ROZPORZĄDZENIE WYKONAWCZE RADY (UE) 2020/1125

z dnia 30 lipca 2020 r.

wykonujące rozporządzenie (UE) 2019/796 w sprawie środków ograniczających w celu zwalczania cyberataków zagrażających Unii lub jej państwom członkowskim

RADA UNII EUROPEJSKIEJ,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej,

uwzględniając rozporządzenie Rady (UE) 2019/796 z dnia 17 maja 2019 r. w sprawie środków ograniczających w celu zwalczania cyberataków zagrażających Unii lub jej państwom członkowskim ([1]), a w szczególności jego art. 13 ust. 1,

uwzględniając wniosek Wysokiego Przedstawiciela Unii do Spraw Zagranicznych i Polityki Bezpieczeństwa,

a także mając na uwadze, co następuje:

(1) W dniu 17 maja 2019 r. Rada przyjęła rozporządzenie (UE) 2019/796.

(2) Ukierunkowane środki ograniczające w celu zwalczania cyberataków wywołujących poważne skutki, które to ataki stanowią zewnętrzne zagrożenie dla Unii lub jej państw członkowskich, należą do środków przewidzianych w unijnych ramach wspólnej reakcji dyplomatycznej na szkodliwe działania w cyberprzestrzeni (zestaw narzędzi dla dyplomacji cyfrowej) i są niezbędnym instrumentem powstrzymywania takich działań i reagowania na nie. Środki ograniczające mogą być również stosowane w odpowiedzi na wywołujące poważne skutki cyberataki wymierzone przeciwko państwom trzecim lub organizacjom międzynarodowym, w przypadku gdy uznaje się to za konieczne do osiągnięcia celów wspólnej polityki zagranicznej i bezpieczeństwa określonych w odpowiednich przepisach art. 21 Traktatu o Unii Europejskiej.

(3) W dniu 16 kwietnia 2018 r. Rada przyjęła konkluzje, w których stanowczo potępiła szkodliwe użycie technologii informacyjno-komunikacyjnych, w tym cyberataki powszechnie znane jako „WannaCry" i „NotPetya", które spowodowały znaczne szkody i straty gospodarcze w Unii i poza nią. W dniu 4 października 2018 r. przewodniczący Rady Europejskiej i Komisji Europejskiej oraz Wysoki Przedstawiciel Unii do Spraw Zagranicznych i Polityki Bezpieczeństwa (zwany dalej „Wysokim Przedstawicielem") wyrazili we wspólnym oświadczeniu poważne zaniepokojenie w związku z próbą cyberataku mającego na celu podważenie integralności Organizacji ds. Zakazu Broni Chemicznej (OPCW) w Niderlandach; był to akt agresji pokazujący pogardę dla słusznego celu OPCW. W oświadczeniu złożonym w imieniu Unii w dniu 12 kwietnia 2019 r. Wysoki Przedstawiciel wezwał podmioty do zaprzestania szkodliwych działań w cyberprzestrzeni, mających na celu naruszenie integralności, bezpieczeństwa i gospodarczej konkurencyjności Unii, w tym coraz częstszych przypadków kradzieży własności intelektualnej z wykorzystaniem cyberprzestrzeni. Takie kradzieże z wykorzystaniem cyberprzestrzeni obejmują kradzieże przeprowadzone przez podmiot powszechnie znany jako „APT10" („Advanced Persistent Threat 10").

(4) W tym kontekście oraz w celu zapobiegania nieustannym i coraz liczniejszym szkodliwym działaniom w cyberprzestrzeni, w celu zniechęcania do nich, ich powstrzymywania i reagowania na nie, w wykazie osób fizycznych i prawnych, podmiotów i organów podlegających środkom ograniczającym zawartym w załączniku I do rozporządzenia (UE) 2019/796 należy zamieścić sześć osób fizycznych i trzy podmioty lub organy. Te osoby i podmioty lub organy są odpowiedzialne za cyberataki lub próby cyberataków, w tym próbę cyberataku przeciwko OPCW oraz cyberataki powszechnie znane jako „WannaCry" i „NotPetya", a także „Operation Cloud Hopper"; wspierały te ataki lub były w nie zaangażowane, lub je ułatwiały.

(5) Należy zatem odpowiednio zmienić rozporządzenie (UE) 2019/796,

PRZYJMUJE NINIEJSZE ROZPORZĄDZENIE:

Artykuł 1

W załączniku I do rozporządzenia (UE) 2019/796 wprowadza się zmiany zgodnie z załącznikiem do niniejszego rozporządzenia.

([1]) Dz.U. L 129I z 17.5.2019, s. 1.

Artykuł 2

Niniejsze rozporządzenie wchodzi w życie z dniem jego opublikowania w *Dzienniku Urzędowym Unii Europejskiej*.

Niniejsze rozporządzenie wiąże w całości i jest bezpośrednio stosowane we wszystkich państwach członkowskich.

Sporządzono w Brukseli dnia 30 lipca 2020 r.

W imieniu Rady
M. ROTH
Przewodniczący

ZAŁĄCZNIK

Następujące osoby i podmioty lub organy dodaje się do wykazu osób fizycznych i prawnych, podmiotów i organów zamieszczonego w załączniku I do rozporządzenia (UE) 2019/796:

„A. Osoby fizyczne

	Nazwisko i imię	Dane identyfikacyjne	Powody	Data umieszczenia
1.	GAO Qiang	Miejsce urodzenia: prowincja Szantung, Chiny Adres: Room 1102, Guanfu Mansion, 46 Xinkai Road, Hedong District, Tianjin, China Obywatelstwo: chińskie Płeć: mężczyzna	Gao Qiang jest zaangażowany w »Operation Cloud Hopper«, serię cyberataków wywołujących poważne skutki, pochodzących spoza Unii i stanowiących zewnętrzne zagrożenie dla Unii lub jej państw członkowskich, oraz cyberataków wywołujących poważne skutki dla państw trzecich. »Operation Cloud Hopper« był skierowany w systemy informacyjne przedsiębiorstw wielonarodowych na sześciu kontynentach, w tym przedsiębiorstw mających siedzibę w Unii, oraz uzyskał nieuprawniony dostęp do danych wrażliwych pod względem handlowym, powodując znaczne straty gospodarcze. »Operation Cloud Hopper« został przeprowadzony przez podmiot powszechnie znany jako »APT10« (»Advanced Persistent Threat 10«) (alias »Red Apollo«, »CVNX«, »Stone Panda«, »MenuPass« i »Potassium«). Gao Qiang może zostać powiązany z APT10, w tym przez jego związek z infrastrukturą sterowania i kontroli APT10. Ponadto Gao Qiang był zatrudniony przez Hujaing Haitai, podmiot wskazany w związku ze wspieraniem i ułatwianiem »Operation Cloud Hopper«. Gao Qiang ma powiązania z Zhang Shilong, który jest również wskazany w związku z »Operation Cloud Hopper«. Gao Qiang ma zatem powiązania zarówno z Huaying Haitai, jak i Zhang Shilong.	30.7.2020
2.	ZHANG Shilong	Adres: Hedong, Yuyang Road No 121, Tianjin, China Obywatelstwo: chińskie Płeć: mężczyzna	Zhang Shilong jest zaangażowany w »Operation Cloud Hopper«, serię cyberataków wywołujących poważne skutki, pochodzących spoza Unii i stanowiących zewnętrzne zagrożenie dla Unii lub jej państw członkowskich, oraz cyberataków wywołujących poważne skutki dla państw trzecich. »Operation Cloud Hopper« był skierowany w systemy informacyjne przedsiębiorstw wielonarodowych na sześciu kontynentach, w tym przedsiębiorstw mających siedzibę w Unii, oraz uzyskał nieuprawniony dostęp do danych wrażliwych pod względem handlowym, powodując znaczne straty gospodarcze. »Operation Cloud Hopper« został przeprowadzony przez podmiot powszechnie znany jako »APT10« (»Advanced Persistent Threat 10«) (alias »Red Apollo«, »CVNX«, »Stone Panda«, »MenuPass« i »Potassium«). Zhang Shilong może zostać powiązany z APT10, w tym przez złośliwe oprogramowanie, które opracował i testował w związku z cyberatakami przeprowadzonymi przez APT10. Ponadto Zhang Shilong był zatrudniony przez Hujaing Haitai, podmiot wskazany w związku ze wspieraniem i ułatwianiem »Operation Cloud Hopper«. Zhang Shilong ma powiązania z Gao Qiang, który jest również wskazany w związku z »Operation Cloud Hopper«. Zhang Shilong ma zatem powiązania zarówno z Huaying Haitai, jak i Gao Qiang.	30.7.2020

3.	Alexey Valeryevich MININ	Алексей Валерьевич МИНИН Data urodzenia: 27 maja 1972 r. Miejsce urodzenia: Obwód Perm, ZSRR (obecnie Federacja Rosyjska) Numer paszportu: 120017582, wydany przez Ministerstwo Spraw Zagranicznych Federacji Rosyjskiej, ważny od dnia 17 kwietnia 2017 r. do dnia 17 kwietnia 2022 r. Miejsce: Moskwa, Federacja Rosyjska Obywatelstwo: rosyjskie Płeć: mężczyzna	Alexey Minin wziął udział w próbie cyberataku przeciwko Organizacji ds. Zakazu Broni Chemicznej (OPCW) w Niderlandach, który mógł wywołać poważne skutki. Jako oficer wsparcia wywiadu osobowego Głównego Zarządu Sztabu Generalnego Sił Zbrojnych Federacji Rosyjskiej (GU GRU) Alexey Minin należał do zespołu czterech rosyjskich oficerów wywiadu wojskowego, którzy w kwietniu 2018 r. dokonali próby uzyskania nieuprawnionego dostępu do sieci Wi-Fi OPCW w Hadze w Niderlandach. Próba cyberataku miała na celu włamanie się do sieci Wi-Fi OPCW; gdyby atak ten się udał, zagroziłby bezpieczeństwu sieci i pracom dochodzeniowym prowadzonym przez OPCW. Wywiad Wojskowy i Służby Bezpieczeństwa Niderlandów (Militaire Inlichtingen- en Veiligheidsdienst – MIVD) przerwały tę próbę cyberataku, uniemożliwiając w ten sposób wyrządzenie poważnej szkody OPCW.	30.7.2020
4.	Aleksei Sergeyvich MORENETS	Алексей Сергеевич МОРЕНЕЦ Data urodzenia: 31 lipca 1977 r. Miejsce urodzenia: Obwód Murmański, ZSRR (obecnie Federacja Rosyjska) Numer paszportu: 100135556, wydany przez Ministerstwo Spraw Zagranicznych Federacji Rosyjskiej, ważny od dnia 17 kwietnia 2017 r. do dnia 17 kwietnia 2022 r. Miejsce: Moskwa, Federacja Rosyjska Obywatelstwo: rosyjskie Płeć: mężczyzna	Aleksei Morenets wziął udział w próbie cyberataku przeciwko Organizacji ds. Zakazu Broni Chemicznej (OPCW) w Niderlandach, który mógł wywołać poważne skutki. Jako cyberoperator Głównego Zarządu Sztabu Generalnego Sił Zbrojnych Federacji Rosyjskiej (GU GRU) Aleksei Morenets należał do zespołu czterech rosyjskich oficerów wywiadu wojskowego, którzy w kwietniu 2018 r. dokonali próby uzyskania nieuprawnionego dostępu do sieci Wi-Fi OPCW w Hadze w Niderlandach. Próba cyberataku miała na celu włamanie się do sieci Wi-Fi OPCW; gdyby atak ten się udał, zagroziłby bezpieczeństwu sieci i pracom dochodzeniowym prowadzonym przez OPCW. Wywiad Wojskowy i Służby Bezpieczeństwa Niderlandów (Militaire Inlichtingen- en Veiligheidsdienst – MIVD) przerwały tę próbę cyberataku, uniemożliwiając w ten sposób wyrządzenie poważnej szkody OPCW.	30.7.2020
5.	Evgenii Mikhaylovich SEREBRIAKOV	Евгений Михайлович СЕРЕБРЯКОВ Data urodzenia: 26 lipca 1981 r. Miejsce urodzenia: Kursk, ZSRR (obecnie Federacja Rosyjska) Numer paszportu: 100135555, wydany przez Ministerstwo Spraw Zagranicznych Federacji Rosyjskiej, ważny od dnia 17 kwietnia 2017 r. do dnia 17 kwietnia 2022 r. Miejsce: Moskwa, Federacja Rosyjska Obywatelstwo: rosyjskie Płeć: mężczyzna	Evgenii Serebriakov wziął udział w próbie cyberataku przeciwko Organizacji ds. Zakazu Broni Chemicznej (OPCW) w Niderlandach, który mógł wywołać poważne skutki. Jako cyberoperator Głównego Zarządu Sztabu Generalnego Sił Zbrojnych Federacji Rosyjskiej (GU GRU) Evgenii Serebriakov należał do zespołu czterech rosyjskich oficerów wywiadu wojskowego, którzy w kwietniu 2018 r. dokonali próby uzyskania nieuprawnionego dostępu do sieci Wi-Fi OPCW w Hadze w Niderlandach. Próba cyberataku miała na celu włamanie się do sieci Wi-Fi OPCW; gdyby atak ten się udał, zagroziłby bezpieczeństwu sieci i pracom dochodzeniowym prowadzonym przez OPCW. Wywiad Wojskowy i Służby Bezpieczeństwa Niderlandów (Militaire Inlichtingen- en Veiligheidsdienst – MIVD) przerwały tę próbę cyberataku, uniemożliwiając w ten sposób wyrządzenie poważnej szkody OPCW.	30.7.2020

6.	Oleg Mikhaylovich SOTNIKOV	Олег Михайлович СОТНИКОВ Data urodzenia: 24 sierpnia 1972 r. Miejsce urodzenia: Uljanowsk, ZSRR (obecnie Federacja Rosyjska) Numer paszportu: 120018866, wydany przez Ministerstwo Spraw Zagranicznych Federacji Rosyjskiej, ważny od dnia 17 kwietnia 2017 r. do dnia 17 kwietnia 2022 r. Miejsce: Moskwa, Federacja Rosyjska Obywatelstwo: rosyjskie Płeć: mężczyzna	Oleg Sotnikov wziął udział w próbie cyberataku przeciwko Organizacji ds. Zakazu Broni Chemicznej (OPCW) w Niderlandach, który mógł wywołać poważne skutki. Jako oficer wsparcia wywiadu osobowego Głównego Zarządu Sztabu Generalnego Sił Zbrojnych Federacji Rosyjskiej (GU GRU) Oleg Sotnikov należał do zespołu czterech rosyjskich oficerów wywiadu wojskowego, którzy w kwietniu 2018 r. dokonali próby uzyskania nieuprawnionego dostępu do sieci Wi-Fi OPCW w Hadze w Niderlandach. Próba cyberataku miała na celu włamanie się do sieci WiFi OPCW; gdyby atak ten się udał, zagroziłby bezpieczeństwu sieci i pracom dochodzeniowym prowadzonym przez OPCW. Wywiad Wojskowy i Służby Bezpieczeństwa Niderlandów (Militaire Inlichtingen- en Veiligheidsdienst – MIVD) przerwały tę próbę cyberataku, uniemożliwiając w ten sposób wyrządzenie poważnej szkody OPCW.	30.7.2020

B. Osoby prawne, podmioty i organy

	Nazwa	Dane identyfikacyjne	Powody	Data umieszczenia
1.	Tianjin Huaying Haitai Science and Technology Development Co Ltd (Huaying Haitai)	Alias Haitai Technology Development Co. Ltd Miejsce: Tiencin, Chiny	Huaying Haitai udzielił finansowego, technicznego lub materialnego wsparcia na rzecz »Operation Cloud Hopper«, serii cyberataków wywołujących poważne skutki, pochodzących spoza Unii i stanowiących zewnętrzne zagrożenie dla Unii lub jej państw członkowskich, oraz cyberataków wywołujących poważne skutki dla państw trzecich; ułatwił także te cyberataki. »Operation Cloud Hopper« był skierowany w systemy informacyjne przedsiębiorstw wielonarodowych na sześciu kontynentach, w tym przedsiębiorstw mających siedzibę w Unii, oraz uzyskał nieuprawniony dostęp do danych wrażliwych pod względem handlowym, powodując znaczne straty gospodarcze. »Operation Cloud Hopper« został przeprowadzony przez podmiot powszechnie znany jako »APT10« (»Advanced Persistent Threat 10«) (alias »Red Apollo«, »CVNX«, »Stone Panda«, »MenuPass« i »Potassium«). Huaying Haitai może zostać powiązany z APT10. Ponadto Gao Qiang i Zhang Shilong, obaj wskazani w związku z »Operation Cloud Hopper«, byli zatrudnieni przez Hujaing Haitai. Huaying Haitai ma zatem powiązania zarówno z Gao Qiang, jak i Zhang Shilong.	30.7.2020
2.	Chosun Expo	Chosen Expo; Korea Export Joint Venture Miejsce: KRLD	Chosun Expo udzielił finansowego, technicznego lub materialnego wsparcia na rzecz serii cyberataków i ułatwił serię cyberataków, wywołujących poważne skutki, pochodzących spoza Unii i stanowiących zewnętrzne zagrożenie dla Unii lub jej państw członkowskich, oraz cyberataków wywołujących poważne skutki dla państw trzecich, w tym cyberataków powszechnie znanych jako »WannaCry« oraz cyberataków przeciwko polskiej Komisji Nadzoru Finansowego oraz Sony Pictures Entertainment, a także kradzieży w cyberprzestrzeni z Bangladesh Bank i próby kradzieży w cyberprzestrzeni z Vietnam Tien Phong Bank.	30.7.2020

			»WannaCry« zakłócił systemy informacyjne na całym świecie poprzez uderzenie w systemy informacyjne za pomocą oprogramowania typu ransomware i blokowanie dostępu do danych. Wpłynął on na systemy informacyjne przedsiębiorstw w Unii, w tym systemy informacyjne związane z usługami niezbędnymi do utrzymania podstawowych usług i działalności gospodarczej w państwach członkowskich. »WannaCry« został przeprowadzony przez podmiot publicznie znany jako »APT38« (»Advanced Persistent Threat 38«) lub »grupa Lazarus«. Chosun Expo może zostać powiązany z APT38 lub grupą Lazarus, w tym przez konta wykorzystywane do cyberataków.	
3.	Główny Ośrodek Specjalnych Technologii (GTsST) Głównego Zarządu Sztabu Generalnego Sił Zbrojnych Federacji Rosyjskiej (GU GRU)	Adres: ulica Kirowa 22, Moskwa, Federacja Rosyjska	Główny Ośrodek Specjalnych Technologii (GTsST) Głównego Zarządu Sztabu Generalnego Sił Zbrojnych Federacji Rosyjskiej (GU GRU), znany również jako jednostka numer 74455, jest odpowiedzialny za cyberataki wywołujące poważne skutki, pochodzące spoza Unii i stanowiące zewnętrzne zagrożenie dla Unii lub jej państw członkowskich, oraz cyberataki wywołujące poważne skutki dla państw trzecich, w tym cyberataki powszechnie znane jako »NotPetya« lub »EternalPetya« w czerwcu 2017 r. oraz cyberataki skierowane w ukraińską sieć elektroenergetyczną zimą 2015 i 2016 r. »NotPetya« lub »EternalPetya« spowodowały brak dostępności danych w wielu przedsiębiorstwach w Unii, szerzej w Europie i na całym świecie poprzez uderzenie w komputery za pomocą oprogramowania typu ransomware i zablokowanie dostępu do danych, co doprowadziło między innymi do znacznych strat gospodarczych. Cyberatak na ukraińską sieć elektroenergetyczną spowodował wyłączenie jej części zimą.	30.7.2020”
			»NotPetya« lub »EternalPetya« zostały przeprowadzone przez podmiot powszechnie znany jako »Sandworm« (alias »Sandworm Team«, »BlackEnergy Group«, »Voodoo Bear«, »Quedagh«, »Olympic Destroyer« i »Telebots«), który stoi również za atakiem na ukraińską sieć elektroenergetyczną. Główny Ośrodek Specjalnych Technologii Głównego Zarządu Sztabu Generalnego Sił Zbrojnych Federacji Rosyjskiej odgrywa czynną rolę w działaniach w cyberprzestrzeni podejmowanych przez Sandworm i może zostać powiązany z Sandworm.	