2025/887

13.5.2025

DECYZJA RADY (WPZiB) 2025/887

z dnia 12 maja 2025 r.

zmieniająca decyzję (WPZiB) 2019/797 w sprawie środków ograniczających w celu zwalczania cyberataków zagrażających Unii lub jej państwom członkowskim

RADA UNII EUROPEJSKIEJ,

uwzględniając Traktat o Unii Europejskiej, w szczególności jego art. 29,

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 decyzję (WPZiB) 2019/797 ([1]).

(2) Decyzję (WPZiB) 2019/797 stosuje się do dnia 18 maja 2025 r. Na podstawie przeglądu tej decyzji Rada uważa, że jej stosowanie należy przedłużyć do dnia 18 maja 2028 r.

(3) Na podstawie przeglądu załącznika do decyzji (WPZiB) 2019/797 należy przedłużyć do dnia 18 maja 2026 r. stosowanie środków określonych w art. 4 i 5 tej decyzji w odniesieniu do osób fizycznych i prawnych, podmiotów i organów wymienionych w tym załączniku. Ponadto należy zaktualizować powody umieszczenia sześciu osób w wykazie osób fizycznych i prawnych, podmiotów i organów objętych środkami ograniczającymi.

(4) Należy zatem odpowiednio zmienić decyzję (WPZiB) 2019/797,

PRZYJMUJE NINIEJSZĄ DECYZJĘ:

Artykuł 1

W decyzji (WPZiB) 2019/797 wprowadza się następujące zmiany:

1) art. 10 otrzymuje brzmienie:

„*Artykuł 10*

Niniejszą decyzję stosuje się do dnia 18 maja 2028 r. Jest ona poddawana stałemu przeglądowi. Środki określone w art. 4 i 5 stosuje się do osób fizycznych i prawnych, podmiotów i organów wymienionych w załączniku do dnia 18 maja 2026 r.";

2) w załączniku wprowadza się zmiany zgodnie z załącznikiem do niniejszej decyzji.

Artykuł 2

Niniejsza decyzja wchodzi w życie następnego dnia po jej opublikowaniu w *Dzienniku Urzędowym Unii Europejskiej*.

Sporządzono w Brukseli dnia 12 maja 2025 r.

W imieniu Rady

Przewodnicząca

B. NOWACKA

([1]) Decyzja Rady (WPZiB) 2019/797 z dnia 17 maja 2019 r. w sprawie środków ograniczających w celu zwalczania cyberataków zagrażających Unii lub jej państwom członkowskim (Dz.U. L 129 I z 17.5.2019, s. 13, ELI: http:/data.europa.eu/eli/dec/2019/797/oj).

ZAŁĄCZNIK

W załączniku do decyzji (WPZiB) 2019/797 pod nagłówkiem „A. Osoby fizyczne” pozycje 3 – 8 otrzymują następujące brzmienie:

	Imię i nazwisko	Dane identyfikacyjne	Powody	Data umieszczenia
„3.	Alexey Valeryevich MININ	Алексей Валерьевич МИНИН Data urodzenia: 27.5.1972 Miejsce urodzenia: obwód permski, rosyjska FSRR (obecnie Federacja Rosyjska) Nr paszportu: 120017582 wydany przez: Ministerstwo spraw zagranicznych Federacji Rosyjskiej Okres ważności: od 17 kwietnia 2017 r. do 17 kwietnia 2022 r. Miejsce: Moskwa, Federacja Rosyjska Obywatelstwo: rosyjskie Płeć: mężczyzna	Alexey Minin wziął udział w próbie cyberataku na Organizację ds. Zakazu Broni Chemicznej (OPCW) w Niderlandach, mogącego wywołać poważne skutki, oraz w cyberatakach na państwa trzecie, wywołujących 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 powiódł, zagroziłby bezpieczeństwu sieci i pracom dochodzeniowym prowadzonym przez OPCW. Wywiad Wojskowy i Służby Bezpieczeństwa Niderlandów (Militaire Inlichtingen- en Veiligheidsdienst) przerwały tę próbę cyberataku, uniemożliwiając w ten sposób wyrządzenie poważnej szkody OPCW. Alexey Minin jako oficer GRU został przez wielką ławę przysięgłych w Sądzie Okręgowym dla Okręgu Zachodniego w Pensylwanii (Stany Zjednoczone) uznany za winnego hakerstwa, internetowych oszustw finansowych, kwalifikowanej kradzieży tożsamości i prania pieniędzy. GRU nadal czynnie dokonuje cyberataków przeciwko Unii lub jej państwom członkowskim. Jako członek GRU Alexey Minin bierze zatem udział w cyberatakach wywołujących poważne skutki – w tym w usiłowaniu przeprowadzenia cyberataków mogących wywoływać poważne skutki – które to ataki stanowią zewnętrzne zagrożenie dla Unii lub jej państw członkowskich.	30.7.2020

	Imię i nazwisko	Dane identyfikacyjne	Powody	Data umieszczenia
4.	Aleksei Sergeyvich MORENETS	Алексей Сергеевич МОРЕНЕЦ Data urodzenia: 31.7.1977 Miejsce urodzenia: obwód murmański, rosyjska FSRR (obecnie Federacja Rosyjska) Nr paszportu: 100135556 wydany przez: Ministerstwo spraw zagranicznych Federacji Rosyjskiej Okres ważności: od 17 kwietnia 2017 r. do 17 kwietnia 2022 r. Miejsce: Moskwa, Federacja Rosyjska Obywatelstwo: rosyjskie Płeć: mężczyzna	Aleksei Morenets wziął udział w próbie cyberataku na Organizację ds. Zakazu Broni Chemicznej (OPCW) w Niderlandach, mogącego wywołać poważne skutki, oraz w cyberatakach na państwa trzecie, wywołujących 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 powiódł, zagroziłby bezpieczeństwu sieci i pracom dochodzeniowym prowadzonym przez OPCW. Wywiad Wojskowy i Służby Bezpieczeństwa Niderlandów (Militaire Inlichtingen- en Veiligheidsdienst) przerwały tę próbę cyberataku, uniemożliwiając w ten sposób wyrządzenie poważnej szkody OPCW. Aleksei Morenetes jako członek jednostki wojskowej 26165 został przez wielką ławę przysięgłych w Sądzie Okręgowym dla Okręgu Zachodniego w Pensylwanii (Stany Zjednoczone) uznany za winnego hakerstwa, internetowych oszustw finansowych, kwalifikowanej kradzieży tożsamości i prania pieniędzy. GRU nadal czynnie dokonuje cyberataków przeciwko Unii lub jej państwom członkowskim. Jako członek GRU Aleksei Morenets bierze zatem udział w cyberatakach wywołujących poważne skutki – w tym w usiłowaniu przeprowadzenia cyberataków mogących wywoływać poważne skutki – które to ataki stanowią zewnętrzne zagrożenie dla Unii lub jej państw członkowskich.	30.7.2020

	Imię i nazwisko	Dane identyfikacyjne	Powody	Data umieszczenia
5.	Evgenii Mikhaylovich SEREBRIAKOV	Евгений Михайлович СЕРЕБРЯКОВ Data urodzenia: 26.7.1981 Miejsce urodzenia: Kursk, rosyjska FSRR (obecnie Federacja Rosyjska) Nr paszportu: 100135555 wydany przez: Ministerstwo spraw zagranicznych Federacji Rosyjskiej Okres ważności: od 17 kwietnia 2017 r. do 17 kwietnia 2022 r. Miejsce: Moskwa, Federacja Rosyjska Obywatelstwo: rosyjskie Płeć: mężczyzna	Evgenii Serebriakov wziął udział w próbie cyberataku na Organizację ds. Zakazu Broni Chemicznej (OPCW) w Niderlandach, który mógł wywołać poważne skutki, oraz w cyberatakach na państwa trzecie o poważnych skutkach. 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 powiódł, zagroziłby bezpieczeństwu sieci i pracom dochodzeniowym prowadzonym przez OPCW. Wywiad Wojskowy i Służby Bezpieczeństwa Niderlandów (Militaire Inlichtingen- en Veiligheidsdienst) przerwały tę próbę cyberataku, uniemożliwiając w ten sposób wyrządzenie poważnej szkody OPCW. Od wiosny 2022 r. Evgenii Serebriakov stoi na czele zajmującej się wojną cybernetyczną grupy hakerów »Sandworm« (inne nazwy: »Sandworm Team«, »BlackEnergy Group«, »Voodoo Bear«, »Quedagh«, »Olympic Destroyer« i »Telebots«) powiązanej z jednostką 74455 rosyjskiego Głównego Zarządu Wywiadowczego. Sandworm przeprowadziła cyberataki na Ukrainę, w tym ukraińskie agencje rządowe, w związku z rosyjską wojną napastniczą przeciwko Ukrainie. GRU nadal czynnie dokonuje cyberataków przeciwko Unii lub jej państwom członkowskim. Jako członek GRU Evgenii Serebriakov bierze zatem udział w cyberatakach wywołujących poważne skutki – w tym w usiłowaniu przeprowadzenia cyberataków mogących wywoływać poważne skutki – które to ataki stanowią zewnętrzne zagrożenie dla Unii lub jej państw członkowskich.	30.7.2020

	Imię i nazwisko	Dane identyfikacyjne	Powody	Data umieszczenia
6.	Oleg Mikhaylovich SOTNIKOV	Олег Михайлович СОТНИКОВ Data urodzenia: 24.8.1972 Miejsce urodzenia: Uljanowsk, rosyjska FSRR (obecnie Federacja Rosyjska) Nr paszportu: 120018866 wydany przez: Ministerstwo spraw zagranicznych Federacji Rosyjskiej Okres ważności: od 17 kwietnia 2017 r. do 17 kwietnia 2022 r. Miejsce: Moskwa, Federacja Rosyjska Obywatelstwo: rosyjskie Płeć: mężczyzna	Oleg Sotnikov wziął udział w próbie cyberataku na Organizację ds. Zakazu Broni Chemicznej (OPCW) w Niderlandach, mogącego wywołać poważne skutki, oraz w cyberatakach na państwa trzecie, wywołujących 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 Wi-Fi OPCW; gdyby atak ten się powiódł, zagroziłby bezpieczeństwu sieci i pracom dochodzeniowym prowadzonym przez OPCW. Wywiad Wojskowy i Służby Bezpieczeństwa Niderlandów (Militaire Inlichtingen- en Veiligheidsdienst) przerwały tę próbę cyberataku, uniemożliwiając w ten sposób wyrządzenie poważnej szkody OPCW. Oleg Sotnikov jako oficer GRU został przez wielką ławę przysięgłych w Sądzie Okręgowym dla Okręgu Zachodniego w Pensylwanii (Stany Zjednoczone Ameryki) uznany za winnego hakerstwa, internetowych oszustw finansowych, kwalifikowanej kradzieży tożsamości i prania pieniędzy. GRU nadal czynnie dokonuje cyberataków przeciwko Unii lub jej państwom członkowskim. Jako członek GRU Oleg Sotnikov bierze zatem udział w cyberatakach wywołujących poważne skutki – w tym w usiłowaniu przeprowadzenia cyberataków mogących wywoływać poważne skutki – które to ataki stanowią zewnętrzne zagrożenie dla Unii lub jej państw członkowskich.	30.7.2020

	Imię i nazwisko	Dane identyfikacyjne	Powody	Data umieszczenia
7.	Dmitry Sergeyevich BADIN	Дмитрий Сергеевич БАДИН Data urodzenia: 15.11.1990 Miejsce urodzenia: Kursk, rosyjska FSRR (obecnie Federacja Rosyjska) Obywatelstwo: rosyjskie Płeć: mężczyzna	Dmitry Badin wziął udział w cyberataku, wywołującym poważne skutki, wymierzonym w niemiecki parlament federalny (Deutscher Bundestag) oraz w cyberatakach na państwa trzecie, wywołujących poważne skutki. Dmitry Badin, jako oficer wywiadu wojskowego 85. Głównego Ośrodka Służb Specjalnych (GTsSS) Głównego Zarządu Sztabu Generalnego Sił Zbrojnych Federacji Rosyjskiej (GU GRU), był członkiem zespołu rosyjskich oficerów wywiadu wojskowego, którzy przeprowadzili w kwietniu i maju 2015 r. cyberatak wymierzony w niemiecki parlament federalny. Celem tego cyberataku był system informacyjny parlamentu; atak ten miał wpływ na funkcjonowanie tej instytucji przez kilka dni. Skradziono dużą ilość danych; atak ten obejmował także konta poczty elektronicznej kilkorga parlamentarzystów, w tym byłej kanclerz Angeli Merkel. Dmitry Badin jako członek jednostki wojskowej 26165 został przez wielką ławę przysięgłych w Sądzie Okręgowym dla Okręgu Zachodniego w Pensylwanii (Stany Zjednoczone) uznany za winnego hakerstwa, internetowych oszustw finansowych, kwalifikowanej kradzieży tożsamości i prania pieniędzy. GRU nadal czynnie dokonuje cyberataków przeciwko Unii lub jej państwom członkowskim. Jako członek GRU Dmitry Badin bierze zatem udział w cyberatakach wywołujących poważne skutki – w tym w usiłowaniu przeprowadzenia cyberataków mogących wywoływać poważne skutki – które to ataki stanowią zewnętrzne zagrożenie dla Unii lub jej państw członkowskich.	22.10.2020

	Imię i nazwisko	Dane identyfikacyjne	Powody	Data umieszczenia
8.	Igor Olegovich KOSTYUKOV	Игорь Олегович КОСТЮКОВ Data urodzenia: 21.2.1961 Obywatelstwo: rosyjskie Płeć: mężczyzna	Igor Kostyukow jest obecnie szefem Głównego Zarządu Sztabu Generalnego Sił Zbrojnych Federacji Rosyjskiej (GU GRU), gdzie poprzednio sprawował funkcję pierwszego zastępcy szefa. Jednym z oddziałów pod jego dowództwem jest 85. Główny Ośrodek Służb Specjalnych (GTsSS) (alias »jednostka wojskowa 26165«, »APT28«, »Fancy Bear«, »Sofacy Group«, »Pawn Storm« i »Strontium«). Pełniąc tę funkcję, Igor Kostyukow jest odpowiedzialny za cyberataki przeprowadzone przez GTsSS, w tym cyberataki o poważnych skutkach stanowiące zewnętrzne zagrożenie dla Unii lub jej państw członkowskich. W szczególności oficerowie wywiadu wojskowego GTsSS brali udział w cyberataku wymierzonym w niemiecki parlament federalny (Deutscher Bundestag) w kwietniu i maju 2015 r. oraz w próbie cyberataku, którego celem było włamanie do sieci Wi-Fi Organizacji ds. Zakazu Broni Chemicznej (OPCW) w Niderlandach w kwietniu 2018 r. Celem cyberataku wymierzonego w niemiecki parlament federalny był system informacyjny parlamentu; atak ten miał wpływ na funkcjonowanie tej instytucji przez kilka dni. Skradziono dużą ilość danych; atak ten obejmował także konta poczty elektronicznej kilkorga parlamentarzystów, w tym byłej kanclerz Angeli Merkel. GRU nadal czynnie dokonuje cyberataków przeciwko Unii lub jej państwom członkowskim. Jako członek GRU Igor Kostyukov bierze zatem udział w cyberatakach wywołujących poważne skutki – w tym w usiłowaniu przeprowadzenia cyberataków mogących wywoływać poważne skutki – które to ataki stanowią zewnętrzne zagrożenie dla Unii lub jej państw członkowskich.	22.10.2020”