aut. Sylwia Gliwa 04.05.2021

CZESKIE PRZYGOTOWANIA NA ZAGROŻENIA HYBRYDOWE. POWODEM DZIAŁALNOŚĆ ROSYJSKICH SŁUŻB SPECJALNYCH?

„Działania hybrydowe mają na celu zatarcie granic między pokojem, kryzysem i konfliktem (...) wpływ ten wykorzystuje już istniejące słabości i wewnętrzne podziały w społeczeństwie, dążąc do ich dalszego pogłębienia" – czytamy w zatwierdzonej w kwietniu czeskiej Narodowej Strategii Zwalczania Działań Hybrydowych. Dokument bez wątpienia wskazuje, że rząd naszego południowego sąsiada na poważnie traktuje współczesne zagrożenia dla bezpieczeństwa państwa i zamierza się do nich przygotować.

„Ostatnie wydarzenia dotyczące niedopuszczalnej działalności rosyjskich służb specjalnych na naszym terytorium potwierdzają, że nie żyjemy w bezpiecznym świecie. Dlatego musimy wzmocnić naszą obronę i bezpieczeństwo, zmodernizować armię i wymienić przestarzałe technologie, ale też skutecznie walczyć ze współczesnymi zagrożeniami" – wskazuje czeski resort obrony narodowej. W poniedziałek 19 kwietnia rząd Republiki Czeskiej zatwierdził przekazaną przez ministra obrony Narodową Strategię Zwalczania Działań Hybrydowych. „Jego celem jest reagowanie na pogarszające się środowisko bezpieczeństwa, które wraz z szybkim rozwojem nowych technologii umożliwia w szczególności podmiotom państwowym i niepaństwowym wykorzystanie słabości demokratycznego społeczeństwa" – czytamy w oficjalnym komunikacie.

W 9 stronicowym dokumencie podzielonym na 4 działy nasi południowi sąsiedzi podkreślają wagę zagrożeń hybrydowych oraz wskazują, że odnoszą się one zarówno do jawnych jak i ukrytych działań prowadzonych podmioty państwowe jak i niepaństwowe. Jak podkreślono w treści strategii działania te skierowane są przeciwko demokratycznym państwom jak i społeczeństwu a ich celem jest zakłócenie funkcjonowania instytucji demokratycznych, praworządności i bezpieczeństwa wewnętrznego.

Czesi wskazują na trzy obszary, w których państwo jest narażone na działania hybrydowe – zaliczono do nich ideologię i wartości społeczne oraz konstytucyjny ustrój państwa, gospodarkę oraz bezpieczeństwo i obronę.

„Szybkość, zakres i intensywność interferencji hybrydowej wzrosły, częściowo w wyniku rozwoju nowej technologii" – wskazano w dokumencie, jednocześnie podkreślając, że działania te wykorzystują m.in. narzędzia polityczne, dyplomatyczne, informacyjne, wojskowe, ekonomiczne, finansowe, wywiadowcze do podważenia interesów Republiki Czeskiej. Jednocześnie podkreślono w niej, że celem tych działań jest opóźnianie lub paraliżowanie procesów podejmowania decyzji politycznych a także osłabianie zaufania obywateli do demokratycznych procesów i instytucji państwowych. Zwrócono również uwagę na próby zakłócania procesów gospodarczych, zdobywanie wpływów w sektorach gospodarki kluczowych dla państwa oraz przejmowania kontroli nad środowiskiem informacyjnym. „W tym celu sprawcy ingerencji hybrydowej wykorzystują różnorodne narzędzia, w tym złośliwe działania w cyberprzestrzeni" – zapisano.

W dokumencie bez wskazywania na konkretne podmioty i zjawiska podkreślono raz jeszcze (za strategią bezpieczeństwa tego kraju), że środowisko bezpieczeństwa podlega dynamicznym zmianom a jego przewidywalność zmniejszyła się z uwagi na wzrost zależności „trendów" i „czynników". „Chociaż prawdopodobieństwo masowego ataku wojskowego bezpośrednio zagrażającego terytorium Republiki Czeskiej pozostaje niskie, wrogie działania z wykorzystaniem szerokiego spektrum narzędzi interferencji hybrydowej stanowią zagrożenie dla bezpieczeństwa regionu euroatlantyckiego, w tym Republiki Czeskiej" – czytamy dalej.

W dokumencie zapowiedziano wprowadzenie przejrzystego systemu monitorowania inwestycji zagranicznych podmiotów w strategiczne sektory gospodarki i kluczowe przedsiębiorstwa – „zwłaszcza tych, które obejmują krytyczną lub inną ważną infrastrukturę państwową". Jednocześnie zapowiedziano zmniejszenie strategicznej zależności od krajów o odmiennych systemach ideologicznych i wartościach – „taka zależność mogłaby zostać wykorzystana przeciwko interesom Republiki Czeskiej" – podkreślono w strategii. Oprócz obaw o uzależnienie państwa od strategicznych dostaw materiałów z zagranicy, takich jak ropa naftowa, gaz ziemny czy paliwo jądrowe Czesi wskazują również na obszar nowoczesnych technologii i rozwiązań technologicznych, takich jak sieci 5G i sztuczna inteligencja. Czy zapis ten wskazuje, że Czesi pójdą za słusznym trendem dokonywania przeglądów wykorzystywanej technologii do budowania infrastruktury informacyjnej państwa?

Przypomnijmy, że jeszcze w październiku 2019 roku NIS Cooperation Group - unijna grupa powołana na mocy dyrektywy NIS - wydała raport odnośnie oceny ryzyka w kontekście budowy sieci 5G w którym wskazano, że nadmierne uniezależnienie od jednego dostawcy przy budowie sieci 5G stanowi ryzyko. Jak wskazywano wtedy spostrzeżeniem z raportu, którego nie sposób przeoczyć jest bezpośrednie zwrócenie uwagi na transparentność oraz typ struktury właścicielskiej przy wyborze dostawcy rozwiązań. Dokument bezpośrednio z nazwy wymienia podmioty stanowiące w ich opinii możliwych głównych dostawców, do których zalicza Huawei, Ericsson oraz Nokię a jako innych również biorących udział w kreowaniu rynku wymienił ZTE, Samsunga oraz Cisco. NIS bezpośrednio wskazuje na podmioty, które posiadają swoje siedziby na terenie UE – Ericssona oraz Nokię. Fragment ten, pomimo że nietrudno wyłapać sugestię co do predyspozycji unijnych co do wyboru dostawcy, nie przekazuje żadnej rekomendacji. Jednak w dalszej części raportu czytamy na wskazanie możliwej ingerencji ze strony państwa nie będącego członkiem Unii Europejskiej na funkcjonowanie dostawcy.

Jednocześnie co należy podkreślić, a o czym wielokrotnie pisaliśmy na naszych łamach, w kontekście budowy sieci 5G kraje europejskie stały się areną walk pomiędzy wpływami amerykańskimi próbującymi namówić poszczególne kraje do niestosowania chińskiej technologii a samymi gigantami technologicznymi z Państwa Środka.

W swoim dokumencie strategicznym, Czesi podkreślili konieczność zaangażowania całego społeczeństwa w celu przeciwdziałania zagrożeniom hybrydowym jednocześnie wskazując na wagę takich podmiotów jak służby bezpieczeństwa i organy rządowe, odpowiednie elementy sektorów komercyjnych, medialnych, edukacyjnych oraz organizacje non-profit.

Jest to pierwszy dokument strategiczny Republiki Czeskiej poświęcony temu obszarowi i uzupełniający już istniejące strategiczne dokumenty bezpieczeństwa – wskazuje departament prasowy resortu obrony narodowej w oficjalnym komunikacie do sprawy. Jak podkreślono w oświadczeniu, największą trudnością działań hybrydowych jest fakt, że często wykorzystuje legalne źródła informacji do osiągnięcia wrogich celów – „na przykład poprzez głoszenie teorii spiskowych na renomowanych stronach internetowych". Jak wskazuje dalej czeski resort sprawiedliwości, działania te mogą służyć jako środek szerzenia poparcia dla radykalnych partii lub ruchów politycznych, dezinformacji i wrogiej propagandy a także może objawiać się cyberatakami na infrastrukturę cywilną, różnymi formami presji ekonomicznej lub tworzeniem zależności od wrogich podmiotów poprzez inwestycje w infrastrukturę krytyczną i kluczowe sektory lub technologie lub agresywne rozmieszczanie służb

wywiadowczych lub sił specjalnych innych państw w Republika Czeska. Jest to niewątpliwie również efekt ostatniego skandalu z udziałem rosyjskich służb specjalnych w którym bezpośrednio przypisano im winę za eksplozję składów amunicyjnych, w której zginęło dwóch ich obywateli.