2025/173

27.1.2025

ROZPORZĄDZENIE WYKONAWCZE RADY (UE) 2025/173

z dnia 27 stycznia 2025 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]), 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 i stanowiących zewnętrzne zagrożenie dla Unii lub jej państw członkowskich, należą do środków przewidzianych w unijnych ramach wspólnej reakcji dyplomatycznej na szkodliwe działania w cyberprzestrzeni, to jest do zestawu narzędzi dla dyplomacji cyfrowej, i są jednym z niezbędnych instrumentów zapobiegania takim działaniom, powstrzymywania ich, zniechęcania do nich i reagowania na nie.

(3) Rośnie liczba, częstotliwość i stopień wyrafinowania szkodliwych działań w cyberprzestrzeni skierowanych przeciwko infrastrukturze krytycznej lub usługom kluczowym, prowadzonych m.in. za pomocą oprogramowania szantażującego i oprogramowania niszczącego dane (wiperware), obejmujących też ataki wymierzone w łańcuchy dostaw i akty cyberszpiegostwa, w tym kradzieży własności intelektualnej. Ze względu na swój zakłócający i destrukcyjny wpływ działania te stanowią systemowe zagrożenie dla bezpieczeństwa, gospodarki i demokracji oraz całego społeczeństwa Unii.

(4) W 2020 r. dokonano cyberataków przeciwko Estonii, które wywołały poważne skutki. Przeprowadzono cyberataki przeciwko systemom komputerowym wielu instytucji, których celem było wykorzystanie danych do stworzenia zagrożenia dla bezpieczeństwa Estonii. Dotyczyły one przechowywania informacji niejawnych.

(5) W ramach konsekwentnych, ukierunkowanych i skoordynowanych działań Unii przeciwko podmiotom stale powodującym zagrożenia w cyberprzestrzeni w wykazie osób fizycznych i prawnych, podmiotów i organów podlegających środkom ograniczającym zawartym w załączniku I do rozporządzenia (UE) 2019/796 należy zamieścić trzy osoby fizyczne. Osoby te są odpowiedzialne za cyberataki lub były zaangażowane w cyberataki wywołujące poważne skutki i stanowiące zewnętrzne zagrożenie dla Unii lub jej państw członkowskich.

(6) Należy zatem odpowiednio zmienić załącznik I do rozporządzenia (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.

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 Brukseli dnia 27 stycznia 2025 r.

W imieniu Rady
Przewodnicząca
K. KALLAS

([1]) Dz.U. L 129 I z 17.5.2019, s. 1, ELI: http://data.europa.eu/eli/reg/2019/796/oj.

ZAŁĄCZNIK

W załączniku I do rozporządzenia (UE) 2019/796 w części A. „Osoby fizyczne” dodaje się wpisy w brzmieniu:

	Nazwisko i imię	Dane identyfikacyjne	Powody	Data umieszczenia
„15.	Nikolay Alexandrovich KORCHAGIN	Николай Александрович Корчагин Data urodzenia: 16.9.1997 Obywatelstwo: rosyjskie Płeć: mężczyzna Powiązany podmiot: Główny Zarząd Sztabu Generalnego Sił Zbrojnych Federacji Rosyjskiej	Poprzez prowadzenie działań wywiadowczych skierowanych przeciwko Estonii i uzyskanie nieuprawnionego dostępu do systemu komputerowego Nikolay Korchagin był zaangażowany w cyberataki wywołujące poważne skutki i jest za te ataki odpowiedzialny. Nikolay Korchagin jest oficerem w jednostce wojskowej 29155 w Głównym Zarządzie Sztabu Generalnego Sił Zbrojnych Federacji Rosyjskiej (GRU). Pełniąc tę funkcję, był zaangażowany w cyberataki i odpowiedzialny za cyberataki skierowane przeciwko systemom komputerowym w celu pozyskania danych z systemów danych wielu instytucji, które to dane, pojedynczo lub zbiorczo, pozwalały uzyskać ogląd polityki cyberbezpieczeństwa Estonii, zdolności cyfrowych państwa, wrażliwych danych osobowych i innych danych wrażliwych; celem tych ataków było wykorzystywanie danych do stworzenia zagrożenia dla bezpieczeństwa Estonii. Ataki te dotyczą zatem przechowywania informacji niejawnych. Ataki te dotyczyły sojuszników i partnerów Estonii. Nikolay Korchagin był zatem zaangażowany w cyberataki wywołujące poważne skutki, stanowiące zewnętrzne zagrożenie dla państwa członkowskiego i jest odpowiedzialny za te cyberataki.	27.1.2025
16.	Vitaly SHEVCHENKO	Виталий Шевченко Data urodzenia: 1.9.1997 Obywatelstwo: rosyjskie Płeć: mężczyzna Powiązany podmiot: Główny Zarząd Sztabu Generalnego Sił Zbrojnych Federacji Rosyjskiej	Poprzez prowadzenie działań wywiadowczych skierowanych przeciwko Estonii i uzyskanie nieuprawnionego dostępu do systemu komputerowego Vitaly Shevchenko był zaangażowany w cyberataki wywołujące poważne skutki i jest za te ataki odpowiedzialny. Vitaly Shevchenko jest oficerem w jednostce wojskowej 29155 w Głównym Zarządzie Sztabu Generalnego Sił Zbrojnych Federacji Rosyjskiej (GRU). Pełniąc tę funkcję, był zaangażowany w cyberataki i odpowiedzialny za cyberataki skierowane przeciwko systemom komputerowym w celu pozyskania danych z systemów danych wielu instytucji, które to dane, pojedynczo lub zbiorczo, pozwalały uzyskać ogląd polityki cyberbezpieczeństwa Estonii, zdolności cyfrowych państwa, wrażliwych danych osobowych i innych danych wrażliwych; celem tych ataków było wykorzystywanie danych do stworzenia zagrożenia dla bezpieczeństwa Estonii. Ataki te dotyczą zatem przechowywania informacji niejawnych. Ataki te dotyczyły sojuszników i partnerów Estonii. Vitaly Shevchenko był zatem zaangażowany w cyberataki wywołujące poważne skutki, stanowiące zewnętrzne zagrożenie dla państwa członkowskiego i jest odpowiedzialny za te cyberataki.	27.1.2025

ELI: http://data.europa.eu/eli/reg_impl/2025/173/oj

	Nazwisko i imię	Dane identyfikacyjne	Powody	Data umieszczenia
17.	Yuriy Fedorovich DENISOV	Юрий Федорович Денисов Data urodzenia: 17.6.1980 Obywatelstwo: rosyjskie Płeć: mężczyzna Powiązany podmiot: Główny Zarząd Sztabu Generalnego Sił Zbrojnych Federacji Rosyjskiej	Poprzez prowadzenie działań wywiadowczych skierowanych przeciwko Estonii i uzyskanie nieuprawnionego dostępu do systemu komputerowego Yuriy Denisov był zaangażowany w cyberataki wywołujące poważne skutki i jest za te ataki odpowiedzialny. Yuriy Denisov jest oficerem w jednostce wojskowej 29155 w Głównym Zarządzie Sztabu Generalnego Sił Zbrojnych Federacji Rosyjskiej (GRU). Pełniąc tę funkcję, był zaangażowany w cyberataki i odpowiedzialny za cyberataki skierowane przeciwko systemom komputerowym w celu pozyskania danych z systemów danych wielu instytucji, które to dane, pojedynczo lub zbiorczo, pozwalały uzyskać ogląd polityki cyberbezpieczeństwa Estonii, zdolności cyfrowych państwa, wrażliwych danych osobowych i innych danych wrażliwych; celem tych ataków było wykorzystywanie danych do stworzenia zagrożenia dla bezpieczeństwa Estonii. Ataki te dotyczą zatem przechowywania informacji niejawnych. Ataki te dotyczyły sojuszników i partnerów Estonii. Yuriy Denisov był zatem zaangażowany w cyberataki wywołujące poważne skutki, stanowiące zewnętrzne zagrożenie dla państwa członkowskiego i jest odpowiedzialny za te cyberataki.	27.1.2025”