

SZEF FBI: WYBORY Z 2018 ROKU BYŁY PRÓBĄ GENERALNĄ, A PEKIN KLUCZOWYM ZAGROŻENIEM

Zabezpieczenie ostatnich wyborów stanowiło generalną próbę przed wyzwaniem związanym z ochroną kampanii prezydenckiej w 2020 roku – stwierdził szef FBI Christopher Wray podczas swojego przemówienia w Radzie ds. Stosunków Zagranicznych.

„Nasi wrogowie nieustannie będą podnosić swoje zdolności i umiejętności, dostosowując się do zmieniającego się środowiska” – zaznaczył szef FBI podczas wystąpienia. Równocześnie podkreślił, że wiele państw wyciągnęło wnioski z operacji wpływów Rosji, w tym kampanii dezinformacyjnych oraz prób ingerencji w procesy wyborcze.

W wyniku działalności Moskwy Stany Zjednoczone zdecydowały się na przeznaczenie znacznej ilości środków w celu zabezpieczenia kampanii wyborczej z 2018 roku. Wówczas głosowanie odbyło się bez żadnego złośliwego „wpływu lub ingerencji” w infrastrukturę w wyborczą. Sukces ten Christopher Wray wyraźnie podkreślił stwierdzając, że „to ogromny postęp w zakresie bezpieczeństwa wyborów”.

Obecnie wszystkie amerykańskie służby są skupione na najbliższych wyrobach prezydenckich. Przedstawiciele Departamentu Bezpieczeństwa Wewnętrznego wskazują, że prowadzą specjalistyczne analizy i obserwacje wszelkich prób rosyjskiej ingerencji w europejskie wybory, a NSA „już teraz ciężko pracuje nad wyborami w 2020 roku”.

W trakcie swojego przemówienia Christopher Wray odniósł się do kwestii chińskiej działalności w cyberprzestrzeni, której jednym z głównych celów jest kradzież danych i tajemnic handlowych. „Pekin wydaje się być zdeterminowany, aby poprzez kradzież wspinać się po drabinie gospodarczej. Wszystko naszym kosztem” – tłumaczył dyrektor FBI. – „Żaden kraj nie stanowi tak poważnego zagrożenia dla danych wywiadowczych, jak Chiny” – dodał.

Szef FBI zauważył również, że obecnie zagrożenia w cyberprzestrzeni mają charakter mieszany – cyberprzestępczość i szpiegostwo łączy się ze sobą na wiele różnych sposobów. W związku z tym istotną rolę w całym łańcuchu cyberbezpieczeństwa odgrywają pojedyncze firmy i organizacje, które muszą skupić się na ochronie przede wszystkim swoich sieci przed naruszeniami. „Podmioty te mają tendencje do myślenia o cyberbezpieczeństwie jako o czymś bardzo szerokim, podczas gdy w rzeczywistości najważniejsza jego część znajduje się w samym środku organizacji” – zakończył Christopher Wray.