Oświadczenie złożone
przez senatora Tadeusza Jarmuziewicza
na 67. posiedzeniu Senatu
w dniu 27 października 2026 r.

Oświadczenie skierowane do prezesa Rady Ministrów Donalda Tuska

Szanowny Panie Premierze!

Działając na podstawie przepisów regulujących wykonywanie mandatu senatora, zwracam się do Pana Premiera w kluczowej dla bezpieczeństwa państwa sprawie, jaką jest realna ochrona cybernetyczna krytycznej infrastruktury energetycznej.

Energetyka zawodowa w Polsce, a w szczególności spółki z udziałem Skarbu Państwa, takie jak Polskie Sieci Elektroenergetyczne SA (PSE) czy najwięksi operatorzy systemów dystrybucyjnych (OSD), wchodzi w erę bezprecedensowych inwestycji. Skala wydatków rośnie i będzie gwałtownie rosnąć w najbliższych latach, m.in. w związku z realizacją gigantycznych kontraktów na budowę magazynów energii, rozbudowę sieci przesyłowych oraz masową cyfryzację liczników.

Z niepokojem obserwuję jednak, że brakuje obecnie realnej, dogłębnej kontroli nad cyberbezpieczeństwem urządzeń i systemów wprowadzanych do obrotu w tym sektorze. Realne zagrożenia technologiczne są zbyt często przykrywane przez fasadowe, jedynie formalne próby ograniczenia ryzyka. Polegają one głównie na preferowaniu dostawców z kapitałem unijnym lub polskim, bez faktycznej weryfikacji tego, jakie komponenty, podzespoły i oprogramowanie finalnie trafiają do krytycznych węzłów naszej sieci. Certyfikacja bezpieczeństwa opiera się nierzadko na oświadczeniach i deklaracjach producentów. Wynika to z faktu, że wielkie spółki energetyczne – mimo ogromnych budżetów inwestycyjnych – nie dysponują kompetencjami wewnętrznymi do kompleksowej, głębokiej oceny cyberbezpieczeństwa oprogramowania i hardware'u ani na etapie postępowań przetargowych, ani podczas odbioru dostaw.

Taka sytuacja doprowadzi do scenariusza, w którym miliardy złotych z kieszeni polskich podatników zostaną wydane na infrastrukturę spełniającą wymogi funkcjonalne, lecz całkowicie niezweryfikowaną pod kątem ukrytych furtek, mechanizmów zdalnego dostępu czy podatności w warstwie sprzętowej i programowej.

Mając na uwadze konieczność skoordynowanego działania rządu, za organy właściwe do szczegółowego odniesienia się do poruszonych problemów oraz wypracowania systemowych rozwiązań uznaję ministra cyfryzacji, pana Krzysztofa Gawkowskiego, oraz ministra energii, pana Miłosza Motykę, a także NASK i Instytut Łączności – PIB.

W związku z powyższym zwracam się do Pana Premiera z następującymi pytaniami.

1. Jakie realne, działające w praktyce mechanizmy w zakresie zapewnienia cyberbezpieczeństwa są stosowane obecnie wobec urządzeń dostarczanych do energetyki zawodowej, które posiadają możliwości zdalnej komunikacji (np. routery przemysłowe) lub bezpośredniego sterowania, takie jak np. sterowniki magazynów energii, zaawansowane falowniki, inteligentne liczniki?

2. Jakie są konkretne plany rządu w zakresie zapewnienia realnego wsparcia – zwłaszcza dla spółek Skarbu Państwa – w technicznej i merytorycznej ocenie cyberbezpieczeństwa zamawianych urządzeń, tak aby podmioty te nie były zdane wyłącznie na własne, często niewystarczające zasoby kadrowe i ograniczone wyspecjalizowanie?

3. Czy Ministerstwo Cyfryzacji oraz resort właściwy do spraw energii nie powinny otrzymać polecenia stworzenia centralnego, powtarzalnego systemu weryfikacji i audytu technologicznego sprzętu i oprogramowania trafiającego do polskiej krytycznej infrastruktury energetycznej?

4. Jakie działania zostaną podjęte, aby kryteria przetargowe w energetyce zawodowej przestały opierać się wyłącznie na deklaracjach producentów i formalnym pochodzeniu kapitału, a zaczęły uwzględniać rygorystyczne, niezależne i ustandaryzowane na poziomie krajowym testy penetracyjne oraz analizy kodu źródłowego i architektury sprzętowej?

Z poważaniem
Tadeusz Jarmuziewicz
senator RP