Nota de fundamentare

Secțiunea 1:
Titlul proiectului de act normativ

Lege
privind înființarea și operaționalizarea Centrului de Răspuns la Incidente de Securitate Cibernetică în Energie, precum și pentru modificarea și completarea unor acte normative

Secțiunea a 2-a:
Motivul emiterii actului normativ

2.1. Sursa proiectului de act normativ

Programul de Guvernare PSD-PNL-USR-UDMR - Grupul parlamentar al minorităților naționale din Camera Deputaților 2025-2028 pentru care Guvernul a primit votul Parlamentului prin Hotararea pentru acordarea încrederii Guvernului nr. 25 din 23 iunie 2025 prevede la Capitolul "Energie", pct. V - Măsuri de debirocratizare, digitalizare și guvernanță, subpct. 4, "Înființarea unui Centru de Răspuns la Incidente de Securitate Cibernetică în Energie (CRISCE) și crearea de echipe SOC și CSIRT la nivelul companiilor naționale."

O serie de acte normative naționale, europene sau documente cu caracter programatic prevăd obligația autorităților administrației publice centrale și operatorilor economici esențiali de a constitui, forma și dezvolta personal de securitate cibernetică, respectiv de a lua măsuri active și reactive de prevenire și combatere a amenințărilor și atacurilor cibernetice, dintre care amintim:

a) secțiunea a 4-a din capitolul V, capitolul VI, secțiunea a 2-a din capitolul VII și capitolul VIII din Ordonanța de urgență nr. 155/2024 privind instituirea unui cadru pentru securitatea cibernetică a rețelelor și sistemelor informatice din spațiul cibernetic național civil;
b) art. 2 lit. f) și k), art. 3 alin. (1) lit c) și art. 24 alin. (2) din Legea nr. 58/2023 privind securitatea și apărarea cibernetică a României, precum și pentru modificarea și completarea unor acte normative;
c) pct. 8 și 13 din introducere, pct. 21 din cap. I - România membru activ NATO și UE, stat rezilient, pol de stabilitate regional, pct. 62 din Cap. II - Interese și obiective naționale de securitate, pct. 71, 75, 82, 90 și 92 din cap. III - Evaluarea mediului de securitate, pct. 127, 128, 152 și 163 din Cap. IV - Amenințări, riscuri și vulnerabilități, pct. 177 și 179 din Cap. V - Direcții de acțiune și principalele modalități pentru asigurarea securității naționale a României, ale Strategiei Naționale de Apărare a Țării pentru perioada 2020-2024, aprobată prin Hotărârea Parlamentului României nr. 22/2020;
d) Măsura 4.1 și 4.4.1 din Anexele nr.1 la Hotărârea Guvernului nr. 1321/2021 privind aprobarea Strategiei de securitate cibernetică a României, pentru perioada 2022-2027, precum și a Planului de acțiune pentru implementarea Strategiei de securitate cibernetică a României, pentru perioada 2022-2027;
e) Regulamentul delegat (UE) 2024/1366 al Comisiei din 11 martie 2024 de completare a Regulamentului (UE) 2019/943 al Parlamentului European și al Consiliului prin stabilirea unui cod de rețea privind normele sectoriale pentru aspectele legate de securitatea cibernetică a fluxurilor transfrontaliere de energie electrică;

f) art. 6 și 7 din Regulamentul (UE) 2019/881 al Parlamentului European Și Al Consiliului privind ENISA (Agenția Uniunii Europene pentru Securitate Cibernetică) și privind certificarea securității cibernetice pentru tehnologia informației și comunicațiilor și de abrogare a Regulamentului (UE) nr. 526/2013 (Regulamentul privind securitatea cibernetică);
g) art. 1 și 2 din Regulamentul (UE) 2019/796 din 17 mai 2019 al Consiliului privind măsuri restrictive împotriva atacurilor cibernetice care reprezintă o amenințare la adresa Uniunii sau a statelor sale membre;
h) Punctul 3 din Anexa IV și punctul 3 din Anexa V din Regulamentul (UE) 2017/1938 al Parlamentului European și al Consiliului din 25 octombrie 2017 privind măsurile de garantare a siguranței furnizării de gaze și de abrogare a Regulamentului (UE) nr. 994/2010, cu modificările ulterioare;
i) Paragrafele 3 și 34 din preambulul Regulamentului (UE) 2024/1689 al Parlamentului European și al Consiliului din 13 iunie 2024 de stabilire a unor norme armonizate privind inteligența artificială și de modificare a Regulamentelor (CE) nr. 300/2008, (UE) nr. 167/2013, (UE) nr. 168/2013, (UE) 2018/858, (UE) 2018/1139 și (UE) 2019/2144 și a Directivelor 2014/90/UE, (UE) 2016/797 și (UE) 2020/1828 (Regulamentul privind inteligența artificială);
j) art. 9-11 și art. 13-15, Capitolul IV, Capitolul VII și Anexa 1 din Directiva (UE) 2022/2555 a Parlamentului European și a Consiliului din 14 decembrie 2022 privind măsuri pentru un nivel comun ridicat de securitate cibernetică în întreaga Uniune, de modificare a Regulamentului (UE) nr. 910/2014 și a Directivei (UE) 2018/1972 și de abrogare a Directivei (UE) 2016/1148 (Directiva NIS 2);
k) Pct. 1.2 și Capitolul 2 din Comunicare Comună către Parlamentul European și Consiliu - Strategia de securitate cibernetică a UE pentru deceniul digital JOIN (2020) 18 final din 16.12.2020;
l) punctul 1 al Capitolului IV din Comunicarea Comisiei către Parlamentul European, Consiliul European, Consiliu, Comitetul Economic și Social European și Comitetul Regiunilor referitoare la Strategia UE privind uniunea securității nr. COM/2020/605 final;
m) Recomandarea (UE) 2019/553 a Comisiei privind securitatea cibernetică în sectorul energetic, nr. C (2019) 2400;
n) art. 1 și 3 din propunerea de Regulament al Parlamentului European și al Consiliului de stabilire a unor măsuri de consolidare a solidarității și a capacităților de la nivelul Uniunii pentru detectarea amenințărilor și a incidentelor de securitate cibernetică, pregătirea legată de acestea și contracararea lor nr. COM/2023/209 final;
o) Raportul ENER/B3/2017-465 (UE) privind evaluarea riscurilor de incidente cibernetice și costurile prevenirii incidentelor cibernetice în sectorul energetic;
p) Raportul EECSP-Expert Group (UE) privind securitatea cibernetică în sectorul energetic, în ansamblul său;
q) Raport EECSP-Expert Group privind securitatea cibernetică în sectorul energetic, Recomandări pentru Comisia Europeană privind un cadru strategic european și potențiale acte legislative viitoare pentru sectorul energetic;
r) Planul Agenției Internaționale pentru Energie Atomică nr. GC(65)/24 privind securitatea nucleară 2022-2025;
s) Raportul Agenției Internaționale pentru Energie Atomică nr. 17-T (Rev. 1) privind tehnici de securitate informatică pentru instalațiile nucleare;
t) Raportul Agenției Internaționale pentru Energie Atomică nr. 33-T privind Securitatea informatică a instrumentației și sistemelor de control din instalațiile nucleare;
u) Raportul Agenției Internaționale pentru Energie Atomică nr. 42-G privind securitatea informatică pentru securitatea nucleară;
v) Seria de standarde internaționale ISA/IEC 62443: ISA/IEC 62443 standarde privind securitatea cibernetică a sistemelor de control și automatizare industrială (IACS).

2.2 Descrierea situației actuale

2.2.1. Prezentare a unor situații de vulnerabilitate cibernetică a sectorului energetic. Aspecte globale

Raportul Agenției Uniunii Europene pentru Securitate Cibernetică (ENISA) privind vulnerabilitățile cibernetice la nivelul anului 2023 a reținut că sectorul energetic este o țintă prioritară pentru atacurile cibernetice, datorită infrastructurii critice și impactului semnificativ pe care astfel de atacuri le pot avea asupra economiei și securității naționale. Raportul ENISA privind vulnerabilitățile cibernetice la nivelul anului 2023 evidențiază mai multe amenințări și incidente notabile care au afectat sectorul energetic, dintre care amintim cel puțin:

a) *Ransomware* este una dintre cele mai periculoase amenințări. Atacurile de tip ransomware implică preluarea controlului asupra sistemelor informatice și solicitarea unei răscumpărări pentru restabilirea accesului la acestea. Atacurile ransomware nu sunt doar financiare, pot avea și scopuri geopolitice sau de perturbare strategică. În prima jumătate a anului 2023, numărul incidentelor de ransomware a crescut considerabil, afectând multiple sectoare, inclusiv cel energetic.

b) *Malware* este o amenințare semnificativă. Software-ul malițios poate compromite confidențialitatea, integritatea și disponibilitatea sistemelor. În sectorul energetic, malware-ul este utilizat pentru a perturba procesele industriale și operațiunile automatizate, având potențialul de a cauza pagube financiare majore și întreruperi în furnizarea energiei.

c) *Atacuri de inginerie socială.* Acestea au crescut semnificativ, demarcând phishing-ul ca vector principal de atac. Tehnicile de inginerie socială sunt utilizate pentru a obține acces neautorizat la sisteme critice prin manipularea angajaților pentru a dezvălui informații sensibile;

d) *Amenințări distribuite asupra disponibilității sistemelor (DDoS).* Atacurile de tip Distributed Denial of Service (DDoS) vizează saturarea rețelelor și sistemelor cu trafic excesiv, provocând indisponibilitatea acestora. Aceste atacuri au un impact semnificativ asupra infrastructurilor critice, inclusiv în sectorul energetic, perturbând operațiunile normale și cauzând pierderi financiare;

e) *Manipularea informațiilor și interferențe.* Acestea sunt utilizate pentru a destabiliza procesele decizionale și pentru a influența opinia publică. În contextul agresiunii Federației Ruse împotriva Ucrainei, astfel de tehnici au fost intensificate pentru a submina încrederea în instituțiile critice, inclusiv în sectorul energetic.

f) *Atacuri asupra lanțului de aprovizionare.* Acestea implică compromiterea furnizorilor terți pentru a pătrunde în rețelele țintă. Sectorul energetic este deosebit de vulnerabil la astfel de atacuri datorită complexității și interdependenței sistemelor sale. În 2023, aproximativ 9% dintre atacurile asupra lanțului de aprovizionare au vizat sectorul energetic.

Incidentele de securitate cibernetică notabile, menționate în raportul ENISA, sunt:

a) Industroyer2 și COSMICENERGY. Industroyer2, descoperit în 2022, a vizat substațiile de energie, fiind o variantă a malware-ului Industroyer utilizat de grupul APT Sandworm pentru a întrerupe alimentarea cu energie electrică în Ucraina în 2016. COSMICENERGY, detectat în 2023, a fost proiectat pentru a perturba operațiunile de transmisie și distribuție a energiei electrice. Deși analiza a arătat că nu este la fel de avansat ca Industroyer2, aceste incidente subliniază vulnerabilitatea infrastructurilor industriale critice;

b) Campania DarkSide. În 2021, DarkSide a fost responsabil pentru atacul ransomware asupra Colonial Pipeline, cea mai mare conductă de petrol din SUA, care a dus la o întrerupere semnificativă a aprovizionării cu combustibil pe coasta de est a Statelor Unite. Acest incident a evidențiat impactul potențial devastator al atacurilor cibernetice asupra infrastructurii critice energetice.

c) Atacurile asupra rețelelor electrice ucrainene. În contextul conflictului geopolitic, atacurile cibernetice asupra infrastructurii energetice din Ucraina au fost frecvente. Malware-ul Industroyer2 a fost utilizat pentru a tăia alimentarea cu energie electrică în anumite regiuni, demonstrând modul în care astfel de atacuri pot fi utilizate ca armă în conflictele moderne.

Acțiunile întreprinse de agențiile de aplicare a legii, cum ar fi demantelarea infrastructurii grupurilor infracționale cibernetice, subliniază importanța cooperării internaționale în combaterea amenințărilor cibernetice. Astfel de acțiuni au contribuit la reducerea temporară a activităților unor grupuri cibernetice, deși efectul pe termen lung asupra securității sectorului energetic încă nu poate fi estimat, deoarece depinde de fiecare stat, sector și subsector cum își construiește mecanismele instituționale de prevenire și combatere a atacurilor cibernetice.
Aceste incidente de securitate cibernetică subliniază necesitatea unor măsuri robuste de securitate cibernetică în sectorul energetic. Este esențială implementarea unor strategii proactive de apărare, inclusiv monitorizarea constantă, actualizarea continuă a sistemelor și educarea personalului pentru a recunoaște și răspunde rapid la amenințările cibernetice.
Incidentele recente la nivel regional și național au demonstrat că infrastructura critică este vulnerabilă la atacuri sofisticate, iar protecția acesteia necesită o abordare cuprinzătoare și integrată, care să includă tehnologie avansată, politici de securitate riguroase și cooperare între diferitele părți interesate.
Sectorul energetic trebuie să fie pregătit să facă față unor amenințări cibernetice complexe și în continuă evoluție. Implementarea unor măsuri de securitate cibernetică riguroase și cooperarea internațională sunt esențiale pentru protejarea acestui sector critic împotriva atacurilor sofisticate și persistente.

Cazuistică recentă, din surse deschise, privind securitatea cibernetică în sectorul energetic:
Potrivit unui articol din industria de specialitate (a se vedea Cyber Attack Statistics - Updated July 2024 "- Parachute, disponibil la: https://parachute.cloud/cyber-attack-statistics-data-and-trends), se arată că:
a) 90% dintre cele mai importante companii energetice din lume au suferit de încălcări ale datelor de la terți în 2023;
b) Atacurile cibernetice costă sectorul energetic 4,72 milioane USD per incident în medie.
c) Aproape 60% dintre atacurile cibernetice din sectorul energetic sunt conduse de actori statali.
d) Sectorul energetic este foarte susceptibil la inginerie socială, având în vedere că 60% din toate încălcările de date sunt atacuri de tip phishing.

Dintre cele mai notabile situații de atacuri cibernetice care au vizat sectorul energetic, la nivel global, în ultimii 3 ani amintim:

1. Atacul asupra Eni S.p.A (august 2022)
În august 2022, compania italiană de petrol Eni S.p.A a dezvăluit un atac cibernetic asupra rețelelor sale informatice. Atacul de tip ransomware a cauzat doar daune minore, deoarece sistemele interne ale companiei au identificat activitățile neautorizate în zilele premergătoare atacului. Acest incident a arătat importanța detectării timpurii și a răspunsului rapid pentru a minimiza impactul atacurilor cibernetice. Eni a reușit să evite daune mai mari datorită intervenției prompte, subliniind necesitatea de a avea echipe de securitate cibernetică bine pregătite și tehnologii de monitorizare eficiente.

2. Atacul asupra DESFA (august 2022)
Pe 21 august 2022, DESFA, cel mai mare distribuitor de gaze naturale din Grecia, a anunțat că a suferit un atac cibernetic major care a dus la o breșă de date și o întrerupere semnificativă a sistemelor IT. Echipa IT a companiei a reușit să intervină rapid, prevenind preluarea completă a sistemelor de către atacatori, dar aceștia au reușit totuși să acceseze și să scurgă anumite date sensibile. Atacul a fost revendicat de grupul de ransomware Ragnar Locker, care a demonstrat cât de vulnerabile pot fi companiile energetice la astfel de amenințări. Acest incident a subliniat necesitatea de a avea planuri

de continuitate a afacerii și măsuri de securitate cibernetică bine puse la punct pentru a proteja infrastructura critică.

3. Compromiterea companiilor energetice din Danemarca (mai 2023)
În mai 2023, un atac cibernetic coordonat a vizat 22 de companii energetice din Danemarca. Atacatorii au exploatat vulnerabilități zero-day în dispozitivele Zyxel, reușind să compromită rețelele și să obțină configurațiile dispozitivelor și numele de utilizator. SektorCERT, organizația de securitate cibernetică, a colaborat cu companiile afectate pentru a aplica patch-uri disponibile și pentru a securiza rețelele compromise. Acest atac a evidențiat riscurile asociate vulnerabilităților necunoscute și importanța colaborării între organizațiile de securitate și companiile energetice pentru a minimiza impactul atacurilor cibernetice. În timpul campaniei, unele firewall-uri compromise au fost infectate cu un bot Mirai și folosite în atacuri de tip DDoS împotriva unor entități din SUA și Hong Kong.

4. Atacul asupra unei instalații nucleare israeliene (martie 2024)
În martie 2024, hackeri iranieni au compromis o rețea IT conectată la o instalație nucleară israeliană, scurgând documente sensibile ale instalației. Deși rețeaua tehnologiei operaționale (OT) nu a fost compromisă, incidentul a reprezentat un risc major de securitate, dezvăluind detalii critice despre infrastructura nucleară. Acest atac a demonstrat complexitatea și gravitatea amenințărilor cibernetice la adresa infrastructurilor critice și a subliniat necesitatea unor măsuri robuste de securitate pentru a proteja astfel de active vitale. Incidentul a amplificat tensiunile geopolitice și a evidențiat importanța colaborării internaționale pentru a combate amenințările cibernetice transfrontaliere

5. Atacul asupra Canadian Solar (septembrie 2022)
Pe 11 septembrie 2022, grupul de ransomware LockBit 3.0 a revendicat un atac cibernetic asupra Canadian Solar, un producător de module fotovoltaice solare. Hackerii au operat un atac de tip ransomware pin care au cerut o răscumpărare pentru a nu distruge datele companiei și au oferit extensii ale termenului de plată pentru 10.000 USD/zi. De asemenea, au amenințat că vor publica datele furate pe Dark Web în cazul în care compania nu va plăti răscumpărarea. Acest incident a subliniat riscurile semnificative cu care se confruntă companiile din sectorul energiei solare, mai ales în contextul în care acestea joacă un rol important în tranziția către surse de energie regenerabilă. Evenimentul a demonstrat cât de vulnerabile pot fi companiile de energie la atacurile cibernetice și importanța măsurilor de securitate cibernetică proactivă.

6. Atacul asupra PetroChina (februarie 2023)
În februarie 2023, grupul de ransomware Medusa a atacat PetroChina Indonesia, furând date și cerând o răscumpărare pentru a nu le divulga. Medusa a postat informații despre companie pe blogul lor din Dark Web și a dat companiei un termen de șapte zile pentru a răspunde cererilor. În plus, au cerut 400.000 USD pentru a șterge datele furate și încă 400.000 USD pentru a le recupera. Medusa a amenințat, de asemenea, că va vinde datele către terți dacă cererile lor nu vor fi îndeplinite. Acest atac a evidențiat riscurile majore la care sunt expuse companiile din sectorul petrolier și necesitatea de a avea măsuri de securitate cibernetică eficiente.

7. Atacul asupra ACEA (februarie 2023)
Pe 2 februarie 2023, grupul de ransomware Black Basta a atacat ACEA, o companie italiană care furnizează servicii de gestionare a deșeurilor, electricitate și apă pentru orașul Roma. Atacul a avut ca rezultat indisponibilitatea site-ului oficial al companiei până a doua zi, deoarece echipele de intervenție au trebuit să implementeze măsuri de control al daunelor. Incidentul a demonstrat importanța măsurilor rapide și eficiente de răspuns în caz de atac cibernetic pentru a limita impactul asupra serviciilor publice esențiale. Această situație a subliniat necesitatea de a investi în soluții de

securitate cibernetică robuste și de a dezvolta planuri de continuitate a afacerii pentru a proteja infrastructură critică.

8. Atacul asupra unei companii din sectorul energetic german (2023)
În 2023, două companii energetice din Germania au fost atacate cibernetic, cauzând perturbări minore în aprovizionarea cu petrol în nordul Germaniei. Atacurile au fost similare cu incidentul Colonial Pipeline din SUA, demonstrând vulnerabilitatea infrastructurii energetice la atacuri cibernetice și impactul potențial asupra lanțurilor de aprovizionare și prețurilor energiei. Aceste incidente au amplificat tensiunile geopolitice și au evidențiat importanța măsurilor proactive de securitate cibernetică pentru a proteja infrastructura critică și a preveni perturbările semnificative în aprovizionarea cu energie.

9. Atacul asupra Tata Power (octombrie 2022)
În octombrie 2022, Tata Power, cea mai mare companie integrată de energie din India, a fost victima unui atac cibernetic orchestrat de grupul de ransomware Hive. Atacul a dus la furtul unor cantități semnificative de date personale și financiare ale angajaților, inclusiv numere de identificare națională, numere de conturi fiscale și informații salariale. De asemenea, Hive a publicat planuri de inginerie, înregistrări financiare și informații ale clienților furate de la Tata Power. Impactul asupra companiei a fost major, necesitând implementarea unor măsuri urgente de răspuns și recuperare. Atacul a subliniat vulnerabilitatea companiilor mari din sectorul energetic la astfel de amenințări și a evidențiat necesitatea unor măsuri robuste de securitate cibernetică pentru protejarea datelor sensibile și a infrastructurii critice

10. Campania de spionaj cibernetic asupra guvernului și sectorului energetic indian (martie 2024)
În martie 2024, sectorul guvernamental și energetic din India a fost vizat de o campanie de spionaj cibernetic sofisticată. Hackerii au folosit fișiere malițioase deghizate în scrisori oficiale pentru a accesa comunicațiile electronice și sistemele de guvernanță IT. Scrisorile aparent proveneau de la Forțele Aeriene Regale ale Indiei, având astfel o aparență credibilă care a facilitat compromiterea sistemelor vizate. Această metodă de atac este cunoscută sub numele de spear-phishing, unde atacatorii personalizează mesajele pentru a păcăli țintele să deschidă fișierele infectate. Deși nu s-a stabilit încă cine a efectuat atacul, astfel de campanii sunt adesea asociate cu actori statali sau grupuri de hackeri sponsorizate de state, având în vedere complexitatea și specificitatea țintelor. Scopul principal al acestei campanii a fost colectarea de informații sensibile legate de infrastructura energetică și de securitatea națională a Indiei.

2.2.2. Atacuri cibernetice în contextul agresiunii Rusiei împotriva Ucrainei
În contextul agresiunii Federației Ruse împotriva Ucrainei s-au constatat o serie de operații militare care s-au concentrat asupra unor infrastructuri energetice de pe teritoriul Ucrainei și, prin atacuri hibride, și asupra statelor vecine, astfel amintim:
- atacuri asupra infrastructurii energetice, inclusiv prin mijloace cyber, care a indisponibilizat 50% din sistemul Energetic al Ucrainei în 16.12.2022;
- atac cibernetic de tip malware, denumit Industroyer2, asupra sistemelor informatice din electricitate din Ucraina, lansat de gruparea Sandworm controlată de serviciile de informații rusești, la data de 8 aprilie 2022 ;

Toate aceste atacuri, convenționale sau hibride, au fost de natură a pune în incapacitate de funcționare totală sau parțială sistemul energetic al Ucrainei și/sau al statelor vecine. Unul sau mai multe atacuri similare constituie riscuri și pentru securitatea energetică a României, motiv pentru care se impune crearea unei surse de rezervă pentru producerea energiei electrice.

2.2.3. Evaluarea stadiului securității cibernetice la nivel sectorului energetic din România

Stadiul actual al securității cibernetice în sectorul energetic din România este caracterizat prin deficiențe majore care necesită intervenții urgente pentru a proteja infrastructurile critice și a asigura continuitatea serviciilor esențiale. Analiza detaliată a rapoartelor rezultate din exercițiul național de securitate cibernetică din perioada 15-16 aprilie 2024, intitulat "Energy CyberGuard", dezvăluie o imagine clară a competențelor cibernetice ale companiilor energetice din România.
Reglementările naționale, precum Ordonanța de urgență nr. 155/2024 privind instituirea unui cadru pentru securitatea cibernetică a rețelelor și sistemelor informatice din spațiul cibernetic național civil și Legea nr. 58/2023 privind securitatea și apărarea cibernetică a României, impun măsuri clare pentru protejarea infrastructurilor critice.
Directiva (UE) 2022/2555 a Parlamentului European și a Consiliului din 14 decembrie 2022 (Directiva NIS2) extinde cerințele de securitate și măsurile de raportare a incidentelor pentru un număr mai mare de sectoare și entități esențiale, inclusiv energie, în timp ce Regulamentul UE 2019/881 (Cybersecurity Act) consolidează rolul ENISA și stabilește un cadru european de certificare a securității cibernetice pentru produse și servicii TIC.
Strategia UE de securitate cibernetică promovează o abordare holistică a securității cibernetice la nivelul UE, cu accent pe protecția infrastructurilor critice și colaborarea între statele membre. Pe baza acestor reglementări și cerințe, crearea unui CSIRT (Computer Security Incident Response Team) sectorial în domeniul energiei este absolut necesară. Această structură ar centraliza eforturile de securitate cibernetică, oferind suport specializat și coordonare pentru a proteja infrastructurile critice împotriva atacurilor cibernetice.
Un CSIRT sectorial ar facilita coordonarea și schimbul de informații între entitățile din sectorul energetic, autorități și alte părți relevante, asigurând un răspuns unitar și eficient la incidente. Cantitativ, datele din documentele analizate indică că doar o parte din companiile participante la evenimentul CTF reușit să abordeze provocările de nivel la extrem.
Capacitatea limitată de a gestiona amenințările cibernetice complexe și angajamentul redus față de securitatea cibernetică impun necesitatea stringentă de a crea un CSIRT sectorial dedicat. Acestea vor contribui la protejarea infrastructurilor critice, asigurarea continuității serviciilor esențiale și conformitatea cu reglementările naționale și europene. Crearea unui CSIRT sectorial ar reprezenta un pas crucial în îmbunătățirea capacității de răspuns la incidente și în consolidarea securității cibernetice a sectorului energetic din România.
În cadrul exercițiului paneuropean intitulat „Europa Cibernetică", desfășurat în luna iunie 2024, la care a participat și Ministerul Energiei din România, menit să testeze gradul de pregătire în cazul unui atac cibernetic la scară largă asupra sectorului energetic european, exercițiul a constatat că, la nivelul Ministerului Energiei, capacitățile de coordonare, de cooperare și de gestionare a crizelor pentru în evaluarea reziliența sectorului energetic prezintă vulnerabilități sistemice, cauzate primordial de faptul că nu există o structură responsabilă de securitatea cibernetică a ministerului, pe de-o parte, și a sectorului energetic, pe de altă parte. Ultimul element prezintă o vulnerabilitate cu atât mai mare cu cât cadrul european și național de reglementare în domeniul cyber security impun crearea și operaționalizarea unei structuri de securitate cibernetică la nivel sectorial, cu rol de CSIRT sectorial.

În adresa Directoratului Național pentru Securitate Cibernetică nr. D876/09.08.2024 privind Rezultatele exercițiului Cyber Europe 2024 s-a reținut următoarea situație de fapt:
"- În lipsa CSIRT-ului din sectorul energetic, coordonarea echipei tehnice naționale a fost asigurată de către specialiștii CSIRT național, din DNSC, iar activitatea s-a desfășurat de la locul de muncă al fiecărui participant. Echipa de comunicare a fost coordonată de specialiștii DNSC, iar activitatea s-a desfășurat în format mixt, atât de la sediul DNSC, cât și de la locul de muncă al participanților.

- S-a simțit acut lipsa CSIRT-ului sectorial în domeniul energetic, care să monitorizeze infrastructura hardware și software specifică acestui sector, în special în zona echipamentelor SCADA.
- Necesitatea înființării și operaționalizării CSIRT sectorial din sectorul energetic pentru crearea imaginii operaționale integrate privind situația în spațiul cibernetic."

În data de 9 decembrie 2024, Distribuție Energie Electrică România (DEER), parte a Grupului Electrica, a fost ținta unui atac cibernetic de tip ransomware, evidențiind vulnerabilitățile semnificative ale infrastructurii energetice naționale în fața amenințărilor cibernetice avansate. Atacul a vizat criptarea datelor din sistemele informatice ale companiei, cu scopul de a solicita o răscumpărare pentru deblocarea acestora. Deși sistemele critice, precum SCADA, au fost izolate și au rămas complet funcționale, incidentul subliniază pericolul real și prezent la care sunt expuse infrastructurile esențiale ale României. Analiza preliminară a incidentului a relevat că atacatorii au utilizat tehnici sofisticate pentru a compromite rețeaua internă a DEER. Se presupune că vectorul inițial de atac a fost un e-mail de tip phishing, care a permis infiltrarea malware-ului în sistem. Odată pătrunși în rețea, atacatorii au escaladat privilegiile și au distribuit ransomware-ul, criptând datele esențiale și paralizând operațiunile companiei. Această metodologie indică o pregătire minuțioasă și o cunoaștere aprofundată a infrastructurii țintă, sugerând implicarea unei grupări cibernetice bine organizate.

Fondul pentru Modernizare instituit în conformitate cu Ordonanța de urgență a Guvernului nr. 60/2022 *privind stabilirea cadrului instituțional și financiar de implementare și gestionare a fondurilor alocate României prin Fondul pentru modernizare, precum și pentru modificarea și completarea unor acte normative*, aprobată cu completări prin Legea nr. 376/2023, cu modificările și completările ulterioare, reprezintă o alocare pentru România de peste 15 miliarde euro, și care vizează tranziția către un sistem energetic cu emisii reduse de carbon, prin stimularea investițiilor în surse regenerabile de energie, rețelele de transport și distribuție a energiei termice în zonele rezidențiale și comerciale, interconectări de rețele pentru transportul de electricitate și gaze naturale, capacități de stocare a energie, modalități de îmbunătățire a eficienței energetice în diferite sectoare economice și asigurarea unei tranziții echitabile în regiunile dependente de cărbune, se constată utilizarea unor sisteme și rețele informatice tot mai sofisticate, finanțate de acest Fond, care, dacă ar fi atacate cibernetic, ar putea periclita întreaga infrastructură energetică finanțată prin Fond.
Fondul pentru Modernizare este una dintre cele mai mari șanse de dezvoltare pe care România o are în istoria recentă, iar astfel Ministerul Energiei gestionează o investiție strategică pentru viitorul României și România Viitorului. Valoarea totală la zi a contractelor aferente investițiilor din Fondul pentru Modernizare este de 17.138.864.454 lei, echivalentul a 3.427.772.891 euro. Toate proiectele dețin noi tehnologii care utilizează fie rețele interconectate, fiind acționate de la distanță, fie funcționarea lor depinde de interconectarea cu alte infrastructuri energetice.
Remarcăm în acest context că, protecția cibernetică a acestor proiecte nu a fost nici prevăzută în cheltuielile eligibile și finanțate, nici acoperite prin orice mijloace post-implementare. Astfel, avem de-a face cu o nouă infrastructură energetică națională, finanțată prin Fondul pentru Modernizare, total vulnerabilă în fața amenințărilor cibernetice specifice sistemului energetic.

2.2.4. Cu privire la necesitatea desemnării autorității competente potrivit art. 4 din Regulamentul delegat (UE) 2024/1366 al Comisiei de completare a Regulamentului (UE) 2019/943 al Parlamentului European și al Consiliului prin stabilirea unui cod de rețea privind normele sectoriale pentru aspectele legate de securitatea cibernetică a fluxurilor transfrontaliere de energie electrică, precizăm următoarele:

În conformitate cu prevederile art. 4 alin. (1) din Regulamentul Delegat (UE) 2024/1366 al Comisiei din 11 martie 2024 de completare a Regulamentului (UE) 20191943 al Parlamentului European și al Consiliului prin stabilirea unui cod de rețea privind normele sectoriale pentru aspectele legate de securitatea cibernetică a fluxurilor transfrontaliere de energie electrică (denumit în continuare Codul de securitate cibernetică):
"Cât mai curând posibil și, în orice caz, până la 13 decembrie 2024, fiecare stat membru desemnează o autoritate națională guvernamentală sau de reglementare responsabilă cu îndeplinirea sarcinilor care îi sunt atribuite prin prezentul regulament („autoritate competentă"). Până când autorității competente i se încredințează îndeplinirea sarcinilor prevăzute în prezentul regulament, autoritatea de reglementare desemnată de fiecare stat membru în temeiul articolului 57 alineatul (1) din Directiva (UE) 2019/944 îndeplinește sarcinile autorității competente în conformitate cu prezentul regulament".
Astfel, indiferent de entitatea care va fi desemnată să preia sarcinile stabilite de acest regulament, România trebuie să îndeplinească obligația de desemnare ANRE având doar rolul interimar de a asigura punerea în aplicare a regulamentului pâna la data desemnării. Desemnarea autorității competente trebuie să fie corelată cu implementarea prevederilor Directivei (UE) 2022/2555 privind măsuri pentru un nivel comun ridicat cle Securitate cibernetică în Uniune (denumită în continuare Directiva NIS2), proces în curs de desfășurare în majoritatea statelor membre ale Uniunii Europene, astfel încât să nu existe suprapuneri de sarcini datorită prevederilor celor două documente europene.

2.2.5. Concluziile evaluării de risc și scenarii privind securitatea și reziliența cibernetică în sectoarele telecomunicații și energie electrică, publicat, în extras, în data de 24 iulie 2024, care a fost realizată de Comisia Europeană și Grupul de Cooperare NIS, în consultare permanentă cu Serviciul de Acțiune Externă al UE, în urma concluziilor Consiliului Uniunii Europene (9364/22 din 23 mai 2022) privind dezvoltarea poziției cibernetice a Uniunii Europene.

Evaluarea efectuată de Comisia Europeană și Grupul de Cooperare NIS oferă o perspectivă recentă privind securitatea cibernetică conexă inclusiv domeniului energetic, indicând necesitatea unor măsuri cu relevanță deosebit de ridicată, care conduc către necesitatea înființării într-un interval de timp cât mai redus a unor structuri de tip CSIRT. Prezentul proiect de act normativ constituie o reacție a statului român cu privire la evaluarea Comisiei Europene, care subliniază nivelul crescut al riscurilor de securitate cibernetică.

În cadrul acestor concluzii, Consiliul a evidențiat cele cinci funcții ale UE în domeniul cibernetic, anume:
1) consolidarea rezilienței și a capacităților de protecție;
2) consolidarea solidarității și gestionarea cuprinzătoare a crizelor;
3) promovarea viziunii UE în spațiul cibernetic;
4) consolidarea cooperării cu țările partenere și organizațiile internaționale;
5) prevenirea, apărarea și răspunsul la atacurile cibernetice.

În acest context, a fost realizată o evaluare de risc privind segmentul securității cibernetice ale cărei concluzii au fost cuprinse în cadrul unui raport în care au fost evidențiate o serie de riscuri cibernetice, inclusiv pe linia lanțului de aprovizionare, lipsa resursei umane specializate și amenințările generate de actori motivați financiar și strategic.

În încheiere, în cadrul raportului este menționată o invitația fermă adresată atât SM UE cât și organizațiilor de cooperare în domeniul cibernetic, de a lua în considerare evaluarea și scenariile prezentate în cadrul elaborării unor exerciții de securitate cibernetică cu reprezentativitate atât la nivel comunitar cât și național. De asemenea, este specificat faptul că raportul elaborat în urma evaluării de risc, a pus bazele unui set de instrumente standardizat pentru viitoare inițiative similare ce vor fi derulate la nivelul UE. Suplimentar, este recomandat ca acest set de instrumente să fie

îmbunătățite prin colaborare și deliberare internațională pentru a facilita procesul evaluărilor viitoare, iar rezultatele acestora să poată fi comparate cu mai mare ușurință.

Totodată, elaborarea raportului a avut la bază o serie de documente și inițiative care vizează consolidarea securității cibernetice la nivelul UE, precum Directiva NIS 2, recomandări și comunicări ale Comisiei, Regulamentul UE 2019/941 privind pregătirea pentru riscuri în sectorul energiei electrice, Task Force-ul UE-NATO privind reziliența infrastructurilor critice etc.

În lumina celor prezentate, se evidențiază importanța asigurării unui nivel optim de securitate cibernetică în domeniul energiei, fapt pentru care la nivel comunitar sunt derulate diverse inițiative în acest sens, iar SM UE sunt invitate să se ralieze acestor eforturi.

Evaluarea a relevat o serie de riscuri cibernetice, atât de natură tehnică cât și non-tehnică, sectorul energiei electrice fiind expus amenințărilor provenite din spațiul cibernetic pe componentele lanțului de aprovizionare (atât la adresa componentelor software și hardware cât și în privința serviciilor furnizate de părți terțe, față de care operatorii energetici care se află într-o relație de dependență) și a infrastructurii de energie regenerabilă. O preocupare permanentă este reprezentată de amenințările de tip ransomware, data wipers și exploatarea vulnerabilităților zero-day care generează o serie de provocări, mai ales în privința tehnologiei operaționale (OT). De asemenea, pentru sectorul energiei electrice, amenințările de tip insider threat prezintă un grad ridicat de risc, întrucât sunt amplificate de lipsa unor proceduri adecvate de vetting a personalului nou angajat, dublate de dificultatea atragerii de noi specialiști în domeniu. Mare parte din aceste riscuri ar fi diminuate la nivelul României prin înființarea acestui mecanism de tip CSIRT sectorial, într-un interval redus de timp, pentru a nu permite materializarea acestora.

În cadrul evaluării au fost indicate o serie de scenarii de risc care au presupus derularea unor activități nelegitime împotriva infrastructurii IT&C și a echipamentelor OT, dintre care amintim:

- insider threats: în beneficiul unor actori cu motivație statală, financiară ori ideologică, prin compromiterea unor servere, aplicații sau conturi de utilizatori în urma exploatării unor vulnerabilități cibernetice de tip CVE documentate public;
- spionaj: compromiterea unor resurse informatice, facilitată prin exploatarea unor CVE, vulnerabilități zero-day ori prin intermediul unor servicii furnizate de terți, față de care operatorul vizat este dependent;
- atacuri de tip hibrid în vederea indisponibilizării unui segment larg al infrastructurii energetice derulate de actori statali ori motivați financiar, prin compromiterea unor echipamente OT în urma exploatării unor vulnerabilități de tip zero-day ori a unor servicii furnizate de terți, față de care operatorul vizat este dependent;
- generarea unui deficit în furnizarea serviciilor energetice, prin derularea unui atac cibernetic de către un actor statal, în urma exploatării unor vulnerabilități CVE ori a compromiterii unor servicii furnizate de terți, față de care operatorul vizat este dependent.

Din perspectiva asigurării unui răspuns optim la riscurile cibernetice evidențiate în urma evaluării, au fost punctate o serie de recomandări defalcate pe patru direcții de acțiune, după cum urmează:

1. reziliența și capacitatea de răspuns la incidente de cibernetice pot fi îmbunătățite prin intermediul unor măsuri conexe unui mecanism de tip CSIRT precum:
   - schimb de bune practici cu privire la atacurile ransomware;
   - monitorizarea vulnerabilităților de securitate cibernetică;
   - implementarea unor politici de securitate umană și fizică;
   - gestionarea eficientă a activelor organizațiilor;
   - intensificarea cooperării pe segmentul securității cibernetice la nivel comunitar, cu entitățile CSIRT, instituțiile de aplicare a legii și partenerii internaționali;
   - realizarea de către SM UE a unor evaluări de securitate cibernetică în conformitate cu prerogativele Directivei NIS 2, pentru sectoarele cuprinse în cadrul acesteia (inclusiv energie).

2. Activitățile de awareness și schimbul de informații trebuie să fie consolidate prin includerea în cadrul acestora a unor aspecte cu privire la contextul geopolitic, potențiale pericole la adresa integrității fizice și dezinformarea;
3. Consolidarea planurilor de contingență, management al crizelor și colaborare operațională, în materie de proceduri, prin scurtarea liniilor de comunitare dintre sectoarele implicate și autoritățile responsabile în domeniul securității cibernetice;
4. Securitatea lanțurilor de aprovizionare ar trebui abordată prin realizarea de evaluări care să vizeze identificarea dependențelor față de furnizori din state terțe care prezintă un grad ridicat de risc și dezvoltarea unui cadru UE pentru asigurarea lanțului de aprovizionare.

În acest sens, cu toate că evaluarea amintită mai sus face referire cu precădere la sectorul energiei electrice, concluziile pot fi aplicate tuturor sectoarelor din domeniul energiei, întrucât la nivel macro acestea sunt deservite și operează în baza unor principii similare, fiind totodată interconectate. Astfel, toți operatorii energetici gestionează infrastructuri IT&C care deservesc segmentul administrativ (enterprise) și sisteme OT (infrastructura de proces și control industrial). De asemenea, având în vedere evoluția tehnologică, separarea fizică și logică a acestor sisteme, care deservesc scopuri diferite, nu mai poate fi realizată pe deplin, din rațiuni care țin de administrarea eficientă a sistemelor energetice.

Suplimentar, sectorul energiei este caracterizat de integrarea unor echipamente OT de diferite tipuri, implementate și operaționalizate în diverse perioade de timp, majoritatea aflându-se în uz anterior apariției amenințărilor din spectrul cibernetic (existând cazuri de exploatare a unor astfel de echipamente de peste 20 de ani).

Sistemele OT sunt în centrul administrării proceselor din energie, acestea facilitând monitorizarea stării surselor de generare a energiei, liniilor de transport și rețelelor de distribuție în timp real. Astfel, acest lucru le permite operatorilor de rețea să echilibreze cererea și oferta, să prevină supraîncărcările și să răspundă rapid la urgențe. În acest sens, este vitală adoptarea unor măsuri suplimentare în vederea creșterii nivelului de securitate cibernetică pentru a se asigura furnizarea serviciilor de energie în regim de continuitate.

Contextual, la nivel european, sistemele energetice au un grad foarte ridicat de interconectivitate, fapt pentru care indisponibilizarea continuității serviciilor, inclusiv ca urmare a unui atac cibernetic, este de natură să producă efecte în cascadă la nivelul mai multor state membre UE.

2.2.6. În ultimii ani a fost identificată o creștere a numărului de vulnerabilități de securitate cibernetică, care sunt documentate inclusiv în surse deschise, la nivelul unor soluții VPN și de control a accesului, furnizate de diverși vendori. Astfel, în contextul în care operatorii energetici administrează sisteme și rețele cu acoperire geografică mare, pentru a căror administrare se apelează frecvent la accesarea de la distanță, crește riscul compromiterii acestor soluții. Exploatarea acestora permite unui potențial atacator să obțină acces neautorizat de la distanță, în mod neautentificat, fapt ce i-ar conferi:

- posibilitatea de a executa, în mod nelegitim, comenzi prin care ar putea să preia controlul asupra echipamentelor compromise;
- eludarea mecanismelor de autentificare și obținerea accesului la resurse restricționate din infrastructura compromisă;
- instalarea unor backdoor-uri, iar ulterior să execute tehnici specifice de mișcare laterală prin care ar putea compromite alte resurse din cadrul operatorului vizat;
- exfiltrarea de fișiere și credențiale de acces.

Înființarea unui mecanism de tip CSIRT în domeniul energetic ar susține semnificativ eforturile de prevenire a exploatării acestor vulnerabilități de securitate cibernetică care pot afecta furnizarea în condiții optime a serviciilor energetice. Mai mult, numărul constant în creștere de vulnerabilități

critice ce afectează acest domeniu necesită adresare din partea statului român în regim de urgență, prin măsuri de securitate adecvate, precum este cea de dezvoltare a CSIRT sectorial.

2.2.7. Informații relevante salarizare în domeniul securității energetice

Pentru identificarea de informații relevante cu privire la salarizarea din domeniul securității cibernetice, relative la domeniul nișat al zonei de înalt specializare operațională și cu particularizare pentru domeniul energetic, autorii proiectului de act normativ au făcut apel la:

a) Surse de informații relevante din internet (cu date suficiente, care să evidențieze o situație cât mai reală din industrie);

b) Surse de informații oficiale, de la instituții care dețin date referitoare la salariile reale și elocvente (nu doar statistici medii generale – precum cele de la INS – ci statistici exacte pentru posturile vizate – de ex. de la ITM).

c) Evidențierea exactă a tipurilor de posturi vizate: înaltă specializare și competență.

De asemenea, în stabilirea regimului juridic derogatoriu de la normele privind salarizarea personalului din sectorul public se au în vedere faptul că finanțarea CRISCE nu se realizează din bugetul de stat, ci se realizează exclusiv din (1) cheltuielile administrative prevăzute la art. 8 din O.U.G. nr. 60/2022, constituite din dobânzi acumulate în conturile și la dispoziția Ministerului Energiei la sumele virate de Banca Europeană pentru Investiții (BEI), precum și din (2) veniturile obținute din prestarea de servicii de securitate cibernetic pentru sectorul energetic.

Posturile necesare pentru operaționalizarea CRISCE trebuie să fie de nivelul cel mai înalt posibil, din perspectiva experienței și performanței în domeniul de specialitate, pentru a putea garanta succesul operațiunilor de securitate cibernetică.

În general, salariile de top în domeniul securității cibernetice pot atinge următoarele niveluri valorice:

- Pentru SUA: 242.000 USD anual (respectiv 20.166 USD brut/ lună sau 18.500 EUR brut/lună);
- Pentru Canada: 216.000 CAD anual (respectiv 18.000 CAD brut/lună sau, respectiv 12.000 EUR brut/lună);
- Pentru Elveția: 180.000 EUR pe an (respectiv 15.000 EUR brut pe lună) ;
- Pentru Germania: 140.000 EUR pe an (respectiv 11.666 EUR brut pe lună);
- Pentru UK: 145.000 EUR pe an (respectiv 12.083 EUR brut pe lună).

Salariul unui manager/director de securitate cibernetică (CISO) atinge valori medii între 178.000 USD brut anual și 394.401 USD brut anual .

În România, piața securității cibernetice este relativ tânără și nu conține date statistice relevante, nici la nivel de surse deschise (în internet), nici la nivelul INS. Aceste două categorii de surse conțin informații despre un nivel mediu al salariilor raportate în piață, provenind în mod majoritar de la angajatori care utilizează salarii la nivelul pieței muncii generale din România (cel mai adesea, acești angajatori au nevoie de îndeplinirea unor sarcini de rutină/ de nivel mediu, ci nu solicită performanțe și creativitate ridicată, precum situația de la CRISCE). Astfel, informațiile statistice generale indică salarii medii care ating valori de 4500-5000 EUR brut lunar.

Pe de altă parte, ITM, deși deține date concrete privind salariile, cel mai probabil că nu poate oferi o statistică relevantă per job-uri specializate în domeniul securității cibernetice, întrucât codurile COR din România nu au permis alocarea diferențiată a angajaților pe posturi de specialitate în securitate cibernetică (în lipsa existenței/definirii acestor specializări la nivelul COR), ci au condus la încadrarea specialiștilor de securitate cibernetică pe posturi din spectrul general al ocupațiilor

specifice tehnologiei informației (astfel, mai relevantă ar fi analizarea în bazele de date ale ITM, a salariilor de top din subdomenii ale tehnologiei informației în care angajatorii au încadrat cu preponderență specialiștii în securitate cibernetică, în ultimii ani).
Salariile reale din piața de specialitate, din România, sunt rareori cunoscute în spațiul deschis, întrucât reprezintă valori substanțial mai mari decât media pieței și conțin seturi extinse de beneficii (inclusiv bonusuri per proiecte, anuale, acțiuni la bursă etc.). Salariile din echipe operaționale precum cele propuse în cadrul CRISCE ating în mod frecvent valori de 13.000-20.000 EUR brut lunar, iar în situațiile în care se oferă și acțiuni la bursă, acestea depășesc considerabil aceste praguri.
Un alt exemplu relevant este reprezentat de contractele realizate de către instituții precum NATO și UE pentru externalizarea serviciilor de specialitate, care negociază în mod uzual prețuri între 80-110 EUR brut per oră (respectiv 13.440-18.480 EUR brut lunar) sau mai mult.

Totodată, prezintă relevanță și salariile medii globale ale specialiștilor cu certificări de cel mai înalt nivel (așa cum se doresc a fi și posturile din CRISCE), respectiv:
- CISSP: 103.493 USD brut anual în regiunea Europa;
- ISSAP: 129.671 USD brut anual în regiunea Europa;
- ISSEP: 147.550 USD brut anual în regiunea Europa;
- ISSMP: 144.173 USD brut anual în regiunea Europa;
- SANS/GIAC-GSE: 189.000 USD brut anual ;
- SANS/GIAC-GSLC: 152.143 USD brut anual;
- Six Sigma Master Black Belt: 169.170 USD brut anual.

Principalele sursele publice aferente datelor menționate sunt următoarele:

1. Analiza de specialitate "Top Countries for Cyber Security Salaries (cybersecurity-insiders.com)", disponibilă la: https://www.cybersecurity-insiders.com/top-paying-countries-for-cybersecurity-experts.
2. Chief Information Security Officer Salary in 2024 | PayScale, disponibil la https://www.payscale.com/research/US/Job=Chief_Information_Security_Officer/Salary.
3. Top Paying IT Certifications in 2023 | Best Computing Certs (itcareerfinder.com), disponibil la: https://www.itcareerfinder.com/brain-food/blog/entry/top-paying-it-certifications.html.
4. Chief Information Security Officer Salary | Salary.com, disponibil la: https://www.salary.com/research/salary/benchmark/chief-information-security-officer-salary.
5. Salary: Ciso in United States 2024 | Glassdoor, disponibil la: https://www.glassdoor.com/Salaries/ciso-salary-SRCH_KO0,4.htm.
6. "LIVE: Industrii Inteligente 2024. Cum se poate transforma economia românească într-una mai competitivă, productivă și durabilă? Transmisiune ZF Partner Events", disponibil la:https://www.zf.ro/un-salariu-pe-zi/un-salariu-pe-zi-un-specialist-in-cybersecurity-castiga-intre-2-000-20502856.
7. "Joburile viitorului care sunt plătite cu salarii de mii de euro: Specialiști în cyber security, în energie regenerabilă sau inginer de mediu/ Topul joburilor viitorului în România; disponibil la: https://economedia.ro/joburile-viitorului-care-sunt-platite-cu-salarii-de-mii-de-euro-specialisti-in-cyber-security-in-energie-regenerabila-sau-inginer-de-mediu-topul-joburilor-viitorului-in-romania.html.
8. ISC2 Reveals Global ISC2 Certification Salaries; accesat la data de: https://www.isc2.org/Insights/2024/05/ISC2-Reveals-Global-ISC2-Certification-Salaries.

În lumina datelor colectate și a specificității domeniului securității cibernetice, mai ales în sectorul energetic, menținerea unui nivel ridicat de salarizare pentru personalul CRISCE (Centrul de Răspuns la Incidente de Securitate Cibernetică în Energie) este esențială și justificată printr-o serie de argumente obiective, atât calitative, cât și cantitative. Acestea depășesc prevederile de drept comun ale Legii-cadru nr. 153/2017 *privind salarizarea personalului plătit din fonduri publice, având în vedere exigențele și caracteristicile unice ale posturilor vizate.*

În primul rând, securitatea cibernetică, mai ales într-un sector strategic precum cel energetic, necesită angajarea unor specialiști cu înaltă competență, capabili să gestioneze incidente complexe și să implementeze măsuri proactive de prevenție, ce depășesc cu mult cerințele posturilor standard din alte domenii ale tehnologiei informației. Potrivit datelor furnizate, salariile medii din domeniul securității cibernetice la nivel internațional se situează la valori considerabile. De exemplu, un manager de securitate cibernetică poate ajunge la un venit anual brut între 178.000 USD și 394.401 USD, ceea ce evidențiază cererea globală pentru astfel de competențe și nevoia de a oferi pachete salariale competitive pentru a atrage și reține specialiști de top.

Pentru a contextualiza în mod adecvat în cadrul pieței românești, trebuie subliniat faptul că salariile medii din domeniul securității cibernetice raportate de surse generale nu reflectă realitatea specifică a cerințelor pentru CRISCE. Astfel, salariile medii din România pentru specialiștii IT, adesea cu sarcini de rutină și performanță medie, se încadrează în intervalul de 4500-5000 EUR brut lunar. Totuși, în situațiile în care se cere înaltă calificare și competențe avansate, salariile reale ajung frecvent la 13.000-20.000 EUR brut lunar. De asemenea, instituții internaționale precum NATO și UE externalizează servicii similare la tarife de 80-110 EUR brut pe oră, adică între 13.440-18.480 EUR brut lunar, subliniind astfel valoarea de piață a acestor competențe.

Situația actuală din domeniul securității cibernetice în sectorul energetic impune reglementarea unor regimuri derogatorii atât de la Codul Muncii, cât și de la Legea nr. 153/2017 privind salarizarea personalului plătit din fonduri publice. Aceste derogări sunt fundamentate pe specificul activităților, necesitatea atragerii și menținerii personalului de înaltă specializare și complexitatea amenințărilor cibernetice care vizează infrastructurile critice naționale.

Sectorul energetic reprezintă una dintre cele mai vulnerabile infrastructuri critice, fiind ținta unor atacuri cibernetice complexe care pot afecta securitatea națională și stabilitatea economică. Amenințările cibernetice din acest domeniu se caracterizează prin:

- Complexitate tehnologică ridicată, incluzând atacuri avansate asupra sistemelor SCADA/ICS, care necesită cunoștințe tehnice aprofundate pentru detectare și prevenire;
- Evoluție rapidă a tehnologiilor și metodelor de atac, care impune un răspuns proactiv și continuu;
- Impact direct asupra funcționării serviciilor publice esențiale, cum ar fi distribuția energiei electrice, gaze naturale și alte resurse critice.

În acest context, personalul CRISCE trebuie să posede competențe tehnice avansate, inclusiv certificări internaționale (de exemplu, CISSP, CEH, GIAC), care nu pot fi asigurate prin mecanismele tradiționale de recrutare și salarizare prevăzute de legislația generală aplicabilă.

Domeniul securității cibernetice este caracterizat de o cerere globală ridicată pentru specialiști calificați, ceea ce determină un nivel salarial semnificativ mai mare decât cel din alte sectoare. Salariile medii ale experților în securitate cibernetică în Europa variază între 8.000 și 20.000 de euro brut lunar, depășind cu mult plafonul stabilit de Legea nr. 153/2017. În lipsa unui regim salarial competitiv, CRISCE riscă să nu poată atrage și reține specialiștii necesari pentru îndeplinirea atribuțiilor critice, expunând astfel sectorul energetic unor riscuri inacceptabile.

Regimul derogatoriu se justifică, de asemenea, prin cerințele suplimentare de specializare impuse de certificările internaționale și formările periodice obligatorii în domeniul securității cibernetice. Aceste certificări sunt esențiale pentru menținerea unui nivel ridicat de competență profesională, dar presupun costuri financiare și investiții semnificative din partea angajatorului.
Procesul standard de recrutare prevăzut de Codul Muncii nu răspunde nevoilor de urgență și specificitate ale CRISCE, deoarece:

- Procedurile de recrutare generală sunt rigide și nu permit adaptarea rapidă la evoluția nevoilor operaționale ale CRISCE;
- Recrutarea prin concursuri și evaluări standardizate limitează accesul la specialiști din mediul privat, unde criteriile de selecție sunt mult mai flexibile și orientate spre competențe practice.

În acest sens, derogările propuse permit implementarea unor mecanisme adaptate sectorului, inclusiv selecția pe bază de competențe certificate și experiență demonstrată în proiecte de securitate cibernetică.
În acest context, derogarea de la prevederile legii-cadru și stabilirea unor salarii conforme cu piața internațională și cu natura deosebit de specializată a activităților CRISCE reprezintă o necesitate obiectivă, care asigură atât competitivitatea, cât și performanța centrului. În absența unui astfel de nivel salarial, CRISCE riscă să piardă accesul la resurse umane critice, expunându-se vulnerabilităților în fața unor amenințări cibernetice care, prin natura lor, devin din ce în ce mai sofisticate și periculoase.

Cu privire la existența unor alte soluții derogatorii de la prevederile Legii-cadru nr. 153/2017 privind salarizarea personalului plătit din fonduri publice, cu modificările ulterioare, arătăm că prevederile art. 7 din proiectul de act normativ cuprinde soluții legislative adoptate și în vigoare în dreptul pozitiv, în alte în situații specifice, dintre care amintim:

a) *Ordonanța de Urgență a Guvernului nr. 104/2021 privind înființarea* ***Directoratului Național de Securitate Cibernetică***, aprobată prin Legea nr. 11/2022, cu modificările ulterioare - art. 13 alin. (4), art. 14 și art. 20 alin. (8^1);
Pentru claritate, citățm norma prevăzută la art. 20 alin. (8^1):
"*Prin derogare de la prevederile art. 16 alin. (1) din Legea-cadru nr. 153/2017 privind salarizarea personalului plătit din fonduri publice, cu modificările și completările ulterioare, personalul nominalizat în echipele proiectelor finanțate prin programe, instrumente, mecanisme, fonduri europene sau internaționale în care DNSC participă este plătit la tariful orar/zilnic/lunar specificat prin contractul de finanțare.* În cazul în care contractul de finanțare nu specifică tariful orar/zilnic/lunar, se utilizează plafoanele stabilite în Planul național de cercetare-dezvoltare și inovare aflat în vigoare."

b) *Ordonanța de urgență nr. 30/2022 privind unele măsuri pentru consolidarea capacității instituționale și administrative a Ministerului Cercetării, Inovării și Digitalizării și a* ***Autorității pentru Digitalizarea României*** *necesare implementării componentei C7 - Transformare digitală din Planul național de redresare și reziliență, precum și alte categorii de măsuri*, aprobată cu completări prin Legea nr. 43/2024 - art. 5, art. 7 și art. 13.

c) Ordonanța de urgență nr. 33/2007 privind organizarea și funcționarea **Autorității Naționale de Reglementare în Domeniul Energiei** - art. 7 alin. (3).
Pentru claritate, citățm norma menționată:
"*Prin excepție de la prevederile Legii-cadru nr. 284/2010 privind salarizarea unitară a personalului plătit din fonduri publice, cu modificările ulterioare, precum și de la legile anuale de salarizare a*

personalului plătit din fonduri publice, salarizarea personalului ANRE şi celelalte drepturi de personal, inclusiv drepturile băneşti şi cheltuielile de cazare pentru perioada delegării şi detaşării în altă localitate în interesul serviciului, se stabilesc prin negociere în cadrul contractului colectiv de muncă la nivelul ANRE şi al contractului individual de muncă."

d) Ordonanţa de urgenţă nr. 22/2009 *privind înfiinţarea* ***Autorităţii Naţionale pentru Administrare şi Reglementare în Comunicaţii,*** cu modificările şi completările ulterioare - art. 17 alin. (2) şi art. 18 alin. (4);

e) Legea concurenţei nr. 21/1996, cu modificările şi completările ulterioare - art. 14 alin. (1^3).
Pentru claritate, citãm norma menţionată:
" (1^3) Prin derogare de la prevederile art. 12 alin. (2) din Legea-cadru nr. 153/2017 privind salarizarea personalului plătit din fonduri publice, cu modificările şi completările ulterioare, **personalul Consiliului Concurenţei** care desfăşoară activităţi de examinare preliminară, analiză a unei plângeri şi investigare a unei posibile încălcări a dispoziţiilor art. 101 şi 102 din TFUE de către întreprinderi sau asocieri de întreprinderi, prin acte sau fapte care pot afecta comerţul dintre statele membre ale Uniunii Europene, avizare pentru legalitate a ordinelor şi deciziilor rezultate din acestea ori activităţi de reprezentare în litigiile generate de investigarea şi/sau luarea deciziilor în temeiul acestor dispoziţii beneficiază, pe parcursul derulării acestor activităţi, precum şi a activităţilor-suport desfăşurate în acest scop, de o majorare a salariilor de bază de la 15% până la 35%.

f) Ordonanţa de urgenţă nr. 109/2011 *privind guvernanţa corporativă a întreprinderilor publice*, aprobată cu modificări prin Legea nr. 111/2016, cu modificările şi completările ulterioare - art. 4^4 alin (2).
Pentru claritate, citãm norma menţionată:
" (2) Salarizarea **personalului AMEPIP** se realizează la nivelul maxim al drepturilor salariale prevăzut pentru funcţiile publice din cadrul aparatului de lucru al Guvernului, majorat cu 50%, prin derogare de la prevederile Legii-cadru nr. 153/2017 privind salarizarea personalului plătit din fonduri publice, cu modificările şi completările ulterioare."

g) Ordonanţa de urgenţă nr. 126/2005 privind reprezentarea României sau a instituţiilor publice în faţa Curţii de Arbitraj *Internaţionale a Centrului Internaţional pentru Reglementarea Diferendelor Relative la Investiţii şi în faţa altor instanţe judiciare şi arbitrale internaţionale*, cu modificările şi completările ulterioare - art. 3 alin. (1);
Pentru claritate, citãm norma menţionată
" (1) Prin derogare de la prevederile Legii-cadru nr. 153/2017 privind salarizarea personalului plătit din fonduri publice, cu modificările şi completările ulterioare, personalul de specialitate juridică din cadrul Direcţiei generale juridice a Ministerului Finanţelor, care are în fişa postului atribuţii în legătură cu asigurarea asistenţei şi reprezentării juridice în litigiile prevăzute la art. 1, personalul din cadrul Secretariatului General al Guvernului cu atribuţii în asigurarea suportului documentar şi arhivistic, respectiv a asistenţei juridice de specialitate, precum şi personalul de specialitate juridică asimilat judecătorilor şi procurorilor din cadrul Ministerului Justiţiei cu atribuţii în asigurarea asistenţei juridice de specialitate beneficiază de o majorare salarială de 50% aplicată la salariul de bază brut. Fişa postului trebuie să cuprindă atribuţii obiective cuantificabile în mod individual.".

h) Legea nr. 284/2024 *pentru realizarea capabilităţii operaţionale de apărare aeriană prevăzute în Concepţia de realizare a capabilităţii operaţionale de apărare aeriană cu avioane multirol de generaţia a V-a, în cadrul programului de înzestrare "Avion multirol de generaţia a V-a, F-35", Faza I, şi unele măsuri privind derularea contractelor Guvern la Guvern specifice Programului Foreign Military Sale* - art. 8 alin. (5);

Pentru claritate, citãm norma menţionată:
"(5) Prin derogare de la prevederile art. 1 alin. (3) din Legea-cadru nr. 153/2017, cu modificările şi completările ulterioare, pe perioada de derulare a contractelor prevăzute la art. 1 alin. (1) lit. a), personalului cu responsabilităţi în derularea şi implementarea acordurilor şi contractelor necesare pentru realizarea capabilităţii operaţionale prevăzute la art. 1 alin. (1) lit. a) i se acordă o majorare de până la 50% din solda de funcţie actualizată/salariul de bază actualizat, cu încadrarea în bugetul aprobat.

2.3 Schimbări preconizate

Proiectul de Ordonanţă de urgenţă pentru înfiinţarea şi operaţionalizarea Centrului de Răspuns la Incidente de Securitate Cibernetică în Energie (CRISCE) introduce o serie de schimbări esenţiale şi aduce inovaţii semnificative în gestionarea securităţii cibernetice în sectorul energetic din România. Drept obiectiv, prin această ordonanţă, se urmăreşte consolidarea protecţiei infrastructurilor critice energetice împotriva ameninţărilor cibernetice, având în vedere vulnerabilităţile actuale şi cerinţele stricte impuse de reglementările naţionale şi europene.
În conformitate cu reglementările naţionale şi europene, precum Ordonanţa de urgenţă nr. 155/2024 privind instituirea unui cadru pentru securitatea cibernetică a reţelelor şi sistemelor informatice din spaţiul cibernetic naţional civil şi Legea nr. 58/2023, care impun măsuri clare pentru protejarea infrastructurilor critice, proiectul de act normativ aduce inovaţii semnificative.
Acesta include crearea unei structuri de tip CSIRT sectorial, care va fi responsabilă de monitorizarea continuă, răspunsul la incidente, investigaţiile de tip forensic şi coordonarea măsurilor de securitate cibernetică la nivel naţional şi internaţional.
CRISCE va avea în componenţa sa un număr de posturi de specialişti, stabilit prin ordin al ministrului energiei, structurate pentru a asigura o acoperire completă a funcţiilor necesare. Aceste posturi includ funcţii de conducere, cum ar fi manager superior securitate cibernetică şi coordonator superior securitate cibernetică, precum şi funcţii de execuţie pentru experţi în diverse domenii ale securităţii cibernetice. Această structură organizatorică este esenţială pentru a răspunde eficient la ameninţările cibernetice şi pentru a implementa măsurile de securitate necesare.
CRISCE acţionează:
o ca o umbrelă pentru entităţile din sectorul energiei, contribuind prin:
o integrarea eforturilor de management al incidentelor de securitate cibernetică de la nivelul întregului sector (în caz de incidente corelate sau prezente în mai multe entităţi);
o sprijin şi facilitarea managementului incidentelor cibernetice din cadrul entităţilor din sector;
o coordonarea strategică a măsurilor de prevenţie şi răspuns la incidente cibernetice la nivel de sector;
o facilitarea construirii mecanismelor tehnice de securitate cibernetică (ex. macro sisteme de management integrat al securităţii cibernetice) care protejează în mod unitar întregul sector;
o sprijin către entităţi pentru recuperarea în caz de pagube produse de incidentele cibernetice, raportarea şi cooperarea cu CSIRT-ul naţional în caz de incidente cibernetice.
Însă, CRISCE nu asigură răspunderea juridică pentru entităţi; fiecare entitate îşi păstrează răspunderea juridică pentru implementarea mecanismelor şi a măsurilor de securitate cibernetică. CSIRT Energy vine doar ca un sprijin extern, cu viziune integrată, independent, obiectiv şi echidistant faţă de entităţile din sector.
- ca structură responsabilă de managementul intern al securităţii cibernetice din Ministerul Energiei.
- ca structură de politici şi proceduri interne de securitate cibernetică, în Ministerul Energiei.
- ca structură de punere în implementare a cerinţelor legislative şi de standardizare în domeniul securităţii cibernetice, cu aplicabilitate în domeniul energetic.
Analistul tehnic monitorizează SIEM şi asigură detecţia incidentelor.
Administratorul gestionează incidentele şi asigură reacţia rapidă.

Activitatea se desfăşoară în ture (1 tură = 12 ore). Într-o echipă de 4 persoane, fac cu schimbul doi câte doi.
Pentru menţinerea unui randament ridicat al echipelor din CSIRT, este necesar lucrul în reprize de max 2-3 ore per pereche de analist + administrator, urmat de perioadă de odihnă. Astfel, se asigură permanenţa 24/7 cu câte 2 specialişti activi (analist + administrator) apţi fizic şi intelectual să reacţioneze prompt.
Calculele din practică, arată că pentru asigurarea funcţionării de ture de 12 ore în acest ritm, este nevoie de minim 18 specialişti + 1 rezervă. Având în vedere că echipele sunt formate din 4 specialişti, prin urmare numărul minim este 20, care înseamnă 5 echipe. Concediile trebuie planificate strict.
(O simulare privind desfăşurătorul organizării turelor este prezentat în documentul "Model ture 12 ore x echipe de câte 4.csv").
o Specialist management proiecte IT - asigură coordonarea implementării proiectelor de dezvoltare.
o Arhitect integrator soluţii IT/OT/Cloud - asigură integrarea tuturor soluţiilor IT/OT/Cloud agreate la nivelul viitorului sistem de securitate cibernetică din sectorul energetic.
o Arhitect de securitate cibernetică - specializat în soluţii şi arhitecturi de securitate cibernetică.
o Specialist dezvoltare soluţii - asigură dezvoltarea de interfeţe, integrarea soluţiilor, funcţionarea personalizată pentru nevoile specifice ale CRISCE.
o Administrator de securitate cibernetică (pentru Minister) - asigură, în principal, protecţia infrastructurii Ministerului, din perspectivă de administrare (este complementar şi face echipă cu specialiştii din departamentul de administrare IT).
o 2x Specialişti forensic IT/OT (investigaţii, reverse engineering) - sunt specialiştii de bază care asigură analiza forensic a incidentelor identificate în Minister şi în industria energetică.
o Specialist strategii şi proceduri - abordează aspectele de strategie şi proceduri, inclusiv necesităţile de aliniere la reglementări şi standarde.
o Analist de securitate cibernetică (analiză, raportare, comunicare) - abordează aspectele de punere în practică a reglementărilor + comunicarea bottom-up (raportarea şi comunicările către management)
o Specialist managementul riscurilor - abordează din perspectivă strategică managementul riscurilor (mix de teorie cu expertiza provenită din zona practică)
o 2x Auditori de securitate cibernetică - gestionează monitorizarea conformităţii cu reglementările (verifică implementarea practică şi asigură dubla-verificare a măsurilor puse în practică)
Specialist R&D&I şi asimilare tehnologii emergente - monitorizează şi actualizează constant nevoile de evoluţie tehnologică + participă în proiectele de inovare şi update tehnologic (mix între cunoaşterea teoretică + evoluţia pieţei de profil + input din zona practică)
CRISCE va conţine cel puţin următoarele tipuri de posturi, astfel:
o CISO, cu rol de Director de Securitate Cibernetică – este responsabil cu managementul întregii structuri, raportarea directă către ministrul energiei şi reprezentarea CRISCE în interiorul şi exteriorul Ministerului Energiei.
o 5 echipe x 4 posturi operaţionale per tură
1 echipă = 2x (Analist tehnic + Administrator securitate)
Proiectul de Ordonanţă de urgenţă prevede că CRISCE va funcţiona sub directă şi nemijlocită subordine a ministrului energiei şi va colabora cu toate structurile organizatorice din cadrul Ministerului Energiei, precum şi cu entităţile din sectorul energetic. Acest cadru de colaborare este crucial pentru a asigura o gestionare integrată a securităţii cibernetice la nivel sectorial.
Art. 2 defineşte funcţiile principale ale CRISCE. În conformitate cu acest articol, CRISCE va îndeplini funcţiile de Computer Security Incident Response Team (CSIRT) la nivel sectorial. Aceasta presupune că CRISCE va monitoriza continuu reţelele şi sistemele informatice din sectorul energetic pentru a detecta şi răspunde la incidente de securitate cibernetică, precum şi pentru a coordona

răspunsul la incidentele majore şi pentru a furniza suport tehnic specializat în investigarea şi remedierea acestora. Importanţa acestui articol constă în clarificarea responsabilităţilor CRISCE, asigurând astfel un răspuns integrat şi coordonat la ameninţările cibernetice.
Articolul 3 descrie structura organizatorică a CRISCE, care va include un număr de posturi de specialişti stabilit prin ordin al ministrului energiei. Aceştia vor fi angajaţi cu contract individual de muncă pe perioadă determinată şi vor ocupă funcţii de coordonare şi execuţie. Funcţiile de conducere includ Manager Superior Securitate Cibernetică, Manager Securitate Cibernetică, Coordonator Superior Securitate Cibernetică şi Coordonator Securitate Cibernetică. Funcţiile de execuţie, împărţite în funcţii cu studii superioare şi studii medii, vor cuprinde experţi în diverse domenii ale securităţii cibernetice, cum ar fi analiza şi investigarea incidentelor, administrarea infrastructurilor, evaluarea impactului financiar şi dezvoltarea competenţelor.
Articolul 4 prevede evaluarea periodică a performanţelor profesionale ale specialiştilor din CRISCE, la fiecare 12 luni, pe baza unor criterii şi proceduri aprobate prin ordin al ministrului energiei. Evaluarea se va baza pe indicatori de performanţă, impact, realizare, produs şi rezultat. Aceasta asigură menţinerea unui nivel ridicat de competenţă şi eficienţă în cadrul CRISCE, motivând personalul să-şi îmbunătăţească continuu performanţele.
Articolul 5 detaliază atribuţiile specifice ale CRISCE. Printre acestea se numără intervenţia proactivă şi reactivă, în timp real, la atacurile cibernetice din sectorul energetic, monitorizarea continuă a reţelelor şi sistemelor informatice din sectorul energetic, detectarea şi analiza ameninţărilor şi vulnerabilităţilor cibernetice, implementarea şi actualizarea măsurilor de securitate cibernetică, coordonarea răspunsului la incidentele de securitate cibernetică, dezvoltarea şi menţinerea relaţiilor de colaborare cu alte CSIRT-uri şi instituţii relevante, realizarea de investigaţii forensice detaliate pentru a analiza urmele lăsate de atacatori şi pentru a înţelege pe deplin mecanismele de atac utilizate, şi protejarea proprie împotriva atacurilor cibernetice. Acest articol reglementează rolul complex şi multidimensional al CRISCE, necesar pentru a asigura o protecţie robustă şi cuprinzătoare a infrastructurilor energetice.
Articolul 5, alineatele (3) şi (5) din proiectul de Ordonanţă de Urgenţă reglementează atribuţiile specifice exercitate de CRISCE în vederea implementării Regulamentului delegat (UE) 2024/1366 al Comisiei, care completează Regulamentul (UE) 2019/943 al Parlamentului European şi al Consiliului prin stabilirea unui cod de reţea privind normele sectoriale pentru securitatea cibernetică a fluxurilor transfrontaliere de energie electrică (Codul de securitate cibernetică în energie).
Alineatul (3) din articolul 5 prevede că CRISCE are responsabilitatea de a implementa măsurile necesare pentru asigurarea conformităţii cu normele stabilite prin Codul de securitate cibernetică în energie, inclusiv monitorizarea şi protejarea fluxurilor transfrontaliere de energie electrică. În acest sens, CRISCE trebuie să colaboreze cu autorităţile şi operatorii de reţea din alte state membre ale Uniunii Europene pentru a coordona măsurile de securitate cibernetică în conformitate cu prevederile Codului. Aceste obligaţii sunt fundamentale pentru a asigura o coordonare eficientă la nivel european şi pentru a garanta că reţelele energetice din România sunt protejate împotriva atacurilor cibernetice care ar putea afecta stabilitatea energetică nu doar la nivel naţional, ci şi în contextul fluxurilor transfrontaliere. Adoptarea acestui cadru legislativ european impune implementarea unor măsuri coordonate şi uniforme, astfel încât să se asigure integritatea şi securitatea energetică într-un spaţiu interconectat, precum cel al Uniunii Europene.
Alineatul (5) din acelaşi articol reglementează atribuţiile CRISCE legate de monitorizarea şi evaluarea permanentă a riscurilor cibernetice în ceea ce priveşte fluxurile transfrontaliere de energie electrică. CRISCE are obligaţia de a elabora şi implementa politici şi proceduri pentru gestionarea riscurilor de securitate cibernetică, având ca obiectiv principal protecţia reţelelor şi sistemelor implicate în fluxurile de energie electrică la nivel transfrontalier. Această prevedere este deosebit de importantă, având în vedere faptul că fluxurile transfrontaliere sunt vulnerabile la atacuri cibernetice sofisticate, care pot avea consecinţe de amploare asupra stabilităţii energetice nu doar a României, ci şi a altor state membre interconectate. Implementarea acestui regulament european impune un

nivel ridicat de vigilență și cooperare internațională, asigurând că România contribuie activ la protejarea securității energetice europene, în conformitate cu standardele stabilite de Codul de securitate cibernetică în energie.
Această soluție legislativă, adoptată prin alineatele (3) și (5) ale articolului 5, este necesară pentru a respecta obligațiile asumate de România în calitate de stat membru al Uniunii Europene și pentru a asigura alinierea la reglementările europene privind securitatea cibernetică în sectorul energetic. Importanța acestei soluții constă în protejarea eficientă a rețelelor energetice transfrontaliere și în garantarea stabilității sistemului energetic național, într-un context internațional complex și interconectat.
În plus, CRISCE va fi autorizat prealabil de Directoratul Național de Securitate Cibernetică (DNSC) pentru a exercita funcția de echipă de răspuns la incidente (CSIRT) sectorială. Această funcție include elaborarea de strategii și proceduri de securitate cibernetică, monitorizarea conformității, evaluarea și auditarea măsurilor de securitate, precum și coordonarea răspunsului la incidente.
Potrivit articolului 5 alin. (7) din proiect, CRISCE va funcționa într-un imobil special destinat, diferit de sediul Ministerului Energiei. Imobilul va fi echipat cu sisteme avansate de securitate fizică și cibernetică, control al accesului, monitorizare video, sisteme de alimentare cu energie de backup, răcire și ventilare adecvată, rețea de comunicații redundantă, și alte dotări tehnice necesare pentru a asigura protecția și eficiența operațiunilor. Pentru un CSIRT sectorial precum CRISCE, amplasarea într-o clădire separată de sediul Ministerului Energiei este esențială din motive critice de securitate fizică și cibernetică, fiind necesară o izolare completă de vulnerabilitățile care ar putea compromite funcționarea și integritatea operațională a unui centru de securitate cibernetică de importanță strategică. Câteva argumente fundamentale care motivează această cerință sunt prezentate mai jos:
a) Un CSIRT sectorial necesită măsuri stricte de securitate fizică, deoarece infrastructurile și sistemele care monitorizează și răspund la incidente cibernetice sunt ținte potențiale pentru atacuri fizice care ar putea afecta grav continuitatea operațională. Într-o clădire separată, CRISCE poate implementa un control acces strict, zone securizate cu baricade fizice, și personal dedicat de securitate care să prevină orice acces neautorizat. Sediul Ministerului Energiei, cu personal și fluxuri administrative variate, nu poate asigura acest grad de control și securitate specific cerințelor unui centru de securitate cibernetică, ceea ce creează un risc de acces necontrolat în proximitatea unor informații și sisteme critice.
b) Din perspectivă tehnică, amplasarea CRISCE într-un imobil separat și specializat este fundamentată pe cerințele de securitate cibernetică avansată, specifice unui CSIRT sectorial care protejează infrastructura energetică națională. Un exemplu concret îl constituie utilizarea Camerei Faraday, o tehnologie esențială în securitatea comunicațiilor și echipamentelor cibernetice. O astfel de cameră blochează complet câmpurile electromagnetice din exterior, prevenind orice tentativă de interceptare sau influență externă asupra comunicațiilor și echipamentelor electronice. Implementarea unei camere Faraday este imposibilă într-un mediu administrativ comun, cum este sediul Ministerului Energiei, care nu poate fi izolat corespunzător din punct de vedere electromagnetic fără a afecta alte activități și fluxuri operaționale ale ministerului.
c) Într-un centru de securitate cibernetică, securitatea comunicațiilor este de o importanță crucială, iar interferențele electromagnetice și riscul de interceptare a semnalelor radio pot compromite grav operațiunile. O clădire separată permite implementarea unor măsuri speciale de izolare a semnalelor, protecție împotriva atacurilor de tip „emanation" (extracția datelor din echipamentele electronice prin captarea radiațiilor electromagnetice) și protecția împotriva atacurilor radio care pot influența comunicațiile și echipamentele din cadrul CRISCE. Fără această izolare, un atac sofisticat ar putea afecta capabilitățile de monitorizare, analiză și răspuns ale CRISCE, creând riscuri mari de vulnerabilitate pentru întreg sectorul energetic.
d) Amplasarea într-un imobil separat permite CRISCE să își asigure independența operațională, cu dotări redundante precum surse alternative de energie (UPS și generatoare de rezervă) și rețele de comunicații independente de infrastructura Ministerului Energiei. Astfel, CRISCE poate continua să

funcționeze în caz de întrerupere a rețelelor principale sau de atac cibernetic asupra sediului central al ministerului. Într-o criză cibernetică, continuitatea și reziliența operațională sunt vitale, iar dependența de infrastructura comună a ministerului ar crește vulnerabilitatea în fața atacurilor menite să dezactiveze simultan atât ministerul, cât și capacitatea de răspuns a CRISCE.

e) Într-un centru de securitate cibernetică de importanță strategică, cum este CRISCE, există riscul de interceptare a comunicațiilor interne și a sistemelor prin echipamente avansate care pot capta sau altera datele critice transmise. Într-un sediu separat, CRISCE poate utiliza tehnologie de comunicații securizate, inclusiv telefoane criptate, sisteme de videoconferință și echipamente de comunicații izolate, astfel încât să reducă drastic riscul de interceptare și influență externă. Într-o clădire comună cu ministerul, ar fi mult mai greu să se evite interceptările, întrucât orice acces neautorizat în spațiile ministerului ar putea oferi oportunitatea unui atac indirect asupra CRISCE.

f) Partajarea infrastructurii IT sau a rețelelor de comunicații în aceeași clădire crește riscul ca eventualele vulnerabilități ale rețelei ministerului să fie exploatate și propagate în rețeaua CRISCE. Separarea fizică a echipamentelor și rețelelor asigură segmentarea strictă a rețelei, prevenind astfel contaminarea accidentală cu malware sau atacuri care pot exploata conexiuni comune sau puncte de intrare partajate. În acest context, segmentarea oferită de o clădire separată este esențială pentru a reduce expunerea la atacuri cibernetice ce vizează vulnerabilități la nivel de infrastructură comună.

g) În situații de criză cibernetică, un CSIRT sectorial necesită un spațiu de gestionare a crizelor (situation room) unde echipa să poată coordona răspunsul la incidente în condiții de maximă confidențialitate și securitate. Acest tip de spațiu, destinat gestionării incidentelor cibernetice și organizării măsurilor de contracarare, nu poate funcționa eficient în spațiile administrative comune, întrucât necesita acces restricționat și izolare completă față de alte activități administrative ale ministerului.

h) Prin urmare, un sediu separat pentru CRISCE nu doar că îndeplinește cerințele de securitate cibernetică specifice unui CSIRT sectorial, dar și consolidează reziliența și capacitatea de protecție a acestuia împotriva atacurilor fizice, radio și cibernetice, asigurându-se că infrastructura critică a sectorului energetic rămâne protejată și funcțională în orice condiții. Această izolare permite menținerea unor standarde de securitate deosebit de ridicate, critice pentru protejarea datelor sensibile și prevenirea oricăror interferențe care ar putea periclita siguranța întregului sector energetic și capacitatea națională de răspuns la crize cibernetice.

Facem precizarea fermă că, prin aceast proiect de act normativ, nu se modifică sediul social al Ministerului Energiei.

Proiectul de act normativ introduce dispoziții specifice care modifică și completează regimul general al raporturilor de muncă, astfel:

- Flexibilitatea procedurii de recrutare și selecție

Codul Muncii prevede un proces rigid și uniform pentru ocuparea posturilor, bazat pe concursuri și alte proceduri standardizate. În cazul CRISCE, derogările permit utilizarea unor metode de recrutare adaptate specificului domeniului de securitate cibernetică, bazate tot pe concurs, dar cu criterii mai stricte reglementate prin ordin de ministru. Astfel, personalul poate fi selectat pe baza unor criterii de competență tehnică și certificări profesionale internaționale (ex.: CISSP, CEH), eliminând barierele care ar întârzia procesul de ocupare a posturilor critice.

- Durata determinată a contractelor de muncă

Derogările permit încheierea de contracte de muncă pe durată determinată, fără limitările stricte impuse de Codul Muncii, pentru a permite angajarea unor specialiști pentru proiecte specifice sau intervenții punctuale. Această flexibilitate este indispensabilă pentru a răspunde rapid la amenințările cibernetice emergente.

- Regimul specific al încetării raporturilor de muncă

Proiectul introduce reguli adaptate pentru evaluarea performanţelor şi încetarea raporturilor de muncă în cazul neîndeplinirii indicatorilor de performanţă specifici, aspect care depăşeşte regimul standard de răspundere disciplinară prevăzut de Codul Muncii. Această abordare asigură menţinerea unui nivel ridicat de competenţă şi eficienţă operaţională.
Proiectul de act normativ instituie un regim derogatoriu clar pentru salarizarea personalului CRISCE, introducând următoarele noutăţi:

- Stabilirea unui regim salarial competitiv

Salariile personalului CRISCE sunt reglementate printr-o anexă specială cu grila de salarizare prevăzută de Legea nr. 153/2017, fiind stabilite în funcţie de specificul posturilor, nivelul de calificare şi competenţele tehnice avansate ale angajaţilor. Această completare permite oferirea unor pachete salariale care să reflecte realitatea pieţei internaţionale de securitate cibernetică, unde salariile sunt semnificativ mai mari decât cele din sectorul public românesc.

- Actualizarea periodică a salariilor

Proiectul prevede mecanisme de actualizare automată a salariilor, în funcţie de evoluţia pieţei muncii, performanţele angajaţilor şi modificările salariului mediu brut pe economie. Această flexibilitate asigură competitivitatea continuă a CRISCE pe piaţa muncii şi previne pierderea personalului calificat în favoarea sectorului privat sau a instituţiilor internaţionale.

- Corelarea cu cerinţele internaţionale

Derogările permit salarizarea personalului CRISCE la un nivel care să atragă şi să reţină experţi cu certificări internaţionale şi experienţă în proiecte complexe de securitate cibernetică. Aceasta reflectă bunele practici din alte state membre UE, unde structurile CSIRT sectoriale au regimuri salariale derogatorii pentru a răspunde nevoilor operaţionale specifice.
Noutatea fundamentală adusă de aceste derogări constă în crearea unui regim juridic adaptat exclusiv necesităţilor CRISCE, care:

- îmbunătăţeşte capacitatea de reacţie rapidă la ameninţările cibernetice;
- Asigură competitivitatea pe piaţa muncii prin atragerea specialiştilor necesari;
- Evită blocajele administrative care ar putea apărea din aplicarea regimului general al Codului Muncii şi al Legea nr. 153/2017, cu modificările şi completările ulterioare.

Articolul 6 prevede şi finanţarea şi resursele necesare pentru funcţionarea CRISCE. Cheltuielile de organizare şi funcţionare, inclusiv cheltuielile de personal, sunt considerate cheltuieli administrative în sensul art. 8 alin. (2) din OUG nr. 60/2022 şi vor fi finanţate exclusiv din dobânzile acumulate în conturile Ministerului Energiei. De asemenea, activitatea CRISCE va fi finanţată şi din veniturile proprii obţinute din activităţile de prestări servicii de securitate cibernetică în condiţiile art. 8 din proiectul de act normativ.
Tot la Art. 6, pentru buna funcţionare a CRISCE, este esenţială derogarea de la prevederile articolelor II-IV din OUG nr. 34/2023. Aceste derogări sunt fundamentale pentru a asigura resursele materiale, umane şi financiare necesare unui centru care va juca un rol strategic în securitatea cibernetică a sectorului energetic naţional, mai ales având în vedere complexitatea şi specificul funcţiilor pe care le va îndeplini. În primul rând, derogarea de la articolul II, care interzice achiziţionarea sau închirierea de autoturisme, mobilier şi aparatură birotică, este indispensabilă pentru dotarea iniţială a CRISCE. Fiind o instituţie nou-înfiinţată, centrul necesită mijloace materiale adecvate pentru a-şi desfăşura activitatea în mod eficient. În absenţa acestei derogări, CRISCE nu ar putea asigura infrastructura necesară pentru birouri, echipamente IT, sisteme de monitorizare şi analiză cibernetică, precum şi mijloace de transport esenţiale pentru intervenţii rapide în cazul unor incidente de securitate. Spre deosebire de alte instituţii deja existente, care pot redistribui resurse, CRISCE are nevoie de echipamente specifice pentru a răspunde cerinţelor tehnologice complexe din domeniul cibernetic. De asemenea, derogarea de la articolul III, care impune reducerea cu 10% a cheltuielilor

pentru bunuri şi servicii, este vitală pentru a permite CRISCE să îşi aloce bugetul necesar funcţionării în primele etape. Reducerea cheltuielilor la o instituţie nou-creată ar crea blocaje operaţionale majore, limitând accesul la servicii esenţiale precum mentenanţa infrastructurii IT, formarea personalului şi achiziţia licenţelor pentru software-uri avansate de securitate cibernetică. În plus, având în vedere că CRISCE are ca misiune protejarea unor infrastructuri critice din sectorul energetic, orice restricţie bugetară în acest sens ar compromite capacitatea sa de a reacţiona adecvat la incidente cibernetice care ar putea avea consecinţe economice şi sociale semnificative. Nu în ultimul rând, derogarea de la articolul IV, care suspendă ocuparea posturilor vacante sau temporar vacante, este esenţială pentru a permite angajarea rapidă a personalului calificat necesar operaţionalizării CRISCE. Structura instituţională a CRISCE impune angajarea de experţi în securitate cibernetică, analişti de date, tehnicieni şi specialişti în gestionarea crizelor, competenţe care nu pot fi asigurate doar prin redistribuirea personalului din alte structuri publice. În contextul actual, marcat de un deficit de specialişti în domeniul securităţii cibernetice, organizarea de concursuri şi recrutarea rapidă devin cruciale pentru funcţionalitatea centrului. Lipsa unei derogări ar întârzia în mod semnificativ procesul de recrutare, afectând negativ obiectivele de securitate energetică. Mai mult decât atât, derogările propuse ar asigura faptul că CRISCE poate accesa fonduri europene şi implementa proiecte de securitate fără a fi supus restricţiilor bugetare sau operaţionale care ar întârzia utilizarea acestor resurse. Misiunea centrului include colaborarea cu entităţi internaţionale şi participarea la reţele de securitate cibernetică, ceea ce necesită o flexibilitate administrativă şi financiară incompatibilă cu prevederile restrictive din OUG 34/2023. Un alt risc semnificativ îl constituie imposibilitatea aplicării coerente a actului normativ de înfiinţare. Fără derogările necesare, actul normativ devine inaplicabil, ceea ce poate genera situaţii de blocaj instituţional. În lipsa dotărilor, finanţării şi personalului, CRISCE nu ar putea îndeplini obiectivele pentru care a fost creat, iar consecinţele ar include pierderea credibilităţii internaţionale a României în sectorul securităţii energetice şi expunerea infrastructurilor critice la riscuri cibernetice necontrolate. În concluzie, derogările de la articolele II-IV din OUG nr. 34/2023 sunt imperative pentru a garanta funcţionarea optimă şi operaţionalizarea rapidă a CRISCE. Prin eliminarea acestor restricţii, centrul va avea capacitatea să-şi îndeplinească obiectivele strategice, să răspundă prompt incidentelor cibernetice şi să contribuie în mod eficient la protecţia infrastructurilor critice din sectorul energetic naţional. Aceasta nu este doar o necesitate administrativă, ci şi o cerinţă strategică pentru securitatea naţională.

Articolul 8 reglementează faptul că Ministerul Energiei, prin CRISCE, poate realiza venituri din prestaţii de servicii de securitate cibernetică, în limitele atribuţiilor şi activităţilor prevăzute la art. 5, persoanelor fizice şi juridice de drept public sau privat din sectorul energetic. Serviciile şi tarifele se stabilesc în baza unei metodologii de calcul realizată în baza unor standarde de cost stabilite prin ordin al ministrului energiei, cu avizul prealabil şi conform al DNSC şi al Consiliului Concurenţei, care se publică în Monitorul Oficial al României, Partea I. Tarifele reglementate din sectorul energetic aferente costurilor cu auditul de securitate cibernetică, pentru serviciile prestate de CRISCE către operatorii economici se recuperează prin tarife de reţea sau alte mecanisme similare stabilite de prevederile legale aplicabile, potrivit Regulamentului delegat UE 2024/1366. Sumele încasate din sursele prevăzute la alin. (1) se reţin integral ca venituri proprii, cu titlu permanent, la dispoziţia Ministerului Energiei şi vor fi folosite în conformitate cu prevederile bugetului de venituri şi cheltuieli al ministerului, conform clasificaţiei bugetare distincte, pentru funcţionarea, organizarea şi dezvoltarea CRISCE. Prin excepţie, prestarea serviciilor către Ministerul Energiei, unităţile din sectorul energetic aflate în subordinea sau sub autoritatea Ministerului Energiei sau ale altor organe de specialitate ale administraţiei publice centrale, beneficiarii proiectelor finanţate prin Fondul pentru Modernizare, către Centrul Naţional de Coordonare din cadrul Organismului intermediar pentru promovarea societăţii informaţionale din cadrul Autorităţii pentru Digitalizarea României, precum şi către operatorii naţionali de transport al energiei electrice şi al gazelor naturale se realizează cu titlu gratuit.

La articolul 9 se reglementează faptul că, pentru înființarea, funcționarea, organizarea și dezvoltarea CRISCE, se înființează pe lângă Ministerul Energiei o activitate finanțată integral din venituri proprii. Veniturile proprii ale activității prevăzute la alin. (1) se constituie din contravaloarea în lei a sumelor primite din prestarea serviciilor de securitate cibernetică prestate în temeiul art. 8, precum și din dobânzile prevăzute la art. 8 alin. (4[1]) din Ordonanța de urgență a Guvernului nr. 60/2022, aprobată cu completări prin Legea nr. 376/2023, cu modificările și completările ulterioare, și virate în contul de venituri al activității deschis la Activitatea de Trezorerie și Contabilitate Publică a Municipiului București pe numele Ministerului Energiei și se aprobă la o subdiviziune distinctă de venituri bugetare și se înregistrează ca venituri ale bugetului respectiv la data transferului sumelor în lei în contul de trezorerie. Cheltuielile aferente îndeplinirii activității se suportă și din veniturile proprii. Bugetul de venituri și cheltuieli pentru activitatea finanțată integral din venituri se întocmește la venituri pe surse de proveniență, iar la cheltuieli după natura și destinația acestora, potrivit clasificației bugetare și se aprobă în anexă distinctă la bugetul Ministerului Energiei. Excedentul anual rezultat din execuția bugetului de venituri și cheltuieli se reportează în anul următor și se utilizează cu aceleași destinații.

Articolele 10 - 11 din proiectul de ordonanță de urgență aduc soluții legislative fundamentale pentru protejarea datelor, confidențialității și drepturilor persoanelor implicate în colectarea, prelucrarea și transmiterea datelor necesare pentru îndeplinirea atribuțiilor CRISCE, în conformitate cu cadrul european și național de protecție a datelor cu caracter personal. Aceste soluții sunt esențiale pentru a asigura o implementare conformă cu normele UE și respectarea drepturilor fundamentale, consolidând funcționarea eficientă și responsabilă a CRISCE.

Articolul 10 completează acest cadru de protecție prin dispoziții specifice care asigură că prelucrarea datelor cu caracter personal se desfășoară în strictă conformitate cu Regulamentul (UE) 2016/679 (RGPD) și reglementările naționale relevante. CRISCE va fi autorizată să prelucreze date cu caracter personal doar în limitele necesare pentru prevenirea și răspunsul la incidentele de securitate cibernetică, respectând drepturile persoanelor și garantând confidențialitatea. Notificările realizate în temeiul prezentei ordonanțe de urgență, în special cele care privesc incidentele de securitate, vor respecta obligațiile operatorilor de date prevăzute de RGPD, asigurând astfel o protecție juridică riguroasă a drepturilor persoanelor. Această soluție legislativă este indispensabilă pentru conformitatea activităților CRISCE cu standardele UE de protecție a datelor, oferind un cadru clar și strict de prelucrare a datelor.

Articolul 11 extinde și consolidează respectarea drepturilor fundamentale prin precizarea explicită că ordonanța de urgență nu afectează legislația națională privind protecția datelor cu caracter personal și asigură conformitatea cu Carta drepturilor fundamentale a Uniunii Europene. Acest articol reiterează că orice acțiuni desfășurate de CRISCE vor fi în conformitate cu dreptul la viață privată și la protecția datelor, precum și cu prevederile relevante din legislația națională, precum Legea nr. 506/2004 și Legea nr. 190/2018. Aceste dispoziții sunt fundamentale pentru a alinia funcționarea CRISCE cu angajamentele României în materie de protecție a drepturilor omului și de respectare a normelor internaționale privind confidențialitatea și viața privată, asigurând că activitatea CRISCE este desfășurată în cadrul unor limite juridice clare și responsabile.

Prin aceste articole, proiectul de ordonanță de urgență se stabilește un echilibru esențial între cerințele de securitate cibernetică și respectarea drepturilor și libertăților fundamentale, oferind un cadru de protecție juridică atât pentru datele colectate, cât și pentru persoanele implicate. Măsurile introduse garantează că funcționarea CRISCE va fi aliniată cu reglementările europene și naționale, consolidând protecția datelor și încrederea în utilizarea responsabilă a acestora în sectorul de securitate cibernetică. Aceste soluții legislative contribuie, astfel, la consolidarea unui sistem de securitate robust, respectuos față de drepturile fundamentale ale cetățenilor și conforme cu angajamentele internaționale ale României.

Articolul 13 din proiectul de Ordonanță de urgență reglementează modificările și completările aduse Ordonanței de Urgență a Guvernului nr. 60/2022, care stabilește cadrul instituțional și financiar pentru implementarea și gestionarea fondurilor alocate României prin Fondul pentru modernizare.
O modificare importantă este dată de introducerea unei delegări către Banca de Investitii și Dezvoltare S.A. (BID) de atribuții privind implementarea și/sau administrarea de instrumente financiare finanțate din fonduri naționale/europene/de modernizare, precum și implementarea oricăror forme de sprijin financiar destinate investitiilor pentru crearea, dezvoltarea și/sau modernizarea infrastructurii din domeniul energiei. În situația în care organismul delegat este BID, acordul de delegare va avea ca obiect exclusiv încredințarea atribuțiilor definite la art. 1 alin (22) și se încheie între Ministerul Energiei, Ministerul Finanțelor și BID.
De asemenea, se introduce definiția Banca de Investiții și Dezvoltare SA (BID), respectiv, organism delegat ce are rol de Intermediar Financiar, astfel cum acesta este definit la art. 2 pct. 34 din Regulamentul (UE) nr. 651/2014 al Comisiei, căruia îi pot fi încredințate exclusiv atribuții de implementare și/sau administrare de instrumente financiare sau alte forme de sprijin financiar, inclusiv granturi, finanțate din Fondul pentru modernizare.
Pot fi delegate către BID exclusiv atributii de implementare și/sau administrare de instrumente financiare sau alte forme de sprijin financiar, inclusiv granturi, finanțate din Fondul de modernizare.
Se statuează că documentația aferentă oricărui proiect de măsură susceptibilă a reprezenta ajutor de stat sau ajutor de minimis, inclusiv prenotificarea sau notificarea Comisiei Europene, cu privire la finantarile din Fondul pentru modernizare nu este în responsabilitatea BID, avand în vedere calitatea acesteia de Intermediar Financiar, astfel cum acesta este definit la art. 2 pct. 34 din Regulamentul (UE) nr. 651/2014 al Comisiei.
De asemenea, articolul 13 prevede că, la articolul 8 alin. (2) din O.U.G. nr. 60/2022 se introduc și modifică mai multe tipuri de cheltuieli administrative eligibile în cadrul Fondului pentru modernizare, inclusiv cheltuieli pentru activități de management, evaluare și control, necesare pentru implementarea Fondului. Printre acestea se numără și cheltuieli pentru asistență tehnică, care pot include angajarea de personal, atât în cadrul organigramei, cât și în afara acesteia, pe perioadă determinată, pentru a asigura implementarea proiectelor finanțate din Fondul pentru modernizare.
De asemenea, articolul introduce posibilitatea finanțării tuturor cheltuielilor administrative necesare pentru înființarea, organizarea și funcționarea Centrului de Răspuns la Incidente de Securitate Cibernetică în Energie (CRISCE).
O modificare privește activitatea Ministerului Transporturilor și Infrastructurii care este organism delegat pentru gestionarea sectorului eficiență energetică, subsector transporturi pentru investițiile finanțate din Fondul pentru modernizare, sens în care s-a propus ca fiind necesar și oportun ca și personalul Ministerului Transporturilor și Infrastructură implicat în gestionarea și implementarea investițiilor cu finanțare FM să beneficieze de aceste stimulente financiare, ținând cont de gradul de complexitate al procesului de programare/implementare. Gradul de complexitate al procesului de programare/implementare se referă la întreg setul de activități de elaborare și avizare a ghidurilor, de organizare a competițiilor de proiecte, de evaluare a proiectelor și de monitorizare a acestora.
Menționăm că valoarea totală a proiectelor care pot fi finanțate prin Fondul pentru Modernizare în România este estimată la aproximativ 15 miliarde de euro până în anul 2030. În acest context, angajații organismelor delegate/ Ministerului Energiei poartă o răspundere imensă asupra corectitudinii, eficienței și eficacității absorbție, fiind remunerați, din cauza restricțiilor financiar-bugetare, sub valoarea muncii lor. De aceea, pentru a asigura un tratament egal tuturor implementărilor proiectelor finanțate prin FM, s-a propus ca stimulentul să se acorde tuturor organismelor delegate, nu doar Ministerului Energiei.
O altă modificare privește modificarea propusă la articolul 13 din OUG nr. 60/2022, prin introducerea alineatelor (6) și (7), care este justificată de necesitatea armonizării cadrului legislativ național cu prevederile aplicabile la nivel european, în special cele reglementate de articolul 28 din Ordonanța de Urgență nr. 23/2023, inclusiv o normă tranzitorie privind aplicarea modificărilor și

pentru contractele de finanațare aflate în derulare. Aceste dispoziții oferă cadrul legal necesar pentru o monitorizare riguroasă a implementării proiectelor, menținând totodată un echilibru între flexibilitatea financiară a beneficiarilor și necesitatea de a proteja interesul public. În plus, adoptarea acestor prevederi contribuie la asigurarea unui cadru juridic coerent, adaptat nevoilor reale ale beneficiarilor și cerințelor de implementare rapidă a investițiilor strategice. În contextul actual, caracterizat de urgența implementării proiectelor energetice pentru a sprijini tranziția verde și securitatea energetică a României, modificarea legislativă propusă devine indispensabilă pentru a răspunde exigențelor practice ale beneficiarilor și pentru a garanta utilizarea eficientă a fondurilor alocate prin Fondul pentru Modernizare. Totodată, această măsură susține obiectivele Pactului Verde European, integrându-se în eforturile naționale și europene de tranziție către o economie sustenabilă și rezilientă.

De asemenea se propune modificarea și completarea art. XLIV din Ordonanța de urgență nr. 107/2024 pentru reglementarea unor măsuri suri fiscal-bugetare în domeniul gestionării creanțelor bugetare și a deficitului bugetar pentru bugetul general consolidat al României în anul 2024, precum și pentru modificarea și completarea unor acte normative, după cum urmează:

"(1) Autoritățile de management ale programelor operaționale pentru perioada de programare 2021-2027 sau, după caz, coordonatorii de reformă/investiții ai Planului național de redresare și reziliența, organismul delegat pentru sectorul eficiență energetică, subsectorul transporturi al Fondului pentru Modernizare, stabiliți potrivit legii, pot încheia contracte/acte adiționale la contractele de finanțare încheiate cu beneficiarii pentru infrastructura de transport feroviar și/sau pentru infrastructura de transport cu metroul, cu avizul Ministerului Finanțelor, în limita sumelor disponibil a fi alocate provenind din împrumuturi contractate de România din emisiunile de obligațiuni verzi, pentru a asigura finanțarea categoriilor de cheltuieli neeligibile, a cofinanțărilor sau, după caz, a finanțării publice naționale, a contribuției proprii aferente Fondului pentru Modernizare sau oricăror alte categorii de cheltuieli stabilite potrivit legii cu respectarea legislației privind datoria publică și a Hotărârii Guvernului nr. 83/2024 privind aprobarea Cadrului referitor la finanțarea unor proiecte care sunt destinate protejării mediului înconjurător și combaterii schimbărilor climatice și doar în limita creditelor de angajament și a creditelor bugetare alocate cu această destinației prin legea bugetului de stat."

"(11) În situația prevăzută la alin. (1), se va avea în vedere principiul respectării specialității surselor bugetare prin mențiunea contabilității separate pe fiecare sursă".

Având în vedere că acest articol face referire doar la cofinanțarea aferentă proiectelor finanțate din Politica de Coeziune și PNRR, Ministerul Transporturilor și Infrastructurii a solicitat includerea susținerii cofinanțării/ a contribuției beneficiarului din subordinea ministerului care a transmis și a primit aprobare Băncii Europene pentru proiecte finanțate din Fondul pentru Modernizare. Suplimentar, este necesară acoperirea cheltuielilor aferente sistemului de siguranță și automatizare pe cale pentru linia de metrou M4, în valoare de 32.504.955 euro. Valoarea totală a investiției este de 165.152.450,42 euro TVA inclus, 132.647.495,42 EUR fiind suma aprobată din fondul pentru Modernizare.

În funcție de tipul proiectelor individuale propuse la finanțare din FM, va fi necesară asigurarea cofinanțării/ costurile neeligibile din FM din obligațiuni sau alte surse de finanțare europene sau buget de stat.

Această soluție legislativă a fost adoptată din considerente practice și juridice care derivă din necesitatea de a asigura resurse suficiente și sigure pentru administrarea și gestionarea eficientă a Fondului pentru modernizare, dar și pentru consolidarea capacităților de securitate cibernetică în sectorul energetic, inclusiv pentru rețelele și sistemele informatice rezultate din proiectele finanțate prin Fondul pentru Modernizare. În contextul tranziției energetice și al interconectării rețelelor energetice la nivel european, protecția împotriva riscurilor cibernetice este esențială pentru stabilitatea și siguranța acestor sisteme. Astfel, alocarea unui procent din fondurile Fondului pentru modernizare pentru cheltuielile administrative necesare funcționării CRISCE vine ca o măsură de

suport pentru a proteja infrastructurile energetice critice de potențiale atacuri cibernetice și de alte amenințări cibernetice emergente, ca parte a politicii naționale de patriotism energetic.
Modificarea propusă la art. 16 drin proiectul de act normativ, ce prevede introducerea unei derogări limitate pentru Ministerul Energiei de la aplicabilitatea unor prevederi din capitolul III al Legii nr. 296/2023, este fundamentată pe specificitatea și urgența nevoilor asociate înființării, organizării și funcționării CRISCE. Această modificare este indispensabilă pentru a asigura îndeplinirea obligațiilor naționale și internaționale ale României în domeniul securității cibernetice și pentru a proteja infrastructurile critice din sectorul energetic. Spre deosebire de derogările generale incluse în Legea nr. 296/2023 pentru alte instituții, modificarea propusă prin proiectul de act normativ limitează aplicabilitatea derogării exclusiv la activitățile aferente înființării, organizării și funcționării CRISCE. Scopul acestei derogări este de a permite centrului să funcționeze la parametrii necesari pentru protejarea infrastructurilor critice și pentru integrarea în rețelele internaționale de cooperare cibernetică. CRISCE va fi prima structură sectorială de acest tip din România dedicată exclusiv securității cibernetice a sectorului energetic, un domeniu esențial pentru siguranța națională.
Funcționarea eficientă a centrului necesită un regim juridic special care să asigure:
a) Alocarea resurselor financiare și umane necesare, fără constrângeri financiare disproportionate.
b) Flexibilitatea operațională pentru a răspunde rapid și eficient amenințărilor cibernetice.
c) Integrarea cu sisteme internaționale de monitorizare și prevenire a incidentelor cibernetice.
Sectorul energetic este unul dintre cele mai expuse atacurilor cibernetice, fiind țintă pentru atacuri complexe care vizează infrastructuri critice precum sistemele SCADA și ICS. Lipsa resurselor necesare și a capacităților specifice de răspuns ar expune România la riscuri semnificative, inclusiv:
a) Întreruperi ale furnizării de energie electrică sau gaze naturale.
b) Prejudicii financiare majore pentru operatorii economici din domeniu.
c) Vulnerabilități la nivel național, cu impact asupra stabilității economice și sociale.
CRISCE va avea un rol crucial în prevenirea și gestionarea acestor riscuri, dar pentru a-și îndeplini atribuțiile, derogarea este esențială.
Directiva NIS2 impune statelor membre să asigure funcționarea unor structuri sectoriale capabile să protejeze infrastructurile critice de atacurile cibernetice. Derogarea propusă sprijină alinierea legislației naționale cu aceste cerințe prin:
a) Permisiunea de a aloca resursele necesare pentru achiziționarea de echipamente și tehnologii specifice (platforme de threat intelligence, firewall-uri avansate, soluții de criptare).
b) Acordarea unor drepturi salariale competitive pentru a atrage personal cu înaltă calificare.
c) Permisiunea integrării rapide în rețelele internaționale de cooperare, care impun standarde tehnice și operaționale ridicate.
Derogarea în raport cu capitolul III al Legii nr. 296/2023 este motivată de următoarele elemente concrete:
1. Art. XXIV – Limitarea cheltuielilor cu bunuri și servicii
Derogarea permite achiziționarea de tehnologii critice pentru securitatea cibernetică, care nu pot fi limitate la plafonările bugetare generale. Aceste achiziții includ:

- Sisteme de prevenire a intruziunilor (IPS/IDS);
- Camere Faraday pentru protecția comunicațiilor interne;
- Licențe software și echipamente hardware avansate.

2. Art. XXVI – Restricții privind angajările
În absența derogării, CRISCE nu ar putea angaja specialiști certificați internațional (ex.: CISSP, CEH, GCIH) necesari pentru îndeplinirea funcțiilor sale. Derogarea permite recrutarea rapidă, prin proceduri flexibile, a personalului esențial.
3. Art. XXVII – Limitarea cheltuielilor de personal

Sectorul securității cibernetice este extrem de competitiv pe piața muncii, iar salariile oferite de sectorul public conform grilelor standard din Legea nr. 153/2017 sunt insuficiente pentru a atrage personal calificat. Derogarea permite stabilirea unor pachete salariale compatibile cu piața internațională a muncii.
Modificarea a fost analizată în cadrul procedurii de avizare interministerială, iar Ministerul Finanțelor a emis un aviz cu observații care au fost integrate în Nota de fundamentare. Ministerul Finanțelor a recunoscut necesitatea derogării în contextul specific al activităților CRISCE, subliniind că măsura este proporțională și nu afectează sustenabilitatea bugetară generală, CRISCE fiind exclusiv finanțat prin dobânzile aferente Fondului pentru Modernizare și din venituri proprii reprezentând venituri din prestarea de servicii de securitate cibernetică.
Adoptarea modificării propuse este urgentă pentru a permite operaționalizarea CRISCE în conformitate cu obligațiile internaționale ale României și pentru a respecta termenele impuse de legislația europeană. În lipsa acestei derogări, capacitatea României de a proteja infrastructurile critice energetice ar fi grav afectată, cu consecințe negative asupra securității naționale.
În contextul proiectului de act normativ privind înființarea, organizarea și funcționarea Centrului de Răspuns la Incidente de Securitate Cibernetică în Energie (CRISCE), derogarea de la prevederile art. I-II, IV, VII și XV din Ordonanța de urgență nr. 156/2024 *privind unele măsuri fiscal-bugetare în domeniul cheltuielilor publice pentru fundamentarea bugetului general consolidat pe anul 2025, pentru modificarea și completarea unor acte normative, precum și pentru prorogarea unor termene* este fundamentată pe specificitatea atribuțiilor și nevoilor critice ale CRISCE. Această derogare este indispensabilă pentru asigurarea funcționării eficiente a centrului, în contextul protecției infrastructurilor critice energetice și respectării angajamentelor internaționale în domeniul securității cibernetice.
CRISCE reprezintă o structură de importanță strategică națională, având ca principal obiectiv protecția infrastructurilor critice din sectorul energetic împotriva atacurilor cibernetice. Acest sector este unul dintre cele mai vulnerabile în fața amenințărilor cibernetice complexe, având un impact major asupra securității naționale și a economiei. Derogarea propusă este justificată de:
Necesitatea dotării și operaționalizării rapide a centrului pentru a răspunde cerințelor Directivei NIS2 (Directiva (UE) 2022/2555) și Regulamentului (UE) 2024/1366. Alinierea urgentă la cerințele internaționale privind monitorizarea și prevenirea incidentelor cibernetice, prin asigurarea unor resurse financiare și umane adecvate.
Cu privire la prevederile Art. I-II și IV – Limitarea cheltuielilor salariale și de personal, prevederile Ordonanța de urgență nr. 156/2024 limitează cheltuielile salariale, sporurile și alte drepturi conexe pentru sectorul public. În cazul CRISCE, aceste restricții ar afecta grav capacitatea de recrutare și retenție a personalului de înaltă calificare. CRISCE necesită un regim salarial competitiv pentru a atrage specialiști cu certificări internaționale (CISSP, CEH, GCIH) indispensabili pentru protecția infrastructurilor critice energetice. Restricțiile privind numărul maxim de posturi finanțabile ar împiedica angajarea rapidă a personalului tehnic și operativ necesar pentru îndeplinirea atribuțiilor strategice.
Cu privire la art. VII – Suspendarea angajărilor, suspendarea angajărilor prevăzută de Ordonanța de urgență nr. 156/2024 ar întârzia semnificativ operaționalizarea CRISCE. Derogarea permite angajarea rapidă a personalului esențial, evitând blocajele administrative incompatibile cu specificul urgent al activităților centrului.
Cu privire la art. XV – Restricții privind drepturile salariale pe durata delegării/detașării, în contextul internațional al activităților CRISCE, este necesar ca personalul detașat pentru participarea la rețele internaționale de cooperare în domeniul securității cibernetice să beneficieze de condiții salariale adecvate. Derogarea asigură conformitatea cu standardele internaționale și permite participarea efectivă la astfel de inițiative.
Situația extraordinară care justifică derogarea este generată de obligațiile urgente ale României în domeniul securității cibernetice, inclusiv termenele strânse impuse de Directiva NIS2 și

Regulamentul (UE) 2024/1366. În lipsa derogării, România riscă să nu își îndeplinească angajamentele internaționale, expunând infrastructurile energetice unor riscuri majore. Derogarea propusă este indispensabilă pentru a asigura operaționalizarea rapidă și eficientă a CRISCE. Aceasta răspunde nevoilor specifice ale centrului, evitând limitările impuse de cadrul general aplicabil și asigurând compatibilitatea cu cerințele naționale și internaționale din domeniul securității cibernetice. Beneficiile directe pentru securitatea națională și pentru protecția sectorului energetic justifică pe deplin măsura adoptată.
Proiectul de Ordonanță de Urgență a Guvernului pentru modificarea și completarea Ordonanței de Urgență nr. 60/2022 privind stabilirea cadrului instituțional și financiar de implementare și gestionare a fondurilor alocate României prin Fondul pentru modernizare, precum și pentru modificarea și completarea unor acte normative

2.4 Alte informații *)
Nu este cazul.

Secțiunea a 3-a:
Impactul socioeconomic **)

3.1. Descrierea generală a beneficiilor și costurilor estimate ca urmare a intrării în vigoare a actului normativ
Implementarea măsurilor stabilite prin prezentul act normativ va genera beneficii semnificative și costuri specifice, direct proporționale cu impactul strategic și operativ al înființării și funcționării CRISCE. Actul normativ contribuie la consolidarea securității naționale și la respectarea angajamentelor internaționale asumate de România în domeniul securității cibernetice, în special pentru protecția infrastructurilor energetice cu impact critic.

1. Beneficiile estimate:
1.1. Consolidarea protecției infrastructurilor critice din sectorul energetic
CRISCE va deveni un centru operațional dedicat prevenirii, monitorizării și gestionării incidentelor cibernetice care afectează sectorul energetic, contribuind direct la protejarea infrastructurilor naționale cu impact critic cum sunt cele ale Ministerului Energiei, ale companiilor naționale din sectorul energetic și ale beneficiarilor proiectelor finanțate prin Fondul pentru Modernizare. Beneficiile includ:

- Reducerea riscurilor asociate atacurilor cibernetice asupra sistemelor SCADA și ICS, esențiale pentru funcționarea rețelelor energetice.
- Îmbunătățirea capacității de reacție și prevenire a atacurilor cibernetice prin utilizarea unor tehnologii avansate și a unor metodologii aliniate la standardele internaționale.
- Creșterea rezilienței sectorului energetic și reducerea vulnerabilităților sistemice.

1.2. Îndeplinirea obligațiilor internaționale asumate de România
Prin operaționalizarea CRISCE, România își respectă angajamentele internaționale și europene, în special cele prevăzute de Directiva NIS2 (Directiva (UE) 2022/2555). Beneficiile includ:

- Crearea unui CSIRT sectorial care să îndeplinească cerințele impuse de Directiva NIS2, inclusiv pentru monitorizarea și gestionarea riscurilor cibernetice.
- Integrarea în rețele internaționale de cooperare și schimb de informații în domeniul securității cibernetice.

- Consolidarea imaginii şi credibilităţii României ca partener european de încredere în domeniul securităţii cibernetice.

1.3. Crearea de locuri de muncă specializate
Înfiinţarea şi funcţionarea CRISCE vor genera locuri de muncă pentru experţi în securitate cibernetică, contribuind la formarea şi retenţia talentelor în domeniul tehnologiei informaţiei şi securităţii. Regimul salarial competitiv asigurat de acest act normativ va contribui la reducerea migraţiei specialiştilor în străinătate.

2. Costurile estimate
2.1. Costuri directe asociate înfiinţării şi funcţionării CRISCE
Estimările iniţiale indică necesitatea alocării unor resurse financiare, acoperite din dobânzile aferente Fondului pentru Modernizare şi veniturile din prestarea de servicii de securitate cibernetică, pentru:
- Dotări tehnologice şi infrastructură: achiziţionarea de echipamente IT avansate (firewall-uri, sisteme de prevenire a intruziunilor, soluţii de criptare), precum şi amenajarea unor facilităţi speciale, cum ar fi camere Faraday pentru protecţia comunicaţiilor;
- Salarizarea personalului specializat: atragerea şi retenţia personalului calificat impun un regim salarial competitiv, adaptat cerinţelor pieţei internaţionale de muncă în domeniul securităţii cibernetice;
- Participarea în reţele internaţionale: implicarea CRISCE în platforme internaţionale de cooperare va necesita finanţarea unor activităţi de formare, schimb de informaţii şi reprezentare externă.

2.2. Costuri indirecte asociate implementării derogărilor
Aplicarea derogărilor prevăzute în proiectul de act normativ nu va genera ajustări bugetare specifice pentru depăşirea limitărilor impuse de Legea nr. 296/2023 pentru achiziţii şi cheltuieli cu personalul şi flexibilizarea procesului de recrutare şi salarizare a experţilor necesari pentru funcţionarea CRISCE, deoarece CRISCE nu este finanţat din venituri de la bugetul de stat.
3. Raportul cost-beneficiu
Analiza raportului cost-beneficiu indică un impact net pozitiv al implementării măsurilor propuse. Costurile estimate sunt justificate de beneficiile semnificative obţinute la nivel strategic, naţional şi internaţional, printre care:
- Protejarea infrastructurilor cu impact cu un impact major asupra securităţii naţionale şi economice;
- Reducerea vulnerabilităţilor sistemice şi a pierderilor financiare asociate atacurilor cibernetice;
- Respectarea obligaţiilor europene şi creşterea gradului de integrare a României în reţelele internaţionale de securitate cibernetică.

3.2 Impactul social
CRISCE va contribui la creşterea siguranţei, securităţii şi stabilităţii sectorului energetic, asigurând - din perspectivă de suport tehnic înalt specializat - continuitatea furnizării de energie. Acest lucru va aduce beneficii directe populaţiei, contribuind la consolidarea mecanismelor de prevenţie a întreruperilor de furnizare a energiei şi protejând serviciile esenţiale de care depinde calitatea vieţii cetăţenilor. Pe termen lung, prin creşterea rezilienţei la atacuri cibernetice, CRISCE va sprijini protecţia infrastructurii energetice, reducând vulnerabilităţile sociale şi economice generate de potenţialele perturbări. Astfel, cetăţenii şi economia naţională vor beneficia de securitate sporită şi de o stabilitate energetică îmbunătăţită.

3.3 Impactul asupra drepturilor şi libertăţilor fundamentale ale omului
Proiectul de act normativ nu se referă la acest subiect

3.4 Impactul macroeconomic
Operaţionalizarea CRISCE va avea un impact macroeconomic direct nesemnificativ, însă va contribui la generarea unui impact macroeconomic indirect semnificativ, în sens pozitiv.
Finanţarea necesară operaţionalizării CRISCE nu produce impact asupra echilibrului macroeconomic.
Totuşi, prin măsurile propuse, actul normativ va contribui la stabilitatea şi securitatea sectorului energetic, un pilon esenţial pentru economia României. Prin prevenirea şi combaterea atacurilor cibernetice, CRISCE va proteja continuitatea aprovizionării cu energie, prevenind astfel materializarea unor riscuri specifice şi reducând impactul negativ asupra industriei şi serviciilor care depind de această resursă.
De asemenea, creşterea siguranţei energetice va atrage investiţii atât în infrastructura energetică, cât şi în domeniul securităţii cibernetice, consolidând competitivitatea României pe piaţa energetică regională şi internaţională.
Prin aportul la asigurarea continuităţii în furnizarea energiei, CRISCE va contribui la menţinerea echilibrului macroeconomic, reducând riscurile de instabilitate economică, cu efecte benefice asupra principalilor indicatori macroeconomici.

3.4.1 Impactul asupra economiei şi asupra principalilor indicatori macroeconomici

Pentru proiectul de ordonanţă de urgenţă privind înfiinţarea CRISCE, impactul asupra economiei şi principalilor indicatori macroeconomici include multiple avantaje derivate din activităţile şi atribuţiile CRISCE, care contribuie direct la protecţia şi continuitatea sectorului energetic naţional, sector de importanţă strategică pentru economia României. Atribuţiile CRISCE sunt esenţiale pentru securitatea cibernetică a infrastructurilor critice şi generează o serie de efecte economice pozitive prin reducerea riscurilor cibernetice, prevenirea pierderilor financiare şi atragerea de investiţii.
Prin protecţia sporită a infrastructurilor critice energetice, CRISCE contribuie la stabilitatea şi continuitatea furnizării de energie, un factor crucial pentru funcţionarea fără întreruperi a economiei naţionale. Securitatea cibernetică a sectorului energetic previne riscurile de atacuri care ar putea genera întreruperi semnificative, ducând la pierderi economice majore şi afectând grav sectoarele industriale şi comerciale dependente de energie. Investiţiile în infrastructura de securitate cibernetică susţinute de CRISCE reduc riscul de incidente cibernetice cu impact financiar considerabil, contribuind astfel la o creştere economică stabilă şi la protecţia valorii adăugate de acest sector în PIB.
Implementarea proiectului CRISCE presupune crearea de noi locuri de muncă specializate în securitate cibernetică, IT, inginerie de reţea şi management de criză, contribuind la diversificarea oportunităţilor de carieră şi dezvoltare profesională în domenii emergente. Acest lucru stimulează atât ocuparea forţei de muncă, cât şi pregătirea profesională în sectoare cu înaltă calificare, unde cererea este în creştere, generând oportunităţi pentru tinerii specialişti şi reducând astfel fenomenul de migraţie a resurselor umane calificate. Pe termen lung, acest efect se traduce prin creşterea gradului de competenţă profesională naţională în securitatea cibernetică şi asigură o forţă de muncă stabilă în faţa provocărilor cibernetice actuale.
Un CSIRT sectorial în domeniul energetic, cum este CRISCE, contribuie la creşterea rezilienţei economice prin capacitatea sa de a preveni şi răspunde prompt la atacuri cibernetice asupra infrastructurilor critice. Atacurile cibernetice asupra sistemelor de energie pot genera pierderi de ordinul miliardelor de euro şi întreruperi de lungă durată în aprovizionarea cu energie. Activitatea CRISCE reduce aceste riscuri financiare prin prevenţia avariilor, asigurarea unui sistem de răspuns

rapid și menținerea unei funcționări stabile a sectorului energetic, contribuind astfel la diminuarea riscurilor financiare asociate cu atacurile cibernetice și la protecția stabilității macroeconomice.
Consolidarea securității cibernetice a sectorului energetic prin activitatea CRISCE atrage investiții străine și stimulează parteneriatele internaționale, demonstrând angajamentul României față de protejarea infrastructurilor critice în conformitate cu standardele europene de securitate cibernetică.
Prin alinierea la Directivele NIS și NIS2 și la alte reglementări de securitate la nivel european, CRISCE sporește încrederea investitorilor și a operatorilor economici care activează în domenii asociate, oferind un climat economic stabil și sigur pentru dezvoltarea de proiecte de infrastructură și energie.
Un sistem energetic sigur și protejat de riscuri cibernetice reduce fluctuațiile de prețuri cauzate de întreruperi neprevăzute sau crize de aprovizionare. Prin activitatea CRISCE, sistemele energetice beneficiază de protecție continuă împotriva riscurilor care ar putea afecta lanțul de distribuție, contribuind astfel la stabilitatea prețurilor la energie și reducând presiunile inflaționiste cauzate de creșterile neprevăzute ale prețurilor la energie.

3.4.2 Impactul asupra mediului concurențial si domeniul ajutoarelor de stat

Din perspectiv normelor în materie de concurență, CRISCE nu va concura direct cu furnizorii privați de soluții de securitate cibernetică, întrucât serviciile oferite sunt destinate sprijinirii gratuite a sectorului public, a companiilor de stat din sectorul energetic și beneficiarilor proiectelor de infrastructură energetică finanțate prin Fondul pentru Modernizare (FM). În conformitate cu legislația specifică, CRISCE va activa pe o nișă de interes public, destinată exclusiv asigurării securității cibernetice în sectoare esențiale.
Totodată, tarifele percepute pentru anumite servicii de audit și monitorizare vor respecta metodologiile de cost avizate, conform regulilor Consiliului Concurenței și DNSC, pentru a evita perturbarea mediului concurențial
CRISCE va opera în conformitate cu reglementările europene și naționale referitoare la ajutoarele de stat, fiind finanțat prin fonduri dedicate, din dobânzile Fondului pentru Modernizare, fără a atrage resurse financiare care ar putea distorsiona piața.

3.5. Impactul asupra mediului de afaceri

Operaționalizarea CRISCE va aduce un impact pozitiv asupra mediului de afaceri prin asigurarea unui cadru mai sigur și stabil pentru companiile din sectorul energetic. Prin reducerea riscurilor asociate atacurilor cibernetice, companiile vor putea funcționa într-un mediu protejat, minimizând pierderile economice generate de astfel de incidente. În plus, CRISCE va oferi sprijin tehnic și consultanță pentru companii, facilitând implementarea măsurilor de securitate cibernetică. Aceasta va stimula investițiile în domeniul energiei, va crește competitivitatea companiilor și va crea un mediu de afaceri mai previzibil și sigur pe termen lung.
Operaționalizarea CRISCE oferă un grad de încredere ridicat investitorilor străini din sectorul energetic, arătând că România ia măsuri proactive, complexe și integrate de a asigura funcționarea continuă a rețelelor și sistemelor informatice din sectorul energetic, fiind unul dintre pionierii europeni ai CSIRT-urilor sectoriale în Energie.

3.6 Impactul asupra mediului înconjurător

Impactul CRISCE asupra mediului înconjurător este indirect, dar benefic, prin protejarea infrastructurilor din sectorul energetic. Prin prevenirea atacurilor cibernetice care ar putea afecta funcționarea eficientă a rețelelor de energie, CRISCE contribuie la asigurarea continuității serviciilor și la reducerea riscului unor incidente tehnice ce ar putea provoca daune ecologice sau întreruperi în procesele de monitorizare a emisiilor.

3.7 Evaluarea costurilor și beneficiilor din perspectiva inovării și digitalizării

Evaluarea costurilor și beneficiilor CRISCE din perspectiva inovării și digitalizării relevă o balanță pozitivă, cu beneficii pe termen lung. Pe de o parte, costurile includ investiții inițiale în tehnologie avansată, securitate cibernetică și atragerea specialiștilor necesari pentru operarea centrului. De

asemenea, este necesară dezvoltarea arhitecturii de soluții IT și sisteme de monitorizare performante, care să asigure protecția rețelelor energetice.
Aducem aminte că CRISCE va utiliza sistem control-acces, monitorizare video, personal de securitate, baricade fizice, generatoare de rezervă și Uninterruptible Power Supply (UPS), sisteme de răcire și ventilație, rețele de comunicații redundante, sisteme de detectare a intruziunilor (IDS/IPS), Security Information and Event Management (SIEM), telefoane securizate, sisteme de videoconferință și alte mijloace de comunicare, servere și echipamente de stocare a datelor securizate, segmentarea rețelei și spațiu de gestionare a crizelor (situation room) și echipamente specializate de securitate cibernetică. Pe de altă parte, beneficiile includ creșterea capacității de răspuns la incidente cibernetice, protecția investițiilor în infrastructură și prevenirea întreruperilor cauzate de atacuri cibernetice care pot genera pierderi economice semnificative. CRISCE va stimula inovația în securitatea cibernetică, va sprijini dezvoltarea unor soluții tehnologice avansate și va consolida digitalizarea sectorului energetic. Pe termen lung, aceste investiții vor duce la un mediu de afaceri mai sigur, protejând infrastructura critică și facilitând transformarea digitală a sectorului, cu un impact economic și social favorabil.
Totodată, operaționalizarea CRISCE va genera o valoare adăugată considerabilă din perspectiva inovării și digitalizării instituționale, acționând ca un model de abordare a autorităților competente în domeniul energetic, la nivel european și internațional.

3.8 Evaluarea costurilor și beneficiilor din perspectiva dezvoltării durabile

Evaluarea costurilor și beneficiilor CRISCE din perspectiva dezvoltării durabile reflectă un impact pe termen lung asupra securității energetice și sustenabilității. Costurile inițiale implică investiții în infrastructură, tehnologie și atragerea resurselor umane pentru gestionarea și operarea centrului. Aceste cheltuieli sunt esențiale pentru implementarea unui sistem robust de securitate cibernetică în sectorul energetic.

Beneficiile sunt considerabile, în special prin prisma protejării infrastructurilor, prevenirea întreruperilor în furnizarea energiei și reducerea impactului negativ al atacurilor cibernetice asupra economiei și mediului. CRISCE contribuie la menținerea unui flux energetic stabil, sprijinind astfel proiectele de energie regenerabilă și tranziția către un sistem energetic mai sustenabil. Protejarea rețelelor de energie asigură continuitatea operațiunilor ecologice și protejează mediul de eventuale accidente cauzate de perturbările în sistem. În plus, crearea unui mediu de securitate cibernetică robust sprijină dezvoltarea durabilă prin reducerea riscurilor economice și ecologice.

3.9. Alte informații

Un centru de operațiuni de securitate (Security Operation Center - SOC) poate fi definit ca o structură care furnizează un serviciu de detectare a incidentelor prin observarea evenimentelor tehnice din rețele și sisteme informatice și poate fi, de asemenea, responsabil de reacția la incidente și de gestionarea acestora. În organizațiile mari, SOC-urile se concentrează, uneori, doar pe serviciile de monitorizare și de detectare după care predau gestionarea incidentelor unei echipe CSIRT separate. În organizațiile și entitățile mai mici mai mici, CSIRT-urile și SOC-urile sunt adesea considerate cvasi-sinonime.

De obicei, echipele SOC operează în locații specifice, unde analiștii stau la stațiile de lucru în fața unui display video care proiectează un rezumat al situației curente (riscuri, amenințări etc). Echipele SOC au evoluat, de obicei, din echipele de securitate din domeniul tehnologiei informației (IT) care își automatizează activitatea prin utilizarea SIEM (Security Information and Event Management) și a altor tehnologii de automatizare și orchestrare a securității pentru monitorizarea securității. De obicei, echipele SOC își concentrează indicatorii-cheie de performanță (KPI) în jurul indicatorilor de calitate - viteza de detectare, amploarea detecției, acoperirea, ratele fals-pozitive - precum și al

incidentelor gestionate, raportul alerte/evenimente/incidente, numărul de escaladări şi volumul de muncă per incident.

Pe lângă funcţionarea fizică, SOC-urile pot fi formate din personal virtual şi externalizat sau dintr-un model hibrid de personal intern şi externalizat. Este o practică obişnuită ca, de-a lungul timpului, SOC-urile să alterneze între operaţiunile externalizate şi cele interne.

Termenul CSIRT (Computer Security Incident Response Team) sau echipă de răspuns la incidente de securitate cibernetică, a fost stabilit în anii 1990. CSIRT-urile sunt cunoscute şi sub numele de CIRT-uri (Computer Incident Response Teams), CERT-uri (Computer Emergency Response Teams), SIRT (Security Incident Response Teams) etc. Echipele naţionale pot fi denumite şi Centre naţionale de securitate cibernetică (NCSC), cărora, prin lege, li se atribuie de regulă rolul unui CSIRT, precum şi furnizarea de servicii suplimentare pentru naţiune (de exemplu, gestionarea sistemelor de clasificare a informaţiilor unei ţări). Fiecare echipă îşi alege numele în funcţie de preferinţa organizaţiei.

CSIRT a devenit un nume generic pentru o echipă care furnizează un set de servicii cu un caracter aparte, şi anume: informaţii şi gestionarea incidentelor de securitate cibernetică (ca serviciu de bază), monitorizarea securităţii, gestionarea vulnerabilităţilor, conştientizarea situaţiei şi gestionarea cunoştinţelor de securitate cibernetică.

În termeni simpli, un CSIRT este o echipă însărcinată cu gestionarea incidentelor de securitate informatică (denumită adesea, securitate cibernetică). Adesea, aceasta include responsabilităţi suplimentare, de la detectare la analiza şi chiar repararea practică, precum şi diferite activităţi de cunoaştere a situaţiei, de transfer de cunoştinţe şi activităţi de gestionare a vulnerabilităţilor. De-a lungul anilor, rolul CSIRT a evoluat de la furnizarea de servicii de monitorizare şi gestionare a incidentelor la coordonarea şi comunicare cu diferite părţi interesate, ţări şi sectoare specifice.

În noiembrie 1988, un incident de securitate informatică cunoscut sub numele de „viermele internetului" a afectat părţi importante ale internetului. Reacţia la acest incident a fost izolată şi necoordonată, ceea ce a dus la dublarea multor eforturi şi la soluţii contradictorii. Câteva săptămâni mai târziu, a fost înfiinţat Centrul de coordonare CERT. La scurt timp după aceea, Departamentul pentru Energie al Statelor Unite a înfiinţat echipa denumită Computer Incident Advisory Capability (CIAC) pentru a-şi deservi clienţii.

În următorii doi ani, numărul echipelor de răspuns la incidente a continuat să crească, fiecare având propriul său scop, finanţare, cerinţe de raportare şi grup de interese. Interacţiunea dintre aceste echipe a întâmpinat dificultăţi din cauza diferenţelor de limbă, fus orar şi standarde sau convenţii internaţionale. În octombrie 1989, un incident major numit „viermele Wank" a evidenţiat necesitatea unei mai bune comunicări şi coordonări între echipe.

Forumul echipelor de răspuns la incidente şi de securitate (Forum of Incident Response and Security Teams FIRST) a fost creat în 1990 ca răspuns la această problemă. De atunci, acesta a continuat să crească şi să evolueze ca răspuns la nevoile în schimbare ale echipelor de securitate şi de răspuns la incidente şi ale grupurilor lor de interese.

Până în 2002, internetul a crescut de la 60 000 de sisteme informatice gazdă la 150 de milioane (în aproape toate ţările lumii). Multe întreprinderi se bazează în prezent pe internet în tranzacţiile lor zilnice. Membrii FIRST sunt echipe dintr-o mare varietate de organizaţii, inclusiv organizaţii

educaționale, comerciale, furnizori, guvernamentale și militare. FIRST coagulează comunitatea globală de răspuns la incidente, având mai mult de 700 de membri, răspândiți în Africa, America, Asia, Europa și Oceania.

Serviciul Trusted-Introducer (TI) a fost înființat în Europa în anul 2000 pentru a facilita colaborarea între de echipe de răspuns și, prin urmare, pentru a crește nivelul de securitate prin răspunsul mai rapid la atacurile în desfășurare și a amenințărilor de tip nou. TI asigură o bază de încredere, cu servicii adiționale specializate pentru toate echipele de răspuns la incidente de securitate. De asemenea, serviciul TI menține baza de date europeană a echipelor de securitate cibernetică, inclusiv CSIRT-uri, CERT-uri, SOC-uri, PCSIRT-uri, ISAC-uri etc. Echipele din directorul TI sunt cunoscute sub denumirea de echipe „listate". Echipele listate au fost aprobate de acele echipe care - pe lângă faptul că au fost listate - au fost acreditate și/sau certificate. Echipele acreditate și certificate sunt un subset al echipelor listate și îndeplinesc cerințele acreditării formale TI. Acesta este mecanismul de acreditare și certificare bazat pe cele mai bune practici dezvoltate și testate de-a lungul timpului în cadrul aceleiași comunități de echipe TI și oferă o imagine de ansamblu actualizată asupra nivelului lor demonstrat de maturitate și abilitate.

Instituționalizarea capacităților cibernetice este o caracteristică bine cunoscută de zeci de ani încoace. Odată cu implementarea instituționalizării, este nevoie și de un cadru de reglementare care să contureze și să modeleze organizarea și mandatul acestora, precum și rolul lor în cadrul mecanismelor naționale de gestionare a crizelor. Capacitățile tehnice sunt de obicei organizate în echipe CERT/CSIRT, care au evoluat ca un standard pentru răspunsul la incidente, cu proceduri și standarde stabilite, urmate la nivel cvasi-global. Echipele de tip CERT/CSIRT au devenit o parte obișnuită a cadrelor naționale de securitate.

Necesitatea de a proteja infrastructura informatică critică și de a crea capacitățile naționale corespunzătoare a fost subliniată atât de NATO, cât și de UE timp de mulți ani. În timp ce „securitate cibernetică" și „incident cibernetic" sunt termeni acceptați, în ceea ce privește infrastructura critică și infrastructura informatică critică, nu există o astfel de definiție echivalentă la nivelul NATO. Termenul și conținutul său au rămas astfel în sfera de competență a națiunilor individuale.

Pentru țările membre UE, situația a fost clarificată în 2016 prin adoptarea Directivei (EU) 2016/1148 privind securitatea rețelelor și a sistemelor informatice, așa-numita directivă NIS. Deși evită termenii „infrastructură critică" și „infrastructură informatică critică", directiva a furnizat o listă de bază a sectoarelor și serviciilor care trebuie protejate, a subliniat funcțiile pe care un stat ar trebui să le garanteze și structurile pe care trebuie să le pună în aplicare pentru a asigura o astfel de protecție.

Printre alte aspecte, directiva NIS a obligat țările să instituie cel puțin o autoritate competentă și cel puțin o echipă de tip CSIRT pentru a acoperi serviciile reglementate, precum și elaborarea unei strategii naționale de securitate cibernetică.

Directiva totuși nu a prescris un model specific de guvernanță. Chiar și acele țări din UE care, până atunci, au întârziat în construirea structurilor lor naționale de guvernanță în domeniul securității cibernetice, au trebuit acum să se conformeze directivei NIS. Țările candidate la UE au încercat, de asemenea, să-și alinieze cadrele legislative și instituționale legislative și instituționale.

Revizuirea din 2022 a directivei a extins obligațiile legate de guvernanță și capacitate pentru a acoperi și mai multe servicii și entități și a conferit autorităților competente puteri sporite de supraveghere și punere în aplicare. Directiva (UE) 2022/2555 privind măsuri pentru un nivel comun

ridicat de securitate cibernetică în UE, cunoscută sub numele de NIS 2, stabileşte un cadru comun de reglementare cu scopul de a spori nivelul de securitate cibernetică în UE. Directiva se aplică în principal entităţilor mijlocii şi mari care îşi desfăşoară activitatea în sectoare cu o importanţă critică ridicată (esenţiale) definite în anexa I şi entităţilor importante, definite în anexa II.

Directiva instituie o reţea a echipelor naţionale CSIRT şi un grup de cooperare pentru a sprijini şi a facilita cooperarea strategică şi schimbul de informaţii. Grupul este compus din reprezentanţi ai statelor membre, ai Comisiei şi ai ENISA. După caz, Grupul de cooperare poate invita să participe la lucrările sale Parlamentul European şi reprezentanţi ai părţilor interesate relevante.

Directiva a fost transpusă în legislaţia naţională prin OUG privind instituirea unui cadru pentru securitatea cibernetică a reţelelor şi sistemelor informatice din spaţiul cibernetic naţional civil. Statele membre trebuie să întocmească o listă a entităţilor esenţiale şi importante, precum şi a entităţilor care furnizează servicii de înregistrare a numelor de domenii, până la 17 aprilie 2025. De menţionat că până la momentul prezent, doar România, Belgia şi Croaţia au transpus Directive NIS2 în legislaţia naţională.

Modelele naţionale alese de statele membre variază, reflectând configuraţiile constituţionale şi tradiţiile administrative respective. Astfel, unele ţări au optat pentru o abordare mai centralizată şi au o autoritate competentă şi un CERT/CSIRT care se ocupă de sectoarele identificate în directiva NIS, inclusiv guvernul şi administraţia publică, în timp ce altele au ales o abordare sectorială şi au desemnat o autoritate competentă şi un CERT/CSIRT pentru sectoare individuale sau grupuri ale acestora, sau chiar pentru infrastructura din cadrul unităţii administrative teritoriale a unei ţări . Există, de asemenea, ţări în care un CERT/CSIRT naţional este responsabil pentru serviciile esenţiale în temeiul directivei NIS, în timp ce un altul se ocupă de administraţia publică/ infrastructura guvernamentală.

Deseori structurile de securitate cibernetică au existat, la origine, în cadrul instituţiilor de securitate ale unei ţări, fie în cadrul armatei, fie în cadrul structurilor serviciilor interne. Datorită dezvoltărilor tehnologice şi a riscurilor aferente, serviciile de tehnologia informaţiei au început în anii 1990-2000 să se specializeze în securitate cibernetică şi să se dezvolte ca departamente specializate, conform strategiilor de securitate naţionale ale statelor. Aşadar, la momentul apariţiei Directivei NIS pre-existau în numeroase ţări structuri de acest fel, existau reţelele şi comunităţile profesionale organizate în jurul FIRST sau Trusted Introducer.

Structuri – sau cel puţin nuclee – de cibersecuritate au fost dezvoltate şi în alte domenii precum administraţie, financiar-bancar, sănătate, educaţie-cercetare, telecomunicaţii, furnizori de servicii şi în special furnizori de servicii de internet, companii aeriene, conglomerate comerciale etc.

Deşi sectorul energiei este esenţial pentru societate şi considerat critic, echipele de urgenţe de securitate cibernetică din acest domeniu sunt mai puţin numeroase decât ar fi de aşteptat. În niciuna dintre ţările studiate nu există, în cadrul administraţiei publice, departamente sau servicii dedicate exclusiv securităţii cibernetice în sectorul energiei. Totuşi, legile din unele ţări precum Polonia şi Spania lasă deschisă opţiunea de a avea entităţi coordonatoare pe domenii de activitate. În Austria exista, anterior Directivei NIS, echipa specializată denumită Austrian Energy CERT specializată în răspunsuri la incidente de securitate cibernetică, finanţată în comun de către 20 de operatori din industria energiei. În alte ţări precum Polonia, Franţa, Portugalia, Ungaria companiile majore din

industria energiei deţin propriile echipe de cibersecuritate, echipe care fac parte din reţelele CSIRT naţionale sau internaţionale.

Pentru o imagine de ansamblu a reglementărilor juridice privind CSIRT-uri sectoriale în domeniul energiei în state ale Uniunii Europene, SUA, Israel şi Canada, vom prezenta elemente de drept comparat privind legislaţia Uniunii Europene, a unor state membre ale Uniunii Europene şi ale altor state cu care România are parteneriate în domeniul securităţii cibernetice şi al energiei, astfel:

În **Uniunea Europeană,** cadrul juridic pentru înfiinţarea CSIRT-urilor sectoriale, inclusiv pentru sectorul energetic, este oferit în principal de Directiva NIS 2 (Directiva UE 2022/2555), care impune statelor membre să asigure un nivel comun ridicat de securitate cibernetică în reţelele şi sistemele informatice. Această directivă prevede obligativitatea înfiinţării echipelor de răspuns la incidente (CSIRT-uri) pentru sectoare esenţiale, inclusiv energie, în baza articolelor 9, 10, şi 11, care stabilesc rolurile şi responsabilităţile acestor echipe, inclusiv cooperarea cu alte autorităţi naţionale şi europene pentru gestionarea ameninţărilor cibernetice în sectorul energetic. România, în cadrul Ordonanţei de Urgenţă privind înfiinţarea CRISCE, pune în aplicare unele prevederi din această directivă în legislaţia naţională.

În Statele Unite ale Americii, structura echivalentă CSIRT-urilor sectoriale este reprezentată de ISAC-uri (Information Sharing and Analysis Centers), care au fost stabilite prin legislaţia de securitate cibernetică şi ordine executive. ISAC-ul pentru energie este administrat de North American Electric Reliability Corporation (NERC) şi gestionează ameninţările cibernetice din sectorul energetic. Aceste structuri sunt finanţate în principal din contribuţiile companiilor private din sectorul energetic şi primesc asistenţă de la guvernul federal pentru operaţiuni de coordonare şi răspuns la incidente. NERC Cybersecurity Standards, care sunt obligatorii pentru entităţile critice din domeniul energiei, reglementează compoziţia şi rolul ISAC-ului în domeniul energetic. Bugetul şi compoziţia specifică variază în funcţie de nevoile şi mărimea pieţei, fiind adesea sprijinit prin finanţări federale şi contribuţii private. E-ISAC funcţionează ca principalul centru de partajare a informaţiilor pentru sectorul energetic din America de Nord, concentrându-se pe protejarea infrastructurii electrice. NERC a creat E-ISAC ca o măsură de securitate suplimentară pentru a răspunde ameninţărilor emergente de securitate cibernetică care vizează infrastructura energetică critică. E-ISAC oferă monitorizare continuă, evaluări de risc, alerte de securitate, şi coordonarea răspunsului la incidente pentru sectorul energetic. E-ISAC asigură monitorizarea continuă a reţelelor energetice pentru a detecta activităţile cibernetice maliţioase şi pentru a evalua riscurile care afectează infrastructura critică. În cazul unui atac cibernetic major, E-ISAC colaborează cu organizaţiile energetice şi guvernamentale pentru a coordona un răspuns rapid şi eficient. E-ISAC colectează informaţii despre ameninţările cibernetice şi le diseminează rapid către operatorii din sectorul energetic. Aceasta include atât informaţii în timp real, cât şi analize pe termen lung. E-ISAC asistă operatorii energetici în fazele de recuperare şi remediere post-incident pentru a restabili rapid funcţionarea normală a reţelelor afectate. E-ISAC organizează şi participă la exerciţii de simulare a incidentelor cibernetice, cum ar fi exerciţiile *GridEx*, pentru a testa şi îmbunătăţi răspunsul la incidente. E-ISAC colaborează îndeaproape cu *Cybersecurity and Infrastructure Security Agency* (CISA), care este parte a *Department of Homeland Security* (DHS), şi cu *Federal Energy Regulatory Commission* (FERC). CISA, în calitatea sa de agenţie responsabilă cu protecţia infrastructurii critice, joacă un rol esenţial în susţinerea eforturilor de securitate cibernetică în sectorul energetic. E-ISAC

și CISA schimbă informații, alerte și bune practici în mod regulat pentru a asigura o coordonare eficientă. De asemenea, E-ISAC colaborează cu operatorii din sectorul privat, furnizorii de energie electrică și alți actori din infrastructura energetică, permițând un schimb de informații constant, necesar pentru detectarea timpurie a amenințărilor cibernetice. E-ISAC este finanțat în mare parte prin contribuțiile furnizorilor de energie electrică din America de Nord, fiind susținut de cotizații obligatorii impuse prin legislația de reglementare a securității energetice. De asemenea, E-ISAC primește finanțare suplimentară prin colaborarea cu guvernul federal, inclusiv prin granturi și parteneriate public-private. Bugetul alocat securității cibernetice în sectorul energetic, gestionat prin NERC și E-ISAC, variază, dar în 2022 a fost de aproximativ 10 milioane de dolari, sumă care include și proiectele destinate dezvoltării capacităților de răspuns la incidente cibernetice. CSIRT-urile sectoriale din SUA, inclusiv cele din domeniul energetic, funcționează sub legislația generală de securitate cibernetică. *Energy Policy Act* din 2005 și *Federal Power Act* acordă FERC autoritatea de a reglementa fiabilitatea sistemelor energetice și de a impune standarde de securitate cibernetică obligatorii. De asemenea, *National Institute of Standards and Technology* (NIST) colaborează cu sectorul energetic pentru dezvoltarea și implementarea unor cadre de securitate cibernetică, oferind ghiduri și standarde care trebuie respectate de operatorii energetici.

În Israel, sectorul energetic este protejat prin Cyber Directorate (INCD), o structură guvernamentală care supervizează CSIRT-urile sectoriale. Legislația israeliană în domeniul securității cibernetice este relativ recentă, dar prevederile sunt strict aplicate pentru infrastructurile critice, inclusiv energie. În cadrul INCD, există o unitate dedicată exclusiv sectorului energetic, care are responsabilitatea de a colabora cu operatorii de infrastructură energetică și de a implementa măsurile de securitate necesare. Aceasta unitate funcționează ca un CSIRT sectorial și lucrează direct cu companiile energetice pentru a gestiona riscurile cibernetice. Unitatea sectorială pe energie din cadrul INCD include aproximativ 30-50 de specialiști în securitate cibernetică. Acești experți sunt responsabili de analiza, monitorizarea și răspunsul la incidente cibernetice și colaborează cu echipele tehnice ale operatorilor de energie. Finanțarea acestor structuri vine atât din fonduri guvernamentale, cât și din parteneriate public-private. CSIRT-urile din Israel sunt foarte bine finanțate și organizate, având echipe compuse din specialiști IT și experți în securitate. Bugetul anual pentru securitatea cibernetică a infrastructurilor critice din Israel este de ordinul sutelor de milioane de dolari. O parte semnificativă a acestui buget este alocată sectorului energetic, având în vedere importanța acestui sector pentru securitatea națională.Se estimează că aproximativ 30 de milioane de dolari pe an sunt destinați doar protecției cibernetice a infrastructurii energetice. Acești bani provin din bugetul guvernamental, dar și din contribuțiile operatorilor privați din domeniul energetic, care sunt obligați să implementeze măsuri stricte de securitate.

În Canada, legislația relevantă pentru CSIRT-uri sectoriale în domeniul energiei este gestionată de Canadian Centre for Cyber Security (Cyber Centre), înființat prin Communications Security Establishment Act. Acesta are o echipă dedicată sectorului energetic, iar finanțarea sa provine din bugetul guvernamental. Canada a înființat echipe specializate pentru infrastructurile critice, precum energia, cu un model de colaborare între sectorul public și cel privat similar cu cel din SUA.

În Germania, securitatea cibernetică în domeniul energetic este gestionată de CSIRT-ul sectorial coordonat de Biroul Federal pentru Securitatea Informațiilor (Bundesamt für Sicherheit in der Informationstechnik - BSI). Acesta este reglementat de IT-Sicherheitsgesetz (Legea germană privind

securitatea IT), care a fost adoptată în 2015 și revizuită ulterior pentru a implementa cerințele Directivei NIS 2 (Directiva UE 2022/2555). CSIRT-ul sectorial pe energie face parte dintr-o rețea mai largă de CSIRT-uri gestionate de BSI și are în jur de 50 de experți care monitorizează și răspund la incidente cibernetice. Finanțarea vine în principal din bugetul de stat german, cu o parte din fonduri alocate de către companiile private care gestionează infrastructura energetică. În 2023, BSI a alocat un buget de aproximativ 25 de milioane de euro pentru securitatea cibernetică, din care o parte a fost direcționată către securitatea energetică.

Proiectul de lege NIS2UmsuCG va transpune în legislația germană cerințele minime ale UE privind securitatea cibernetică din Directiva UE NIS2, le va extinde în funcție de particularitățile de reglementare germane și va intra în vigoare la sfârșitul anului 2024. Proiectul de lege al Cabinetului datează din iulie 2024 și mai are de parcurs etapele procesului legislativ până în octombrie 2024. În plus față de NIS2, legea-cadru KRITIS va reglementa operatorii critici cu reziliență, iar EU DORA sectorul financiar.

În sprijinul implementării NIS2, a legii-cadru KRITIS, precum și aplicării legii privind securitatea informatică și a cadrului european pentru operatorii de infrastructuri critice, a fost creată platforma OpenKRITIS.

Au fost inițiate mai multe proiecte de lege, aflate în diferite stadii de finalizare, pentru implementarea NIS2; actualul proiect de lege este elaborat de Ministerul Federal de Interne (BMI). Entitățile vor fi reglementate de Agenția Federală pentru Securitate Cibernetică (BSI). Foaia de parcurs pentru noile proiecte, datele oficiale de publicare și termenul de începere sunt în prezent neclare.

În ceea ce privește transpunerea prevederilor NIS2, în legislația germană vor exista mai multe particularități:

- metoda germană existentă pentru identificarea infrastructurilor critice, KRITIS, va rămâne în NIS2;
- operatorii germani KRITIS pe infrastructuri critice vor fi transferați în NIS2 ca operatori de infrastructuri critice de tipul celei de-a treia entități;
- entitățile esențiale și importante din NIS2 vor fi denumite entități foarte importante și importante;
- sectoarele NIS2 din anexele I și II sunt definite ușor diferit - gestionarea serviciilor TIC și infrastructura digitală sunt incluse în sectorul german IT/Telco;
- sectoarele KRITIS existente vor rămâne ca set separat pentru operatorii critici;
- sectorul administrației publice este definit diferit în Germania și va include (în cea mai mare parte) numai entități ale administrației federale(https://www.openkritis.de/eu/eu-nis-2-germany.html)

În sectorul energetic, operatorii reglementați și instalațiile furnizează publicului larg patru servicii esențiale - furnizarea de energie electrică, gaze, combustibil și păcură și încălzire urbană. Aceste servicii trebuie protejate prin obligații de securitate cibernetică în conformitate cu NIS2 și KRITIS. Operatorii KRITIS furnizează aceste servicii critice în propriile lor instalații și devin KRITIS dacă depășesc valorile-prag(https://www.openkritis.de/it-sicherheitsgesetz/sektor_energie.html)

Autoritatea federală în domeniul securității cibernetice este BSI (Bundesamt für Sicherheit in der Informationstechnik). În cadrul BSI funcționează Centrul Național Operațional IT (Cyber-Abwehr für Deutschland - CAD). Stațiile de lucru din centrul operațional au fost suplimentate și a fost instalată cea mai recentă tehnologie media pentru a putea evalua permanent starea securității

cibernetice a Germaniei, într-un serviciu de informare 24/7. Un concept de cameră multifuncțională sprijină experții în întreaga gamă de sarcini care apar - de la operațiunile de zi cu zi, la incidentele IT.
În timpul orelor de program, CAD este sprijinit de experții BSI pentru infrastructuri critice (KRITIS) și de echipa federală de intervenție în caz de urgență informatică (CERT-Bund), precum și de ofițerii de securitate a informațiilor din cadrul Comandamentului pentru spațiul informatic și informațional (KdoCIR). În afara orelor de program, CERT-Bund și KRITIS sunt de gardă, iar cooperarea cu KdoCIR are loc prin intermediul interfețelor stabilite între cele două autorități. CAD, în calitate de birou central de raportare al BSI, reunește, de asemenea, diverse puncte de raportare legale și voluntare, astfel încât grupurile țintă afectate să poată fi identificate rapid, iar punctele comune și amenințările similare să poată fi recunoscute și prelucrate. Centrele de raportare sunt completate de monitorizarea activă a situației (monitorizarea mass-media, cercetarea în aproximativ 400 de surse publice și senzori proprii etc.).
În cazul unui incident de securitate IT, BSI poate să sprijine organizațiile afectate în determinarea și evaluarea situației. În acest scop, pot fi organizate întâlniri cu experți și specialiști. Pentru administrația federală și infrastructurile critice, expertiza suplimentară a BSI în domeniul analizei programelor malware, al expertizei criminalistice digitale sau al analizei datelor de log poate fi, de asemenea, utilizată în gestionarea incidentului. În cazuri excepționale, BSI poate trimite o echipă mobilă de răspuns la incidente (MIRT) pentru a oferi asistență la fața locului. Acest serviciu este disponibil în principal pentru administrația federală și pentru entitățile critice.
Constatările BSI privind incidentele de securitate IT deja cunoscute pot furniza indicatori tehnici pentru detectarea atacurilor și clarificarea incidentului și pot fi definite în mod specific pentru incident la finalizarea analizei. Cu consimțământul organizației în cauză, rezultatele pot fi transmise terților într-o formă adecvată pentru detectarea tiparelor de atac, în vederea detectării și prevenirii altor daune aduse altor organizații. În plus, BSI poate, de asemenea, să sprijine organizațiile în identificarea unor furnizori de servicii adecvați, care să le sprijine în gestionarea, detectarea sau analiza incidentelor (https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Reaktion/Vorfallunterstuetzung/vorfallsunterstuetzung_node.html)

În Franța, securitatea cibernetică pentru infrastructura energetică este gestionată de Agence nationale de la sécurité des systèmes d'information (ANSSI), care funcționează sub mandatul Loi de Programmation Militaire și Codul Apărării (art. L.1332-6). ANSSI coordonează CSIRT-uri sectoriale pentru diverse infrastructuri critice, inclusiv energie. CSIRT-ul sectorial pentru energie este format din aproximativ 40 de experți. Finanțarea provine din bugetul de stat francez, iar în 2023, ANSSI a avut un buget de 30 de milioane de euro, din care o parte a fost destinată protecției infrastructurilor critice energetice. Aflată sub autoritatea prim-ministrului și subordonată Secretarului General pentru Apărare și Securitate Națională (SGDSN), aceasta este în măsură să implementeze o politică globală de securitate cibernetică și să o coordoneze la nivel interministerial. Această politică vizează apărarea celor mai critice infrastructuri digitale publice și private. ANSSI se adresează, de asemenea, tuturor actorilor implicați în transformarea digitală a țării și favorizează condițiile unui dialog cu omologii săi la nivel european și internațional. Decretul nr. 2009-834 din 7 iulie 2009 privind crearea Agenției Naționale de Securitate a Sistemelor Informatice (ANSI) a

conferit acestei agenții, pe lângă asigurarea securității sistemelor informatice ale statului, misiunea de a consilia și sprijini administrațiile și operatorii de importanță vitală și de a contribui la securitatea societății informaționale, în special prin participarea la cercetarea și dezvoltarea tehnologiilor de securitate și la promovarea acestora.

În conformitate cu orientările stabilite în Carta albă privind apărarea și securitatea națională din 2013, ANSSI contribuie la orientarea cercetării naționale și europene în domeniul securității sistemelor informatice. Atunci când este necesar, ANSSI beneficiază de expertiza unui comitet strategic format din înalți funcționari guvernamentali. Rolul acestui comitet este de a propune strategia statului în acest domeniu.

ANSSI a înlocuit Direcția Centrală pentru Securitatea Sistemelor Informatice (DCSSI) din cadrul Secretariatului General pentru Apărare și Securitate Națională (SGDSN), consolidându-și în același timp competențele, personalul și resursele. În calitate de autoritate națională pentru securitatea și apărarea sistemelor informatice, ANSSI are expertiza pentru a asista departamentele guvernamentale și operatorii de importanță vitală. Totodată, este responsabilă de promovarea tehnologiilor, sistemelor și expertizei naționale. Centrul guvernamental de transmisiuni, plasat sub autoritatea SGDSN, asistă ANSSI prin punerea în aplicare a mijloacelor securizate de comandă și de legătură solicitate de președintele Republicii și de guvern.

Articolul 34 din Legea nr. 2018-607 privind programarea militară pentru perioada 2019-2025 completează, de asemenea, atribuțiile agenției. Acesta precizează punerea în aplicare a sistemelor de detectare în timpul evenimentelor care pot afecta securitatea sistemelor informatice ale statului, ale autorităților publice și ale operatorilor publici și privați, precum și colectarea de informații tehnice referitoare la aceste incidente și sprijinirea în reacția la acestea.

ANSSI este plasată sub autoritatea primului-ministru și atașată Secretariatului General pentru Apărare și Securitate Națională (SGDSN). Activitățile sale sunt axate pe protecția, securitatea și apărarea sistemelor informatice. Modelul francez de securitate și apărare cibernetică se bazează pe o separare clară, în cadrul statului, între misiunile defensive și cele ofensive. Acest model se concretizează în rolul de autoritate națională jucat de ANSSI, ale cărei misiuni acoperă întregul domeniu al apărării și protecției sistemelor informatice. În plus, ANSSI este interesată doar de securitatea rețelelor și nu de informațiile și conținutul pe care aceste rețele le conțin.

Poziționarea instituțională a agenției contribuie, de asemenea, la echilibrul modelului: fiind atașată SGDSN și aflată sub autoritatea prim-ministrului, agenția beneficiază de un statut interministerial care îi permite să lucreze cu toți interlocutorii săi. Statutul ANSSI și caracterul defensiv al misiunilor sale îi permit să își desfășoare acțiunile eficient, în legătură cu partenerii săi ministeriali, cu entitățile victime, cu reprezentanții aleși, cu specialiștii în securitate cibernetică și cu furnizorii privați de servicii.

Conform organigramei ANSSI, în cadrul agenției funcționează 4 direcții[1]: Expertiză, Operațiuni, Resurse și Strategie. Dintre acestea, rolul de echipă de răspuns la incidente de securitate cibernetică la nivel național, CERT-FR/SOC este în sarcina Direcției Operațiuni din cadrul Agenției Naționale pentru Securitatea Sistemelor Informatice (ANSSI). Principalii beneficiari ai activităților desfășurate de CERT-FR sunt:

- organisme publice: ministere, instituții, instanțe, autorități independente, autorități locale;
- operatori de importanță vitală (OIV): operatori publici sau privați care utilizează echipamente și instalații esențiale pentru funcționarea și supraviețuirea națiunii franceze;

- operatori de servicii esențiale (OSE): operatori de rețele sau de sisteme informatice, care furnizează un serviciu esențial a cărui întrerupere ar avea un impact semnificativ asupra funcționării economiei sau a societății.

Deși furnizează informații accesibile tuturor prin intermediul site-ului propriu (lista vulnerabilităților, starea amenințării informatice etc.), CERT-FR nu intervine direct pe lângă persoanele fizice și IMM-uri. Sprijinul pentru aceste grupuri este oferit de site-ul guvernamental cyber malveillance.gouv.fr. In acest context, sarcinile CERT-FR sunt:

- să răspundă solicitărilor de asistență ca urmare a incidentelor de securitate în rețelele și sistemele informatice ale beneficiarilor săi. Aceasta implică primirea cererilor, analizarea simptomelor incidentului, identificarea posibilelor corelații cu alte incidente similare și definirea soluțiilor de recuperare în caz de incident;
- gestionarea alertelor și reacția la atacurile informatice. În acest scop, CERT-FR efectuează o analiză tehnică a atacurilor, participă la schimburi de informații cu alte CERT-uri și contribuie la studii tehnice specifice pe diverse teme de securitate cibernetică;
- detectarea atacurilor care vizează sistemele informatice guvernamentale. În acest scop, CERT-FR operează un serviciu permanent de supraveghere a securității (SOC) pentru departamentele guvernamentale;
- detectarea vulnerabilităților sistemelor, în special prin monitorizarea tehnologică a principalelor produse de pe piață;
- contribuția la prevenirea atacurilor informatice, prin difuzarea de informații privind măsurile de precauție care trebuie luate pentru a reduce riscul de incidente și a minimiza consecințele posibile ale acestora;
- coordonarea prevenirii incidentelor și a răspunsului cu entitățile partenere. Coordonarea operațiunilor înseamnă că CERT-urile naționale și internaționale, centrele de competențe în materie de rețele, operatorii și furnizorii de servicii internet pot fi mobilizați în funcție de necesități.

In Franța, transpunerea Directivei **(EU) 2016/1148 NIS a avut loc printr-o serie de acte, dintre care menționăm** Titlul I din LEGEA nr. 2018-133 din 26 februarie 2018 privind diverse dispoziții de adaptare la dreptul Uniunii Europene în domeniul securității **și** Decretul nr. 2018-384 din 23 mai 2018 privind securitatea rețelelor și a sistemelor informatice ale operatorilor de servicii esențiale și ale furnizorilor de servicii digitale .

Franța dispune de o rețea bine dezvoltată de echipe de răspuns la incidente, în număr de 62 de CSIRT, care acoperă domenii diverse: public guvernamental, militar, furnizori de servicii de internet, educație și cercetare, sectorul financiar, servicii de importanță critică, firme comerciale etc.

Dintre acestea, TotalEnergies, companie globală integrată care produce și comercializează energie – petrol și biocombustibili, gaze naturale și gaze verzi, surse regenerabile și electricitate – dispune de echipa proprie de răspuns la incidente de securitatea cibernetică. Astfel, TotalEnergies CERT **este echipa de intervenție în caz de urgență informatică responsabilă de coordonarea răspunsului la incidente și de evaluarea securității cibernetice în cadrul entităților TotalEnergies Company și al filialelor TotalEnergies Company.**

În Italia, CSIRT-ul pentru energie este gestionat de CERT-EN, parte a Agenzia per la Cybersicurezza Nazionale (ACN). Legea nr. 109/2021, care reglementează securitatea cibernetică în Italia, asigură cadrul pentru funcționarea acestui CSIRT sectorial. Compoziție și finanțare: CERT-EN are aproximativ 30 de experți specializați în securitate cibernetică, cu focus pe sectorul energetic. Bugetul pentru activitatea acestui CSIRT provine din fonduri guvernamentale, iar pentru anul 2022, ACN a primit un buget total de 10 milioane de euro, din care 3 milioane au fost direcționate către CERT-EN.

Autoritatea națională în domeniul securității cibernetice este ACN (Agenzia per la Cybersicurezza Nazionale), înființată prin Decretul Legislativ nr. 82 din 14 iunie 2021 care a redefinit arhitectura națională de securitate cibernetică, cu scopul de a raționaliza și simplifica sistemul de competențe existente la nivel național. ACN este responsabilă cu prevenirea și atenuarea atacurilor cibernetice și cu promovarea realizării autonomiei tehnologice. Una dintre principalele sarcini ale Agenției este implementarea Strategiei Naționale de Securitate Cibernetică , adoptată de primul-ministru, în care sunt prevăzute obiectivele care urmează să fie atinse până în 2026.

CSIRT Italia este înființat în cadrul ACN și este structura tehnico-operațională și hub-ul național al notificărilor de incidente prevăzute de lege. Atribuțiile CSIRT sunt stabilite prin Decretul legislativ nr.65 din 18 mai 2018 și prin Decretul prim-ministrului 8 august 2019: monitorizarea incidentelor la nivel național; emiterea de avertismente timpurii, alerte, anunțuri și difuzarea de informații către părțile interesate cu privire la riscuri și incidente; intervenția în caz de incident; analiza dinamică a riscurilor și incidentelor; conștientizarea situației; participarea la rețeaua CSIRT.

ACN publică lunar un Raport privind starea amenințării cibernetice naționale, denumit „Rezumat operațional". Documentul conține cifre și indicatori legați de activitățile operaționale ale agenției desfășurate de CSIRT Italia. CSIRT Italia colectează, de asemenea, informații din surse deschise și comerciale, precum și de la alte entități omologe naționale și internaționale. Aceste informații, care constituie un larg unghi de vizibilitate asupra stării amenințării cibernetice, sunt studiate și exploatate de operatori și implică o serie de activități în funcție de actorii implicați și de tipul de eveniment analizat. Rezumatul operațional reprezintă un instrument funcțional util pentru înțelegerea fenomenelor și a evoluției lor în timp, vizând, de asemenea, consolidarea nivelului de prevenire pe baza cunoașterii evenimentelor care au avut loc.

CSIRT Italia stabilește relații de cooperare cu sectorul privat. Pentru a facilita cooperarea, CSIRT promovează adoptarea și utilizarea unor practici comune sau standardizate în domeniul procedurilor de gestionare a incidentelor și riscurilor și al sistemelor de clasificare a incidentelor, riscurilor și informațiilor. Profilul complet al CSIRT Italia este inclus în RFC 2350 (https://www.csirt.gov.it/chi-siamo). Italia are 40 de echipe de răspuns la incidente de securitate cibernetică, așa cum apar centralizate de ENISA. Dintre acestea, există 3 care activează în cadrul unor companii din domeniul energiei:

A2A este o firmă care distribuie energie electrică și gaze, apă potabilă și căldură prin sisteme de încălzire urbană. Asigură iluminare, conectare și proiectare pentru orașe și întreprinderi. Totodată găzduiește o echipă de răspuns la incidente, A2A-CERT, care oferă companiei servicii de gestionare a incidentelor de securitate cibernetică (ISIM), informații privind amenințările cibernetice (CTI), gestionarea platformei de securitate (SPM) și apărare activă (AD).

Enel Italia este o altă societate comercială în cadrul căreia există o echipă de răspuns la incidente de securitate cibernetică (care este acreditată cu Trusted Introducer).

De asemnea, în cadrul societății de transport a energiei electrice denumita Terna, funcționează TERNA-CERT, principalul punct de contact pentru colectarea, analiza și schimbul de informații privind amenințările informatice la care este expusă organizația. În plus, TERNA-CERT asigură servicii de asistență, formare, informare și cercetare și dezvoltare.
TERNA-CERT este format dintr-un grup de experți în securitate IT care lucrează împreună cu obiectivul comun de a proteja securitatea activelor Grupului Terna - inclusiv a activelor sale informatice - prin examinarea și monitorizarea naturii în continuă evoluție a amenințărilor cibernetice, desfășurarea de activități de prevenire, gestionarea situațiilor de urgență IT și coordonarea procedurilor de răspuns.
TERNA-CERT este membru al Forum of Incident Response (FIRST.org) și acreditat ca Trusted Introducer de TF-CSIRT și a fost autorizat de Universitatea Carnegie Mellon să utilizeze marca CERT. Colaborează cu alte organizații italiene și internaționale, pentru a promova interacțiunea și schimbul de informații cu privire la aspecte precum noile amenințări, atacurile informatice, noile tehnici de apărare și punctele slabe care pot fi exploatate, inclusiv prin utilizarea Threat Intelligence și a platformelor de schimb de informații.

În Olanda, National Cyber Security Centre (NCSC) gestionează securitatea cibernetică pentru sectorul energetic, conform legislației Wet beveiliging netwerk- en informatiesystemen (Wbni), care implementează Directiva NIS. NCSC Olanda are o echipă de aproximativ 35 de experți care monitorizează securitatea cibernetică în domeniul energetic. Finanțarea provine din bugetul guvernamental, iar în 2022, Olanda a alocat aproximativ 10 milioane de euro pentru securitatea cibernetică a infrastructurii critice, inclusiv energia.

În Spania, securitatea cibernetică este gestionată de Centro Criptológico Nacional (CCN), care funcționează sub Centro Nacional de Inteligencia (CNI). Legislația națională impune operatorilor din sectorul energetic să colaboreze cu CCN pentru gestionarea incidentelor cibernetice. CSIRT-ul sectorial pentru energie din Spania este format din aproximativ 25 de experți. Finanțarea provine din bugetul național pentru securitate cibernetică, care în 2022 a fost de 7 milioane de euro.
În Spania, Directiva NIS este transpusă prin Decretul-lege regal 12/2018, din 7 septembrie, privind securitatea rețelelor și a sistemelor informatice. Decretul este aplicabil celor două categorii principale:

a) operatorilor de servicii esențiale stabiliți în Spania și operatorilor rezidenți sau domiciliați în alt stat care oferă servicii esențiale prin intermediul unui sediu permanent situat în Spania;
b) furnizorilor de servicii digitale care au sediul social în Spania și care își constituie sediul principal în Uniunea Europeană, precum și celor care, nefiind stabiliți în Uniunea Europeană, își desemnează reprezentantul în Uniune în Spania.

Autoritățile competente în domeniu sunt stabilite prin articolul 9 din Decret, iar acestea sunt:

- Pentru operatorii de servicii esențiale/critice: Ministerul de Interne, prin Centrul Național pentru Protecția Infrastructurii și Securitate Cibernetică (CNPIC);
- Pentru operatorii de servicii care nu sunt critice: autoritatea sectorială corespunzătoare, astfel cum se stabilește prin reglementări;

- Pentru furnizorii de servicii digitale: secretarul de stat pentru agenda digitală, din cadrul Ministerului Economiei şi Mediului de Afaceri;
- Pentru operatorii de servicii esenţiale şi furnizorii de servicii digitale care nu sunt operatori critici: Ministerul Apărării, prin Centrul Criptologic Naţional (CCN);
- Consiliul Naţional de Securitate, prin comisia sa specializată în securitate cibernetică, stabileşte mecanismele necesare pentru coordonarea acţiunilor autorităţilor competente
- Decretul defineşte şi aşa numitele echipe de răspuns la incidente de securitate informatică (CSIRT) de referinţă (art. 11):

a) În ceea ce priveşte relaţiile cu operatorii de servicii esenţiale:
- CCN-CERT, al Centrului Criptologic Naţional;
- INCIBE-CERT, al Institutului Naţional de Securitate Cibernetică din Spania;
- ESPDEF-CERT, din cadrul Ministerului Apărării.

b) În ceea ce priveşte relaţiile cu furnizorii de servicii digitale:
- INCIBE-CERT este de asemenea, o echipă de referinţă de răspuns la incidente pentru cetăţeni, entităţi de drept privat şi alte entităţi.

CSIRT-urile de referinţă se coordonează între ele şi cu restul CSIRT-urilor naţionale şi internaţionale de răspuns la incidente şi de gestionare a riscurilor de securitate care le corespund.

În Spania, acţiunile necesare pentru optimizarea securităţii infrastructurilor critice sunt în principal încadrate în domeniul protecţiei împotriva agresiunilor deliberate şi, în special, împotriva atacurilor teroriste şi, prin urmare, sunt conduse de Ministerul de Interne. Legislaţia spaniolă stabileşte necesitatea de a garanta furnizarea adecvată a serviciilor esenţiale, sarcină încredinţată Centrului Naţional pentru Protecţia Infrastructurilor Critice (CNPIC), care îl asistă pe secretarul de stat pentru securitate în funcţiile sale. CNPIC a fost înfiinţat în 2007 ca organismul Ministerului de Interne responsabil cu coordonarea şi supravegherea tuturor activităţilor încredinţate Secretariatului de Stat pentru securitate în legătură cu protecţia infrastructurilor critice de pe teritoriul naţional.

Atunci când activităţile pe care le desfăşoară pot afecta în orice fel un operator critic, CSIRT-urile de referinţă se coordonează cu Ministerul de Interne, prin intermediul Biroului de coordonare cibernetică al CNPIC, în modul stabilit prin reglementări.

Sistemul PIC, inclus în titlul II din Legea 8/2011 pentru protecţia infrastructurilor critice, constă într-un set de agenţi, din sectorul public şi privat, cu competenţe şi responsabilităţi bine definite, astfel încât infrastructurile critice ale statului să furnizeze servicii esenţiale pentru societate cu garanţii suficiente şi fără întreruperi, creând un sistem preventiv care poate anticipa situaţiile de criză. Sistemul PIC spaniol este alcătuit din 12 departamente ministeriale şi 10 agenţii ale administraţiei centrale şi autonome, precum şi din peste 250 de operatori critici - publici şi privaţi - sub autoritatea secretarului de stat pentru securitate. Toate acestea implică gestionarea de către CNPIC a unei reţele de peste 300 de entităţi şi a aproximativ 1 200 de planuri de securitate, atât la nivel strategic, cât şi operaţional.

Centrul Criptologic Naţional (CCN) este organismul însărcinat cu coordonarea acţiunilor diferitelor organisme ale administraţiei care utilizează mijloace sau proceduri de criptare, cu garantarea securităţii tehnologiilor informaţiei în acest domeniu, cu raportarea privind achiziţionarea

coordonată de material criptologic şi cu formarea personalului administraţiei specializat în acest domeniu CCN a fost creat în 2004[2], ataşat Centrului Naţional de Informaţii (CNI). De fapt, Legea 11/2002, care reglementează CNI, încredinţează Centrului exercitarea funcţiilor legate de securitatea tehnologiilor informaţiei şi de protecţia informaţiilor clasificate, conferindu-i secretarului de stat director responsabilitatea de a conduce CCN. Din acest motiv, CCN împarte cu CNI mijloace, proceduri, reglementări şi resurse.

În cadrul CCN funcţionează CCN-CERT care este echipa de răspuns la incidentele de securitate cibernetică. Acest serviciu a fost creat în 2006 în cadrul guvernului naţional spaniol, iar funcţiile sale sunt stabilite în Legea 11/2002 de reglementare a Centrului naţional de informaţii, în Decretul regal 421/2004 de reglementare a CCN şi în Decretul regal 311/2022 din 3 mai, care reglementează sistemul de securitate naţională. La început, CCN-CERT şi-a concentrat activitatea asupra sistemelor diferitelor administraţii (generale, regionale şi locale) şi, ulterior, a extins această responsabilitate la atacurile cibernetice asupra sistemelor întreprinderilor din sectoarele de interes strategic pentru securitatea naţională şi pentru economia ţării în ansamblu.

Misiunea sa este de a contribui la îmbunătăţirea securităţii cibernetice spaniole, fiind centrul naţional de alertă şi răspuns care cooperează şi ajută la un răspuns rapid şi eficient la atacurile, inclusiv coordonarea la nivelul statului a diferitelor echipe de răspuns la incidente sau centre de operaţiuni de securitate cibernetică existente. În cazurile de gravitate deosebită care sunt stabilite prin reglementări şi care necesită un nivel de coordonare mai ridicat decât cel necesar în situaţii obişnuite, CCN-CERT exercita coordonarea naţională a răspunsului tehnic al CSIRT-urilor.

În conformitate cu aceste reglementări, CCN-CERT este responsabil de gestionarea incidentelor informatice care afectează orice organism sau întreprindere publică. În cazul operatorilor critici din sectorul public, gestionarea incidentelor cibernetice va fi realizată de CCN-CERT în coordonare cu (CNPIC).

În acelaşi mod, Strategia naţională de securitate cibernetică acordă CCN-CERT un rol central în linia de acţiune Securitatea sistemelor informatice şi de telecomunicaţii susţinute de administraţiile publice, prin consolidarea capacităţilor de informaţii, detectare, analiză şi răspuns ale CCN-CERT şi ale sistemelor sale de detectare şi avertizare rapidă.

Începând cu 28 octombrie 2014, Institutul Naţional de Tehnologii de Comunicaţii, S.A. (INTECO) a fost redenumit Institutul Naţional de Securitate Cibernetică din Spania M.P., S.A. (INCIBE), în conformitate cu hotărârea adoptată în cadrul Adunării Generale din 27 octombrie 2014. Prin această schimbare de nume şi de imagine, INCIBE a căpătat o identitate în conformitate cu orientarea strategică şi poziţionarea sa ca centru naţional de referinţă în domeniul securităţii cibernetice.

Institutul Naţional de Securitate Cibernetică din Spania M.P., S.A. (INCIBE) este o companie aflată în subordinea Ministerului pentru Transformare Digitală şi Funcţie Publică prin intermediul Secretarului de Stat pentru Digitalizare şi Inteligenţă Artificială şi este entitatea de referinţă pentru dezvoltarea securităţii cibernetice şi a încrederii digitale a cetăţenilor, a reţelei academice şi de cercetare spaniole (RedIRIS) şi a companiilor, în special pentru sectoarele strategice. Ca centru de excelenţă, INCIBE este un instrument al guvernului pentru dezvoltarea securităţii cibernetice. În

acest scop, cu o activitate bazată pe cercetare, furnizarea de servicii şi coordonarea cu agenţi cu competenţe în domeniu, INCIBE coordonează diferite acţiuni pentru securitatea cibernetică la nivel naţional şi internaţional.

INCIBE-CERT este centrul de referinţă de răspuns la incidente de securitate pentru cetăţeni şi entităţi de drept privat din Spania, gestionat de Institutul Naţional de Securitate Cibernetică. În cazul gestionării incidentelor care afectează operatorii critici din sectorul privat, INCIBE-CERT este operat în comun de INCIBE şi OCC, Biroul de coordonare a securităţii cibernetice al Ministerului de Interne. INCIBE-CERT este una dintre echipele de răspuns la incidente de referinţă care se coordonează cu restul echipelor naţionale şi internaţionale pentru a îmbunătăţi eficienţa în lupta împotriva infracţiunilor care implică reţele şi sisteme informatice.

În Portugalia există mai multe act normative prin care s-a reglementat gradual domeniul securităţii cibernetice. Prin Rezoluţia Consiliului de Miniştri nr. 42/2012, din 13 aprilie, este creat comitetul de instalare, care are ca scop crearea, instalarea şi funcţionarea unui Centru Naţional de Securitate Cibernetică în Portugalia. La 6 octombrie 2014, prin Decretul-lege 69/2014 este creat Centrul Naţional de Cibersecuritate (referit atunci ca CNCSeg) în cadrul Oficiului Naţional de Securitate al ţării. Centrul îşi dobândeşte denumirea actuală prin Decretul-lege nr. 136/2017. Odată cu publicarea Legii nr. 46/2018, care stabileşte regimul juridic al securităţii spaţiului cibernetic[1], CNCS primeşte competenţa de autoritate naţională de securitate cibernetică în cadrul Oficiului Naţional de Securitate al Portugaliei, iar ca echipă de răspuns la incidentele de securitate cibernetică este desemnat CERT.PT care exercită coordonarea operaţională în materie de răspuns la incidente, în special în colaborare cu echipele sectoriale de răspuns la incidente de securitate IT.

Regimul juridic al securităţii spaţiului cibernetic se aplică entităţilor administraţiei publice, operatorilor de infrastructuri critice, operatorilor de servicii esenţiale, furnizorilor de servicii digitale, precum şi oricăror alte entităţi care utilizează reţele şi sisteme informatice, respectiv în cadrul notificării voluntare a incidentelor.

Legea 46/2018 instituie, în capitolul II, Structura naţională pentru securitatea spaţiului cibernetic, din care face parte Consiliul Superior pentru Securitatea Spaţiului Cibernetic, ca organism specific de consultare a prim-ministrului cu privire la chestiuni legate de securitatea spaţiului cibernetic. Tot în acest capitol, se instituie Centrul Naţional de Securitate Cibernetică ca autoritate naţională de securitate cibernetică şi „CERT.PT" ca echipă naţională de răspuns la incidente de securitate informatică.

Capitolul III stabileşte că entităţile cărora li se aplică regimul juridic privind securitatea spaţiului cibernetic trebuie să adopte cerinţe de securitate şi să notifice Centrului Naţional de Securitate Cibernetică incidentele cu un impact relevant asupra securităţii reţelelor şi sistemelor lor informatice. În sfârşit, capitolul IV consacră regimul de supraveghere şi sancţiuni, iar capitolul V consacră dispoziţiile finale, cu accent pe regimul de identificare a operatorilor de servicii esenţiale şi a furnizorilor de servicii digitale.

Decretul-lege nr. 65/2021, prevede aplicarea cerinţelor de securitate şi de notificare a incidentelor pentru toate entităţile din domeniu, cu excepţia furnizorilor de servicii digitale cărora, în ceea ce

privește cerințele de securitate și limitele pentru notificarea incidentelor, li se aplică Regulamentul de punere în aplicare (UE) 2018/151 al Comisiei. Obligațiile acestor entități includ, de asemenea:

- să desemneze și să comunice CNCS punctul de contact permanent respectiv și persoana responsabilă cu securitatea;
- să pregătească inventarul activelor și să transmită CNCS o listă a activelor;
- să elaboreze un plan de securitate;
- să elaboreze și să transmită CNCS raportul anual.

În calitate de coordonator operațional și de autoritate națională în materie de securitate cibernetică cu entitățile de stat, Centrul Național de Cibersecuritate își îndreaptă eforturile și către societate în general, alături de operatorii de infrastructuri critice naționale, operatorii de servicii esențiale și furnizorii de servicii digitale din Portugalia. CNCS dezvoltă un set de activități destinate cetățenilor și organizațiilor, cum ar fi:

- sensibilizarea și formarea pentru comportamente și atitudini (mai) sigure și responsabile în utilizarea tehnologiei și a spațiului cibernetic și formare specializată în diverse domenii ale securității cibernetice;
- elaborarea și difuzarea de alerte, orientări și bune practici pentru utilizarea (mai) sigură a tehnologiei de către cetățeni și organizații, precum și recomandări tehnice și elaborarea de reglementări și referințe destinate în special organizațiilor;
- producerea de cunoștințe privind starea securității cibernetice naționale în diferitele sale aspecte, inclusiv definirea nivelului național de alertă de securitate cibernetică;
- prin intermediul serviciului său CERT.PT, acreditat la nivel internațional și în coordonare cu celelalte entități competente, coordonează răspunsul la incidentele care afectează spațiul cibernetic de interes național; și
- în cadrul domeniului de aplicare al regimului juridic pentru securitatea spațiului cibernetic, care transpune directiva europeană privind securitatea rețelelor și a informațiilor, exercită competențe de reglementare și supraveghere pentru diferitele sectoare de activitate economică.

In rețeaua CSIRT, așa cum este actualizată de către ENISA în pagina CSIRTs by Country - Interactive Map — ENISA (europa.eu), pentru Portugalia sunt înregistrate 36 de echipe de răspuns la incidente de cibersecuritate. Acestea operează în diferite domenii: public, militar, financiar, comercial, educație/cercetare, utilități etc.O singură echipă dintre acestea figurează in domeniul energiei, și anume CSIRT EDP, care activează în cadrul societății EDP[3]. Această societate are o activitate complexă, fiind furnizor de energie electrică, gaz dar și de servicii de curierat și de sănătate. Dintre cele 36 de echipe CSIRT înregistrate în Portugalia, observăm că numai 6 sunt membre ale Forumului Echipelor de Răspuns la Incidentele de Securitate (FIRST).

În Suedia, Myndigheten för samhällsskydd och beredskap (MSB) coordonează securitatea cibernetică pentru infrastructura energetică prin CERT-SE. Legea suedeză de transpunere a Directivei NIS reglementează activitățile CERT-SE în domeniul energetic. CERT-SE are aproximativ 20 de experți dedicați sectorului energetic. Finanțarea provine din bugetul de stat, cu

alocări de aproximativ 5 milioane de euro anual pentru securitatea cibernetică a infrastructurii critice

.

În Austria, securitatea cibernetică în sectorul energetic este coordonată de Austrian Energy CERT, care funcționează sub Austrian Power Grid AG (APG). Legea principală care reglementează securitatea cibernetică a infrastructurilor critice în Austria este Netz- und Informationssicherheitsgesetz (NISG), care implementează Directiva NIS. Energy CERT a fost înființat în 2015 și este responsabil de monitorizarea, prevenirea și răspunsul la incidentele cibernetice în rețelele de distribuție și transport al energiei din Austria. CERT-ul austriac din sectorul energetic colaborează cu Computer Emergency Response Team - Austria (CERT-AT), care este echipa națională de răspuns la incidente. Austria este renumită pentru colaborarea sa eficientă între sectorul public și privat, cu un accent pe schimbul de informații între operatorii de infrastructură critică și autoritățile naționale. Austrian Energy CERT este finanțat în principal din fondurile APG și are un buget anual estimat la aproximativ 3-5 milioane de euro, în funcție de proiectele în derulare. Compoziția echipei este flexibilă, cu aproximativ 15-20 de experți permanenți și colaboratori externi din domeniul privat care sunt implicați în proiecte specifice.

Odată cu punerea în aplicare a primei directive NIS a UE prin Legea federală pentru asigurarea unui nivel ridicat de securitate a rețelelor și sistemelor informatice (NISG), GovCERT a primit un temei juridic clar în 2018. Secțiunile 14 și 15 stabilesc sarcinile și cerințele pentru echipele de urgență informatică, așa cum sunt denumite CERT-urile în lege. Odată cu intrarea în vigoare a Legii privind securitatea rețelelor și a sistemelor informatice (NISG) în 2018, funcționarea GovCERT Austria a fost definită legal ca o sarcină a Cancelarului federal. GovCERT Austria este responsabilă de primirea rapoartelor privind riscurile, incidentele și incidentele de securitate la nivelul instituțiilor administrației publice la nivel federal, la nivel de stat și local.

GovCERT Austria este echipa guvernamentală de intervenție în caz de urgență informatică pentru administrația publică din Austria. Din aprilie 2008, Cancelaria Federală operează și această facilitate, prin Departamentul I/8, în cooperare cu CERT.at. De atunci, Cancelaria Federală îndeplinește sarcinile GovCERT Austria – mai precis partea strategică a GovCERT Austria – și utilizează resursele tehnice și calificările tehnice ale CERT.at adică partea tehnică/operațională a GovCERT Austria, pentru a aborda și preveni incidentele de securitate în domeniul tehnologiilor informației și comunicațiilor (TIC) în administrația publică. GovCERT Austria promovează, de asemenea, dezvoltarea unor echipe de intervenție în caz de urgență informatică specifice fiecărui sector. În cazul atacurilor asupra calculatoarelor la nivel național, CERT.at coordonează și informează operatorii de rețea respectivi și echipele locale de securitate responsabile.

Așadar, Cancelaria Federală austriacă se ocupă de coordonarea strategică în domeniul cibernetic, care include atât coordonarea națională, cât și relația cu securitatea europeană în domeniu. În cadrul Cancelariei Federale, Departamentul I/8 Securitatea cibernetică și Centrul de calcul al crizelor este responsabil de domeniul securității cibernetice. Biroul pentru securitatea strategică a rețelelor și a sistemelor informatice face parte din Departamentul I/8 și răspunde pentru de punerea în aplicare a obligațiilor legale care decurg din Directiva NIS (UE) 2016/1148 în Austria și din Legea privind securitatea rețelelor și a sistemelor informatice (Legea NISG). În plus, autoritatea operațională NIS din cadrul Ministerului Federal de Interne îndeplinește sarcini operaționale.

Documentul GovCERT Austria RFC 2350 descrie structura, interfețele și serviciile GovCERT Austria într-o formă standardizată. Scopul principal este de a comunica altor echipe de securitate ce pot aștepta de la GovCERT Austria.

Centrul Național de Coordonare pentru Securitate Cibernetică (NCC-AT) face parte din rețeaua de centre naționale de coordonare la nivelul UE și, împreună cu Centrul European de Competență pentru Securitate Cibernetică (ECCC), formează noul cadru european pentru sprijinirea inovării și a politicii industriale în domeniul securității cibernetice. În Austria, Cancelaria federală operează, de asemenea, NCC-AT cu sprijinul Agenției austriece pentru promovarea cercetării (FFG), îndeplinind astfel mandatul Regulamentului (UE) 2021/887 de stabilire a Centrului european de competențe industriale, tehnologice și de cercetare în domeniul securității cibernetice și a Rețelei de centre naționale de coordonare.

Inițial, a existat „Strategia austriacă pentru securitate cibernetică" (ÖSCS) elaborată în 2013. Ca parte a acestei strategii, a fost definit pentru prima dată în Austria un concept proactiv de protecție a spațiului cibernetic și a persoanelor din spațiul virtual, garantând în același timp respectarea drepturilor omului. O componentă a acestui concept a fost extinderea și consolidarea rolului GovCERT Austria, gestionat de Cancelaria Federală (BKA). Provocările legate de dezvoltarea dinamică a spațiului cibernetic au făcut necesară actualizarea ÖSCS.

Odată cu noua Strategie austriacă de securitate cibernetică, guvernul a adoptat în 2021 un concept reînnoit, cuprinzător și proactiv pentru protecția spațiului cibernetic și a persoanelor din spațiul virtual. ÖSCS 2021 formează cadrul strategic pentru politica națională de securitate cibernetică, precum și pentru crearea pe termen lung a unui spațiu cibernetic sigur, ca o contribuție la creșterea rezilienței Austriei și a Uniunii Europene printr-o abordare la nivelul întregii administrații.

Regulamentul de procedură al GovCERT Austria specifică în esență participarea la schimbul activ de informații și participarea la reuniunile GovCERT Austria: obiectivul explicit al GovCERT Austria este de a promova înființarea de echipe de răspuns la incidentele de Securitate cibernetică (CSIRT) în toate sectoarele. Austria are 10 echipe de răspuns la incidente de cibersecuritate înregistrate formal.

Austrian Energy CERT (AEC), una dintre acestea, este deținută de industria energiei din Austria. Rolul său este să întărească securitatea IT și competențele din acest domeniu. În mod curent, AEC gestionează incidentele de securitate, procesând mesajele și solicitările de informații, oferă instruire, participă la crearea de concept de Securitate pentru industria energiei electrice și a gazului natural. Totodată, AEC are rolul de punct unic de contact petru incidentele de cibersecuritate din domeniul energiei, ceea ce implică o coordonare a experților IT din industrie. AEC este prima echipă de intervenție în caz de urgență informatică (CERT) specifică industriei din Europa pentru întregul sector energetic și funcționează în conformitate cu cerințele Directivei NIS publicată în 2016. AEC coordonează grupul de lucru ARGE E-CERT format din companii din industria energetică austriacă care a fost constituit la sfârșitul lunii octombrie 2015.

Consorțiul ARGE E-CERT cuprinde 20 de parteneri care reprezintă toate companiile din industria energetică austriacă din sectorul energetic (electricitate și gaze). Consorțiul este alcătuit din: 13 companii mari din industria energiei electrice: producția și distribuția de energie electrică, precum și gaz, operatorul sistemului austriac de transport al energiei electrice, cei patru mari operatori de rețele de gaze (operatorii sistemelor de transport și distribuție, TSO și DSO) cel mai mare producător și comerciant de energie electrică din Austria precum și un grup care include toate întreprinderile mici.

Părțile contractante formează un consorțiu sub forma juridică a unui parteneriat de drept civil, adică fără personalitate juridică proprie, care funcționează sub denumirea ARGE „Stabilirea și funcționarea unei echipe de intervenție în caz de urgență informatică pentru industria energetică austriacă" sau, pe scurt, ARGE E-CERT. Conducerea ARGE este formată din două persoane, fiecare dintre acestea fiind numită de adunarea generală pentru un an și putând fi demisă în orice moment. Coordonarea cu autoritățile are loc prin intermediul consiliului consultativ.

Belgia este una dintre cele două țări, alături de Croația, care și-a actualizat legislația în domeniu. Legea din 26 aprilie 2024 de instituire a unui cadru pentru securitatea cibernetică a rețelelor și sistemelor informatice de interes general pentru siguranța publică (Legea NIS2) transpune Directiva (UE) 2022/2555 a Parlamentului European și a Consiliului din 14 decembrie 2022 (Directiva NIS2) în Belgia. Aceasta va intra în vigoare la 18 octombrie 2024.

Legea NIS2 actualizează cadrul juridic belgian privind securitatea cibernetică prin înlocuirea vechii Legi din 7 aprilie 2019 de instituire a unui cadru pentru securitatea rețelelor și sistemelor informatice de interes general pentru securitatea publică (legea NIS1). Noul text este însoțit de Decretul regal din 9 iunie 2024 care pune în aplicare dispozițiile sale, de exemplu prin desemnarea Centrului pentru Securitate Cibernetică din Belgia (CCB) ca autoritate națională de securitate cibernetică. Scopul legii este acela de a consolida măsurile de securitate cibernetică, gestionarea incidentelor și supravegherea entităților care furnizează servicii esențiale pentru menținerea activităților societale sau economice critice. De asemenea, legea vizează îmbunătățirea coordonării politicilor publice în domeniul securității cibernetice. Pentru a fi acoperită de legea belgiană NIS2, o organizație trebuie: să furnizeze un serviciu enumerat în anexele I și II ale legii NIS2 în Uniunea Europeană; să depășească pragurile de mărime ale unei întreprinderi mijlocii stabilite prin Recomandarea 2003/361/CE, și anume să aibă o forță de muncă de cel puțin 50 de lucrători cu normă întreagă sau o cifră de afaceri anuală sau un bilanț total care depășește 10 milioane de euro; și să aibă sediul în Belgia.

Este important, în primul rând, de remarcat faptul că Legea NIS2 se aplică automat tuturor entităților identificate ca operatori de infrastructuri critice în sensul Legii din 1 iulie 2011 privind securitatea și protecția infrastructurilor critice, indiferent de mărimea acestora. În temeiul legii NIS2, acești operatori sunt entități esențiale.

În al doilea rând, entitățile identificate ca operatori de servicii esențiale (OES) sau furnizori de servicii digitale (DSP) în temeiul legii NIS1 intră, în principiu, și sub incidența legii NIS2 dacă depășesc pragurile de mărime necesare. Motivul este simplu: domeniul de aplicare al directivei NIS2 este o extindere a domeniului de aplicare al directivei NIS1. Pentru a intra în domeniul de aplicare al legii NIS2, o organizație trebuie să aibă o anumită dimensiune. În principiu, o organizație trebuie să fie cel puțin o întreprindere mijlocie, calculată utilizând anexa la Recomandarea 2003/361/CE a Comisiei, dar există anumite excepții.

Tipuri de entități ce intră în domeniul de aplicare al legii NIS2 (indiferent de mărimea lor):

- prestatorii de servicii fiduciare calificați (esențial);

- furnizori de servicii fiduciare necalificate (important în cazul microîntreprinderilor, întreprinderilor mici sau mijlocii şi esenţial în cazul întreprinderilor mari);

- furnizori de servicii DNS (esenţial);

- registre de nume TLD (esenţial);

- servicii de înregistrare a numelor de domeniu (numai pentru obligaţia de înregistrare);

- furnizori de reţele publice de comunicaţii electronice (esenţial);

- furnizorii de servicii de comunicaţii electronice accesibile publicului (esenţial);

- entităţi identificate ca operatori de infrastructură critică (esenţial);

- entităţile administraţiei publice care depind de statul federal (esenţial).

Independent de aceste norme, autoritatea naţională de securitate cibernetică (CCB) va putea, de asemenea, să identifice în mod specific entităţile clasificate ca fiind „esenţiale" sau „importante", de exemplu atunci când acestea sunt singurul furnizor al unui serviciu sau atunci când întreruperea serviciului furnizat ar putea avea un impact semnificativ asupra securităţii publice, siguranţei publice sau sănătăţii publice.

Dincolo de plafonul de mărime, condiţia privind serviciile impune unei organizaţii să analizeze pe deplin fiecare dintre serviciile sale furnizate terţilor, pe sectoare şi subsectoare. Acest lucru este important, având în vedere că chiar şi cel mai auxiliar serviciu furnizat poate face ca o organizaţie în ansamblu să intre în domeniul de aplicare al legii NIS2, cu excepţia cazului în care se prevede altfel în definiţia serviciului respectiv.Toate serviciile care intră sub incidenţa legii NIS2 sunt detaliate în anexele I şi II (sau în definiţii) la Lege. În cazul în care o organizaţie furnizează unul dintre serviciile menţionate acolo şi îndeplineşte criteriul de mărime corespunzător, atunci aceasta intră în domeniul de aplicare al legii NIS2 dacă are legătură cu Belgia. Diferitele servicii sunt grupate pe sectoare şi subsectoare. Cu titlu de exemplu:

- Anexa I listează Sectoare extrem de critice: energie, energie electrică, încălzire şi răcire urbană, petrol, gaz, hidrogen, transport (aer, feroviar, pe apă, rutier), sectorul bancar, infrastructura pieţei financiare, sănătate, apă potabilă, apă reziduală, infrastructură digitală, gestionarea serviciilor TIC (B2B), administraţie publică, spaţiu.
- Anexa II enumeră alte servicii critice: servicii poştale şi de curierat, gestionarea deşeurilor, fabricarea, producerea şi distribuţia de produse chimice, Producţia, prelucrarea şi distribuţia de produse alimentare, industria prelucrătoare, fabricarea dispozitivelor medicale şi a dispozitivelor medicale de diagnostic in vitro, fabricarea produselor informatice, electronice şi optice, fabricarea de echipamente electrice, fabricarea de maşini şi echipamente n.c.a., fabricarea autovehiculelor, remorcilor şi semiremorcilor, fabricarea altor echipamente de transport, furnizori de servicii digitale, cercetare.

În principiu, legea belgiană NIS2 se aplică numai entităților stabilite în Belgia care își furnizează serviciile sau își desfășoară activitățile în UE. Două concepte sunt importante aici:

- Conceptul de „stabilire" - implică exercitarea efectivă a unei activități prin intermediul unei instalații permanente, indiferent de forma juridică adoptată, fie că este vorba de sediul social, de o sucursală simplă sau de o filială cu personalitate juridică.
- Noțiunea de „entitate", cum este definită la articolul 8 punctul 37 din legea NIS2 - ca o persoană fizică sau juridică creată și recunoscută ca atare în temeiul legislației naționale a locului său de stabilire și care poate, acționând în nume propriu, să exercite drepturi și să fie supusă unor obligații.

Legea NIS2 definește „incidentul" ca fiind un eveniment care compromite disponibilitatea, autenticitatea, integritatea sau confidențialitatea datelor stocate, transmise sau prelucrate sau a serviciilor oferite de rețele și sisteme informatice sau accesibile prin intermediul acestora.

Un incident „semnificativ" este orice incident care are un impact semnificativ asupra furnizării de servicii în sectoarele sau subsectoarele enumerate în anexele la legea NIS2 și care a cauzat sau este susceptibil de a cauza perturbări grave în funcționarea oricăruia dintre serviciile din sectoarele sau subsectoarele enumerate în anexele I și II sau pierderi financiare pentru entitatea în cauză; sau a cauzat sau este posibil să cauzeze daune materiale, personale sau morale semnificative altor persoane fizice sau juridice.

În cazul în care incidentul în cauză se încadrează în această definiție, notificarea se face către un CSIRT național (CCB). Pe lângă notificarea către CSIRT-ul național, după caz, entitățile în cauză informează destinatarii serviciilor lor cu privire la incidentele semnificative care pot afecta furnizarea serviciilor din anexele I și II care le sunt furnizate. De asemenea, entitățile informează destinatarii serviciilor lor care pot fi afectați de o amenințare cibernetică semnificativă cu privire la amenințarea respectivă și la toate măsurile și corecțiile care pot fi luate pentru a răspunde la aceasta. În cadrul ENISA sunt înregistrate (pentru Belgia) 11 echipe de răspuns la incidente de securitate cibernetică (CSIRT). Acestea își desfășoară activitatea în domeniul public, militar, educație-cercetare, trafic aerian, comercial și al furnizorilor de internet.
În Danemarca, securitatea cibernetică în sectorul energetic este coordonată de Center for Cybersikkerhed (CFC), o organizație care funcționează în cadrul Ministerului Apărării. Conform Legii privind securitatea cibernetică adoptate în 2018, CFC are obligația de a monitoriza rețelele critice din domeniul energetic și de a coordona răspunsurile la incidentele cibernetice.. CFC are o divizie dedicată sectorului energetic, care colaborează strâns cu autoritățile de reglementare a energiei și cu companiile private. Bugetul alocat pentru securitatea cibernetică în acest sector este de aproximativ 10 milioane de euro anual, fonduri provenite din bugetul de stat. Compoziția echipei CFC variază în funcție de necesități, dar în sectorul energetic sunt aproximativ 30 de specialiști angajați permanent. Danemarca pune un accent puternic pe protecția infrastructurii energetice, având un program național de conștientizare și pregătire cibernetică destinat operatorilor de energie.

Polonia și-a înființat CSIRT-ul sectorial pentru energie prin intermediul Narodowe Centrum Bezpieczeństwa Cyberprzestrzeni (NCBC), o agenție națională care funcționează sub Ministerul

Apărării. Legea privind securitatea cibernetică, adoptată în 2018 și actualizată în 2021 pentru a implementa cerințele Directivei NIS 2, prevede înființarea unor echipe de răspuns la incidente pentru sectoarele critice, inclusiv energie. Polonia este una dintre țările UE care a investit puternic în securitatea cibernetică a infrastructurilor sale energetice, având un buget dedicat de aproximativ 15 milioane de euro anual pentru protecția sectorului energetic. Echipa NCBC dedicată energiei este formată din 40 de specialiști și are responsabilitatea de a monitoriza toate rețelele energetice critice din Polonia. NCBC colaborează cu operatorii privați din domeniul energetic pentru a preveni și a răspunde rapid la amenințările cibernetice, în special în contextul unui peisaj geopolitic instabil în regiunea estică a Europei.

La 1 august 2018 Președintele Poloniei a semnat Legea nr. 1560/2018 privind sistemul național de securitate cibernetică, care transpune în sistemul juridic polonez Directiva (UE) privind măsurile pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în întreaga Uniune (Directiva 2016/1148), așa-numita Directivă NIS2. Sistemul național de securitate cibernetică urmărește să asigure securitatea cibernetică la nivel național, în special pentru furnizarea neîntreruptă a serviciilor esențiale și a serviciilor digitale și atingerea unui nivel suficient de ridicat de securitate a sistemelor TIC prin care se furnizează aceste servicii.

Sistemul include operatori de servicii esențiale (în special din sectoarele **energiei**, transporturilor, sănătății și bancar), furnizori de servicii digitale, echipe CSIRT de răspuns la incidente la nivel național, echipe sectoriale și un punct unic de contact (Punctul Național de Contact este în cadrul ministerului pentru digitalizare) pentru comunicare în cadrul cooperării în Uniunea Europeană în domeniul politicii de securitate cibernetică. Operatorii de servicii esențiale trebuie să pună în aplicare măsuri de protecție eficiente, să evalueze riscurile de securitate cibernetică, să comunice și să gestioneze incidentele majore în cooperare cu CSIRT-urile la nivel național. Operatorii de servicii esențiale trebuie, de asemenea, să numească o persoană responsabilă de securitatea cibernetică a serviciilor furnizate, de gestionarea și raportarea incidentelor și de schimbul de cunoștințe privind securitatea cibernetică.

Organele administrației publice și întreprinderile de telecomunicații sunt, de asemenea, incluse în sistemul național de securitate cibernetică - într-un mod armonizat cu reglementările existente în acest domeniu.Furnizorii de servicii digitale, și anume piețele online, serviciile de cloud computing și motoarele de căutare, sunt, de asemenea, responsabili cerințele de securitate cibernetică. Datorită specificității internaționale a acestor entități, obligațiile furnizorilor de servicii digitale fac obiectul unui regim de reglementare armonizat la nivelul UE. Legea se referă aici la decizia de punere în aplicare a Comisiei Europene.

Există trei echipe principale de răspuns la nivel național în domeniul public. Acestea sunt CERT NASK, CSIRT GOV și CSIRT MON. Ale căror sarcini sunt definite in art. 26 din Legea 1560/2018. Echipa CERT Polska funcționează în cadrul structurilor NASK - Institutul Național de Cercetare, unde desfășoară activități științifice, operează registrul național al domeniilor .pl și furnizează servicii TIC avansate. CERT Polska este prima echipă de răspuns la incidente înființată în Polonia. Datorită activității sale dinamice din 1996 în mediul echipelor de intervenție, aceasta a devenit o entitate recunoscută și experimentată în domeniul securității informatice. De la începutul existenței echipei, nucleul activității acesteia a fost gestionarea incidentelor de securitate și cooperarea cu unități similare din întreaga lume, atât în activități operaționale, cât și în activități de cercetare și implementare. Din 1998, CERT Polska a fost membră a forumului internațional al echipelor de

intervenție - FIRST, iar din 2000 a fost membră a grupului de lucru al echipelor europene de intervenție - TERENA TF-CSIRT și a organizației Trusted Introducer care funcționează în cadrul acestuia. În 2005, la inițiativa CERT Polska, a fost înființat Abuse FORUM, iar în 2010 CERT Polska s-a alăturat Grupului de lucru Anti-Phishing, o asociație care reunește companii și instituții care luptă activ împotriva criminalității online.De la intrarea în vigoare a Legii din 5 iulie 2018 privind sistemul național de securitate cibernetică, echipa a îndeplinit unele dintre sarcinile CSIRT NASK, în conformitate cu articolul 26 din această lege. CERT NASK gestionează incidente raportate de:

- unități ale administrației locale
- unități bugetare, instituții bugetare ale administrației locale
- agenții executive, instituții bugetare
- universități publice și Academia Poloneză de Științe
- Oficiul de inspecție tehnică, Agenția poloneză pentru servicii de navigație aeriană, Centrul polonez pentru acreditare
- Fondul național pentru protecția mediului și gestionarea apelor și fondurile provinciale pentru protecția mediului și gestionarea apelor
- societăți de drept comercial care îndeplinesc sarcini de utilitate publică care vizează satisfacerea continuă și neîntreruptă a colectivității
- cetățeni.

Echipa CSIRT GOV[2], condusă de șeful Agenției de Securitate Internă, acționează la nivel național fiind responsabilă de coordonarea răspunsului la incidentele informatice care au loc în domeniul amenințărilor la adresa securității, importante din punctul de vedere al continuității funcționării statului, a sistemelor TIC ale organismelor administrației publice sau a sistemului de rețele TIC acoperit de o listă uniformă de facilități, instalații, dispozitive și servicii incluse în infrastructura critică, precum și a sistemelor TIC ale proprietarilor și deținătorilor de facilități, instalații sau echipamente de infrastructură critică. CSIRT GOV gestionează incidente raportate de: autorități publice, inclusiv organe ale administrației publice, organe de control de stat și de aplicare a legii, instanțe și tribunale, Banca Națională Poloneză, Bank Gospodarstwa Krajowego;

CSIRT MON este echipa aflată în cadrul Ministerului Apărării Naționale și gestionează incidente raportate de:

- entități aflate în subordinea sau sub supravegherea ministrului apărării naționale, inclusiv entități ale căror sisteme TIC sau rețele TIC sunt incluse într-o listă uniformă de facilități, instalații, dispozitive și servicii incluse în infrastructura critică;
- întreprinzători cu o importanță economică și de apărare deosebită, în legătură cu care ministrul apărării naționale este organismul care organizează și supraveghează îndeplinirea sarcinilor de apărare a statului.

Legea din 5 iulie 2018 privind sistemul național de securitate cibernetică definește și **autoritățile competente** în materie de securitate cibernetică **responsabile cu supravegherea operatorilor de servicii esențiale** și servicii digitale. Operatorii de servicii esențiale vor trebui să pună în aplicare măsuri de protecție eficiente, să evalueze riscurile de securitate cibernetică și să raporteze și să

gestioneze incidentele majore în cooperare cu CSIRT-urile la nivel național. Autoritățile competente stabilite de Lege, conform art. 41, sunt:

- pentru **sectorul energetic - ministrul responsabil pentru energie**;
- pentru sectorul transporturilor, cu excepția subsectorului transportului pe apă - ministrul responsabil cu transporturile;
- pentru subsectorul transportului pe apă - ministrul responsabil de economia maritimă și ministrul responsabil de navigația interioară;
- pentru sectorul bancar și infrastructura pieței financiare - Autoritatea poloneză de supraveghere financiară;
- pentru sectorul sănătății, ministrul responsabil cu problemele de sănătate;
- pentru sectorul alimentării și distribuției cu apă potabilă - ministrul delegat pentru gospodărirea apelor
- pentru sectorul infrastructurii digitale, ministrul responsabil cu informatizarea;
- pentru sectorul infrastructurii digitale, ministrul apărării naționale;
- pentru furnizorii de servicii digitale ministrul responsabil cu informatizarea.

Sarcinile autorităților competente enumerate mai sus, sunt precizate in art. 42 din Lege, astfel că autoritățile competente:

- analizează continuu entitățile dintr-un anumit sector pentru recunoașterea/nerecunoașterea acestora ca operator de servicii și emite deciziile necesare;
- imediat după emiterea unei decizii privind recunoașterea ca operator de servicii esențiale sau a unei decizii privind expirarea deciziei privind recunoașterea ca operator de servicii esențiale, înaintează ministrului responsabil cu informatizarea cereri de înscriere în registrul operatorilor de servicii esențiale sau de radiere din acest registru
- elaborează, în cooperare cu CSIRT NASK, CSIRT GOV, CSIRT MON și echipele sectoriale de securitate cibernetică, recomandări privind acțiunile menite să consolideze securitatea cibernetică, inclusiv orientări sectoriale privind raportarea incidentelor;
- monitorizează aplicarea prevederilor Legii de către operatorii de servicii-cheie și furnizorii de servicii digitale;
- solicită, la cererea CSIRT NASK, CSIRT GOV sau CSIRT MON, operatorilor de servicii esențiale sau furnizorilor de servicii digitale să elimine, într-o perioadă determinată, vulnerabilitățile care au condus sau ar fi putut conduce la un incident grav, semnificativ sau critic;
- efectuează inspecții la operatorii de servicii esențiale și la furnizorii de servicii digitale;
- poate coopera cu autoritățile competente din statele membre ale Uniunii Europene prin intermediul Punctului unic de contact;
- prelucrează informații, inclusiv date cu caracter personal, referitoare la serviciile esențiale și serviciile digitale furnizate și la operatorii de servicii esențiale sau furnizorii de servicii digitale;
- participă la exerciții de securitate cibernetică organizate în Republica Polonă sau în Uniunea Europeană.

Legea prevede şi faptul că autoritatea responsabilă pentru cibersecuritate poate stabili echipe sectoriale pentru anumite domenii de activitate, caz în care informează operatorii de servicii cheie despre existenţa şi scopul echipei nou înfiinţate. În Polonia există în total 38 de echipe de răspuns la incidente de cibersecuritate. Dintre acestea, patru echipe sunt constituite în cadrul unor operatori de energie importanţi.

Unul dintre aceşti mari operatori este Enea SA, cu sediul in Poznan. Misiunea CERT ENEA este de a sprijini companiile din Grupul Enea să se protejeze împotriva atacurilor intenţionate şi rău intenţionate care ar împiedica integritatea activelor lor IT şi OT şi ar dăuna intereselor Grupului Enea. Domeniul de aplicare al activităţilor CERT ENEA acoperă prevenirea, detectarea, răspunsul şi recuperarea. Alt operator care deţine o echipă de răspuns la incidente este Energa SA cu sediul în Gdansk. Acesta este unul dintre furnizorii majori de energie electrică dar şi de gaz şi energie termică.

În cadrul operatorului GAZ-SYSTEM îşi desfăşoară activitatea echipa GAZ-SYSTEM CERT care are misiunea de a răspunde activ şi gestiona cuprinzător incidentele de securitate TIC la GAZ-SYSTEM S.A. De asemenea, compania E.ON găzduieşte E.ON CERT care sprijină în primul rând rezistenţa cibernetică a grupului E.ON SE şi a filialelor în care E.ON este acţionar majoritar şi a societăţilor 50/50, la cererea societăţii. Componente sunt echipe de securitate a informaţiilor.

Cehia a implementat măsuri avansate de protecţie cibernetică pentru sectorul energetic prin intermediul National Cyber and Information Security Agency (NÚKIB), care coordonează activităţile de securitate cibernetică la nivel naţional. Legea nr. 181/2014 privind securitatea cibernetică reglementează activitatea NÚKIB şi include obligaţii specifice pentru operatorii de infrastructură critică, inclusiv cei din domeniul energiei. CSIRT-ul sectorial pentru energie din Cehia este responsabil pentru monitorizarea continuă a reţelelor energetice şi pentru furnizarea de sprijin tehnic companiilor care operează infrastructura critică. NÚKIB colaborează strâns cu Ministerul Industriei şi Comerţului, care are responsabilitatea generală pentru sectorul energetic. Finanţarea pentru protecţia cibernetică în sectorul energetic provine din bugetul de stat şi din fonduri UE, cu un buget anual de aproximativ 8 milioane de euro. Echipa este formată din 25-30 de specialişti.
Finlanda şi-a dezvoltat CSIRT-ul pentru sectorul energetic prin intermediul National Cyber Security Centre Finland (NCSC-FI), care funcţionează sub Traficom, autoritatea naţională pentru comunicaţii şi transporturi. Legea privind securitatea cibernetică şi protecţia infrastructurilor critice adoptată în 2018 prevede obligaţia operatorilor de infrastructură critică să coopereze cu NCSC-FI pentru prevenirea şi răspunsul la incidentele cibernetice. Sectorul energetic este considerat o infrastructură de importanţă naţională strategică, iar CSIRT-ul sectorial are un rol esenţial în protejarea acestuia. Finlanda pune un accent puternic pe cooperarea public-privat şi schimbul de informaţii între autorităţile naţionale şi operatorii din domeniul energetic. Finanţarea pentru protecţia cibernetică a infrastructurii energetice este de aproximativ 12 milioane de euro anual, iar echipa dedicată sectorului energetic este formată din aproximativ 30 de experţi în securitate cibernetică. De asemenea, Finlanda participă activ la iniţiativele internaţionale de securitate cibernetică în cadrul ENISA şi NATO.

În Irlanda continuă să lucreze la proiectul legislativ de transpunere a directivei NIS2, având în vedere data scadentă,17 octombrie 2024. Centrul Naţional de Securitate Cibernetică (NCSC) a fost

înființat în 2011 și este o componentă operațională a Departamentului pentru Mediu, Climă și Comunicații (DECC). NCSC este responsabil cu consilierea și informarea furnizorilor de IT guvernamentali și de infrastructură națională critică cu privire la amenințările și vulnerabilitățile actuale asociate cu securitatea informațiilor în rețea. Rolurile principale ale NCSC sunt de a conduce gestionarea incidentelor majore de securitate cibernetică în întreaga guvernare, de a oferi îndrumări și consiliere cetățenilor și întreprinderilor cu privire la incidente majore de securitate cibernetică și de a dezvolta relații internaționale puternice în comunitatea globală de securitate cibernetică. Începând cu 2011, unitatea și-a concentrat eforturile pe consolidarea capacității și stabilirea unei baze stabile pentru activitatea sa operațională.

În cadrul NCSC activează Echipa națională/guvernamentală de răspuns la incidente de securitate informatică (CSIRT-IE). CSIRT-IE reprezintă, de asemenea, punctul național de contact pentru partenerii internaționali care doresc să informeze entitățile din Irlanda cu privire la problemele de securitate cibernetică. Din 2017, CSIRT-IE a fost acreditat de serviciul Trusted Introducer al TF-CSIRT.

În Irlanda mai activează HEAnet-CERT, centrul care deservește rețeaua irlandeză de educație și cercetare. Acesta este punctul unic de contact al rețelei HEAnet pentru clienții care se confruntă cu incidente de securitate informatică. În cazul în care un client suspectează o intruziune sau un atac, HEAnet-CERT oferă rapid sprijin, consiliere și expertiză. HEAnet-CERT oferă următoarele servicii tuturor clienților rețelei HEAnet:

- asistență tehnică cu privire la ce trebuie să facă în cazul unui incident;
- colectarea, analiza și raportarea de statistici privind incidentele;
- notificări către site-uri cu privire la faptul că acestea ar putea fi sursa, intermediarul sau ținta unui atac, deoarece acestea pot fi adesea inconștiente;
- HEAnet-CERT asistă, de asemenea, toți clienții HEAnet care doresc sprijin proactiv pentru probleme de securitate și vulnerabilități percepute.

În domeniul non-guvernamental există Serviciul irlandez de raportare și securitate a informațiilor (IRISS) care este o societate independentă fără scop lucrativ, cu răspundere limitată, înființată în 2008 pentru a oferi o serie de servicii gratuite întreprinderilor și consumatorilor irlandezi în legătură cu problemele de securitate a informațiilor, pentru a contribui la contracararea amenințărilor la adresa securității întreprinderilor irlandeze și a spațiului internet irlandez. Aceste servicii includ:

- furnizarea unui serviciu de alertă privind noile vulnerabilități și amenințări care pot compromite securitatea resurselor informatice și de comunicații pentru persoanele fizice, întreprinderile și organismele guvernamentale din Irlanda;
- furnizarea și alertarea cu privire la atacurile în curs de desfășurare asupra resurselor TIC din Irlanda pentru a permite altor entități să elaboreze și să pună în aplicare măsuri de protecție împotriva unor astfel de atacuri;
- furnizarea de statistici și rapoarte privind activitatea de criminalitate informatică din Irlanda pentru a ajuta organizațiile și persoanele fizice să își concentreze mai bine resursele asupra amenințărilor la adresa securității specifice Irlandei;
- oferă persoanelor și organizațiilor posibilitatea de a raporta incidentele de securitate;

- furnizează orientări şi de tehnici de bune practici privind modul de prevenire a incidentelor de securitate şi cel mai bun mod de a răspunde în cazul în care are loc un astfel de incident.

Gama de servicii de mai sus este asigurată de un nucleu de voluntari dedicaţi, experţi în domeniul securităţii informaţiilor, care îşi oferă gratuit serviciile comunităţii irlandeze de internet. IRISS este finanţat printr-o combinaţie de donaţii şi sponsorizări corporative.

În Ungaria, luând în considerare Strategia de securitate a Ungariei, Strategia naţională de securitate cibernetică a Ungariei şi Strategia de securitate cibernetică a Uniunii Europene, Parlamentul maghiar a adoptat Legea L din 2013 privind securitatea informaţiilor electronice ale organismelor de stat şi ale administraţiilor locale (IBTV)[1], care a intrat în vigoare la 1 iulie 2013. IBTV stabileşte ca obiectiv consolidarea activelor naţionale de date electronice şi securitatea sistemelor informatice electronice ale organismelor guvernamentale de stat şi locale, precum şi a sistemelor informatice vitale şi a componentelor sistemului; declară că organismul de stat care operează şi exploatează sistemele informatice electronice este responsabil pentru securitate. În plus, legea a stabilit sistemul organizaţional maghiar de apărare cibernetică, al cărui scop de bază este de a sprijini şi de a controla îndeplinirea sarcinilor de securitate a informaţiilor de către organismele de stat cu servicii de securitate şi de a dezvolta conştiinţa de securitate cu privire la întregul sistem organizaţional de stat.

Elementul de nivel strategic al sistemului organizaţional este Consiliul Naţional de Coordonare Cibernetică, a cărui sarcină este de a facilita coordonarea activităţilor strategice ale guvernului şi de a monitoriza punerea în aplicare, precum şi Forumul de Securitate Cibernetică, înfiinţat pentru a canaliza opinia profesională a sectorului privat în procesul decizional al guvernului.Elementele operaţionale ale sistemului de organizare sunt:

- autoritatea de securitate a informaţiilor responsabilă de verificarea şi aplicarea cerinţelor legale;
- un centru de gestionare a incidentelor care abordează direct atacurile şi ameninţările din spaţiul cibernetic şi
- organismul responsabil de identificarea punctelor slabe ale sistemelor informatice şi de testarea capacităţilor de protecţie a sistemului (evaluarea vulnerabilităţii).

Ca urmare a modificării IBTV în 2015, Serviciul Special pentru Securitate Naţională (SSNS) a fost desemnat să opereze sarcinile operaţionale de mai sus cu privire la sistemele informatice ale organizaţiilor guvernamentale de stat şi locale. Iar în cadrul acestei organizaţii a fost înfiinţat Centrul Naţional pentru Securitate Cibernetică (NKI) la 1 octombrie 2015. Centrul Naţional de Securitate Cibernetică pentru Ungaria a fost înfiinţat prin unificarea GovCERT-Ungaria, a Autorităţii Naţionale pentru Securitatea Informaţiilor Electronice (NEISA) şi a Autorităţii de Management a Apărării Cibernetice (CDMA). Astfel, Centrul este mai coordonat, iar punerea în aplicare a sarcinilor sunt mai eficiente în această organizaţie unificată. Datorită acestor măsuri, Centrul Naţional de Securitate Cibernetică poate urmări şi ajuta întregul ciclu de viaţă al securităţii informatice a sistemelor informatice electronice, de la evoluţie, faza de planificare, reglementare, până la control şi gestionarea incidentelor.

Ca urmare a modificărilor legislative care au intrat în vigoare la 1 ianuarie 2019, Centrul Național pentru Securitate Cibernetică îndeplinește sarcinile de gestionare a evenimentelor din sistemele informatice critice și componentele sistemelor, precum și gestionează evenimentele și supraveghează oficial furnizorii de servicii care trebuie notificate, conform Legii CVIII din 2001 privind anumite aspecte ale serviciilor de comerț electronic și ale serviciilor societății informaționale, cum ar fi piețele online, serviciile de căutare pe internet și serviciile cloud.

Sarcinile legale ale Centrului Național pentru Securitate Cibernetică includ, de asemenea, funcționarea așa-numitului Punct național de contact (SPOC), care este responsabil pentru coordonarea în Ungaria a incidentelor cibernetice cu impact ridicat în cadrul Uniunii Europene, primirea și trimiterea rapoartelor privind incidentele către organizațiile partenere internaționale.

În anul 2020 a fost emis Decretul guvernamental 374/2020 (VII.30.) privind identificarea, desemnarea și protecția sistemelor și instalațiilor critice din sectorul energetic. Decretul stabilește autoritățile sectoriale pentru definirea infrastructurilor critice din sectorul energetic. Acestea sunt:

- Autoritatea de reglementare în domeniul energiei și al serviciilor publice pentru sistemul de energie electrică, sistemul de gaze naturale și sectorul încălzirii urbane;
- Autoritatea minieră în ceea ce privește industria petrolieră și producția de gaze naturale;
- Primăria Capitalei și birourile guvernamentale / județene în calitatea lor decizională pentru chestiuni metrologice și tehnice pentru prelucrarea petrolului și depozitarea produselor petroliere.

Prin decret sunt definite criteriile sectoriale pentru infrastructură critică europeană, pentru infrastructura critică națională, efectul perturbator semnificativ în sectorul energetic, praguri pentru serviciile de bază în sectorul energetic, cerințele de calificare pentru ofițerul de contact în materie de securitate, norme sectoriale detaliate pentru evenimentele extraordinare și alte norme tehnice

În Ungaria există 3 echipe de răspuns la incidentele de securitate cibernetică, iar dintre acestea, Centrul Național de Securitate Cibernetică acoperă și domeniul energiei.

Secțiunea a 4-a
Impactul financiar asupra bugetului general consolidat atât pe termen scurt, pentru anul curent, cât și pe termen lung (pe 5 ani), inclusiv informații cu privire la cheltuieli și venituri.*)**

- în mii lei (RON) -

Indicatori	**Anul curent**	**Următorii patru ani**				**Media pe cinci ani**
1	2	3	4	5	6	7
	2025	2026	2027	2028	2029	
4.1 Modificări ale veniturilor bugetare, plus/minus, din care:						
a) buget de stat, din acesta:						

i. impozit pe profit ii. impozit pe venit						
b) bugete locale i. impozit pe profit						
c) bugetul asigurărilor sociale de stat: i. contribuţii de asigurări						
d) alte tipuri de venituri (se va menţiona natura acestora)	sumele provenite din dobânzi şi servicii	sumele provenite din dobânzi şi servicii	sumele provenite din dobânzi şi servicii	sumele provenite din dobânzi şi servicii		
4.2 Modificări ale cheltuielilor bugetare, plus/minus, din care:	**-34.200**	**-25.000**	**-50.000**	**-410.800**		
a) buget de stat, din acesta: i. cheltuieli de personal ii. bunuri şi servicii iii. transferuri	-34.200 -34.200	-25.000 -25.000	-50.000 -50.000	-410.800 -410.800		
b) bugete locale: i. cheltuieli de personal ii. bunuri şi servicii						
c) bugetul asigurărilor sociale de stat: i. cheltuieli de personal bunuri şi servicii						
d) alte tipuri de cheltuieli (se va menţiona natura acestora)						
4.3 Impact financiar, plus/minus, din care: a) buget de stat	**-34.200** -34.200	**25.000** -25.000	**-50.000** -50.000	**-410.800** -410.800		

b) bugete locale						
4.4 Propuneri pentru acoperirea creşterii cheltuielilor bugetare						
4.5 Propuneri pentru a compensa reducerea veniturilor bugetare						
4.6 Calcule detaliate privind fundamentarea modificărilor veniturilor şi/sau cheltuielilor bugetare						

4.7 Prezentarea, în cazul proiectelor de acte normative a căror adoptare atrage majorarea cheltuielilor bugetare, a următoarelor documente:
a) fişa financiară prevăzută la art.15 din Legea nr. 500/2002 privind finanţele publice, cu modificările şi completările ulterioare, însoţită de ipotezele şi metodologia de calcul utilizată; -Anexa
b) declaraţie conform căreia majorarea de cheltuială respectivă este compatibilă cu obiectivele şi priorităţile strategice specificate în strategia fiscal-bugetară, cu legea bugetară anuală şi cu plafoanele de cheltuieli prezentate în strategia fiscal-bugetară.

Actul normativ nu se referă la acest subiect.

4.8 Alte informaţii

Cheltuielile necesare pentru finanţarea şi resursele necesare pentru funcţionarea CRISCE, respectiv cheltuielile de organizare şi funcţionare, inclusiv cheltuielile de personal, vor fi finanţate din cheltuielile administrative prevăzute la art. 8 din O.U.G. nr. 60/2022, constituite din dobânzi acumulate în conturile Ministerului Energiei la sumele virate de Banca Europeană pentru Investiţii (BEI), precum şi din venituri proprii, fiind estimate anual, după cum urmează:
- 2025: 12.292 mii lei;
- 2026: 18.311 mii lei;
- 2027: 10.378 mii lei;
- 2028: 10.378 mii lei;
- 2019: 10.378 mii lei

Media anuală de 12.347,4 mii lei.

Secţiunea a 5-a:
Efectele proiectului de act normativ asupra legislaţiei în vigoare

5.1 Măsuri normative necesare pentru aplicarea prevederilor proiectului de act normativ
Nu este cazul

5.2 Impactul asupra legislaţiei în domeniul achiziţiilor publice
Nu este cazul

5.3.1 Conformitatea proiectului de act normativ cu legislația UE

Proiectul de act normativ asigură aplicarea în concret a mai multor acte legislative ale Uniunii Europene, acesta fiind conform cu următoarele prevederi:

a) Regulamentul delegat (UE) 2024/1366 al Comisiei din 11 martie 2024 de completare a Regulamentului (UE) 2019/943 al Parlamentului European și al Consiliului prin stabilirea unui cod de rețea privind normele sectoriale pentru aspectele legate de securitatea cibernetică a fluxurilor transfrontaliere de energie electrică;

b) art. 6 și 7 din Regulamentul (UE) 2019/881 al Parlamentului European Și Al Consiliului privind ENISA (Agenția Uniunii Europene pentru Securitate Cibernetică) și privind certificarea securității cibernetice pentru tehnologia informației și comunicațiilor și de abrogare a Regulamentului (UE) nr. 526/2013 (Regulamentul privind securitatea cibernetică);

c) art. 1 și 2 din Regulamentul (UE) 2019/796 din 17 mai 2019 al Consiliului privind măsuri restrictive împotriva atacurilor cibernetice care reprezintă o amenințare la adresa Uniunii sau a statelor sale membre;

d) Punctul 3 din Anexa IV și punctul 3 din Anexa V din Regulamentul (UE) 2017/1938 al Parlamentului European și al Consiliului din 25 octombrie 2017 privind măsurile de garantare a siguranței furnizării de gaze și de abrogare a Regulamentului (UE) nr. 994/2010, cu modificările ulterioare;

e) art. 9-11 și art. 13-15, Capitolul IV, Capitolul VII și Anexa 1 din Directiva (UE) 2022/2555 a Parlamentului European și a Consiliului din 14 decembrie 2022 privind măsuri pentru un nivel comun ridicat de securitate cibernetică în întreaga Uniune, de modificare a Regulamentului (UE) nr. 910/2014 și a Directivei (UE) 2018/1972 și de abrogare a Directivei (UE) 2016/1148 (Directiva NIS 2);

f) Pct. 1.2 și Capitolul 2 din Comunicare Comună către Parlamentul European și Consiliu - Strategia de securitate cibernetică a UE pentru deceniul digital JOIN (2020) 18 final din 16.12.2020;

g) punctul 1 al Capitolului IV din Comunicarea Comisiei către Parlamentul European, Consiliul European, Consiliu, Comitetul Economic și Social European și Comitetul Regiunilor referitoare la Strategia UE privind uniunea securității nr. COM/2020/605 final;

h) Recomandarea (UE) 2019/553 a Comisiei privind securitatea cibernetică în sectorul energetic, nr. C (2019) 2400;

i) art. 1 și art. 3 din propunerea de Regulament al Parlamentului European și al Consiliului de stabilire a unor măsuri de consolidare a solidarității și a capacităților de la nivelul Uniunii pentru detectarea amenințărilor și a incidentelor de securitate cibernetică, pregătirea legată de acestea și contracararea lor nr. COM/2023/209 final;

5.3.1 Măsuri normative necesare transpunerii directivelor UE

Directiva NIS 2 (Directiva (UE) 2022/2555) impune o serie de obligații clare și precise statelor membre ale Uniunii Europene în ceea ce privește constituirea și funcționarea echipelor de răspuns la incidente de securitate cibernetică.

Potrivit Anexei 1 din Directiva (UE) 2022/2555 a Parlamentului European și a Consiliului din 14 decembrie 2022 privind măsurile pentru un nivel comun ridicat de securitate cibernetică în întreaga Uniune, de modificare a Regulamentului (UE) nr. 910/2014 și a Directivei (UE) 2018/1972 și de abrogare a Directivei (UE) 2016/1148 (Directiva NIS 2), sectorul energetic este încadrat la nivelul ridicat de criticitate. De asemenea, potrivit art. 10 alin. (1) din Directivă, fiecare sector din Anexa 1 trebuie să aibă un CSIRT sectorial. Potrivit art. 10 alin. (2), CSIRT sectorial trebuie să fie suficient de bine finanțat pentru a face față atribuțiilor minime prevăzute la art. 11 (3) din Directivă.

Articolul 11 al directivei specifică cerințele și capacitățile tehnice pe care trebuie să le îndeplinească CSIRT sectoriale. Acestea includ obligația de a asigura un nivel înalt de disponibilitate a canalelor de comunicare, evitarea punctelor unice de eșec, asigurarea confidențialității și încrederii în operațiunile lor, și dotarea cu sisteme redundante pentru a asigura continuitatea serviciilor. În plus,

CSIRT trebuie să fie echipate cu resurse şi personal adecvat pentru a îndeplini aceste cerinţe. Prin urmare, constituirea unui CSIRT sectorial în domeniul energiei este justificată şi necesară pentru a îndeplini aceste cerinţe, având în vedere importanţa critică a acestui sector pentru securitatea naţională şi funcţionarea societăţii.
Mai mult, articolul 10 alineatul (3) impune statelor membre obligaţia de a asigura că fiecare CSIRT dispune de o infrastructură de comunicaţii şi informaţii adecvată, securizată şi rezilientă, care să permită schimbul de informaţii cu entităţile esenţiale şi importante din sectorul respectiv, precum şi cu alţi actori relevanţi. În sectorul energetic, unde securitatea cibernetică este de o importanţă crucială, crearea unui CSIRT sectorial specializat va permite o mai bună gestionare şi coordonare a acestor aspecte, contribuind la protecţia infrastructurilor critice de energie din România.
De asemenea, articolul 10 alineatul (4) stabileşte că CSIRT trebuie să coopereze şi să schimbe informaţii relevante cu comunităţile sectoriale sau intersectoriale ale entităţilor esenţiale şi importante. În contextul specific al sectorului energetic, această cooperare este esenţială pentru a asigura o reacţie rapidă şi eficientă la incidentele de securitate cibernetică, având în vedere interdependenţele complexe şi riscurile la care este supus acest sector. Un CSIRT sectorial în energie ar permite o gestionare mai bine orientată şi adaptată la specificul provocărilor cibernetice din acest domeniu.
Articolul 11 alineatul (3) detaliază sarcinile specifice ale CSIRT, care includ monitorizarea şi analizarea ameninţărilor cibernetice, oferirea de avertismente timpurii şi alerte, răspunsul la incidente şi colectarea şi analizarea datelor forensice. În sectorul energetic, aceste sarcini sunt deosebit de critice, deoarece un atac cibernetic ar putea avea consecinţe devastatoare pentru securitatea naţională şi pentru funcţionarea infrastructurilor esenţiale.
Articolul 12 din directivă prevede, de asemenea, obligaţia fiecărui stat membru de a desemna un CSIRT ca şi coordonator pentru divulgarea coordonată a vulnerabilităţilor, asigurând astfel gestionarea eficientă a vulnerabilităţilor care afectează multiple entităţi. În sectorul energetic, unde vulnerabilităţile pot avea un impact deosebit de mare, un CSIRT sectorial dedicat ar putea îndeplini acest rol cu o eficienţă sporită, având cunoştinţele şi resursele necesare pentru a gestiona astfel de situaţii complexe.

5.3.2 Măsuri normative necesare aplicării actelor legislative UE
Prezentul proiect de act normativ desemnează Ministerul Energiei, prin CRISCE, drept autoritate competentă responsabilă cu îndeplinirea sarcinilor care îi sunt atribuite prin Regulamentul delegat (UE) 2024/1366 al Comisiei de completare a Regulamentului (UE) 2019/943 al Parlamentului European şi al Consiliului prin stabilirea unui cod de reţea privind normele sectoriale pentru aspectele legate de securitatea cibernetică a fluxurilor transfrontaliere de energie electrică. În concret, prezentul proeict de act normativ face o punere în aplicare a prevederilor art. 4 - 5; art. 9 alin. (1); art. 15 alin. (1)-(2); art. 17; art. 20 alin. (2)-(4); art. 23 alin. (1)-(4); art. 24 - 27; art. 29; art. 30 alin. (1)-(2); art. 31 alin. (1) şi (5); art. 33 alin. (6); art. 34 alin. (2) şi art. 37; art. 39 alin. (1)-(2); art. 40 alin. (1); art. 41 alin. (1)-(2) şi alin. (12); art. 42; art. 43 alin. (2) din Regulamentul delegat (UE) 2024/1366

5.4 Hotărâri ale Curţii de Justiţie a Uniunii Europene
Actul normativ nu se referă la acest subiect.

5.5 Alte acte normative şi/sau documente internaţionale din care decurg angajamente asumate
Nu este cazul

5.6. Alte informaţii. – Nu este cazul.

Secţiunea a 6-a:
Consultările efectuate în vederea elaborării proiectului de act normativ

6.1 Informaţii privind neaplicarea procedurii de participare la elaborarea actelor normative **Actul normativ nu se referă la acest subiect.**
6.2 Informaţii privind procesul de consultare cu organizaţii neguvernamentale, institute de cercetare şi alte organisme implicate. **Actul normativ nu se referă la acest subiect.**
6.3 Informaţii despre consultările organizate cu autorităţile administraţiei publice locale Actul normativ nu se referă la acest subiect.
6.4 Informaţii privind puncte de vedere/opinii emise de organisme consultative constituite prin acte normative
6.5. Informaţii privind avizarea de către: a) Consiliul Legislativ – se solicită avizul acestei instituţii de către Secretariatul General al Guvernului; b) Consiliul Suprem de Apărare a Ţării – se solicită avizul acestei instituţii; c) Consiliul Economic şi Social - se solicită avizul acestei instituţii; d) Consiliul Concurenţei – e) Curtea de Conturi.
6.6 Alte informaţii Se solicită punctul de vedere favorabil al Autorităţii Naţionale de Reglementare în domeniul Energiei. Se solicită puncte de vedere de la Serviciul Român de Informaţii, Serviciul de Informaţii Externe, Serviciul de Telecomunicaţii Speciale, Serviciul de Protecţie şi Pază, Oficiul Registrului Naţional al Informaţiilor Secrete de Stat, Autoritatea Naţională pentru Administrare şi Reglementare în Comunicaţii, în temeiul art. 10 din Legea nr. 58/2023. Se solicită punctul de vedere favorabil al Autorităţii Naţionale de Supraveghere a Prelucrării Datelor cu Caracter Personal.
Secţiunea a 7-a: **Activităţi de informare publică privind elaborarea şi implementarea proiectului de act normativ**
7.1 Informarea societăţii civile cu privire la elaborarea proiectului de act normativ Pentru proiectul de act normativ au fost îndeplinite procedurile de transparenţă decizională prevăzute de Legea nr. 52/2003 privind transparenţa decizională în administraţia publică, republicată, cu modificările şi completările ulterioare. Proiectul a fost postat pe site-ul Ministerului Energiei în data de 01.10.2024, persoanele interesate având posibilitatea transmiterii de comentarii, propuneri şi observaţii până la data de 10.10.2024 inclusiv. Forma refăcută a proiectului de act normativ ca urmare a consultărilor realizate a fost postată pe site-ul Ministerului Energiei în data de 14.11.2024.
7.2 Informarea societăţii civile cu privire la eventualul impact asupra mediului în urma implementării proiectului de act normativ, precum şi efectele asupra sănătăţii şi securităţii cetăţenilor sau diversităţii biologice. Actul normativ nu se referă la acest subiect.
7.3 Alte informaţii - Nu este cazul
Secţiunea a 8-a: **Măsuri privind implementarea, monitorizarea şi evaluarea proiectului de act normativ**

8.1 Măsurile de punere în aplicare a proiectului de act normativ

În vederea exercitării funcţiei prevăzute la art. 5, alin. (2) lit. b) din proiectul de act normativ, CRISCE va solicita autorizarea DNSC în maximum 120 de zile de la data intrării în vigoare a prezentei ordonanţe de urgenţă.

Ordinul ministrului energiei prevăzut la art. 3 alin. (1) din proiectul de ordonanţă de urgenţă pentru stabilirea numărului şi a tipurilor de posturi, precum şi a procedurii interne de recrutare şi selecţie se emite în maximum 45 de zile de la data intrării în vigoare a prezentei ordonanţe de urgenţă.

Ordinul ministrului energiei prevăzut la art. 3 alin. (2) din proiectul de ordonanţă de urgenţă privind desemnarea comisiei de concurs se emite în maximum 45 de zile de la data intrării în vigoare a prezentei ordonanţe de urgenţă şi cuprinde cuantumul indemnizaţiei fixe a membrilor comisiei.

Ordinul ministrului energiei prevăzut la art. 4 alin. (1) din proiectul de ordonanţă de urgenţă pentru aprobarea criteriilor şi procedurii de evaluare se emite în maximum 60 de zile de la data intrării în vigoare a prezentei ordonanţe de urgenţă.

Ordinul ministrului energiei prevăzut la art. 4 alin. (4) din proiectul de ordonanţă de urgenţă privind desemnarea comisiei de evaluare se stabileşte în maximum 60 de zile de la data intrării în vigoare a prezentei ordonanţe de urgenţă, şi cuprinde cuantumul indemnizaţiei fixe a membrilor comisiei.

Ordin comun al ministrului energiei şi al directorului DNSC prevăzut la art. 5 alin. (1) lit. d) din proiectul de ordonanţă de urgenţă se emite în termen de 90 de zile de la data intrării în vigoare a prezentei ordonanţe de urgenţă.

Ordinele ministrului energiei prevăzut la art. 6 alin. (1) din proiectul de ordonanţă de urgenţă privind stabilirea organigramei, statului de funcţii şi a regulamentului de organizare şi funcţionare şi procedurile interne ale CRISCE se emit în maximum 45 de zile de la data intrării în vigoare a prezentei ordonanţe de urgenţă.

Ordinul ministrului energiei prevăzut la art. 7 alin. (1) din proiectul de ordonanţă de urgenţă se emite în maximum 45 de zile de la data intrării în vigoare a prezentei ordonanţe de urgenţă.

Ordinul ministrului energiei prevăzut la art. 8 alin. (2) din proiectul de ordonanţă de urgenţă se emite în maximum 90 de zile de la data intrării în vigoare a prezentei ordonanţe de urgenţă.

Ordinul ministrului energiei/actul administrativ al conducătorului organismului delegat pentru aprobarea Metodologiei de acordare a stimulentelor financiare prevăzută la art. 8 alin. (7) din Ordonanţa de urgenţă a Guvernului nr. 60/2022 privind stabilirea cadrului instituţional şi financiar de implementare şi gestionare a fondurilor alocate României prin Fondul pentru modernizare, precum şi pentru modificarea şi completarea unor acte normative, aprobată cu completări prin Legea nr. 376/202, cu modificările şi completările ulterioare, inclusiv cu cele aduse prin prezenta ordonanţă de urgenţă, se emite în termen de 10 zile de la data intrării în vigoare a prezentei ordonanţe de urgenţă.

8.2 Alte informaţii - Nu este cazul

În numele iniţiatorilor,

Sebastian – Ioan BURDUJA

Deputat PNL

EDUARD-TATIAN MITITELU

Tabel susținători

Lege

privind înființarea și operaționalizarea Centrului de Răspuns la Incidente de Securitate Cibernetică în Energie, precum și pentru modificarea și completarea unor acte normative

Nr. crt.	Nume și prenume	Grup parlamentar	Semnătura
1	BURDUJA SEBASTIAN-IOAN	PNL	
2.	ROMAN FLORIN	PNL	
3.	ANDREI ALEXANDRU	PNL	
4.	Alexandru MUKARU	PNL	
5	Cătălin Dobre	PNL	
6.	BOGDAN IONEL	PNL	
7	Lucian BODE	PNL	
8.	ROSCA MIRCEA	PNL	
9.	Vela Ion Marcel	PNL	
10.	Bende Sándor	UDMR	
11	Orea Octavian	PNL	
12.	MITITELU EDUARD-TATIAN	PNL	
13	Cușoveanu Marian	PNL	
14	Mircea Fechet	PNL	
15	Pavel Popescu	PNL	
16	MIHAI COTEȚ	PNL	
17	VARGA GEZA	PNL	
18	Ovidiu Jitaru	PNL	
19	Marian Cotea	PNL	
20	ROȘU LUCIAN	PNL	
21	Popescu Vlad	PNL	

Tabel susținători

Lege

privind înființarea și operaționalizarea Centrului de Răspuns la Incidente de Securitate Cibernetică în Energie, precum și pentru modificarea și completarea unor acte normative

Nr. crt.	Nume și prenume	Grup parlamentar	Semnătura
1	BURDUJA SEBASTIAN-IOAN	PNL	
	Pauliuc Nicoleta	PNL	
	MARIA-GABRIELA HORGA	PNL	

Tabel susținători

Lege

privind înființarea și operaționalizarea Centrului de Răspuns la Incidente de Securitate Cibernetică în Energie, precum și pentru modificarea și completarea unor acte normative

Nr. crt.	Nume și prenume	Grup parlamentar	Semnătura
1	BURDUJA SEBASTIAN-IOAN	PNL	
2.	ROMAN FLORIN	PNL	
3.	ANDREI ALEXANDRU	PNL	
4.	Alexandru MUKARU	PNL	
5	Cijmian Jobne	PNL	
6.	BOGDAN IONEL	PNL	
7	Lucian BODE	PNL	
8.	ROSCA MIRCEA	PNL	
9.	Vela Ion Marcel	PNL	
10.	Bende Sándor	UDMR	
11	Orea Octavian	PNL	
12.	MITITELU EDUARD-TATIAN	PNL	
13	Cușoveanu Marian	PNL	
14	Mircea Felix	PNL	
15	Adrian Mocanu	PNL	
16	NOISIN NAN-MANIN	PNL	
11	TIPLEA DUMITRU	PNL	
12	Gal Călin	PNL	
13	TOMA Cut	PSD	
14	Cotinescu Aurelian	PNL	
15	CIOBANU ADRIAN VIRGIL	PNL	

Tabel susținători

Lege

privind înființarea și operaționalizarea Centrului de Răspuns la Incidente de Securitate Cibernetică în Energie, precum și pentru modificarea și completarea unor acte normative

Nr. crt.	Nume și prenume	Grup parlamentar	Semnătura
16.	STANESCU VERUTA	PNL	
17	RUJV Sebastian Mihai	PNL	
18	CÎMPEAN OVIDIU	PNL	
19	CIGHIARTAU ROBERT	PNL	

Tabel susținători

Lege

privind înființarea și operaționalizarea Centrului de Răspuns la Incidente de Securitate Cibernetică în Energie, precum și pentru modificarea și completarea unor acte normative

Nr. crt.	Nume și prenume	Grup parlamentar	Semnătura
1	BURDUJA SEBASTIAN-IOAN	PNL	
2	Raluca Turcan	PNL	