



2026/1713

13.7.2026

DECYZJA RADY (WPZiB) 2026/1713

z dnia 13 lipca 2026 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) W ramach konsekwentnych, ukierunkowanych i skoordynowanych działań Unii przeciwko podmiotom stale powodującym zagrożenia cyberbezpieczeństwa, do wykazu osób fizycznych i prawnych, podmiotów i organów podlegających środkom ograniczającym zawartego w załączniku do decyzji (WPZiB) 2019/797 należy dodać osiem osób fizycznych i cztery podmioty. Te osoby i podmioty są odpowiedzialne za cyberataki wywołujące poważne skutki, które stanowią zewnętrzne zagrożenie dla Unii lub jej państw członkowskich, wspierają takie ataki lub są w nie zaangażowane.
- (3) Należy zatem odpowiednio zmienić decyzję (WPZiB) 2019/797,

PRZYJMUJE NINIEJSZĄ DECYZJĘ:

Artykuł 1

W załączniku do decyzji (WPZiB) 2019/797 wprowadza się zmiany zgodnie z załącznikiem do niniejszej decyzji.

Artykuł 2

Niniejsza decyzja wchodzi w życie z dniem jej opublikowania w *Dzienniku Urzędowym Unii Europejskiej*.

Sporządzono w Brukseli dnia 13 lipca 2026 r.

W imieniu Rady

Przewodnicząca

K. KALLAS

⁽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 wprowadza się następujące zmiany:

1) w części „A. Osoby fizyczne” dodaje się wpisy w brzmieniu:

	Nazwisko i imię	Dane identyfikacyjne	Powody	Data umieszczenia
„20.	Vitaly Nikolayevich KOVALE	Виталий Николаевич КОВАЛЕВ Alias: »Bentley«, »Bergen«, »Alex Konor«, »Benny«, »Benen«, »Stern« Data urodzenia: 23.6.1988 Adres: Serebristy Bulvar 34 (Serebristyy Bul'var); krp 1; flt 528; 197341; St Petersburg, Russian Federation Obywatelstwo: rosyjskie Płeć: mężczyzna Powiązane podmioty: TrickBot, Wizard Spider, Conti	Vitaly Kovalev jest prominentną postacią związaną ze złośliwym oprogramowaniem »TrickBbot« i »Conti«. Znany jest również pod internetowymi pseudonimami »Bentley«, »Bergen«, »Alex Konor«, »Benny«, »Benen« i »Stern«. Złośliwe oprogramowanie Conti i Trickbot zostało pierwotnie stworzone i opracowane przez Wizard Spider. Wizard Spider prowadziła kampanie z użyciem oprogramowania szantażującego w różnych sektorach, w tym usług kluczowych, takich jak opieka zdrowotna i bankowość; infekowała komputery na całym świecie, a jej złośliwe oprogramowanie zostało przekształcone w modułowy pakiet złośliwego oprogramowania. Kampanie Wizard Spider wykorzystujące złośliwe oprogramowanie, takie jak Conti i TrickBot, powodują znaczne szkody gospodarcze w Unii Europejskiej. Vitaly Kovalev jest zatem odpowiedzialny za cyberataki wywołujące poważne skutki, które stanowią zewnętrzne zagrożenie dla Unii lub jej państw członkowskich oraz jest zaangażowany w te cyberataki.	13.7.2026

	Nazwisko i imię	Dane identyfikacyjne	Powody	Data umieszczenia
21.	Alexander Alexandrovich VOLOSOVIK	Александр Александрович ВОЛОСОВИК Data urodzenia: 30.1.1983 Miejsce urodzenia: ZSRR Obywatelstwo: rosyjskie Nr paszportu: 762988138 Płeć: mężczyzna Powiązane podmioty: Yalishanda, LARVA-34, podzemniyl, Ohyeahhellno, Stas_vl, downlow	Alexander Volosovik jest właścicielem Media Land LLC. Od 2016 r. Media Land LLC świadcząca usługi tzw. bulletproof hostingu ułatwiła realizację szeregu ataków z wykorzystaniem złośliwego oprogramowania zarówno przeciwko Unii, jak i na całym świecie, oferując usługi hostingowe, które ukrywają tożsamość użytkowników i są odporne na próby ich usunięcia przez organy ścigania. Media Land LLC umożliwiła wielkoskalowe operacje z użyciem oprogramowania szantażującego, świadczenie usług dowodzenia i kontroli oraz realizację operacji phishingowych wymierzonych w infrastrukturę krytyczną i usługi kluczowe w państwach członkowskich, co doprowadziło do znacznych strat finansowych. Media Land LLC ułatwiła między innymi przeprowadzenie operacji LockBit, EvilCorp i BlackBasta. Media Land LLC jest zatem zaangażowana w cyberataki wywołujące poważne skutki, które stanowią zewnętrzne zagrożenie dla Unii lub jej państw członkowskich. Alexander Volosovik, jako właściciel Media Land LLC, jest odpowiedzialny za te cyberataki i jest w nie zaangażowany. Jest on również powiązany z Media Land LLC.	13.7.2026

	Nazwisko i imię	Dane identyfikacyjne	Powody	Data umieszczenia
22.	Denis Olegovich DEGTYARENKO	Денис Олегович ДЕГТЯРЕНКО Alias: »Dena« Data urodzenia: 9.10.1989 Miejsce urodzenia: ZSRR Obywatelstwo: rosyjskie Płeć: mężczyzna Adres: 130 Lenina Avenue, Novy Gorod microdistrict, Orsk, Orenburg Region, Russian Federation	Denis Degtyarenko, alias Dena, jest rosyjskim hakerem grupy CARR [ang. Cyber Army of Russia Reborn (Cyberarmia Rosji Odrodzonej)]. CARR odpowiada za cyberataki na usługi niezbędne do utrzymania podstawowej działalności gospodarczej i krytycznych funkcji państwa w państwach członkowskich, a także na infrastrukturę w Ukrainie i innych państwach trzecich. CARR jest powiązany z Głównym Ośrodkiem Specjalnych Technologii (GTsST) w ramach Głównego Zarządu Sztabu Generalnego Sił Zbrojnych Federacji Rosyjskiej (GRU). GTsST nadal czynnie dokonuje cyberataków przeciwko Unii lub jej państwom członkowskim. Cele CARR obejmują agencje rządowe, instytucje finansowe, media i infrastrukturę krytyczną w państwach członkowskich i Stanach Zjednoczonych. CARR przeprowadziła rozproszone ataki typu »odmowa usługi« (DDoS) w Ukrainie oraz przeciwko rządowi i przedsiębiorstwom zlokalizowanym w krajach, które wspierają Ukrainę. Denis Degtyarenko, jeden z głównych hakerów CARR, jest zatem zaangażowany w cyberataki wywołujące poważne skutki, w tym w próby przeprowadzenia cyberataków wywołujących potencjalnie poważne skutki, które to ataki stanowią zewnętrzne zagrożenie dla państw członkowskich, a także w cyberataki wymierzone przeciwko państwom trzecim. Jako członek CARR jest również powiązany z GTsST.	13.7.2026

	Nazwisko i imię	Dane identyfikacyjne	Powody	Data umieszczenia
23.	Yuliya Vladimirovna PANKRATOVA	Юлия Владимировна ПАНКРАТОВА Alias: »YULiYA« Data urodzenia: 6.4.1984 Miejsce urodzenia: ZSRR Obywatelstwo: rosyjskie Płeć: kobieta Adres: 130 Lenina Avenue, Novy Gorod microdistrict, Orsk, Orenburg Region, Russian Federation	Yuliya Pankratova to rosyjska hakerka, która pracowała dla CARR [ang. Cyber Army of Russia Reborn (Cyberarmia Rosji Odrodzonej)] i założyła Z-Pentest, dla którego nadal pracuje. CARR odpowiada za cyberataki na usługi niezbędne do utrzymania podstawowej działalności gospodarczej i krytycznych funkcji państwa w państwach członkowskich, a także na infrastrukturę w Ukrainie i innych państwach trzecich. CARR jest powiązany z Głównym Ośrodkiem Specjalnych Technologii (GTsST) w ramach Głównego Zarządu Sztabu Generalnego Sił Zbrojnych Federacji Rosyjskiej (GRU). GTsST nadal czynnie dokonuje cyberataków przeciwko Unii lub jej państwom członkowskim. Cele CARR obejmują agencje rządowe, instytucje finansowe, media i infrastrukturę krytyczną w państwach członkowskich i Stanach Zjednoczonych. CARR przeprowadziła rozproszone ataki typu »odmowa usługi« (DDoS) w Ukrainie oraz przeciwko rządowi i przedsiębiorstwom zlokalizowanym w krajach, które wspierają Ukrainę. Z-Pentest odpowiada za cyberataki wywołujące poważne skutki, wymierzone m. in. w usługi niezbędne do utrzymania podstawowej działalności w państwach członkowskich. Yuliya Pankratova, jedna z głównych hakerek CARR i Z-Pentest, jest zatem zaangażowana w cyberataki wywołujące poważne skutki, w tym w próby przeprowadzenia cyberataków wywołujących potencjalnie poważne skutki, które to ataki stanowią zewnętrzne zagrożenie dla państw członkowskich, a także w cyberataki wymierzone przeciwko państwom trzecim. Jest ona również powiązana z Z-Pentest.	13.7.2026

	Nazwisko i imię	Dane identyfikacyjne	Powody	Data umieszczenia
24.	Maksim Evgenevich VORONIN	Максим Евгеньевич ВОРОНИН Alias: »Daugn0« Obywatelstwo: rosyjskie (rzekomo) Płeć: mężczyzna	Maksim Voronin, alias Daugn0, jest zaangażowany w opracowywanie, dystrybucję i sprzedaż złośliwego oprogramowania do kradzieży informacji LummaC2 (inne nazwy: Lumma infostealer, Lumma Stealer). LummaC2 to platforma złośliwego oprogramowania oferowanego w formie subskrypcji (Malware-as-a-Service), wykorzystywana do kradzieży danych wrażliwych, danych logowania z przeglądarek, portfeli kryptowalutowych lub informacji systemowych, do umieszczania dodatkowego złośliwego oprogramowania na zainfekowanych urządzeniach, do kradzieży kryptowalut i realizacji kampanii szpiegowskich. Cyberataki z użyciem złośliwego oprogramowania LummaC2 są również wykorzystywane przez dążące do korzyści finansowych podmioty odpowiedzialne za cyberataki, takie jak Storm-113, Storm-1607, Storm-1674, Octo Tempest itp. Złośliwe oprogramowanie LummaC2 zostało użyte do cyberataków na krytyczne funkcje państwa i usługi niezbędne do utrzymania podstawowej działalności społecznej i gospodarczej państw członkowskich. W latach 2024 i 2025 LummaC2 było jednym z najpopularniejszych narzędzi do kradzieży informacji na całym świecie. Maksim Voronin jako twórca, dystrybutor i sprzedawca LummaC2 jest zatem zaangażowany w cyberataki wywołujące poważne skutki, które stanowią zewnętrzne zagrożenie dla państw członkowskich, oraz ułatwia przeprowadzanie takich ataków.	13.7.2026

	Nazwisko i imię	Dane identyfikacyjne	Powody	Data umieszczenia
25.	Maksim Aleksandrovich GORDIENKO Alias: Maxim Alexandrovich GORDIENKO	Максим Александрович ГОРДИЕНКО Alias: »Lummaseller« Obywatelstwo: rosyjskie (rzekomo) Płeć: mężczyzna	Maksim Gordienko, alias Lummaseller, jest zaangażowany w opracowywanie i dystrybucję złośliwego oprogramowania do kradzieży informacji LummaC2 (inne nazwy: Lumma Infostealer, Lumma Stealer). LummaC2 to platforma złośliwego oprogramowania oferowanego w formie subskrypcji (Malware-as-a-Service), wykorzystywana do kradzieży danych wrażliwych, danych logowania z przeglądarek, portfeli kryptowalutowych lub informacji systemowych, do umieszczania dodatkowego złośliwego oprogramowania na zainfekowanych urządzeniach, do kradzieży kryptowalut i realizacji kampanii szpiegowskich. Cyberataki z użyciem złośliwego oprogramowania LummaC2 są również wykorzystywane przez dążące do korzyści finansowych podmioty odpowiedzialne za cyberataki, takie jak Storm-113, Storm-1607, Storm-1674, Octo Tempest itp. Złośliwe oprogramowanie LummaC2 zostało użyte do cyberataków na krytyczne funkcje państwa i usługi niezbędne do utrzymania podstawowej działalności społecznej i gospodarczej państw członkowskich. W latach 2024 i 2025 LummaC2 było jednym z najpopularniejszych narzędzi do kradzieży informacji na całym świecie. Maksim Gordienko jako twórca, dystrybutor i sprzedawca LummaC2 jest zatem zaangażowany w cyberataki wywołujące poważne skutki, które stanowią zewnętrzne zagrożenie dla państw członkowskich, oraz ułatwia przeprowadzanie takich ataków.	13.7.2026

	Nazwisko i imię	Dane identyfikacyjne	Powody	Data umieszczenia
26.	Evgeniy Viktorovich BASHEV	Евгений Викторович БАШЕВ Data urodzenia: 25.1.1980 Miejsce urodzenia: ZSRR Obywatelstwo: rosyjskie Płeć: męczyzna Powiązane osoby: Denis Igorevich Denisenko, Yuriy Fedorovich Denisov, Dmitriy Yuryevich Goloshubov, Nikolay Alexandrovich Korchagin Powiązane podmioty: jednostka GRU nr 29155, »Impuls« LLC	Evgeniy Bashev jest członkiem jednostki nr 29155 rosyjskiej agencji wywiadu wojskowego (GRU). W ramach tej jednostki wspiera i ułatwia – między innymi poprzez kontrolowanie serwera »Aegon«, wykorzystywanego do operacji hakerskich – cyberataki wywołujące poważne skutki dla państw członkowskich. W szczególności zapewnia wsparcie techniczne i materialne na potrzeby cyberataków przeprowadzanych przez jednostkę GRU nr 29155 za pośrednictwem swojego przedsiębiorstwa »Impuls« LLC, które udostępniało ochronę operacyjną, infrastrukturę, umożliwiało płatności oraz zarządzało aktywami technicznymi, w tym serwerami, wykorzystywanymi do cyberataków. Evgeniy Bashev koordynował również współpracę między strukturami GRU a zewnętrznymi sieciami hakerów. Umożliwione przez niego cyberataki były wymierzone przeciwko systemom związanym z krytycznymi funkcjami państwa i usługom niezbędnym do utrzymania podstawowej działalności społecznej lub gospodarczej w państwach członkowskich, zwłaszcza w sektorze transportu. Za pośrednictwem kampanii WhisperGate jednostka GRU nr 29155 prowadziła też ataki wymierzone w infrastrukturę krytyczną Ukrainy. Evgeniy Bashev udziela zatem wsparcia technicznego i materialnego na potrzeby cyberataków wywołujących poważne skutki, w tym prób przeprowadzenia cyberataków wywołujących potencjalnie poważne skutki, które to ataki stanowią zewnętrzne zagrożenie dla państw członkowskich, a także na potrzeby cyberataków wywołujących poważne skutki dla państwa trzeciego, lub jest zaangażowany w inny sposób w takie cyberataki lub próby ich przeprowadzenia. Jako właściciel i dyrektor generalny jest powiązany z przedsiębiorstwem »Impulse« LLC. Jako członek jednostki GRU nr 29155 jest on również powiązany z tą jednostką.	13.7.2026

	Nazwisko i imię	Dane identyfikacyjne	Powody	Data umieszczenia
27.	Roman Alexandrovich PUNTUS	Роман Александрович ПУНТУС Miejsce urodzenia: Federacja Rosyjska Obywatelstwo: rosyjskie Płeć: męczyzna Powiązane osoby: Denis Igorevich Denisenko, Yuriy Fedorovich Denisov, Dmitriy Yuryevich Goloshubov, Nikolay Alexandrovich Korchagin, Evgeniy Viktorovich Bashev Powiązane podmioty: jednostka GRU nr 29155	Roman Puntus jest członkiem jednostki nr 29155 rosyjskiej agencji wywiadu wojskowego (GRU). W tej jednostce odgrywa wiodącą rolę w organizowaniu i koordynowaniu cyberataków wywołujących poważne skutki dla państw członkowskich. Wspiera również rozwój wewnętrznych cyberzdolności tej jednostki, w tym rekrutację i nadzorowanie pracowników, takich jak hakerzy i programiści. Założył przedsiębiorstwo fasadowe »Aegeon-Impulse«, dzięki któremu ułatwiał logistyczne i finansowe aspekty cyberoperacji. Koordynował prowadzone przez przedmiotową jednostkę GRU cyberataki skierowane przeciwko systemom związanym z krytycznymi funkcjami państwa i usługom niezbędnym do utrzymania podstawowej działalności społecznej lub gospodarczej w państwach członkowskich, zwłaszcza w sektorze transportu. Za pośrednictwem kampanii WhisperGate jednostka GRU nr 29155 prowadziła też ataki wymierzone w infrastrukturę krytyczną Ukrainy. Roman Puntus jest zatem odpowiedzialny za cyberataki wywołujące poważne skutki, w tym próby przeprowadzenia cyberataków wywołujących potencjalnie poważne skutki, które to ataki stanowią zewnętrzne zagrożenie dla państw członkowskich, a także za cyberataki wywołujące poważne skutki dla państwa trzeciego, lub jest zaangażowany w inny sposób w takie cyberataki lub próby ich przeprowadzenia. Jako członek jednostki GRU nr 29155 jest on również powiązany z tą jednostką.	13.7.2026”

2) nagłówkiem części „B. Osoby prawne, podmioty i organy” dodaje się wpisy w brzmieniu:

	Nazwa	Dane identyfikacyjne	Powody	Data umieszczenia
„8.	Media Land LLC	Adres: Tsvetnochnaya st., 16 Litera P, Room 27 Moskovskaya Zastava Municipal District St Petersburg, 196006, Russian Federation Rodzaj podmiotu: spółka z ograniczoną odpowiedzialnością Miejsce rejestracji: Sankt Petersburg Data wpisu do rejestru: 19.10.2015 Numer w rejestrze: 1152536009900 Główne miejsce prowadzenia działalności: Sankt Petersburg, Federacja Rosyjska Powiązany podmiot: ML.Cloud	Od 2016 r. Media Land LLC świadcząca usługi tzw. bulletproof hostingu ułatwiła realizację szeregu ataków z wykorzystaniem złośliwego oprogramowania przeciwko państwom członkowskim i na całym świecie, oferując usługi hostingowe, które ukrywają tożsamość użytkowników i są odporne na próby ich usunięcia przez organy ścigania, co prowadzi do znaczących strat finansowych. Media Land LLC umożliwiła wielkoskalowe operacje z użyciem oprogramowania szantażującego, świadczenie usług dowodzenia i kontroli oraz realizację operacji phishingowych wymierzonych w infrastrukturę krytyczną i usługi kluczowe w państwach członkowskich. Media Land LLC ułatwiła między innymi przeprowadzenie operacji LockBit, EvilCorp i BlackBasta. Media Land LLC jest zatem zaangażowana w cyberataki wywołujące poważne skutki, które stanowią zewnętrzne zagrożenie dla państw członkowskich.	13.7.2026

	Nazwa	Dane identyfikacyjne	Powody	Data umieszczenia
9.	ML.Cloud	Adres: Brivibas iela 52, Riga, LV-1011, Latvija; Russian Federation, Kazan, Peterburgskaya st. 52 Miejsce rejestracji: Ryga Powiązane osoby: Alexander Volosovik Inne powiązane podmioty: Media Land LLC	ML.Cloud jest spółką siostrzaną Media Land LLC i zapewnia infrastrukturę techniczną dla Media Land LLC. Od 2016 r. Media Land LLC świadcząca usługi tzw. bulletproof hostingu ułatwiła realizację szeregu ataków z wykorzystaniem złośliwego oprogramowania przeciwko państwom członkowskim i na całym świecie, oferując usługi hostingowe, które ukrywają tożsamość użytkowników i są odporne na próby ich usunięcia przez organy ścigania, co prowadzi do znaczących strat finansowych. Media Land LLC umożliwiła wielkoskalowe operacje z użyciem oprogramowania szantażującego, świadczenie usług dowodzenia i kontroli oraz realizację operacji phishingowych wymierzonych w infrastrukturę krytyczną i usługi kluczowe w państwach członkowskich. Media Land LLC ułatwiła między innymi przeprowadzenie operacji LockBit, EvilCorp i BlackBasta. Media Land LLC jest zatem zaangażowana w cyberataki wywołujące poważne skutki, które stanowią zewnętrzne zagrożenie dla państw członkowskich. ML.Cloud udziela zatem wsparcia technicznego na potrzeby cyberataków wywołujących poważne skutki, które stanowią zewnętrzne zagrożenie dla państw członkowskich.	13.7.2026

	Nazwa	Dane identyfikacyjne	Powody	Data umieszczenia
10.	»Impuls« LLC	Общество с ограниченной ответственностью «Импульс» Adres: 344015, Russian Federation, Rostov Region, Rostov-on-Don, ul. Eremenko, d. 56, k. 6, apt. 88 Rodzaj podmiotu: spółka z ograniczoną odpowiedzialnością Miejsce rejestracji: Interdistrict Inspectorate of the Federal Tax Service No. 26 for the Rostov Region, 344019, Rostov-on-Don, ul. Myasnikova, d. 52/32, Russian Federation Data wpisu do rejestru: 27.9.2010 Numer w rejestrze: Numer identyfikacji podatkowej (INN): 6168033776; Podstawowy państwowy numer identyfikacyjny (OGRN): 1106194004850 Główne miejsce prowadzenia działalności: Federacja Rosyjska Powiązane osoby: Evgeniy Bashev Powiązane podmioty: Jednostka GRU nr 29155	»Impuls« LLC to rosyjskie przedsiębiorstwo będące własnością Evgeniya Viktorovicha Basheva, członka jednostki nr 29155 rosyjskiej agencji wywiadu wojskowego (GRU). Przedsiębiorstwo to zapewnia wsparcie techniczne i materialne na potrzeby cyberataków i prób cyberataków przeprowadzanych przez jednostkę GRU nr 29155. W szczególności »Impuls« LLC pełni funkcję operacyjnego pośrednika umożliwiającego prowadzenie działań hakerskich, które mają być prowadzone za pośrednictwem przedsiębiorstwa formalnie niepowiązanego z państwem rosyjskim. Przedsiębiorstwo to udostępniało ochronę operacyjną, infrastrukturę i umożliwiało płatności na potrzeby cyberataków oraz było powiązane z aktywami technicznymi, w tym serwerami wykorzystywanymi do wspierania działań hakerskich. W szczególności »Impuls« LLC umożliwiło współpracę między strukturami GRU a zewnętrznymi sieciami hakerów. Cyberoperacje ułatwiane przez »Impuls« LLC są wymierzone w krytyczne funkcje państwa i usługi niezbędne do utrzymania podstawowej działalności społecznej i gospodarczej w państwach członkowskich, zwłaszcza w sektorze transportu. Za pośrednictwem kampanii WhisperGate jednostka GRU nr 29155 prowadziła też ataki wymierzone w infrastrukturę krytyczną Ukrainy. »Impuls« LLC zapewnia zatem wsparcie techniczne i materialne na potrzeby cyberataków wywołujących poważne skutki, które stanowią zagrożenie zewnętrzne dla państw członkowskich, a także na potrzeby cyberataków wywołujących poważne skutki dla państw trzecich, lub jest zaangażowane w inny sposób w takie cyberataki i próby ich przeprowadzenia.	13.7.2026

	Nazwa	Dane identyfikacyjne	Powody	Data umieszczenia
11.	Z-Pentest	Inne nazwy: »Z-Pentest Alliance«, »Z-Alliance« Główne miejsce prowadzenia działalności: Federacja Rosyjska Powiązane osoby: Yuliya Pankratova Powiązane podmioty: Cyber Army of Russia Reborn / CARR Konto w serwisie X: ZPentest (konto zawieszone) Konto w serwisie Telegram: Zpentestalliance	Z-Pentest jest prorosyjską grupą hakywistów, składającą się z członków CARR [ang. Cyber Army of Russia Reborn (Cyberarmia Rosji Odrodzonej)] i NoName057, która prowadzi ataki na infrastrukturę krytyczną na całym świecie, zwłaszcza w sektorze energetycznym i wodnym. W grudniu 2024 r. grupa zaatakowała duńskie przedsiębiorstwo wodociągowe. Z-Pentest odpowiada zatem za cyberataki wywołujące poważne skutki, które stanowią zewnętrzne zagrożenie dla państw członkowskich.	13.7.2026”