

## KOREA PÓŁNOCNA ZAGRAŻA AMERYKAŃSKIEJ INFRASTRUKTURZE ENERGETYCZNEJ

---

**W ostatnich tygodniach stale rośnie napięcie związane z północnokoreańskim programem jądrowym. Szczególnie głośno protestują Stany Zjednoczone, będące gwarantem bezpieczeństwa w regionie i zarazem państwem postrzeganym przez reżim Kim Dzong Una jako największy wróg. W ferworze wydarzeń pojawiły się rozważania o potencjalnej eskalacji konfliktu. Gdyby do niej doszło, Korea Północna nie musi uciekać się do użycia sił konwencjonalnych czy broni atomowej. Wystarczy atak wymierzony w amerykańską piętę achillesową, strategiczną infrastrukturę energetyczną.**

Jak boleśnie i w relatywnie prosty sposób uderzyć w Stany Zjednoczone, największego na świecie konsumenta energii elektrycznej? Odpowiedź jest prosta i Amerykanie od lat zdają sobie z niej sprawę: zakłócając funkcjonowanie infrastruktury energetycznej w USA.

Największe zagęszczenie ludności w Stanach przypada na wschodnie wybrzeże, obszar rozległy terytorialnie, lecz bardzo silnie zurbanizowany i w związku z tym gęsto pokryty zarówno siecią linii przesyłowych, jak i elektrowni. Jedynym wydajnym rozwiązaniem na tego typu terenie jest energia nuklearna. Nie dziwi zatem poważne traktowanie przez władze amerykańskie wszelkich ostrzeżeń dotyczących potencjalnych ataków wymierzonych w tę infrastrukturę.

W ostatnich doniesieniach prasowych przewija się wątek sparaliżowania amerykańskiej energetyki impulsem elektromagnetycznym (EMP), który może wygenerować na przykład eksplozja jądrowa w atmosferze ponad wschodnim wybrzeżem USA. Równie istotna z uwagi na skuteczność rozwiązań asymetrycznych wydaje się być możliwość dokonania ataku za pośrednictwem klawiatury. Wymagałby on dokładnego zaplanowania, długich przygotowań, dostępu do odpowiednich narzędzi i zasobów oraz zespołu, który zdolny byłby go przeprowadzić – czyli w praktyce wsparcia ze strony podmiotu o charakterze państwowym. Warunki te w teorii spełnia szereg państw, w tym Korea Północna.

Najczarniejszy scenariusz zakłada uszkodzenie i przeciążenie reaktora jądrowego. Scenariusz bardziej realistyczny i zademonstrowany już w praktyce pod koniec 2015 r. na Ukrainie obejmuje odcięcie konsumentów od dostaw energii elektrycznej. Jej stała dostępność warunkuje nie tylko jakość życia, ale jest też kluczowa dla płynności komunikacji wojskowej i cywilnej oraz funkcjonowania gospodarki. Dla przykładu, czterodniowa awaria sieci w północno-wschodniej części USA w 2003 r. spowodowała brak dostaw prądu dla blisko 50 mln osób oraz straty szacowane w przedziale 4-10 mld dolarów.

**Czytaj też: [Wywiad USA wskazuje największych graczy w cyberprzestrzeni](#)**

Pentagon zareagował przypomnieniem o projekcie Rapid Attack Detection, Isolation and Characterization (RADICS), nad którym pracują wspólnie Agencja Zaawansowanych Projektów Badawczych w Obszarze Obronności (DARPA) oraz koncern BAE Systems. Główne zadania programu

to zwiększenie świadomości sytuacyjnej władz, monitorowanie i analiza sieci kontrolujących infrastrukturę energetyczną, wykrycie przygotowywanego ataku, wczesne o nim ostrzeżenie, odizolowanie i rozpoczęcie obrony sieci jeszcze zanim rozpocznie się właściwa faza ataku. RADICS ma nadto zagwarantować nieprzerwany dostęp do komunikacji kryzysowej dla wojska i władz państwowych, co stanowi priorytet Agencji. System ma według przedstawicieli BAE Systems zostać wdrożony za trzy lata.

Możliwość przeprowadzenia ataków cybernetycznych stała się standardem współczesnych armii. Truizmem jest stwierdzenie, że globalizacja i uzależnienie gospodarki od systemów komputerowych czynią z nich atrakcyjne narzędzie prowadzenia wojny nie tylko dla państw zaawansowanych technologicznie, ale również tych, które poszukują relatywnie tanich i skutecznych sposobów uderzenia w przeciwnika.

W przypadku infrastruktury energetycznej obrona przed takimi atakami powinna objąć również wymianę oprogramowania kontrolującego wiele wchodzących w jej skład sieci. Nierzadko, jak wskazują eksperci, jest ono przestarzałe i nie napisano go z myślą o cyberbezpieczeństwie – dziedzinie, która z uwagi na lawinowy postęp technologiczny wymaga nieustannego dostosowywania się do zmian.

Na przeszkodzie stoją koszty takiej operacji, rozległość infrastruktury oraz rozdrobnienie podmiotów weń zaangażowanych. Wydaje się zatem, że najskuteczniejszym sposobem obrony pozostaje póki co odstraszenie. Pytanie tylko, jak długo będzie się ono sprawdzać w starciu z przeciwnikiem równie dla Amerykanów nieprzewidywalnym co Korea Północna.

Katarzyna Stróż