kao "Red Apollo", "CVNX", "Stone Panda", "MenuPass" i "Potassium") izvršio je operaciju "Operation Cloud Hopper". Zhang Shilong se može povezati sa subjektom "APT10", između ostalog i zbog njegove povezanosti sa kontrolno-upravljačkom infrastrukturom subjekta "APT10". Dalje, Huaying Haitai, subjekt uvršten u prilogu ove odluke zbog pružanja podrške operaciji "Operation Cloud Hopper" i njenog olakšavanja, angažovao je Gao Qiang. Povezan je s Gaom Qiangom, koji je takođe uvršten u prilog ove odluke zbog veza sa operacijom „Operation Cloud Hopper". Zhang Shilong stoga je povezan i sa subjektom Huaying Haitai i s Gaom Qiangom.	30.7.2020.
3.	Alexey Valeryevich Minin	Алексей Валерьевич Минин Datum rođenja: 27. maja 1972.	Alexey Minin (Aleksej Minin) je učestvovao u pokušaju sajber napada sa potencijalno značajnim posledicama na Organizaciju za zabranu hemijskog oružja (OPCW)	30.7.2020.

		godine Mjesto rođenja: Permska oblast, Ruski SFSR (sada Ruska Federacija) Broj pasoša: 120017582 Izdat od: MVP Ruske Federacije Validno: od 17. marta 2017. godine do 17. marta. 2022. Godine Prebivalište: Moskva, Ruska Federacija Državljanstvo: rusko Pol: muški	u Holandiji. Kao službenik za prikupljanje obavještajnih podataka ličnim kontaktima u okviru Centralne uprave generalštaba oružanih snaga Ruske Federacije (GU/GRU) Alexey Minin bio je dio tima od četiri ruska vojnoobavještajna službenika koji su pokušali neovlašćeno pristupiti bežičnoj mreži OPCW-a u Hagu u Holandiji u martu 2018. godine. Pokušaj sajber napada bio je usmjeren na hakovanje bežične mreže i tekuće istražne radnje OPCW-a. Holandska bezbjednosna i obavještajna služba (DISS) (Militaire Inlichtingen- en Veiligheidsdienst- MIVD) spriječila je pokušaj sajber napada i time izbjegla ozbiljnu štetu za OPCW.	
4.	Aleksei Sergeyvich Morenets	Алексей Сергеевич Моренец Datum rođenja: 31. jul 1981. godine Mjesto rođenja: Murmanska oblast, Ruski SFSR (sada Ruska Federacija) Broj pasoša: 100135556 Izdat od: MVP Ruske Federacije Validno: Od 17. marta 2017. godine do 17. marta. 2022. godine Prebivalište:Moskva, Ruska Federacija Državljanstvo:rusko Pol: muški	Aleksei Morenets (Aleksej Morenec) je učestvovao u pokušaju sajber napada sa potencijalno značajnim posledicama na Organizaciju za zabranu hemijskog oružja (OPCW) u Holandiji. Kao službenik za prikupljanje obavještajnih podataka ličnim kontaktima u okviru Centralne uprave generalštaba oružanih snaga Ruske Federacije (GU/GRU) Aleksei Morenets bio je dio tima od četiri ruska vojnoobavještajna službenika koj isu pokušali neovlašćeno pristupiti bežičnoj mreži OPCW-a u Hagu u Holandiji u martu 2018. godine. Pokušaj sajber napada bio je usmjeren na hakovanje bežične mreže i tekuće istražne radnje OPCW-a. Holandska bezbjednosna i obavještajna služba (DISS) (Militaire Inlichtingen- en Veiligheidsdienst- MIVD) spriječila je pokušaj sajber napada i time izbjegla ozbiljnu štetu za OPCW.	30.7.2020.

5.	Evgenii Mikhaylovich Serebriakov	Евгений Михайлович Серебряков Datum rođenja: 26. jul 1981. godine Mjesto rođenja: Kursk, Ruski SFSR (sada Ruska Federacija) Broj pasoša: 100135555 Izdat od: MVP Ruske Federacije Validno: Od 17. marta 2017. godine do 17. marta. 2022. godine Prebialište:Moskva, Ruska Federacija Državljanstvo:rusko Pol: muški	Evgenii Serebriakov (Evgenij Serebriakov) je učestvovao u pokušaju sajber napada sa potencijalno značajnim posledicama na Organizaciju za zabranu hemijskog oružja (OPCW) u Holandiji. Kao službenik za prikupljanje obavještajnih podataka ličnim kontaktima u okviru Centralne uprave generalštaba oružanih snaga Ruske Federacije (GU/GRU) Evgenii Serebriakov bio je dio tima od četiri ruska vojnoobavještajna službenika koj isu pokušali neovlašćeno pristupiti bežičnoj mreži OPCW-a u Hagu u Holandiji u martu 2018. godine. Pokušaj sajber napada bio je usmjeren na hakovanje bežične mreže i tekuće istražne radnje OPCW-a. Holandska bezbjednosna i obavještajna služba (DISS) (Militaire Inlichtingen- en Veiligheidsdienst- MIVD) spriječila je pokušaj sajber napada i time izbjegla ozbiljnu štetu za OPCW.	30.7.2020.
6.	Oleg Mikhaylovich Sotnikov	Олег Михайлович Сотников Datum rođenja: 24. avgust 1972. godine Mjesto rođenja: Uljanovsk, Ruski SFSR (sada Ruska Federacija) Broj pasoša: 120018866 Izdat od: MVP Ruske Federacije Validno: Od 17. marta 2017. godine do 17. marta. 2022. godine Prebivalište: Moskva, Ruska Federacija Državljanstvo:rusko	Oleg Sotnikov je učestvovao u pokušaju sajber napada sa potencijalno značajnim posledicama na Organizaciju za zabranu hemijskog oružja (OPCW) u Holandiji. Kao službenik za prikupljanje obavještajnih podataka ličnim kontaktima u okviru Centralne uprave generalštaba oružanih snaga Ruske Federacije (GU/GRU) Oleg Sotnikov bio je dio tima od četiri ruska vojnoobavještajna službenika koji su pokušali neovlašćeno pristupiti bežičnoj mreži OPCW-a u Hagu u Holandiji u martu 2018. godine. Pokušaj sajber napada bio je usmjeren na hakovanje bežične mreže i tekuće istražne radnje OPCW-a. Holandska bezbjednosna i obavještajna služba (DISS)	30.7.2020.

		Pol: muški	(Militaire Inlichtingen- en Veiligheidsdienst- MIVD) spriječila je pokušaj sajber napada i time izbjegla ozbiljnu štetu za OPCW.	
7.	Dmitry Sergeyevich Badin	Дмитрий Сергеевич Бадин Datum rođenja: 15. novembar 1990. godine Mjesto rođenja: Kursk, Ruski SFSR (sada Ruska Federacija) Državljanstvo:rusko Pol: muški	Dmitry Badin (Dmitri Badin) je učestvovao u sajber napadu sa značajnim posledicama na Njemački savezni parlament (Deutscher Bundestag). Kao vojnoobavještajni oficir 85. glavnog centra za specijalne službe (GTsSS) Centralne uprave generalštaba oružanih snaga Ruske Federacije (GU/GRU) Dmitry Badin je bio dio tima ruskih vojnoobavještajnih oficira koji su izveli sajber napad na njemački savezni parlament (Deutscher Bundestag) u martu i maju 2015. godine. Taj sajber napad bio je usmjeren na informacioni sistem njemačkog saveznog parlamenta i nekoliko je dana uticao na njegovo funkcionisanje. Ukradena je znatna količina podataka i zahvaćeni su mail-ovi više poslanika i poslanica u parlamentu, kao i e-mail kancelarke Angele Merkel.	22.10.2020.
8.	Igor Olegovich Kostyukov	Игор Олегович Костюков Datum rođenja: 21. februar 1961. godine Državljanstvo:rusko Pol: muški	Igor Kostyukov (Igor Kostjukov) je aktuelni načelnik Centralne uprave oružanih snaga Ruske Federacije (GU/GRU), gdje je prethodno obavljao dužnost prvog zamjenika načelnika. Među jedinicama pod njegovim komandom nalazi se 85. glavni centar za specijalne službe (GTsSS), poznat kao “vojna jedinica 26165” (sektorski nadimci “APT28”, “Fancy Bear”, “Sofacy Group”, “Pawn Storm” i “Strontium”). U tom je svojstvu Igor Kostyukov odgovoran za sajber napade koje je izveo GTsSS, uključujući sajber napade sa značajnim posledicama koji predstavljaju vanjsku prijetnju Crnoj Gori i Evropskoj uniji ili njenim državama članicama. Konkretno, vojnoobavještajni oficiri	22.10.2022.

			GTsSS-a učestvovali su u sajbernapadu na njemački savezni parlament (Deutscher Bundestag) u martu i maju 2015. godine kao i pokušaju sajber napada sa ciljem hakovanja bežične mreže Organizacije za zabranu hemijskog oružja (OPCW) u Holandiji u martu 2018. godine. Sajber napad na njemački savezni parlament je bio usmjeren na informacioni sistem parlamenta i nekoliko je dana uticao na njegovo funkcionisanje. Ukradena je znatna količina podataka i zahvaćeni su mail-ovi više poslanika i poslanica u parlamentu, kao i e-mail kancelarke Angele Merkel.	

Prilog 2

	Naziv pravnog lica, odnosno subjekta ili organa	Podaci o pravnom licu, odnosno subjektu ili organu	Obrazloženje	Datum utvrđivanja restriktivne mjere
1.	Tianjin Huaying Haitai Science and Technology Development Co. Ltd (Huaying Haitai)	Takođe poznat kao: Haitai Technology Development Co. Ltd Sjedište: Tianjin, Kina	Huaying Haitai je pružio i olakšao finansijsku, tehničku i materijalnu podršku za operaciju "Operation Cloud Hopper", koja je uključivala niz sajber napada sa značajnim posljedicama koji potiču sa područja van Crne Gore i Evropske unije i predstavljaju vanjsku prijetnju Crnoj Gori i Evropskoj uniji ili njenim državama članicama te sajber napadima na treće države. Meta operacije "Operation Cloud Hopper" su informacioni sistemi multinacionalnih društava na šest kontinenata, uključujući društva sa sjedištem u Crnoj Gori i Evropskoj uniji, i u okviru te operacije je ostvaren neovlašćen pristup poslovno osjetljivim podacima, što je dovelo do značajnih ekonomskih gubitaka. Javni subjekt poznat kao "APT10" ("Advanced persistent Threat 10") (Takođe poznat kao "Red Apollo", "CVNX", "Stone Panda", "MenuPass" i "Potassium") izvršio je operaciju "Operation Cloud Hopper". Huaying Haitai se može povezati sasubjektom "APT10". Dalje, Huaying Haitai angažovao je Gao-a Qiang-a i Zhang-a Shilong-a koji se nalaze u ovom prilogu, u vezi sa operacijom "Operation Cloud Hopper". Huaying Haitai je time povezan sa Gao Qiang-om i Zhang-om Shilong-om.	30.7.2020.
2.	Chosun Expo	Takođe poznat kao: Chosen Expo, Korea Export Joint Venture Lokacija: DNRK (Sjeverna Koreja)	Chosun Expo je pružio finansijsku, tehničku ili materijalnu podršku i olakšao sajber napade sa značajnim posledicama, sa područja van Crne Gore i Evropske unije i koji predstavljaju vanjsku prijetnju Crnoj Gori i Evropskoj uniji ili njenim državama članicama, kao i sajber napadima na treće države, uključujući sajber napade koji su javnosti poznati kao "WannaCry" i sajbernapade na	30.7.2020.

			poljski državni organ za finansijski nadzor i preduzeće Sony Pictures Entertainment, kao i sajber krađu u banci Bangladesh Bank te pokušaj sajber krađe u vijetnamskoj banci Tien Phong Bank. "WannaCry" je uzrokovao poremećaje u informacionim sistemima širom svijeta tako što ih je napao ucijenjivačkim softverom (engl. ransomware) i blokirao pristup podacima. Uticao je na informacione sisteme društava u Crnoj Gori i Evropskoj uniji, uključujući informacione sisteme povezane sa uslugama potrebnim za održavanje ključnih usluga i privrednih aktivnosti u državama članicama. Subjekt javnosti poznat pod nazivom „APT38" („Advanced persistent Threat 38") i grupa „Lazarus Group" su izvršili napad "WannaCry". Chosun Expo može se povezati sa subjektom „APT38" i grupom „Lazarus Group", između ostalog pomoću računa koji su upotrebljeni za sajber napade.	
3.	Glavni centar za posebne tehnologije (GTsST) Centralne uprave generalštaba oružanih snaga Ruske Federacije (GU/GRU)	Adresa: Ul. Kirova, Moskva, Ruska Federacija	Glavni centar za posebne tehnologije (GTsST) Centralne uprave generalštaba oružanih snaga Ruske Federacije (GU/GRU), poznat i pod brojem vojne pošte kao 74455, odgovoran je za sajber napade značajnim posledicama koji potiču sa područja van Crne Gore i Evropske unije i predstavljaju vanjsku prijetnju Crnoj Gori i Evropskoj uniji ili njenim državama članicama, kao i sajber napadima na treće države, uključujući sajber napade u junu 2017. godine koji su u javnosti poznati kao "NotPetya" ili "EternalPetya" i sajber napade na ukrajinsku energetsku mrežu tokom zime 2015. i 2016. godine. "NotPetya" ili "EternalPetya" onemogućili su pristup podacima nizu privrednih društava u Crnoj Gori, Evropskoj uniji, široj Evropi i svijetu tako što su računare napali ucjenjivačkim softverom i blokirali	30.7.2020.

			pristup podacima, što je, između ostalog, dovelo do značajnih ekonomskih gubitaka. Sajber napad na ukrajinsku energetsku mrežu je završio gašenjem djelova te mreže tokom zime. Subjekt u javnosti pozant kao „Sandworm“ (takođe poznat kao “Sandworm Team”, “BlackEnergy Group”, “Voodoo Bear”, “Quedagh”, “Olympic Destroyer” i “Telebots”), koji takođe stoji iza napada na ukrajinsku energetsku mrežu, izvršio je napade “NotPetya” ili “EternalPetya”. Glavni centar za posebne tehnologije Centralne uprave generalštaba oružanih snaga Ruske Federacije ima aktivnu ulogu u sajber aktivnostima koje sprovodi „Sandworm“ i može se povezati sa subjektom „Sandworm“.	
4.	85. glavni centar za specijalne službe (GTsSS) Centralne uprave generalštaba oružanih snaga Ruske Federacije (GU/GRU)	Adresa: Komsomol’skiy Prospekt, 20, Moskva, 119146, Ruska Federacija	85. glavni centar za posebne tehnologije (GTsSS) Centralne uprave generalštaba oružanih snaga Ruske Federacije (GU/GRU), poznat kao “vojna jedinica 26165” (sektorski nadimci “APT28”, “Fancy Bear”, “Sofacy Group”, “Pawn Storm” i “Strontium”), odgovoran je za sajber napade značajnim posledicama koji predstavljaju vanjsku prijetnju Crnoj Gori i Evropskoj uniji i njenim državama članicama. Konkretno, vojnoobavještajni oficiri GTsSS-a učestvovali su u sajber napadu na jjemački savezni parlament (Deutscher Bundestag) u martu i maju 2015. godine kao i pokušaju sajber napada sa ciljem hakovanja bežične mreže Organizacije za zabranu hemijskog oružja (OPCW) u Holandiji u martu 2018. godine. Sajber napad na njemački savezni parlament je bio usmjeren na informacioni sistem parlamenta i nekoliko je dana uticao na njegovo funkcionisanje. Ukradena je znatna količina podataka i zahvaćeni su mail-ovi više poslanika i poslanica u parlamentu, kao i e-mail kancelarke Angele Merkel.	22.10.2022.