A/PNL/405/16.6.2026 Nr.5560A/16.06.2026

ÎNTREBARE PARLAMENTARĂ

Către: Domnului Dan Cîmpean, Directorul Directoratului Național de Securitate Cibernetică

De la: Sebastian-Ioan Burduja, Deputat PNL, Circumscripția Electorală Nr. 42 București

Obiectul întrebării: Securitatea cibernetică a infrastructurii energetice critice și stadiul aplicării Directivei NIS 2 în sectorul energetic

Stimate domnule director,

Infrastructura energetică, de la centrale și rețele de transport la sistemele industriale de comandă și control de tip SCADA, este astăzi una dintre cele mai expuse ținte ale atacurilor cibernetice. Riscul nu este teoretic. Atacurile de tip Industroyer, denumite și CRASH OVERRIDE, au întrerupt alimentarea cu energie în Ucraina în 2016, iar o variantă perfecționată, Industroyer2, a fost folosită din nou împotriva rețelei ucrainene în 2022. Aceste atacuri au demonstrat că un program informatic ostil poate manipula direct echipamentele din stații și poate provoca o cădere de sistem. Convergența dintre tehnologia informației și tehnologia operațională, alături de înmulțirea resurselor distribuite, de la prosumatori și parcuri fotovoltaice la stații de încărcare și contoare inteligente, lărgește continuu suprafața de atac.

Cadrul juridic s-a maturizat. Directiva (UE) 2022/2555, cunoscută drept NIS 2, a fost transpusă în România prin Ordonanța de urgență a Guvernului nr. 155/2024, aprobată prin Legea nr. 124/2025, care desemnează Directoratul Național de Securitate Cibernetică, înființat prin Ordonanța de urgență a Guvernului nr. 104/2021, drept autoritate competentă și încadrează operatorii din energie, electricitate, gaze, petrol, termoficare și hidrogen, în categoria entităților esențiale, cu obligații stricte de gestionare a riscului, cu termene de raportare a incidentelor de 24 de ore, 72 de ore și 30 de zile și cu sancțiuni care pot ajunge la 10 milioane de euro. La nivel european, Regulamentul delegat (UE) 2024/1366, care completează Regulamentul (UE) 2019/943, instituie un cod de rețea cu norme sectoriale pentru securitatea cibernetică a fluxurilor transfrontaliere de energie electrică.

Esența problemei este, însă, una de implementare. Multe sisteme de comandă din rețelele de distribuție și de la producători mai mici au fost proiectate într-o epocă în care securitatea cibernetică nu era o cerință, iar separarea dintre rețelele administrative și cele industriale rămâne adesea incompletă. La acestea se adaugă un risc sistemic de lanț de

aprovizionare, generat de echipamente precum invertoarele fotovoltaice, contoarele inteligente și aparatura de rețea care pot fi actualizate sau controlate de la distanță de către furnizori din afara spațiului euroatlantic.

Având în vedere aceste considerente, în temeiul art. 112 alin. (1) din Constituția României, republicată, precum și al art. 194-201 din Regulamentul Camerei Deputaților, cu modificările și completările ulterioare, vă adresez, în scris, următoarele întrebări:

1. Care este stadiul aplicării efective a Ordonanței de urgență a Guvernului nr. 155/2024 și a Legii nr. 124/2025 pentru operatorii din energie, respectiv câte entități esențiale și importante din sector au fost identificate și notificate și câte au implementat integral măsurile de gestionare a riscului prevăzute de lege?
2. Care este stadiul operaționalizării centrului de răspuns la incidente de securitate cibernetică din energie și al implementării Regulamentului delegat (UE) 2024/1366 privind securitatea fluxurilor transfrontaliere de energie electrică?
3. Câte incidente de securitate cibernetică raportate în ultimele douăsprezece luni au vizat infrastructura energetică, câte dintre acestea au afectat sisteme de tehnologie operațională sau SCADA și care a fost impactul lor asupra continuității alimentării?
4. Ce cerințe de separare a rețelelor de tehnologie a informației de cele de tehnologie operațională și ce aliniere la standardele internaționale specifice, precum IEC 62443 pentru sistemele industriale și IEC 61850 pentru automatizarea stațiilor, sunt impuse operatorilor de transport și de distribuție, și care este gradul actual de conformare?
5. Ce evaluare a riscului de lanț de aprovizionare a realizat DNSC cu privire la invertoarele fotovoltaice, contoarele inteligente și echipamentele de rețea cu funcții de actualizare sau de control de la distanță provenind din afara spațiului euroatlantic, și ce măsuri de izolare, de control al accesului de la distanță sau de interdicție sunt avute în vedere?
6. Cum este asigurat regimul special de securitate cibernetică al Centralei Nuclearoelectrice Cernavodă, în coordonare cu Comisia Națională pentru Controlul Activităților Nucleare și în acord cu ghidurile Agenției Internaționale pentru Energie Atomică?
7. Ce teste de penetrare, exerciții de tip echipă roșie și capacități de centru operațional de securitate funcționează la nivelul operatorilor strategici, precum Transelectrica și Transgaz, pentru protecția sistemelor de comandă a rețelelor de transport?
8. Ce exerciții de reziliență la scenarii de cădere de sistem provocată cibernetic au fost organizate, cum participă România la rețeaua europeană a echipelor de răspuns și la exercițiile coordonate de Agenția Uniunii Europene pentru Securitate Cibernetică, și ce fonduri, inclusiv din Planul Național de Redresare și Reziliență, sunt alocate pentru întărirea apărării tehnologiei operaționale?

9. Există planuri actualizate de continuitate și de repornire a sistemului energetic, inclusiv capacitatea de pornire autonomă a centralelor, pentru scenariul unui atac cibernetic major soldat cu întreruperea pe scară largă a alimentării?

Cu deosebit respect,

Sebastian-Ioan BURDUJA

Deputat PNL