DIRECTORATUL NAȚIONAL
DE SECURITATE CIBERNETICĂ

# Raport anual de activitate
# 2024

**(aprobat prin HCSAT nr. 77/30.06.2025)**

**- DOCUMENT DESTINAT PUBLICĂRII -**

TLP:CLEAR

# Cuprins

# 1 CUVÂNTUL DIRECTORULUI

În anul 2024, Directoratul Național de Securitate Cibernetică (DNSC) și-a îmbunătățit și consolidat capabilitățile și rolul de autoritate competentă la nivel național pentru spațiul cibernetic național civil, precum și pentru gestionarea riscurilor și a incidentelor de securitate cibernetică.

Activitățile Directoratului au fost concentrate pe ceea ce înseamnă asigurarea securității cibernetice a spațiului cibernetic național civil, în colaborare cu instituțiile și autoritățile competente, cu mediul privat, cu cel academic și cu partenerii internaționali.

Începutul anului 2024 a fost unul intens, marcat de două incidente cibernetice majore care au reprezentat un test solid pentru capacitățile Directoratului și pentru reziliența în materie de securitate cibernetică la nivel național: atacul cibernetic asupra Camerei Deputaților și atacul asupra sectorului național de sănătate și a lanțului său de aprovizionare IT&C.

Acestea au fost o ilustrare a faptului că echipa DNSC și partenerii noștri instituționali pot face față cu succes (cel puțin) unui atac cibernetic major pe săptămână și că ecosistemul cibernetic național public-privat poate livra rezultate, chiar și într-o situație apropiată de criză cibernetică. Toate acestea, într-un interval de două săptămâni, extrem de încărcate, dar ilustrative pentru activitatea Directoratului, care:

- A organizat un workshop hibrid de o zi cu peste 100 de factori de decizie din sectorul sănătății, experți IT&C și de securitate cibernetică, la doar două zile după atacul cibernetic asupra spitalelor;
- A susținut un workshop de o zi despre managementul riscurilor cibernetice în Constanța, alături de actorii-cheie din industria transportului maritim și pe Dunăre;
- A fost prezent la Chișinău, Republica Moldova, pentru a sprijini frații noștri la lansarea Agenției Naționale de Securitate Cibernetică;
- A avut o echipă pe teren la Kiev, Ucraina;
- A obținut locul 4 în exercițiul european de securitate cibernetică pentru sectorul energetic, desfășurat la Varșovia, Polonia;
- A oferit briefing-uri la sediul Directoratului pentru mai mulți reprezentanți ai ambasadelor străine la București;
- A depus 5 noi aplicații pentru granturi destinate dezvoltării capacităților cibernetice naționale și am pregătit alte 12;
- A sprijinit lansarea cu succes a capitolului românesc al Women for Cyber (W4C), cu o întâlnire online dedicată femeilor active în domeniul securității cibernetice;
- A monitorizat, analizat și prioritizat peste jumătate de milion de evenimente cibernetice distincte și relevante și câteva mii de incidente;
- A avut peste 25 de intervenții în mass-media centrală pe tema celor două atacuri cibernetice sau a securității cibernetice, în general.

În această notă, intervenția rapidă și decisivă a echipelor Directoratului în 2024 în cazul unor incidente cibernetice majore la nivel național a dovedit atingerea capabilităților inițiale ale instituției, conform obiectivelor stabilite.

Pe linia consolidării capacității interne organizaționale a Directoratului, este relevant de menționat aprobarea în 2024 prin Hotărârea Consiliului Suprem de Apărare a Țării HCSAT nr. 196 din 11.11.2024, a noului Regulament de Organizare și Funcționare al DNSC.

De asemenea, în 2024, Directoratul și-a exercitat efectiv și cu succes rolul de a reprezenta România în formatele de cooperare internațională pe domeniul său de competență, pentru asigurarea cooperării interinstituționale, informarea reciprocă și susținerea unei poziții coerente la nivel internațional.

La nivelul UE, Directoratul reprezintă România într-o serie de organisme specializate privind securitatea cibernetică, precum Grupul de Cooperare NIS, Rețeaua echipelor de răspuns la incidente cibernetice (CSIRT

Network), Rețeaua Europeană de legătură în domeniul crizelor cibernetice (EU-CyCLONe), Agenția Europeană de Securitate Cibernetică (ENISA) Management Board și National Liaison Officers' Network, precum și alte organisme specializate similare.

Finalul anului 2024 a fost în aceeași notă cu începutul acestuia și s-a caracterizat cu o activitate foarte intensă, atât operațional, de cooperare internațională cât și la nivelul activităților de reglementare.

În contextul alegerilor și al declasificării de către Consiliul Suprem de Apărare a Țării (CSAT) a rapoartelor prezentate de Serviciul Român de Informații, Serviciul de Informații Externe și Ministerul Afacerilor Interne în cadrul ședinței CSAT, din data de 28 noiembrie 2024, Directoratul a primit de la reprezentanți ai unor instituții și grupuri de lucru de la nivelul Uniunii Europene, precum și de la autorități competente în domeniul securității cibernetice din state membre ale UE, întrebări și solicitări de informații cu privire la aspectele de securitate cibernetică relevate de comunicatul de presă al CSAT din 28 noiembrie 2024 și de documentele publicate la data de 4 decembrie 2024.

În acest sens, Directoratul a desfășurat o serie de activități de informare și dialog cu organismele și instituțiile internaționale implicate și a activat cu succes, conform procedurilor standard, mecanismele de cooperare și asistență europene disponibile ale EU-CyCLONe și respectiv CSIRT Network.

Mai mult, la finalul lui Decembrie 2024, Directoratul și actorii cheie ai ecosistemului național de securitate cibernetică au livrat unul dintre cele mai elaborate și bine concepute acte normative privind implementarea într-un stat membru al UE a Directivei (UE) 2022/2555 (Directiva NIS2): Ordonanța de Urgență a Guvernului nr. 155/2024 privind stabilirea unui cadru pentru securitatea cibernetică a rețelelor și sistemelor informatice în spațiul cibernetic civil național.

Acest act normativ consolidează capacitatea României de a face față provocărilor actuale în domeniul securității cibernetice, aliniind țara la standardele europene și asigurând o protecție îmbunătățită a sectoarelor de infrastructură critică și a spațiului cibernetic.

Pentru aceasta, am organizat un proces extins de consultare, dezbatere transparentă și implicare a tuturor părților interesate și experților relevanți din sectorul public și privat din România pentru elaborarea acestui act normativ, proces care a durat aproape întregul an 2024 și necesitat peste o mie de zile de muncă depuse de zeci de experți în securitate cibernetică, reglementare și legislație, la nivel național.

A fost un an intens, dar care a dat posibilitatea Directoratului să își reafirme angajamentul de a proteja infrastructurile critice ale României, de a reglementa, sprijini și facilita implementarea unor masuri adecvate de securitate cibernetică la nivel național și de a colabora strâns pentru aceasta cu partenerii naționali și internaționali pentru a dezvolta o cultură robustă de reziliență și securitate cibernetică.

Dan Cîmpean

Directorul Directoratului Național de Securitate Cibernetică

# 2 COMBATEREA AMENINȚĂRILOR CIBERNETICE

## 2.1 Nivelul general al amenințării cibernetice în România

Nivelul general al amenințării cibernetice în România, care a reprezentat ipoteza de lucru principală a Directoratului Național de Securitate Cibernetică în anul 2024, a fost unul ridicat:

**↑ Ridicat**

### Nivelul amenințării cibernetice în România

Anul 2024 a marcat o intensificare a amenințărilor aplicabile spațiului cibernetic național civil al României, conturând un peisaj digital volatil și imprevizibil.

Principalele amenințări cibernetice observate și cu privire la care Directoratul a inițiat și derulat acțiuni preventive și reactive în anul 2024 au fost următoarele:

- **Ransomware:** Această amenințare a continuat să fie prezentă, fiind asociată aproape în totalitate cu grupări pro-ruse precum Lockbit, Lynx, Akira și RansomHub, care s-au remarcat prin activitatea lor intensă. Aceste atacuri au vizat atât organizațiile mari, cât și întreprinderile mici și mijlocii, cauzând perturbări operaționale semnificative.
- **Malware:** Peisajul malware a devenit tot mai diversificat, fiind utilizate echipamente software de tip infostealer, preponderent AgentTesla, FormBook și RedLine. Tacticile de distribuție au evoluat, atacatorii utilizând în mod intens metode precum fișierele OneNote și ISO/LNK dar și arhive protejate prin parola, ceea ce face detectarea și prevenirea mai dificile.
- **Atacuri DDoS**: Numărul atacurilor Distributed Denial-of-Service (DDoS) a scăzut datorită implementării metodelor de protecție bazate pe filtrarea traficului, dar acestea continuă să reprezinte o amenințare, fiind preferată de grupări precum NoName057(16). În principal, ele vizează sectorul public și cel al infrastructurilor critice.
- **Ingineria socială**: Phishing-ul rămâne un vector de atac preferat în principal pentru grupările infracționale, motivate financiar. Utilizarea Inteligenței Artificiale (IA) pentru crearea de mesaje mai convingătoare și a tehnologiei Deepfake pentru atacuri de tip vishing adaugă un nivel suplimentar de complexitate. În plus, spoofing-ul telefonic a devenit o tehnică din ce în ce mai frecvent utilizată.
- **Atacuri asupra lanțului de aprovizionare:** Grupările infracționale și cele de tip Advanced Persistent Threat (APT) și-au intensificat eforturile de a compromite lanțurile de aprovizionare, vizând în special angajații cu privilegii extinse. Atacurile au un impact devastator, deoarece permit actorilor rău intenționați să acceseze simultan sistemele și datele mai multor organizații.

Intensificarea războiului hibrid purtat de Federația Rusă în contextului războiului de agresiune declanșat în Ucraina în 2022, a continuat să influențeze peisajul cibernetic global în 2024. Acest conflict a consolidat rolul hacktivismului și al grupărilor APT (Advanced Persistent Threat) ca instrumente strategice, demonstrând capacitatea acestor actori de a influența și derula campanii complexe asupra infrastructurilor IT&C din spațiul cibernetic național civil.

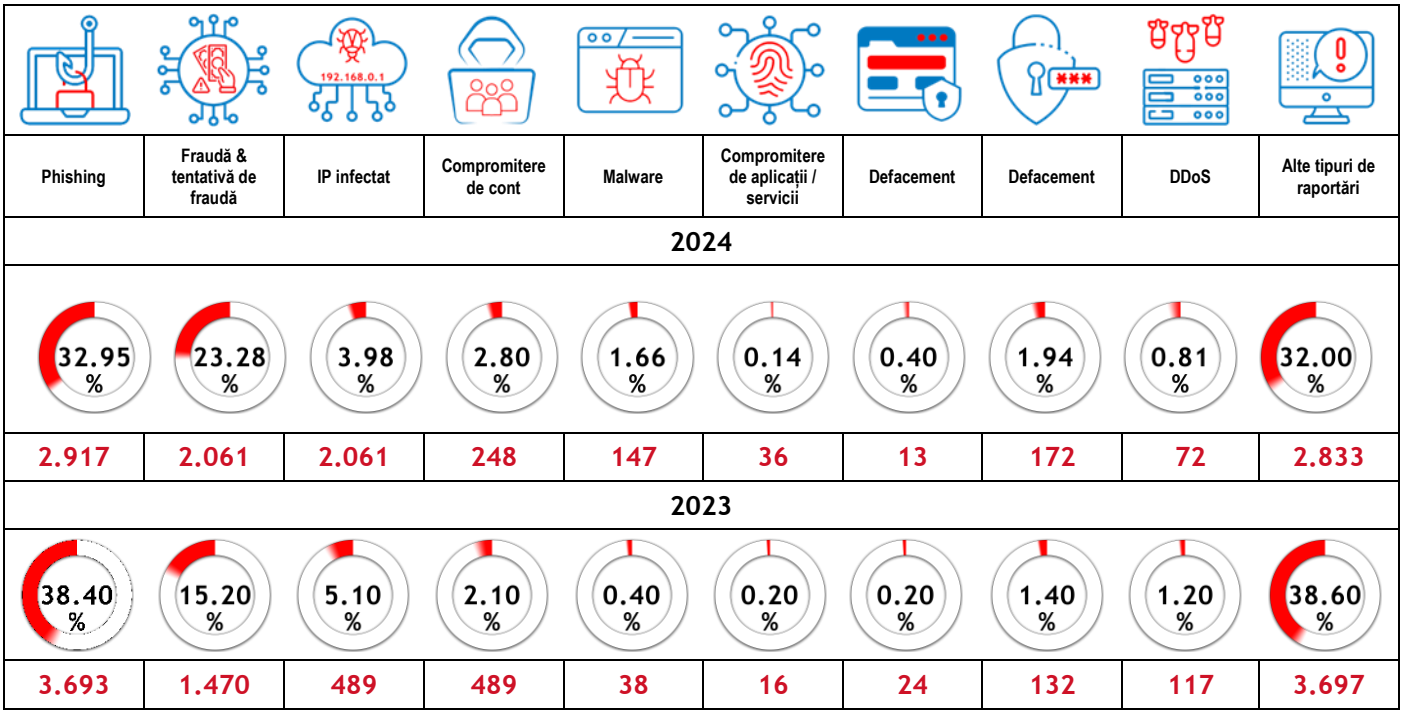
Peisajul atacurilor cibernetice a fost marcat de operațiuni derulate atât de hacktiviști pro-ruși, cât și de grupări APT statale și non-statale, vizând nu doar Ucraina, ci și numeroase țări europene. Țintele au inclus atât instituții guvernamentale cât și operatori din sectoare critice, precum cel energetic, financiar, transporturi, telecomunicații și sănătate.

Hacktiviști independenți sau afiliați unor grupuri precum NoName057(16) au susținut atacuri constante asupra site-urilor media și infrastructurilor digitale din Europa, iar activitatea combinată a acestor grupuri a evidențiat faptul că linia dintre hacktivism și operațiunile APT, sponsorizate de către stat, devine tot mai fină, contribuind astfel la escaladarea dimensiunii cibernetice a conflictului hibrid.

## 2.2 Atacuri și incidente cibernetice notabile

### 2.2.1 Situația de ansamblu a atacurilor și incidentelor raportate către Directorat

În cursul anului 2024 la nivelul Directoratului au fost raportate, investigate și analizate următoarele:



| Phishing | Fraudă & tentativă de fraudă | IP infectat | Compromitere de cont | Malware | Compromitere de aplicații / servicii | Defacement | Defacement | DDoS | Alte tipuri de raportări |
|---|---|---|---|---|---|---|---|---|---|
| **2024** | | | | | | | | | |
| 32.95 % | 23.28 % | 3.98 % | 2.80 % | 1.66 % | 0.14 % | 0.40 % | 1.94 % | 0.81 % | 32.00 % |
| 2.917 | 2.061 | 2.061 | 248 | 147 | 36 | 13 | 172 | 72 | 2.833 |
| **2023** | | | | | | | | | |
| 38.40 % | 15.20 % | 5.10 % | 2.10 % | 0.40 % | 0.20 % | 0.20 % | 1.40 % | 1.20 % | 38.60 % |
| 3.693 | 1.470 | 489 | 489 | 38 | 16 | 24 | 132 | 117 | 3.697 |

Comparativ cu anul 2023, în anul 2024 s-au observat următoarele tendințe cu privire la datele privind incidentele raportate către Directorat:

**Scăderi semnificative:**

- **Phishing (-21%)**: Declinul se datorează în principal succesului campaniilor de educare a utilizatorilor dar și a demersurilor efectuate de către Directorat pentru implementarea de către organizații, la scară largă, a măsurilor de securizare a serverelor de email (SPF/DKIM/DMARC).
- **IP infectat (-27.8%)**: Scăderea poate reflecta o mai bună protecție la nivel de rețea și adoptarea unor soluții de securitate mai avansate de către organizații.
- **Defacement (-45.8%)** și **DDoS (-38.5%)**: Aceste scăderi indică o îmbunătățire a monitorizării serverelor și a protecției împotriva atacurilor volumetrice la nivel național, organizațiile din sectorul public și privat adoptând din ce în ce mai mult servicii și soluții de protecție cibernetică.

**Creșteri semnificative:**

- **Fraude (+40.2%)**: Creșterea detectată este în linie cu tendințele la nivel global și al UE privind fraudele informatice. Este o consecință a tehnicilor, tacticilor și protocoalelor tot mai agresive și inovative ale infractorilor, fiind corelată cu intensificarea atacurilor ce utilizează tehnici de spoofing telefonic și a schemelor de tip investiții financiare, care exploatează încrederea victimelor prin oportunități financiare false promovate agresiv. Creșterea numărului de fraude raportate către Directorat este influențată și de mesajele și demersurile Directoratului în spațiul public încurajând raportarea acestora către autorități.
- **Malware (+286.8%)** și **Aplicații Compromise (+125%)**: Acest trend arată o evoluție semnificativă și îngrijorătoare a capabilităților și expertizei atacatorilor cibernetici, care au devenit foarte prolifici în crearea de noi varietăți de programe malițioase (estimare de ordinul 500.000 programe malware generate zilnic). De asemenea, este o indicație clară a intenției atacatorilor de a exploata vulnerabilitățile din lanțul de furnizori (prin aplicațiile produse de aceștia). De asemenea, trendul indică necesitatea utilizării cu prioritate a soluțiilor antimalware.

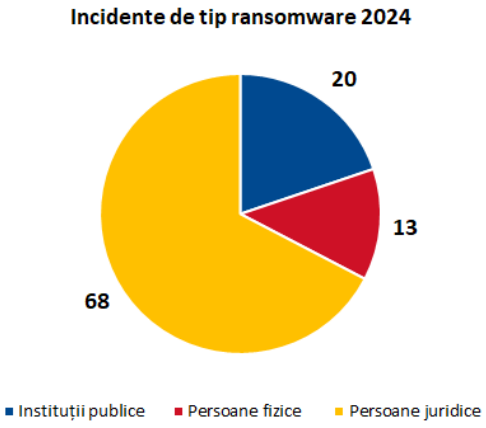
- **Bruteforce (+30.3%)** și **Cont Compromis (+21%)**: Tendința poate fi explicată de creșterea numărului de atacuri automate, dar și de implementarea slabă a autentificării cu mai mulți factori la nivelul utilizatorilor, coroborată cu o proliferare a activității utilizatorului standard pe un număr semnificativ crescut de platforme și aplicații, cu re-utilizarea prudențialelor de utilizator.

În 2024, Directoratul a intervenit conform atribuțiilor sale legale, în vederea sprijinirii actorilor impactați de o serie de atacuri și incidente cibernetice precum:

- **DDoS (Distributed Denial of Service)**; în acest sens, prezentăm următoarele exemple ilustrative de atacuri DDOS de proveniență rusească vizând în principal următoarele sectoare și entități:
  - **Energie**: 2 (Rompetrol, Mol România)
  - **Bancar**: 17 (Alpha Bank, Banca Transilvania, Banca Comercială Română, Creditcoop, Exim Bank, Edificium, Banca Națională a României, Banca Română de Credite și Investiții, Bursa de Valori București, Fondul Garantare a Depozitelor Bancare)
  - **Infrastructură digitală / telecomunicații**: 3 (Orange, Telekom, GTS)
  - **Transport**: 12 (Compania Națională de Căi Ferate (CFR), Compania Națională de Administrare a Infrastructurilor Rutiere (CNAIR), Compania Națională Aeroporturi București, Portul Constanța, Astra Trans Carpatica Feroviar, Aeroportul Băneasa, Metrorex)
  - **Administrație publică centrală și locală:** 13 (Guvernul României, Serviciul de Telecomunicații Speciale, Directoratul Național de Securitate Cibernetică, Ministerul Afacerilor Interne, Senatul României, Ministerul Afacerilor Externe, Ministerul Dezvoltării Lucrărilor Publice și Administrației, Ministerul Turismului, Primăria Municipiului București)
- **Website defacement** (inclusiv dar fără a se limita la paginile oficiale ale unor partide politice – e.g. Alianța pentru Unirea Românilor).
- **Criptare și exfiltrare de date sensibile** spre exemplu exfiltrarea de date de la Camera Deputaților.
- **Atacuri de tip brute-force**, sens în care menționăm cu titlu exemplificativ atacurile care au vizat infrastructurile Primăriei Municipiului București, Societății de Transporturi București, Autorității Feroviare Române, Universității din București, având la bază IP-uri sursă găzduite în Rusia.

### 2.2.2 Situația incidentelor de tip ransomware gestionate la nivelul Directoratului în 2024

Fenomenul ransomware este unul dintre cele mai persistente și grave. Un număr de 101 astfel de incidente au fost detectate și gestionate în 2024 de către Directorat:




Printre cele mai relevante:

- **Atac de tip ransomware care a vizat societatea Romanian Soft Company**, dezvoltatorul platformei Hipocrate, care oferă servicii de fluxuri interne către unități spitalicești. În urma atacului **un număr de 26 de spitale au fost vizate în mod direct**, fiind în imposibilitatea de a-și desfășura activitatea pentru aproximativ o săptămână. Prin activitatea sa, DNSC a analizat și investigat binarul malițios identificat în infrastructura companiei, ulterior a generat un set de reguli YARA și a emis recomandări

ce au fost diseminate către toate spitalele cât și partenerilor europeni, membrii ai CSIRT Network, pentru a identifica posibila existență a programului malițios pe sistemele informatice utilizate.

- **Atac de tip ransomware care a vizat societățile din grupul Electrica S.A**, având un impact major asupra serviciilor publice oferite de către Electrica Furnizare S.A. și Distribuție Energie Electrică Romania S.A., **cu consecința afectării unui număr de peste 800 servere și 4.000 stații de lucru** aflate la nivelul sucursalelor București, Ploiești, Brașov și Cluj. Atacul a fost notificat către DNSC la data de 9 decembrie 2024 și s-a procedat la colectarea de probe de la fața locului. Urmare a analizei efectuate a fost identificat criptorul folosit de către atacatori, s-a creat o regulă YARA care a fost publicată pe site-ul Directoratului. Totodată, au fost transmis un raport specific ce conținea indicatorii de compromitere, tehnicile și tacticile utilizate de către atacatori pentru compromiterea infrastructurii în vederea sanitizării complete a acesteia.
- **Atac de tip ransomware care a vizat Primăria Municipiului Timișoara** precum și instituții din subordinea acestora precum Direcția Fiscală a Municipiului Timișoara și Direcția Generală a Poliției Locale Timișoara, **fiind afectate aproximativ 112 sisteme**. În urma activităților specifice derulate de către specialiștii Directoratului, s-a reușit recuperarea completă a datelor critice precum și o parte din datele neesențiale. De asemenea, au fost emise recomandări pentru securizarea infrastructurii în vederea evitării de alte atacuri de acest tip.
- **Atac de tip ransomware direcționat asupra infrastructurii proiectului "Sistemul Național de Management privind Dizabilitatea"** având ca beneficiar Autoritatea Națională pentru Protecția Drepturilor Persoanelor cu Dizabilități (ANPDPD) și care cuprinde toate informațiile despre persoanele cu dizabilități și în care operează toate structurile specifice ale Direcția Generală de Asistență Socială și Protecția Copilului (DGASPC). Specialiștii Directoratului au identificat mai multe exfiltrări de conturi compromise (leaked), fiind făcute îndrumări privind măsurile necesar a fi urmate pentru securizarea infrastructurii în vederea evitării de alte atacuri de acest tip și transmis un raport detaliat cu privire la mecanismele producerii incidentului cibernetic pornind de la premisele analitice și datele informatice prelevate conform activităților specifice.
- **Atac de tip ransomware care a vizat Primăria Sectorului 5 a Municipiului București**, care a avut un impact major asupra serviciilor puse la dispoziție cetățenilor, **fiind afectate serverele de tip Domain Controller, centrala telefonică a Poliției Locale și stații de lucru**. Specialiștii Directoratului au identificat exfiltrări de conturi compromise (leaked făcute îndrumări privind masurile necesare a fi urmate pentru limitarea eventualelor prejudicii, suplimentar înaintării unui raport detaliat.
- **Atac de tip ransomware care a vizat companiile SoftTehnica și FreyaPOS** (prestatori de soluții software), fiind **afectate mașini virtuale din producție precum și copiile de siguranță aferente**, blocându-se astfel activitatea pentru aproximativ o săptămână. În urma activităților specifice derulate, s-a reușit recuperarea completă a datelor critice precum și o parte din datele neesențiale.
- **Atac de tip ransomware care a vizat societatea Binbox Global Services**, furnizoare de servicii de găzduire web, cloud computing și alte servicii conexe**, fiind compromisă întreaga infrastructură**. În urma activităților specifice derulate, s-a reușit recuperarea completă a datelor critice precum și o parte din datele neesențiale.
- **Atac de tip ransomware ce a vizat compania Dotro Telecom SRL**, furnizoare de servicii de telefonie și internet, f**iind afectată întreaga infrastructură și, implicit, nu mai puțin de 100 sisteme și peste 700 utilizatori**. S-a reușit recuperarea în proporție de peste 99% a datelor criptate.
- **Atac de tip ransomware ce a vizat societatea Agricola International S.A.**, entitate care desfășoară activități de producție, procesare și distribuție de alimente, fiind afectate peste 200 sisteme și 250 utilizatori, cu consecința blocării activității companiei pentru aproximativ 48 ore. Prin activitatea sa, Directoratul a identificat o serie de Indicatori de Compromitere (IoC) precum și mai multe conturi de utilizator compromise, fiind transmis un raport detaliat cu privire la mecanismele producerii incidentului cibernetic pornind de la premisele analitice și datele informatice prelevate.

În aceste situații, Directoratul a îndeplinit un rol crucial în asigurarea intervenției rapide, evaluarea impactului, limitarea prejudiciilor precum și remedierea, recuperarea datelor și restabilirea funcționalității infrastructurii IT&C la parametrii optimi.

De remarcat este și faptul că în cursul anului anterior, în urma unei analize complexe asupra mediilor de stocare aparținând Primăriei Municipiului Bistrița, puse la dispoziție ca urmare a unui atac cibernetic, a fost identificată o nouă variantă de ransomware și a fost creat un program de decriptare a datelor în urma unui proces de reverse engineering pe binarul folosit de atacatori. De asemenea, au mai fost identificate cheile de decriptare și recuperarea datelor ca urmare a atacurilor ce au vizat Inspectoratul Teritorial pentru Calitatea Semințelor și Materialului Săditor Galați și alte 6 companii private.

Directoratul este unul dintre actorii instituționali cheie care sprijină angajamentul României de a lupta împotriva ransomware-ului, refuzând atacatorilor accesul la finanțarea activităților lor malițioase sau la obținerea oricărei recunoașteri sau faime din activitățile lor infracționale.

### 2.2.3 Evenimente de securitate cibernetică detectate de senzorii Directoratului

Totodată, în perioada de referință au fost înregistrate 27.079.485 de evenimente de securitate cibernetică relevante, extrase din senzorii de detecție instalați/configurați de către Directorat, defalcate astfel:

Se observă o creștere a volumului de alerte în primele, respectiv ultimele 4 luni ale anului 2024 comparativ cu anul precedent, ceea ce indică o intensificare a numărului de atacuri cibernetice, inclusiv atacuri automatizate, distribuția unor noi variante de malware, apariția unor vectori de atac sofisticați care sunt capabili să declanșeze mai multe alerte generate de către senzori.

*Tabel 1 - Situația evenimentelor colectate de senzorii DNSC în 2024*

| Eveniment | 01.01-30.04 | 01.05-31.08 | 01.09-31.12 |
|---|---|---|---|
| Evenimente de securitate cibernetică cu sursă rețele de botnet | 448.406 | 784.951 | 647.529 |
| Scanări ce urmăresc colectarea de informații | 2.444.235 | 2.054.143 | 2.050.698 |
| Evenimente legate de trafic provenind de la adrese IP cu reputație îndoielnică | 367.630 | 417.614 | 406.413 |
| Încercări de penetrare a infrastructurilor prin exploatarea unor vulnerabilități | 17.320 | 10.121 | 2.737 |
| Evenimente legate de volume de trafic nejustificate cu scopul identificării vulnerabilităților și colectării de informații | 2.076.605 | 1.636.529 | 2.457.111 |
| Încercări de penetrare a infrastructurilor prin campanii de tip phishing | 607.980 | 687.230 | 811.555 |
| Încercări de penetrare a infrastructurilor prin atacuri de tip brute force | 5.884.754 | 950.318 | 1.125.887 |
| Software malițios - malware | 158.378 | 71.867 | 54.643 |
| Posibile atacuri DDoS prin cereri DNS suspecte | 292.326 | 291.523 | 320.982 |
| **Total 2024 vs.** | **12.297.634** | **6.904.296** | **7.877.555** |
| **Total 2023** | **9.832.262** | **7.241.210** | **4.396.023** |

Un rol esențial în colectarea acestor date l-a reprezentat operaționalizarea Platformei Naționale pentru Raportarea Incidentelor de Securitate Cibernetică (PNRISC) de la începutul anului 2024, în conformitate cu prevederile Legii 58/2023 privind securitatea și apărarea cibernetică a României.

De asemenea, în anul 2024, Directoratul a colectat și soluționat alerte de securitate cibernetică, provenite din raportările formulate de către cetățeni prin intermediul PNRISC, de la numărul unic de urgență la nivel național **1911**, senzorii instalați și configurați în infrastructuri IT&C naționale, din senzoristică darknet, cât și din cooperarea cu partenerii instituționali naționali sau internaționali.

### 2.2.4 Alte evoluții și activități relevante

Activitățile desfășurate de către Directorat au evidențiat două fenomene care au luat amploare în ultima jumătate a anului 2024, după cum urmează:

- **Spoofing-ul telefonic**: una dintre cele mai utilizate tehnici în atacurile de tip inginerie socială și care constă în falsificarea numărului de telefon afișat destinatarului pentru a imita/impersona numere legitime, precum cele ale instituțiilor financiare, organizațiilor guvernamentale ori chiar ale unor persoane de încredere. Acest fenomen a devenit tot mai sofisticat, fiind adesea utilizat împreună cu alte tehnici de atac, precum vishing sau mesaje persuasive generate cu ajutorul Inteligenței Artificiale. **Impactul a fost unul semnificativ, fiind înregistrate prejudicii materiale în cuantum de peste 450.000 euro**.
- **Smishing-ul (phishing prin sms)** a rămas o provocare majoră, fiind de asemenea o tehnică des utilizată în atacurile de tip inginerie socială și care constă în transmiterea de mesaje text frauduloase, care par a fi trimise de către instituții legitime și nu numai, precum unități bancare, companii de telecomunicații, furnizori de servicii sau organizații guvernamentale cu scopul de final de a determina victimele să divulge informații confidențiale sau să acceseze link-uri malițioase de unde pot descărca programe malware.
- **Atacurile de tip SQLinjection sunt o categorie aparte relevantă, cum este cazul atacului care a vizat portalul de training al Institutului Național de Administrație (INA)**, cu consecința **compromiterii unei de date și exfiltrarea datelor a 32.455 utilizatori**. Datele exfiltrate au inclus adrese de email, nume, prenume, hash-uri ale parolelor precum și alte date sensibile. Specialiștii Directoratului s-au deplasat cu celeritate la data center-ul Serviciului de Telecomunicații Speciale (STS) unde era găzduit serverul ce deservea portalul compromis. În urma analizei efectuate la fața locului a fost identificat modulul vulnerabil precum și vectorul inițial de atac, fiind identificată sursa atacului. S-a procedat de îndată la remedierea vulnerabilității și repunerii în funcțiune în condiții optime a aplicației web. De asemenea au fost oferite recomandări specifice securizării codului sursă, întocmindu-se și un raport detaliat cu privire la mecanismele producerii incidentului cibernetic pornind de la premisele analitice și datele informatice prelevate conform activităților specifice.
- Cu titlu de măsură proactivă, în cursul anului 2024 Directoratul **a informat 827 de instituții publice și operatori de servicii esențiale cu privire la vulnerabilități identificate asupra infrastructurii IT&C expuse public**, **scurgeri de date confidențiale** care au fost diseminate de către atacatori prin diverse canale de comunicare, inclusiv platforme populare precum Telegram, WhatsApp și alte medii online mai puțin reglementate, fiind **transmise prin acest demers recomandări de aplicare urgentă a unor măsuri de remediere și igienă** de securitate cibernetică. Scurgerile de date au vizat, în unele cazuri, informații sensibile legate de infrastructuri critice, date financiare și informații personale ale utilizatorilor. Detectarea și raportarea acestor incidente au fost efectuate prin intermediul unor instrumente de monitorizare și analiză a activităților din spațiul cibernetic, combinate cu o analiză atentă a tiparelor de diseminare utilizate de atacatori.

În ultimul trimestru al anului 2024, Directoratul a observat o intensificare a atacurilor cibernetice care au vizat în mod specific firmele și angajații din domeniul contabil. Aceste atacuri, orchestrate prin email-uri de tip phishing, au fost caracterizate de o complexitate crescută și o abilitate de a exploata vulnerabilitățile umane, transformându-se într-o provocare semnificativă pentru acest sector.

Acest compartiment este unul esențial pentru funcționarea oricărei companii, însă atacatorii urmăresc nu doar datele financiare, ci și accesul la rețelele organizaționale, de unde pot extinde atacurile către alte sectoare sau clienți ai firmelor vizate. În plus, presiunea exercitată asupra angajaților din acest domeniu, cu precădere în perioadele aglomerate, îi face mai vulnerabili la astfel de încercări de manipulare.

Pentru a face față acestei provocări, Directoratul a colaborat cu multiple companii din domeniul contabil în scopul de a lansa campanii de informare. Campaniile derulate au avut drept scop educarea angajaților în recunoașterea semnelor unui email de tip phishing și implementarea unor bune practici pentru a preveni compromiterea datelor.

## 2.3 Vulnerabilități critice și riscuri de securitate cibernetică

Identificarea și gestionarea vulnerabilităților critice reprezintă un element central pentru protejarea infrastructurilor naționale și a intereselor de securitate națională și una din activitățile curente importante ale Directoratului.

Conform Strategiei de securitate cibernetică a României[1] vulnerabilitățile din spațiul cibernetic se referă la slăbiciuni în proiectarea și implementarea infrastructurilor cibernetice sau a măsurilor de securitate aferente, care pot fi exploatate de către amenințări cibernetice.

Principalele vulnerabilități identificate în 2024 în infrastructura cibernetică din spațiul cibernetic național, sunt:

*CVE-urile (Common Vulnerabilities and Exposures) reprezintă un sistem standardizat pentru identificarea și numirea vulnerabilităților în securitatea cibernetică.*

*Atunci când cercetătorii de securitate sau organizațiile descoperă noi vulnerabilități, acestea sunt adăugate în baza de date CVE gestionată de Corporația MITRE.*

*Fiecare vulnerabilitate primește un ID CVE unic, ceea ce permite identificarea rapidă și implementarea măsurilor de protecție adecvate.*

**CVE-2024-0012** este o vulnerabilitate critică de tip escaladare a privilegiilor care afectează sistemele de operare Linux, utilizate pe scară largă în infrastructurile IT. Problema constă într-un mecanism defectuos de validare a permisiunilor pentru anumite procese, ceea ce permite utilizatorilor locali să manipuleze fișiere temporare critice pentru a obține acces root.

Atacatorii care exploatează această vulnerabilitate pot prelua controlul complet asupra sistemului, permițând executarea de comenzi arbitrare, modificarea configurărilor sensibile sau chiar implementarea de backdoor-uri pentru acces persistent. Exploatarea este relativ simplă și poate afecta rapid integritatea, confidențialitatea și disponibilitatea resurselor afectate.

**CVE-2024-9474** este o vulnerabilitate de severitate ridicată, de tip deserializare nesigură, care afectează aplicațiile Java construite pe framework-ul Spring, un instrument de bază în dezvoltarea software-ului modern. Vulnerabilitatea apare în cazul în care aplicația deserializează date primite fără o validare adecvată, permițând atacatorilor să trimită payload-uri malițioase care sunt procesate greșit de server. Prin exploatarea acestei probleme, atacatorii pot obține acces la sistemul gazdă pentru a executa cod arbitrar, a accesa date confidențiale, a compromite alte componente interconectate sau chiar a folosi serverul drept platformă pentru atacuri ulterioare asupra altor ținte.

**CVE-2024-36401** reprezintă o vulnerabilitate severă de tip injecție SQL, ce afectează mai multe platforme de management al conținutului (CMS). Problema apare atunci când aplicația nu validează corect inputul primit de la utilizatori prin câmpurile de date, permițând includerea de comenzi SQL periculoase. Această vulnerabilitate poate fi exploatată de atacatori pentru a accesa neautorizat baze de date, obținând astfel informații sensibile, cum ar fi datele utilizatorilor, credențiale sau conținut privat. În unele cazuri, atacatorii pot folosi această vulnerabilitate pentru a modifica sau șterge date, ceea ce afectează grav funcționarea aplicației și poate duce la pierderi de date importante.

**CVE-2024-20401** este o vulnerabilitate critică de tip traversare de directoare care afectează serverele de stocare în cloud și alte sisteme de administrare a fișierelor. Această vulnerabilitate apare atunci când intrările utilizatorilor nu sunt validate corect, ceea ce permite atacatorilor să manipuleze căile fișierelor utilizând caractere speciale precum „../”. Exploatarea acestei probleme permite accesarea fișierelor aflate în afara directorului permis, ceea ce expune date sensibile sau critice. În plus, un atacator ar putea modifica sau șterge fișiere importante, afectând atât confidențialitatea, cât și disponibilitatea datelor pentru utilizatori sau organizații.

**CVE-2024-6387** este o vulnerabilitate critică de tip cross-site scripting (XSS) stocat, care afectează aplicațiile web construite pe framework-uri populare precum React și Angular. Vulnerabilitatea apare din cauza lipsei de filtrare și validare a inputului utilizatorilor înainte de afișarea acestuia în interfața utilizatorului. Atacatorii pot exploata această problemă prin introducerea de scripturi malițioase în

[1] https://legislatie.just.ro/Public/DetaliiDocumentAfis/250235

câmpuri vizibile altor utilizatori, ceea ce permite rularea codului în browser-ul acestora. Aceasta poate duce la furtul sesiunilor de autentificare, deturnarea conturilor, manipularea datelor afișate sau chiar la alte atacuri complexe, precum redirecționarea către pagini malițioase.

**CVE-2024-23113** este o vulnerabilitate extrem de periculoasă de tip execuție de cod de la distanță (RCE), care afectează componentele API ale unui sistem ERP utilizat pe scară largă. Vulnerabilitatea rezultă dintr-o lipsă de validare a datelor trimise prin solicitări API, ceea ce permite atacatorilor să introducă payload-uri periculoase. Exploatarea acestei vulnerabilități oferă posibilitatea executării de cod arbitrar pe serverele afectate, permițând accesul la baze de date, furtul informațiilor sensibile și modificarea configurărilor critice. În plus, atacatorii pot folosi infrastructura compromisă ca punct de plecare pentru lansarea altor atacuri cibernetice în rețelele interconectate.

**CVE-2024-38063** este o vulnerabilitate de tip buffer overflow care afectează componentele de procesare media dintr-o aplicație mobilă populară, utilizată de milioane de utilizatori. Problema apare atunci când aplicația nu gestionează corect dimensiunile fișierelor media primite, permițând atacatorilor să trimită fișiere special modificate pentru a provoca depășirea limitei memoriei tampon. Această exploatare poate duce la executarea de cod arbitrar pe dispozitivele afectate, rezultând în compromiterea datelor utilizatorilor, interceptarea comunicărilor private sau chiar blocarea dispozitivului. Exploatarea poate fi realizată fără interacțiune semnificativă din partea victimei, ceea ce face vulnerabilitatea extrem de periculoasă.

**CVE-2024-30103** este o vulnerabilitate de tip denial-of-service (DoS) care afectează serverele de baze de date utilizate de aplicații critice. Vulnerabilitatea apare din cauza unei erori în modul de gestionare a cererilor procesate simultan, ceea ce permite unui atacator să trimită un volum mare de cereri special create. Exploatarea acestui defect duce la consumul excesiv al resurselor sistemului, rezultând încetinirea semnificativă a performanței sau oprirea completă a serviciului. Aceasta afectează direct disponibilitatea aplicațiilor dependente de serverele compromise, având un impact major asupra activităților utilizatorilor și organizațiilor.

Din punctul de vedere al direcției de evoluție, se observă faptul că în anul 2024 numărul de vulnerabilități raportate a crescut semnificativ față de 2023, reflectând atât creșterea complexității sistemelor IT&C, cât și intensificarea activității de cercetare în securitatea cibernetică.

Exemplele includ creșterea numărului de CVE-uri legate de tehnologii emergente, cum ar fi containerele, mediile cloud hibride și aplicațiile IoT. De asemenea, se constată faptul că CVE-urile din 2024 au arătat o tendință de a include exploatări mai sofisticate care necesită competențe avansate pentru a fi remediate, vulnerabilitățile de tip zero-day și cele exploatate în atacuri țintite au fost mai frecvente.

Analizele de risc efectuate de Directorat în 2024, coroborate cu istoricul incidentelor cibernetice, relevă că sectorul sănătății, administrația publică și sectorul energetic sunt cele mai vizate de amenințările cibernetice. Sectorul sănătății se confruntă cu amenințări semnificative din cauza volumului mare de date sensibile și a infrastructurii critice subfinanțate. Administrația publică este adesea ținta atacurilor cibernetice, acestea având impact direct asupra serviciilor și a încrederii cetățenilor. La rândul său, sectorul energetic rămâne un obiectiv prioritar pentru atacatori, ce urmăresc atât testarea și perturbarea infrastructurilor IT/OT, cât și obținerea de beneficii financiare, având în vedere importanța sectorului.

Lipsa personalului specializat în domeniul securității cibernetice, în special pentru răspuns la incidente, rămâne unul dintre cele mai presante riscuri cu care se confruntă organizațiile din România. Concomitent, nivelul redus de conștientizare din partea publicului larg și interesul limitat al managementului privind amenințările cibernetice amplifică vulnerabilitățile existente. Fenomenul este agravat de atacurile tot mai complexe desfășurate de actori malițioși cu capacități avansate.

Având în vedere aceste riscuri și sectoarele cu cel mai mare nivel de expunere, s-au planificat și implementat o serie de măsuri ce vizează atât consolidarea capacităților de securitate cibernetică, cât și îmbunătățirea gradului de conștientizare la nivel național.

Acțiunile desfășurate au urmărit colaborarea strânsă între instituții publice, mediul privat și parteneri internaționali, pentru a asigura o abordare unitară și eficientă în contracararea amenințărilor cibernetice.

## 2.4 Demersurile efectuate de DNSC în contextul securității cibernetice a alegerilor și al declasificării informațiilor prezentate în cadrul ședinței Consiliului Suprem de Apărare a Țării, din data de 28 noiembrie 2024

Pe întreg parcursul anului 2024, Directoratul a efectuat o serie de activități și demersuri legate de subiectul securității cibernetice a alegerilor și al infrastructurii aferente, după cum urmează.

- Conducerea pe toată perioada anului 2024 a ședințelor Work Stream on Elections din cadrul NIS Cooperation Group (The Network and Information Systems Cooperation Group / NIS CG) organizat la nivelul Uniunii Europene. NIS Cooperation Group a fost înființat prin Directivă a UE pentru a asigura cooperarea și schimbul de informații între Statele Membre ale UE. Este alcătuit din reprezentanți ai Statelor Membre ale UE, ai Comisiei Europene și ai Agenției UE pentru Securitate Cibernetică (ENISA), președinția fiind asigurată de statul membru care deține președinția Consiliului Uniunii Europene (UE).
- Facilitarea participării Republicii Moldova ca observator în cadrul formatului Work Stream on Elections din cadrul NIS Cooperation Group. Sub această calitate, reprezentanții agențiilor cu atribuții în securitate cibernetică din Republica Moldova au prezentat liniile de acțiune pe care le-au implementat în contextul alegerilor prezidențiale din 2024 din această țară.
- Începând cu luna mai 2024 Directoratul și **ANSSI (Agence nationale de la sécurité des systèmes d'information - Agenția națională de securitate cibernetică a Franței)** au ținut deschise și utilizate linii de comunicare bilaterale. Subiectele discuțiilor au fost politicile CVD, **schimbul de bune practici pentru securitatea cibernetică a alegerilor (în colaborare cu STS),** securitatea cibernetică în contextul olimpiadei, organizarea celor două instituții.
- În contextul alegerilor parlamentare și prezidențiale desfășurate în România în 2024, Directoratul a desfășurat **activități de sprijin și evaluare** pe linia securității cibernetice asupra infrastructurii Autorității Electorale Permanente (AEP), **fiind identificate și raportate de către DNSC peste 34 de conturi de utilizator compromise și multiple vulnerabilități ale infrastructurii IT&C utilizată în asigurarea procesului electoral**.

În contextul general al alegerilor din noiembrie – decembrie și al declasificării informațiilor prezentate de Serviciul Român de Informații, Serviciul de Informații Externe și Ministerul Afacerilor Interne în cadrul ședinței Consiliului Suprem de Apărare a Țării, din data de 28 noiembrie 2024, DNSC a primit de la reprezentanți ai unor instituții și grupuri de lucru de la nivelul UE întrebări și solicitări de informații cu privire la aspectele de securitate cibernetică relevate de comunicatul de presă al CSAT și la documentele publicate la data de 4 decembrie 2024. Urmare a acestora, au fost efectuate o serie de demersuri concrete:

- În răspuns la solicitările primite, în perioada 5-6 decembrie 2025, Directoratul a desfășurat o serie de activități de informare și dialog cu organismele și instituțiile la nivelul UE și al Statelor membre UE, cu următoarele obiective:
    - Informarea cu privire la disponibilitatea informațiilor declasificate publicate – în acest sens DNSC punând la dispoziție o traducere inițială neoficială a acestora;
    - Solicitarea de informații pe care statele membre și organismele contactate le dețin cu privire la amenințări, actori, tactici și atacuri similare relevante pentru România din perspectiva securității cibernetice în context electoral;
    - Exprimarea disponibilității de a retransmite la nivel național, în calitate de punct național de contact, către instituțiile abilitate, eventualele întrebări sau solicitări de informații suplimentare cu privire la conținutul documentelor publicate.
- Directoratul a organizat și participat la o serie de reuniuni online pe acest subiect, astfel:
    - **Cu Agenția UE pentru Securitate Cibernetică (ENISA)** – Conducerea ENISA a asigurat DNSC și România de tot suportul necesar , au inițiat mecanismul aferent răspunsului la crize cibernetice (EU CyCLONe) și instrumentele de suport și schimb de informații aferente.

- **Cu Cybersecurity Task Force** (Comisia Europeana, DG CONNECT) – grup specializat de nivel tehnic din cadrul DG Connect. Au participat reprezentanți din partea Comisiei, CERT-EU, ENISA, SEAE (Serviciul Extern al UE) etc. DNSC a informat cu privire la publicarea documentelor CSAT și a solicitat date și informații cu privire la amenințări și atacuri relevante în contextul actual, precum și informarea reciprocă în cadrul grupului Task-Force în următoarea perioadă.
    - Reprezentanții Task-Force au prezentat măsurile luate referitoare la TikTok pentru retenția datelor referitoare la alegeri pentru intervalul 24 noiembrie 2024 – 21 martie 2025; În replică DNSC a atras atenția că pentru a obține date relevante pentru alegerile din România, este necesară retenția datelor pentru un interval anterior datei de 24 noiembrie.
    - Reprezentanții Task-Force au relevat faptul că sub aspectul conținutului de pe TikTok sunt în contact cu ANCOM la nivel național, care a ridicat aceeași problemă cu privire la intervalul de retenție;
    - Reprezentanții Task-Force s-au interesat despre existența de date cu privire la atacuri împotriva cetățenilor români în alte state membre;
    - Reprezentanții Task-Force au menționat că a fost activat mecanismul de Răspuns Rapid cu privire la alegerile din România, cooperează cu reprezentanți ai societății civile și organizații media și monitorizează conținutul online în contextul alegerilor;
    - Reprezentantul SEAE s-a interesat despre posibilitatea ca RO să activeze și Cyber Diplomacy Toolbox. În replică reprezentanții DNSC au menționat că aceasta e o decizie inter-instituțională la nivel național neputând oferi informații în prezent.
- **Cu EU CyCLONe** – reuniune la nivel de ofițeri - în urma reuniunii în format virtual convocată la 5 decembrie, pe baza informațiilor prezentate de către DNSC, nivelul de alertă al rețelei a fost escaladat la **Warning Mode** – care presupune activități de informare și tehnice, canale de informare dedicate, precum și coordonare între membrii rețelei.
- **Cu ENISA NLO Network Meeting** – la solicitarea DNSC, a fost inclus pe ordinea de zi un punct de informare cu privire la rapoartele declasificate și solicitarea de informații relevante;
- **Cu EU CSIRT Network** – reuniunea a avut loc la data de 6 decembrie, cu participarea reprezentanților de nivel tehnic ai Statelor Membre, ENISA și din partea DNSC fiind luată în discuție trecerea la nivelul **Alert Cooperation Mode**.

- DNSC a remis către rețeaua CSIRT și către EU-CyCLONe solicitările formale de activare și asistență, transmițând informațiile tehnice deținute aferent problematicii alegerilor, din perspectiva securității cibernetice.
- Atât în discuțiile bilaterale cu ENISA și DG CONNECT cât și în reuniunile multilaterale în din formatele de mai sus, reprezentanții celor două instituții europene precum și cei ai unor SM (DE, BE, HU, LU, ES, SE, PL, CZ etc.) au exprimat solidaritate și au arătat flexibilitate în adaptarea procedurilor aferente formatelor de lucru, susținând activarea mecanismelor de cooperare și creșterea nivelului de alertă.

Directoratul a informat cu celeritate și constant instituțiile naționale competente cu privire la evoluția acestor demersuri.

# 3 STADIUL DE ÎNDEPLINIRE A OBIECTIVELOR DIRECTORATULUI

## 3.1 Întărirea cadrului legislativ și de reglementare

Directoratul a întreprins o serie de acțiuni pentru a susține și dezvolta cadrul legislativ și de reglementare în domeniul securității cibernetice:

### 3.1.1 Modificări și completări legislative

În calitate de inițiator, Directoratul a elaborat și a susținut aprobarea ORDONANȚEI DE URGENȚĂ nr. 155 din 30 decembrie 2024 privind instituirea unui cadru pentru securitatea cibernetică a rețelelor și sistemelor informatice din spațiul cibernetic național civil pentru transpunerea în legislația națională a Directivei (UE) 2022/2555 (Directiva NIS2), evitând astfel demararea procesului de infringement pentru România, țara noastră fiind în prezent una dintre cele 7 țări ale Uniunii care au transpus directiva europeană.

- Procesul de legiferare a fost unul complex, care a presupus derularea unor **multiple consultări publice în intervalul aprilie-septembrie 2024**.
- De asemenea, în vederea asigurării obiectivității, transparenței, neutralității, echidistanței, nediscriminării și legalității proiectului, Directoratul a făcut demersurile necesare pentru **operaționalizarea Comitetului de Reglementare**, **cu avizul CSAT** (conform HCSAT nr. 126/2024).
- Proiectul de act normativ a fost supus **consultării interinstituționale cu 28 de instituții publice** și **a obținut peste 30 de avize interinstituționale**, precum și **avizul CSAT** (conform HCSAT nr. 177/2024).

### 3.1.2 Suport legislativ și colaborare inter-instituțională

Pe parcursul anului 2024, Directoratul a participat la grupuri de lucru în parteneriat cu Ministerul Cercetării, Inovării și Digitalizării (MCID), în domeniul securității cibernetice din cadrul Digital for Development Hub (D4D). În vederea dezvoltării unei strategii naționale în IA, DNSC a participat la sesiunile de consultare și expunere de opinii cu privire la Memorandumul Înființarea Comitetului Român pentru Inteligență Artificială și a unor inițiative privind domeniul inteligenței artificiale în România.

Directoratul a fost cooptat în grupul de lucru înființat în cadrul Comisiei tehnice privind riscul sistemic din componența Comitetului Național pentru Supravegherea Macroprudențială, având în vedere obligativitatea BNR (în calitate de punct principal de contact conform DORA) de a informa Directoratul (în calitate de punct unic de contact conform NIS 2) cu privire la incidentele majore care au loc în sistemul financiar, în vederea anticipării unor efecte negative și la nivelul altor entități esențiale sau importante.

Sprijinirea Ministerului Energiei pentru elaborarea actului normativ în vederea înființării unui CSIRT sectorial în domeniul energetic și a desemnării autorității naționale conform Regulamentul delegat (UE) 2024/1366 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.

Reprezentații Directoratului au colaborat cu Autoritatea Aeronautică Civilă Română pe parcursul anului 2024 cu privire la stabilirea modului de colaborare și cooperare în vederea îndeplinirii de către România, în calitate de stat membru UE, a obligațiilor din Regulamentul de punere în aplicare (UE) 2023/203 al Comisiei din 27 octombrie 2022 (Part-IS).

### 3.1.3 Recomandări strategice

În 2024, Directoratul a lucrat la formularea de recomandări pentru adoptarea de acte normative, bune practici în organizarea ecosistemului național în domeniul securității cibernetice din Republica Moldova și armonizarea acestuia cu cel din România, organizând în acest sens multiple vizite și consultări bilaterale cu Agenția pentru Securitate Cibernetică din țara vecină.

### 3.1.4 Norme metodologice și ordine

Directoratul a avut un rol esențial în elaborarea în elaborarea și avizarea a două a hotărâri de guvern inițiate de Ministerul Cercetării, Inovării și Digitalizării (MCID) pentru punerea în aplicare a obligațiilor rezultate din Legea nr. 58/2023 privind securitatea și apărarea cibernetică a României:

- Hotărârea nr. 62 din 31 ianuarie 2024 pentru aprobarea Normelor metodologice privind solicitarea și comunicarea datelor și informațiilor prevăzute la art. 25 alin. (1) din Legea nr. 58/2023 privind securitatea și apărarea cibernetică a României, precum și pentru modificarea și completarea unor acte normative;
- Hotărârea nr. 831 din 11 iulie 2024 pentru stabilirea categoriilor de persoane prevăzute la art. 3 alin. (1) lit. c) din Legea nr. 58/2023 privind securitatea și apărarea cibernetică a României, precum și pentru modificarea și completarea unor acte normative.

Este important de menționat că Directoratul a emis cele două acte de reglementare necesare pentru punerea în aplicare a obligațiilor rezultate din Legea nr. 58/2023 privind securitatea și apărarea cibernetică a României:

- Ordinul Directorului DNSC nr. 100 din 31 ianuarie 2024 privind aprobarea politicilor de confidențialitate și transparență ale Platformei Naționale pentru Raportarea Incidentelor de Securitate Cibernetică;
- Ordinul Directorului DNSC nr. 180 din 21 februarie 2024 pentru aprobarea Metodologiei privind nivelurile de alertă cibernetică și modalitățile de acțiune în situații de alertă cibernetică.

În vederea implementării Directivei NIS 2, Directoratul a semnat, în luna octombrie 2024, un acord cu Centrul pentru Securitate cibernetică Belgia (CCB) prin care instituția noastră a devenit membru fondator al schemei de certificare de securitate cibernetică Cyber Fundamentals (CyFun).

Directoratul a inițiat un proiect de evaluare a necesităților de actualizare și transpunere, în concordanță cu prevederile Directivei NIS2 și a altor acte normative ale Uniunii Europene, în actele de reglementare a politicii de Divulgare Coordonată a Vulnerabilităților (CVD), dezvoltată anterior de CERT-RO.

### 3.1.5 Activități de supraveghere și control

În baza legislației NIS (Legea nr. 362/2018, respectiv OUG 155/2024), Directoratul a reglementat în 2024 și a avut atribuții de verificare și control la nivelul a:

- 833 de operatori de servicii esențiale (OSE) din sectoare cu impact economic și social foarte ridicat pentru țara noastră (ex: energie, transporturi, sănătate, bănci și infrastructuri ale pieței financiare)
- 8 furnizori de servicii digitale (FSD)
- 51 auditori de securitate cibernetică atestați (persoane juridice),
- 122 auditori de securitate cibernetică atestați (persoane fizice)
- 7 furnizori de servicii de formare în domeniul securității cibernetice autorizați pentru un număr de 3 programe de formare respectiv: auditori de securitate cibernetică, responsabili NIS și membri ai echipelor CSIRT.

În 2024, Directoratul a emis 52 de atestate de auditori de securitate cibernetică, o autorizație pentru furnizorii de servicii de formare, 285 de certificate de specializare emise, și a încasat 428.600 lei din tarifele pentru servicii din activitățile de atestare și autorizare.

Procesul de înregistrare a operatorilor de servicii esențiale a continuat, fiind înregistrați 24 de noi operatori și radiați 90 de operatori (majoritatea ca urmare a comasării operatorilor din grupul CATENA).

## 3.2 Capacități operaționale consolidate în 2024

### 3.2.1 Atragerea de personal calificat

Ca urmare a adoptării Hotărârii Consiliului Suprem de Apărare a Țării nr. S-241/2023 privind modificarea organigramei și a statului de funcții ale DNSC, **numărul de posturi ale Directoratului este de 1.063**.

Din punctul de vedere al **capacităților operaționale**, în anul 2024, Directoratul a avut o serie de provocări majore în ceea ce privește încadrarea cu personal de specialitate de securitate cibernetică. Creșterea numărului de posturi ocupate s-a menținut ca o prioritate în 2024, și a rezultat din obligativitatea îndeplinirii atribuțiilor stabilite prin OUG 104/2021 privind înființarea Directoratului, care conferă noii instituții atribuțiile de autoritate de securitate cibernetică la nivel național, cu un număr de 18 atribuții și funcții instituționale distincte, multe dintre acestea fiind complet noi la nivel național.

Astfel, în scopul urmăririi priorității stabilite pentru anul 2024, privind continuarea operaționalizării structurilor Directoratul prin atragerea resursei umane, în contextul provocărilor asociate lipsei acute a încadrării statului de funcții cu personal înalt calificat necesar îndeplinirii la un nivel ridicat de calitate a atribuțiilor instituționale, a fost înaintat către Guvernul României un **memorandum de aprobare a organizării în 2024 de concursuri de angajare a unui număr total de 60 de posturi de experți**. Memorandumul a fost aprobat în ședința de Guvern din 30 mai 2024.

La momentul ianuarie 2025, **Directoratul are încadrate un număr de 156 persoane (un grad de ocupare de 14,67%)**, prin prezentarea la post la date diferite a persoanelor declarate admise în urma concursurilor organizate pe parcursul anului 2024 în urma aprobării Guvernului.

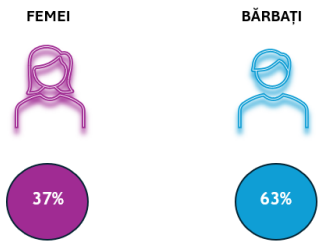
Similar cu anul 2023 și 2024, continuarea recrutării de personal specializat și calificat reprezintă o prioritate majoră, deoarece lipsa **cronică de experți afectează în mod grav capacitatea operațională a DNSC** de asigurare a serviciilor cibernetice de intervenție rapidă 24/7/365 sau de implementare a proiectelor aflate în derulare sau în pregătire, cu impact negativ asupra securității cibernetice din domeniul civil, inclusiv pentru furnizarea serviciilor esențiale, dar și a serviciilor digitale din România.

Funcțiile specifice de conducere și de execuție din cadrul Directoratului pot fi ocupate doar de specialiști cu o stăpânire a fundamentelor securității cibernetice și cu o înțelegere profundă a modului în care sistemele IT sau rețelele / infrastructura și lanțul de furnizori digitali ai unei organizații funcționează.

Toate funcțiile de experți ale DNSC implică stăpânirea unui set complex de cunoștințe și abilități esențiale, incluzând printre altele: o înțelegere a regulamentelor și standardelor internaționale aplicabile, a arhitecturii IT și de securitate IT, a datelor, a criptografiei, a rețelelor de telecomunicații, a principiilor de codificare securizată și a sistemelor de operare, precum și competențe în utilizarea de noi tehnologii digitale, fluență în limbaje de programare și familiarizarea cu metodele comune de exploatare a vulnerabilităților, cu tehnicile de atenuare / limitare a riscurilor cibernetice, cunoștințe privind politicile, reglementările și normele de securitate cibernetică; cunoștințe juridice și economice privind impactul riscurilor, incidentelor, crizelor și atacurilor cibernetice.

Sunt absolut necesare aptitudini, atitudini și un mod de lucru ce necesită profile profesionale care la acest moment nu există în sistemul public național și trebuie a fi atrase din sectorul privat, din cel academic sau din rândul experților români ce activează în străinătate, în cadrul marilor firme și organizații din domeniul securității cibernetice.

De menționat că una dintre prioritățile Directoratului este asigurarea unei cat mai bune împărțiri pe sexe a ocupării posturilor. Situația curentă este următoarea:



### 3.2.2 Operaționalizarea compartimentelor funcționale cheie ale Directoratului

**În 2024, Directoratul a reușit recrutarea sau detașarea de personal** în unele compartimente funcționale care în 2023 aveau încadrate zero (0) persoane:

- Direcția Programe de Educație, Prevenire, Conștientizare și Instruire - 46 posturi
- Serviciul Management al Crizelor Cibernetice – 12 posturi

**În 2025, se va continua efortul pentru recrutarea sau detașarea de personal** în următoarele structuri ale Directoratului care au încadrate zero (0) persoane:

- Serviciul Dezvoltare și Implementare Strategii și Politici de Securitate Cibernetică – 11 posturi (din care 0 ocupate)
- Direcția Atestare și Autorizare – 22 posturi (din care 0 ocupate)
- Direcția Evaluare și Certificare Securitate Cibernetică Noi Tehnologii, Produse și Servicii – 66 posturi (din care 0 ocupate)
- Serviciul Relații Instituționale ECCC, NCC – 11 posturi (din care 0 ocupate)
- Serviciul Protecție Cibernetică VIP, ECCC și alte instituții – 17 posturi (din care 0 ocupate)
- Serviciul PSIRT (Product Security Incident Response Team) – 12 posturi (din care 0 ocupate)
- Direcția Proiecte și Programe Naționale – 23 posturi (din care 0 ocupate)

În special în contextul din ce în ce mai complex al anului 2024, marcat la nivel național și internațional, atât în regiune, cât și pe teritoriul unor state mai îndepărtate, de o serie de alegeri, rolul Directoratului a devenit tot mai relevant, cu premise de continuare și pe parcursul anului 2025, de **reprezentant al României într-o serie de organisme specializate privind securitatea cibernetică**, precum Grupul de Cooperare NIS, Rețeaua echipelor de răspuns la incidente cibernetice (CSIRT Network), Rețeaua Europeană de legătură în domeniul crizelor cibernetice (EU-CyCLONe), Agenția Europeană de Securitate Cibernetică (ENISA) Management Board și National Liaison Officers' Network (NLOs), precum și alte organisme specializate similare.

Cu toate acestea, din motive obiective, un număr de structuri cheie ale Directoratului care au atribuții concrete în implementarea OUG nr. 155/2024, în implementarea activităților testare, evaluare și certificare a securității cibernetice a produselor tehnologiilor, produselor și serviciilor (inclusiv 5G, inteligență artificială, cloud), sau în prevenirea riscurilor și incidentelor cibernetice legate de tehnologiile și platformele informatice, au niveluri de încadrare zero, sau insuficiente comparativ cu nivelul de personal calificat necesar.

Din punct de vedere operațional, prezintă relevanță consolidarea, pe parcursul anului 2024, a capacității de consultanță și reprezentare juridică a Directoratului în fața instanțelor judecătorești, autorităților publice, instituțiilor de orice natură, precum și în raporturile cu orice persoană fizică sau juridică, română ori străină.

Totodată, în cursul anului 2024, s-a constatat necesitatea de a recruta experți în securitate cibernetică, pe poziții în afara organigramei, având în vedere faptul că resursa umană internă fie este insuficientă, fie nu are specializarea necesară ducerii la îndeplinire a unor categorii de activități din cadrul proiectelor de securitate cibernetică cu finanțare externă nerambursabilă. În acest sens, a fost elaborată o procedură internă de angajare pe posturi în afara organigramei și efectuate demersuri necesare pentru comunicarea, spre aprobare, ordonatorului principal de credite.

În contextul geopolitic actual, al riscurilor cibernetice legate de alegerile prezidențiale din mai 2025, al cerințelor de transpunere a Directivei NIS2 (prin OUG nr. 155/2024), precum și pentru asigurarea unui nivel optim de protecție a spațiului cibernetic național civil, precum și în temeiul prevederilor art. VII alin.(4) din OUG nr. 156 din 30.12.2024, este necesară aprobarea organizării de noi concursuri de recrutare pentru continuarea demersurilor de ocupare a posturilor din cadrul DNSC (execuție/conducere).

### 3.2.3 Înaintarea spre avizare a statutului Comitetului Director

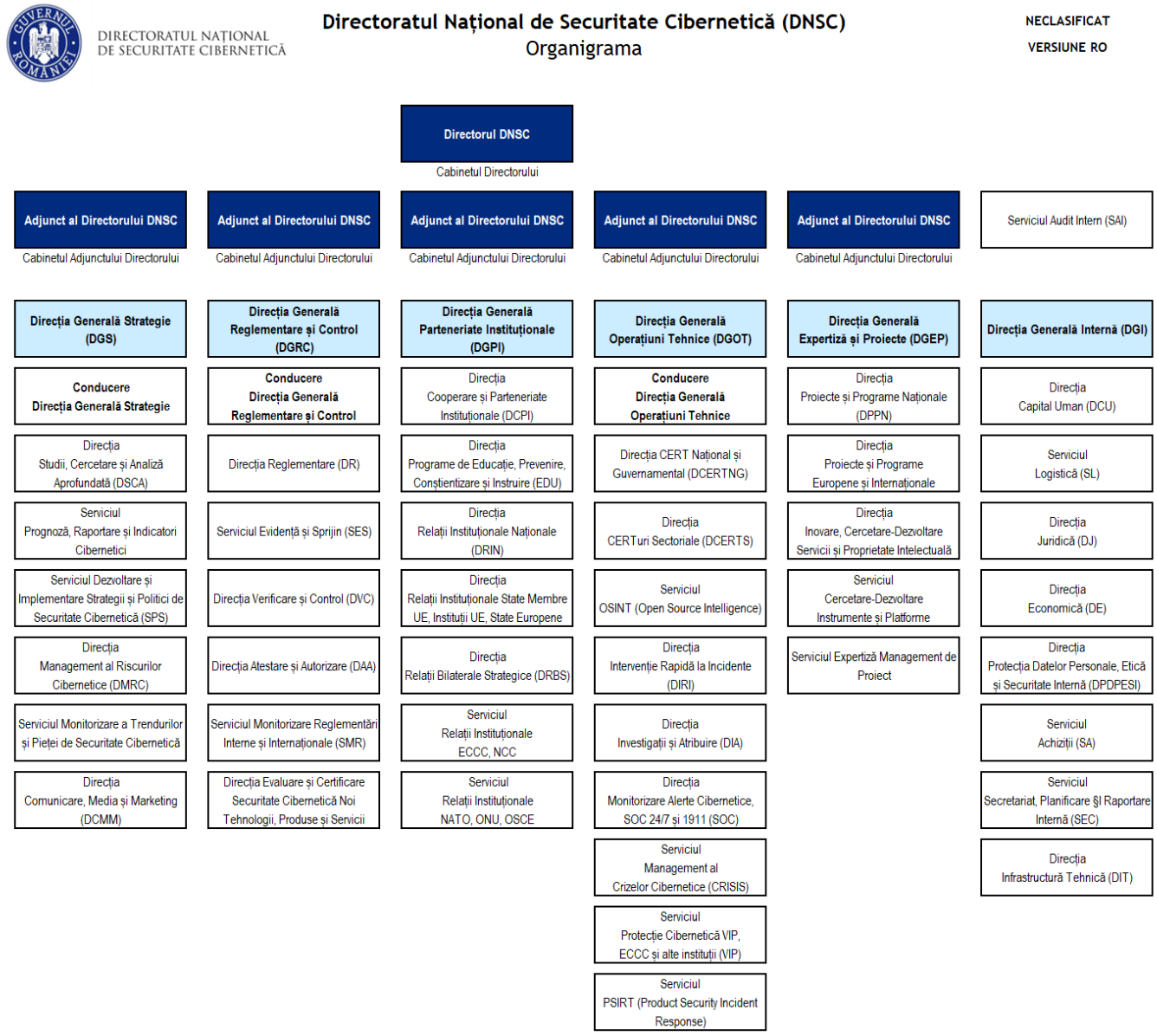
În completarea activităților desfășurate, au fost derulate demersurile necesare realizării unui alt obiectiv instituțional major, prevăzut de OUG. nr. 104/2021, art. 9, referitor la Comitetul Director al DNSC.

Statutul Comitetului Director a fost transmis pentru avizare către Consiliul Suprem de Apărare a Țării (CSAT) și ulterior pentru aprobare către primul-ministru.

Rolul Comitetului Director al DNSC, așa cum este prevăzut în statut, include atribuții esențiale precum avizarea strategiilor de dezvoltare ale Directoratului și propunerilor de politici publice elaborate, destinate prevenirii și contracarării incidentelor din cadrul infrastructurilor cibernetice.

### 3.2.4 Aprobarea de către CSAT a noului Regulament de Organizare și Funcționare al DNSC

În scopul îndeplinirii atribuțiilor pe palierul modului de organizare a activității, prin Hotărârea Consiliului Suprem de Apărare a Țării HCSAT nr. 196 din 11.11.2024, a fost aprobat noul Regulament de Organizare și Funcționare al Directoratului, ce detaliază obiectivele, organizarea și funcționarea structurilor DNSC:



### 3.2.5 Creșterea nivelului de apărare juridică a drepturilor și intereselor Directoratului

Litigiile rezultate din activitatea specifică a DNSC se soluționează de către instanțele de contencios administrativ competente (după caz, secțiile specializate ale curților de apel, respectiv ale Înaltei Curți de Casație și Justiție). Suplimentar, DNSC a deținut/ deține calitatea de parte în litigii de contencios administrativ dar și de conflicte de muncă de competența unor instanțe de grad inferior.

Litigiile aflate în curs de judecată ori soluționate pe parcursul anului 2024, în cadrul cărora Directoratul a avut calitate procesuală de reclamant, sunt rezultatul **i) aplicării de măsuri de recuperare a unor prejudicii** constatate în cadrul unor acțiuni de control ale Curții de Conturi cât și **ii) exercitării dreptului de contestare a actelor administrative al căror destinatar este DNSC, prin care au fost stabilite corecții** financiare în cadrul unor proiecte europene.

În perioada de referință, DNSC a avut calitate de pârât în litigii decurgând din exercitarea dreptului de control al legalității unor a) acte administrative privind înscrierea în Registrul operatorilor de servicii esențiale, b) acte administrative emise în legătură cu desfășurarea examenelor de promovare în grad superior cât și c) măsuri de încetare a raporturilor de muncă cu personalul contractual.

| | | |
|---|---|---|
| **Materie** | Contencios administrativ | 4 |
| | Conflicte de muncă | 3 |
| | Pretenții | 1 |

| | | |
|---|---|---|
| ***Stadiu*** | Dosare câștigate definitiv | 3 |
| | Dosare în curs de soluționare | 5 |
| | Dosare pierdute | 0 |

Pe parcursul anului 2024, Directoratul a fost parte în 5 litigii în curs, alte 3 litigii soluționate definitiv.

În cursul anului 2024, în scopul reparării unor prejudicii aduse bugetului instituției, au fost inițiate demersuri de recuperare a creanțelor atât pe cale amiabilă, în colaborare cu alte compartimente funcționale de specialitate ale DNSC, cât și pe cale litigioasă.

**Acestea au rezultat într-o valoare totală recuperată de:**

**6.714,92 RON**

În ceea ce privește petițiile și adresele primite de la cetățeni sau persoane juridice, în cursul anului 2024 au fost primite și soluționate **30 de petiții pe problematici aflate în sfera de competență legală a DNSC**.

Directoratul nu are atribuția legală de a desfășura activități de cercetare, încadrare juridică și stabilire a existenței și întrunirii elementelor de tipicitate ale faptelor de natură penală ori de a emite puncte de vedere/ opinii/ clarificări, obligatorii/ consultative în scopul soluționării unor spețe particulare ce intră în competența generală, material-funcțională și/sau teritorială a altor structuri/ instituții/ autorități/ organisme. Cu toate acestea, în exercitarea rolului său de autoritate națională competentă pentru spațiul cibernetic național civil și pentru gestionarea riscurilor și incidentelor de securitate cibernetică, DNSC se consultă și cooperează cu organele de urmărire penală în termenele și condițiile prevăzute de lege, dispozițiile art. 3 alin. (4) lit. f) din O.U.G. nr. 104/2021 aplicându-se în mod corespunzător.

În scopul asigurării conformității în raport cu cerințele sistemului integrat de control intern managerial în cadrul DNSC, în cursului anului 2024 au fost continuate demersurile de elaborare și revizuire a unor proceduri interne și norme, având ca scop optimizarea proceselor operaționale și consolidarea mecanismelor de control intern la nivelul DNSC din cadrul mai multor structuri funcționale.

Astfel în perioada de referință, **Directoratul a primit și înaintat spre competentă soluționare 20 de petiții transmise greșit subscrisei.**

**Activitatea de soluționare a petițiilor și/sau scrisorilor cetățenilor**

| | |
|---|---|
| **30** | **20** |
| Petiții adresate instituției | Petiții înaintate spre competentă soluționare |

### 3.2.6 Gradul de realizare anual a tuturor tipurilor de plăți de către DNSC (cumulate) față de sumele alocate și primite, pe total cheltuieli finanțate de la bugetul de stat

Directoratul a respectat termenele de depunere a situațiilor financiare conform prevederilor legale în vigoare cât și a termenelor de depunere.

| Denumire indicator | Cod | Buget 2024 final | Execuție bugetara la data de 31.12.2024 | % |
|---|---|---|---|---|
| ***1*** | ***2*** | ***3*** | ***4*** | ***5=4/3*** |
| Titlul I Cheltuieli de personal | 10 | 23.472 | 21.729 | 92.6 |
| Titlul II Bunuri si servicii | 20 | 1.742 | 1.154 | 66.2 |
| Titlul VII transferuri | 55 | 35 | 7 | 20.0 |
| Titlul VIII Proiecte cu finanțare din fonduri externe nerambursabile aferente cadrului financiar 2021-2027 | 56 | 2.350 | 1 | 0.0 |
| Titlul X Proiecte cu finanțare din fonduri externe nerambursabile aferente cadrului financiar 2014-2020 | 58 | 5.311 | 3.226 | 60.7 |
| Titlul X Alte cheltuieli | 59 | 200 | 186 | 93.0 |
| Titlul XII Cheltuieli de capital | 70 | 1.414 | 1.334 | 94.3 |
| ***Capitolul comunicații*** | ***85.01*** | ***34.524*** | ***27.637*** | ***80,1*** |
| Titlul VIII Proiecte cu finanțare din fonduri externe nerambursabile aferente cadrului financiar 2021-2027 | 56 | 2.062 | 1 | 0,0 |
| Titlul X Proiecte cu finanțare din fonduri externe nerambursabile aferente cadrului financiar 2014-2020 | 58 | 4.065 | 2.314 | 56,9 |
| ***Fonduri externe nerambursabile -Sursa D*** | ***5008*** | ***6.127*** | ***2.315*** | ***37.8*** |
| **Total general buget** | | **40.651** | **29.952** | **73,7** |

### 3.2.7 Alte aspecte logistice

În vederea asigurării capacității operaționale din punct de vedere logistic, pe parcursul perioadei supuse analizei au fost realizate demersuri apte de a conduce la demararea activităților de reabilitare, termoizolare și schimbare a ferestrelor la sediul DNSC din str. Italiană, nr.22, sect. 2, București.

Pentru eficientizare energetică, la sediul Directoratului au fost înlocuite, o parte dintre instalațiile de climatizare, precum si corpurile de iluminat cu tuburi de neon cu lămpi pe bază de tehnologie LED.

De asemenea, au fost remediate temporar și în regim de urgență unele deficiențe legate de alimentarea cu energie electrică a clădirii, fiind înlocuit întrerupătorul general, din tabloul de alimentare cu energie electrică, datorită întreruperilor frecvente a energiei, care apăreau din cauza acestuia.

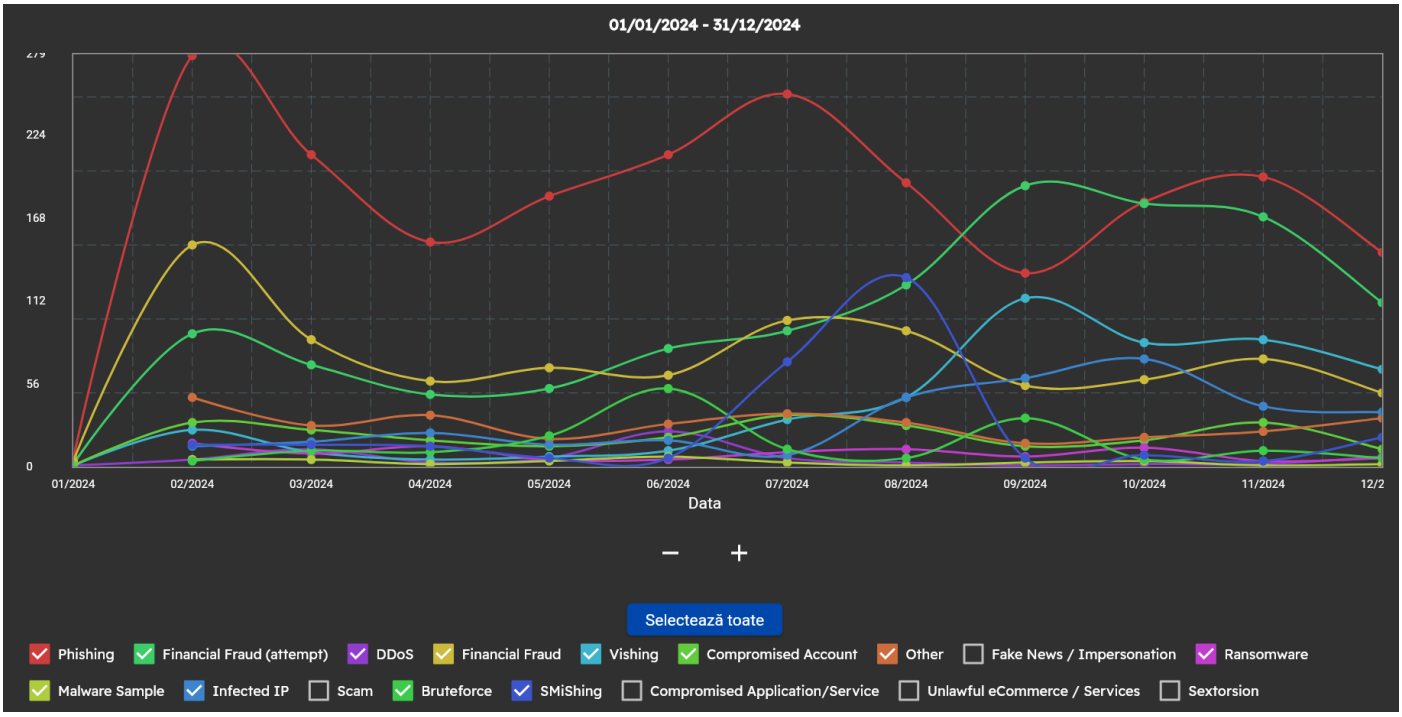
S-a realizat achiziția și dotarea clădirii cu truse de prim ajutor, ca parte a masurilor privind securitatea și sănătatea în muncă, situațiile de urgență și protecția mediului.

## 3.3 Capacități tehnice consolidate în 2024

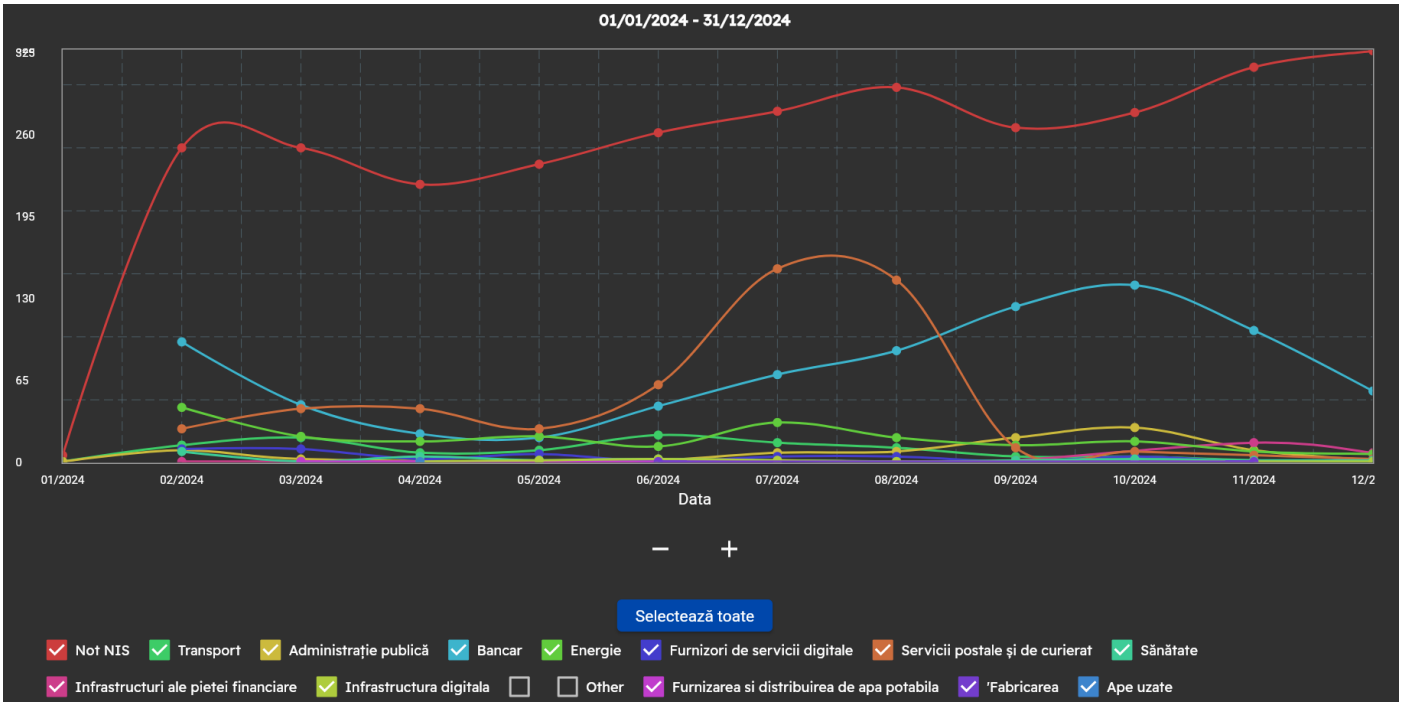
### 3.3.1 Operaționalizarea de capabilități tehnice

În ceea ce privește **capacitățile tehnice** operaționalizate în cursul anului 2024, menționăm următoarele:

- În continuarea demersurilor DNSC din anul 2023, de elaborare și avizare a Ordinului nr. 180/2024 privind metodologia nivelurilor de alertă cibernetică și a Ordinului nr. 100/2024 privind aprobarea politicilor de confidențialitate și transparență ale PNRISC, aceasta a fost operaționalizată, ceea ce a condus la oferirea unui instrument de raportare, destinat persoanelor fizice sau juridice responsabile, a tuturor activităților care să asigure securitatea și/sau apărarea sistemelor, rețelelor și serviciilor informatice, cu respectarea principiului colaborării, cooperării și coordonării.
- Operaționalizarea Platformei RO-SAT „Sistem de alertă timpurie și informare în timp real – RO-SAT”, finanțat prin POC 2014-2020, ce are obiectivul de creștere a capacității operaționale a DNSC în vederea asigurării capabilităților naționale de prevenire, identificare, analiză și reacție la incidentele de securitate cibernetică.
- Operaționalizarea Platformei Naționale de Cooperare în Domeniul Securității Cibernetice (PNCDSC), între instituțiile de stat, mediul privat, mediul academic și organizații non-guvernamentale.
- Constituirea unei rețele comune de analiză a amenințărilor și a unui grup deschis de colaborare al CSIRT-urilor europene, cu accent pe colectarea, partajarea și analiza informațiilor tehnice, operaționale și strategice privind amenințările prin proiectul „Joint Threat Analysis Network – JTAN”, finanțat prin programul UE CEF TELECOM.
- Stabilirea și operaționalizarea de grupuri de lucru ale DNSC în vederea derulării de activități de sprijin tehnice și non-tehnice către Republica Moldova și Ucraina.
- La nivelul Directoratului a fost **inițiată activitatea de implementare a platformei unice pentru evaluarea și gestionarea integrată a riscurilor de securitate cibernetică**. Obiectivul urmărit de către DNSC este de a gestiona platforma unică la nivel național și de a oferi suport pentru implementarea acestui instrument în instituții publice și private.
- Directoratul a finalizat în 2024 operaționalizarea platformei tehnice de raportare consolidată a trendurilor privind atacurile / incidentele cibernetice, care permite urmărirea unor tendințe relevante:




*Figură 1 - Evoluția incidentelor înregistrate în anul 2024*




*Figură 2 - Evoluția incidentelor înregistrate în anul 2024 defalcate pe sectorul vizat (conform taxonomiei Directivei NIS2)*

- În cursul anului 2024, a fost demarat **procesul de operaționalizare a Centrului Național de Gestionare a Crizelor de Securitate Cibernetică (CNGCSC)**. Prima etapă a fost reprezentată de verificarea conceptului în cadrul exercițiului CYBER Europe 24, unde au fost testate module funcționale din cadrul CNGCSC, inclusiv cu reprezentanții celorlalte instituții din Sistemul Național de Apărare, Ordine Publică și Securitate Națională (SNAOPSN). Modul de funcționare al CNGCSC a fost testat din nou în marja exercițiului Histria 24, îmbunătățindu-se deficiențele constatate în cadrul primului exercițiu. Pe baza lecțiilor învățate din cele două exerciții a fost inițiat procesul de elaborare a Regulamentului de Organizare și Funcționare a CNGCSC, la sfârșitul anului 2024 fiind elaborată o versiune preliminară.

### 3.3.2 Operaționalizarea de capabilități tehnice cu instituțiile naționale competente

Pentru îndeplinirea funcției de cooperare și colaborare prevăzute de OUG nr. 104/2021, art. 5, Directoratul a elaborat un set de șapte (7) protocoale bilaterale, destinate membrilor Consiliului Operativ de Securitate Cibernetică COSC (SRI, SIE, SPP, STS, MApN, MAI și MAE), având ca scop principal facilitarea accesului acestora la două platforme gestionate de DNSC:

- Request Tracker for Incident Response (RTIR) și
- Platforma Națională pentru Raportarea Incidentelor de Securitate Cibernetică (PNRISC).

Dat fiind rolul operațional și strategic de importanță majoră al acestor platforme în asigurarea unui răspuns prompt și coordonat la incidentele de securitate cibernetică, accesul instituțiilor partenere a fost reglementat prin protocoale bilaterale, în conformitate cu principiile de transparență și cu respectarea strictă a prevederilor OUG nr. 104/2021, ale Legii nr. 58/2023, precum și actelor normative de organizare și funcționare aplicabile fiecărui partener.

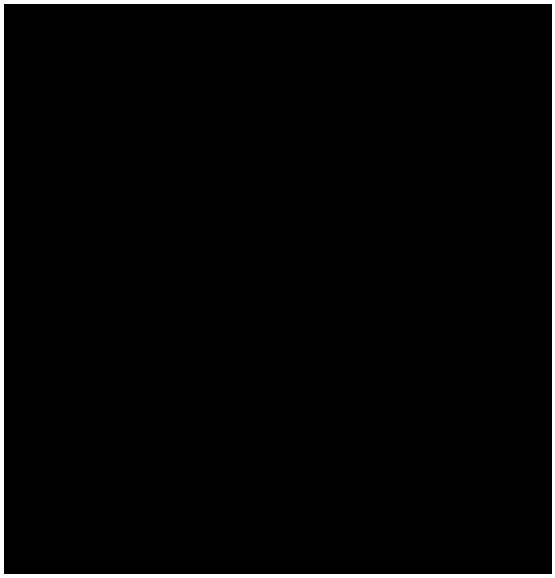
Clauzele protocoalelor au fost adaptate pentru a răspunde cât mai bine nevoilor specifice fiecărui partener și pentru a asigura o implementare eficientă a acestora, fiind elaborate nu doar pentru a formaliza accesul, ci și pentru a stabili responsabilități clare și proceduri transparente, astfel încât parteneriatul să fie eficient.

În 2024, cooperarea cu instituțiile membre COSC a avut loc și prin schimbul de corespondență clasificată, atât secret de serviciu, cât și secret de stat (preponderent SRI, Administrația Prezidențială, MApN și MAE), documentele reprezentând în principal adrese de informare/ atenționare/ verificare, transmise în

contextul evenimentelor din Ucraina, al alegerilor, precum și al unor evenimente de interes pe spațiul cibernetic.

### 3.3.3 Buletine de informare (cyber dashboard) destinate factorilor de decizie naționali

Similar anului 2023, în vederea consolidării și actualizării nivelului de conștientizare la nivel înalt privind starea de securitate cibernetică, **au fost întocmite 252 buletine de informare (cyber dashboard) de securitate cibernetică** cu actualizări privind amenințările din spațiul cibernetic și dinamica activităților malițioase la nivel național și internațional, transmise direct către factori de decizie din structurile guvernamentale. Distribuția acestor buletine de informare, în cursul anului 2024, a fost astfel:



- Ianuarie - 20 buletine
- Februarie - 21 buletine
- Martie - 21 buletine
- Aprilie - 22 buletine
- Mai - 20 buletine
- Iunie - 19 buletine
- Iulie - 23 buletine
- August - 21 buletine
- Septembrie - 21 buletine
- Octombrie - 23 buletine
- Noiembrie - 21 buletine
- Decembrie - 20 buletine

### 3.3.4 Menținerea și gestionarea capacitaților tehnice proprii

Din punctul de vedere al infrastructurii tehnice proprii, Directoratul a depus toate diligențele pentru asigurarea funcționării optime a infrastructurii informatice și menținerea unui flux constant și sigur al informațiilor în cadrul instituției.

Au fost implementate măsurile necesare pentru operarea, întreținerea și îmbunătățirea infrastructurii, conform nevoilor identificate la nivelul DNSC și a fost asigurată consultanța tehnică de specialitate în cadrul Comisiei Tehnice de Specialiști / Comitetul Tehnico-Economic pentru Societatea Informațională (CTE).

Procesele implementate au vizat definirea arhitecturii, managementul și dezvoltarea rețelelor, platformelor informatice și sistemelor de comunicații (IT&C) la nivel instituțional, contribuind semnificativ la realizarea obiectivelor strategice. Prin aplicarea unor soluții tehnice și operaționale eficiente, s-a asigurat funcționarea optimă a infrastructurii informatice, precum și furnizarea unui suport tehnologic de specialitate pentru întregul personal.

La nivelul Directoratului, în 2024 au fost instalate și configurate peste 250 de echipamente IT, inclusiv laptopuri, desktopuri și imprimante multifuncționale proprii. S-au realizat activități de mentenanță și service la peste 80 de laptop-uri și 30 de servere fizice ale instituției.

Au fost administrate un număr de aproximativ 275 de servere din care 243 de servere virtuale, 238 calculatoare și laptop-uri, respectiv 45 de alte tipuri de echipamente (tablete, telefoane) utilizate în mod curent de către personalul DNSC.

## 3.4 Implementarea de proiecte în domeniul securității cibernetice

### 3.4.1 Proiecte de securitate cibernetică în derulare

Anul 2024 a fost unul marcant pentru Directorat, consolidându-se ca un pilon esențial în securitatea cibernetică națională și internațională. Prin coordonarea unui portofoliu diversificat de proiecte naționale și internaționale, DNSC a contribuit la creșterea rezilienței cibernetice, dezvoltarea de competențe și implementarea de soluții inovatoare pentru protecția infrastructurilor critice și a societății digitale.

La finalul anului 2024, Directoratul efectua un număr de 26 proiecte de securitate cibernetică, cu finanțare națională și internațională:

| Nr. | ACRONIM | DENUMIRE PROIECT | BUGET TOTAL | BUGET DNSC | DEADLINE |
|---|---|---|---|---|---|
| 1. | DYNABIC | Dynamic business continuity of critical infrastructures on top of adaptive multi-level cybersecurity | 4.999.695 EUR | 151.000 EUR | 30.11.2025 |
| 2. | RO-CCH | Romanian Cyber Care Health | 578.870 EUR | 578.870 EUR | 31.03.2025 |
| 3. | DNS4EU | The DNS4EU and European DNS Shield | 6.173.310 EUR | 203.600 EUR | 31.12.2025 |
| 4. | INFORB | Implementation of the NIS Directive in the sector production, processing and distribution of Food in Romania and Bulgaria | 1.105.598 EUR | 455.820 EUR | 31.08.2025 |
| 5. | SIEMBIOT | Modular, open, research platform integrating SIEM, NOC, SOC, CTI and Vulnerability Management | 3.358.195 EUR | 538.210 EUR | 30.08.2026 |
| 6. | CYRESRANGE | Cyber Ranges Resiliency Networks | 1.750.033 EUR | 77.896 EUR | 31.08.2026 |
| 7. | CYDERCO | CYber DEtection, Response and COllaboration | 2.881.082 EUR | 819.192 EUR | 30.09.2026 |
| 8. | 5G-TACTIC | 5G Trusted And seCure network servICes | 5.211.184 EUR | 241.606 EUR | 30.11.2026 |
| 9. | SECUR-EU | Enhancing Security of European SMEs in Response to Cybersecurity Threats | 3.777.100 EUR | 230.585 EUR | 30.11.2026 |
| 10. | INTERSOC | INTERconnected Security Operation Centres | 6.566.561 EUR | 475.080 EUR | 31.12.2026 |
| 11. | ENSOC | ENSOC-CROSSBORDER PLATFORM | 15.654.928 EUR | 1.165.230 EUR | 31.12.2026 |
| 12. | PNRR – Măsura 183 | Crearea de noi competențe de securitate cibernetică pentru societate și economie | 71.442.240 RON | 71.442.240 RON | 30.06.2026 |
| 13. | PNRR – Măsura 184 | Crearea de noi competențe de securitate cibernetică pentru societate și economie | 51.912.759 RON | 51.912.759 RON | 30.06.2026 |
| 14. | CYSSDE | CyberSecurity Deplopyment Preparedness Support, Capacity & Capabilities | 6.984.087 EUR | 228.445 EUR | 31.05.2028 |
| 15. | ECYBRIDGE | Towards a Civil Defence Synergic Approach in The New Age of Cybersecurity | 2.493.118 EUR | 165.208 EUR | 31.05.2026 |
| 16. | IPRADAR | SOL-2024 - 25 - Sistem de scanare și cartografiere a resurselor IP din România, cu scopul detectării timpurii a amenințărilor cibernetice | 15.436.519 RON | 3.000.000 RON | 11.08.2026 |
| 17. | aSIEMmetry | Employ entropy models to pre-emptively detect novel risks for monitored SIEM assets and enhance SOC analysts with AI capabilities | 1.461.299 EUR | 370.434 EUR | 31.12.2027 |
| 18. | ACSOC | Advanced Cooperative SOC | 3.037.730 EUR | 400.608 EUR | 31.12.2027 |
| 19. | CYBERGUARD | Fortifying SOCs Against Evolving Cyber Threats | 7.690.250 EUR | 481.500 EUR | 30.11.2027 |
| 20. | EU-INSPIRE | INnovative multi-diSciPlinary Industry focused cybersecurity education for upskilling and ReskIlling the EU workforcE | 19.477.569 EUR | 289.756 EUR | 31.12.2028 |
| 21. | SAFE | Security AI for Enhanced SOC | 7.998.210 EUR | 692.504 EUR | 31.12.2027 |

| Nr. | ACRONIM | DENUMIRE PROIECT | BUGET TOTAL | BUGET DNSC | DEADLINE |
|---|---|---|---|---|---|
| 22. | CRA-AI | The CRA-AI project will build highly automated AI enabled software to support SMEs and Micro SMEs on every step of their journey to achieve compliance with the Cyber Resilience Act | 2.979.094 EUR | 177.834 EUR | 31.12.2026 |
| 23. | CONFIRMATE | Conformity assesment, methrics and compliance automation for the CRA | 1.191.766 EUR | 447.902 EUR | 30.06.2026 |
| 24. | ENDURANCE | Strategies and Services for Enhanced Disription Resilience and Cooperation in Europe | 4.999.776 EUR | 119.250 EUR | 30.09.2027 |
| 25. | TRUSTBOOST | Unifying & Upgrading Certification Capabilities Across Europe | 3.169.019 EUR | 243.960 EUR | 31.08.2027 |
| 26. | CYBERFORT | Strengthening Cyber Defenses of SMEs for Cyber Resilience Act (CRA) Compliance | 3.728.629 EUR | 315.008 EUR | 31.05.2026 |

Aceste proiecte vizează domenii/ teme precum:

- Infrastructuri critice;
- Sectorul sanitar;
- Protejarea utilizatorilor europeni împotriva amenințărilor cibernetice;
- Lanțul de aprovizionare alimentar;
- Integrarea funcțiilor SIEM (Security Information and Event Management), NOC (Network Operations Center), SOC (Security Operations Center), CTI (Cyber Threat Intelligence) și managementul vulnerabilităților;
- Poligoane cibernetice pentru simularea, testarea și instruirea în medii de securitate cibernetică;
- Platforme colaborative pentru detectarea, analiza și răspunsul la incidente cibernetice;
- Soluții 5G sigure pentru infrastructuri critice cum ar fi sănătatea, transportul și energia;
- IMM;
- Rețea SOC interconectată;
- Cooperarea transfrontalieră în gestionarea amenințărilor cibernetice;
- Pregătirea organizațiilor pentru implementarea eficientă a soluțiilor de securitate cibernetică;
- Abordarea integrată pentru apărarea civilă și cibernetică în Europa;
- Modele avansate de entropie pentru a detecta riscuri emergente în sistemele SIEM și pentru a sprijini analiștii SOC cu soluții bazate pe AI;
- Centre SOC care colaborează pentru a gestiona incidente complexe;
- Întărirea centrelor SOC în fața amenințărilor cibernetice emergente;
- Programe educaționale inovatoare pentru forța de muncă europeană;
- Integrarea inteligenței artificiale în centrele SOC;
- Soluții software automatizate bazate pe AI pentru a sprijini IMM-urile să respecte Cyber Resilience Act (CRA);
- Strategii și servicii pentru reziliență sporită împotriva atacurilor și perturbărilor cibernetice;
- Standardizarea procesului de certificare pentru a asigura interoperabilitatea între soluțiile de securitate cibernetică.

### 3.4.2 Proiecte de securitate cibernetică în pregătire – finanțare națională

**În anul 2024, Directoratul a pregătit propunerile de finanțare națională** pentru o serie de proiecte a căror implementare a fost planificată pentru **anul 2025,** proiecte în care bugetul DNSC are o valoare de **17.570.209 €,** respectiv de **87.851.047 LEI.**

Temele pe care se concentrează aceste proiecte sunt:

- Dezvoltarea unui centru național de excelență pentru digitalizare și tehnologii emergente, în colaborare cu parteneri din domeniile academic și privat;
- Dezvoltarea unei soluții experimentale pentru identificarea și gestionarea amenințărilor cibernetice utilizând inteligența artificială;
- Crearea unui laborator dedicat certificării soluțiilor și serviciilor de securitate cibernetică;
- Creșterea conștientizării și educației în domeniul securității cibernetice la nivel național;
- Dezvoltarea unei platforme digitale pentru sprijinirea pacienților;
- Îmbunătățirea rezilienței infrastructurilor critice prin cercetare și dezvoltare;
- Crearea unei platforme integrate pentru securitatea cibernetică avansată;
- Creșterea competențelor digitale ale forței de muncă din România.

Aceste propuneri reflectă angajamentul DNSC de a aborda provocările complexe ale securității cibernetice și digitalizării, consolidând capacitatea națională de răspuns la amenințările emergente și promovând inovația tehnologică.

### 3.4.3 Proiecte de securitate cibernetică în pregătire – finanțare internațională

**În anul 2024, Directoratul a pregătit propunerile de finanțare internațională** pentru o serie de proiecte a căror implementare a fost planificată pentru **anul 2025,** proiecte în care bugetul DNSC are o valoare de **3.554.355 €** respectiv de **17.771.775 LEI.**

Temele pe care se concentrează aceste proiecte sunt:

- Optimizarea infrastructurilor tehnologice și proceselor DNSC pentru dezvoltarea serviciilor digitale destinate instituțiilor publice, academice și cetățenilor;
- Implementarea Directivei NIS2 în sectorul sănătății pentru sporirea securității cibernetice a instituțiilor medicale;
- Dezvoltarea unui Centru Național de Excelență pentru Digitalizare și Autonomie Strategică în Tehnologii Emergente;
- Crearea unui sistem inteligent bazat pe inteligență artificială pentru detectarea și răspunsul la amenințări cibernetice;
- Implementarea unui laborator de certificare tehnică pentru soluții și servicii de securitate cibernetică;
- Educație și conștientizare în securitatea cibernetică pentru publicul larg și IMM-uri;
- Dezvoltarea unei soluții inovative de distribuție a cheilor criptografice cuantice prin intermediul dronelor;
- Integrarea tehnologiilor Distributed Ledger în fluxurile organizaționale pentru îmbunătățirea colaborării între instituțiile de securitate națională;
- Proiectarea unei platforme de management a datelor multi-sursă pentru analiza predictivă a situațiilor de risc;
- Tranziția către criptografia post-cuantică în administrațiile publice și infrastructurile critice;
- Dezvoltarea unei platforme integrate pentru detectarea și gestionarea în timp real a incidentelor cibernetice;
- Îmbunătățirea capacităților SOC (Security Operations Center) prin implementarea de soluții bazate pe AI;
- Consolidarea securității IoT (Internet of Things) printr-o platformă avansată pentru investigații;

- Crearea unui ecosistem rezilient în industria alimentară, integrând securitatea cibernetică și infrastructura spațială;
- Crearea unei rețele europene de poligoane cibernetice pentru pregătirea practică și creșterea rezilienței infrastructurilor critice;
- Dezvoltarea competențelor digitale avansate prin programe de formare axate pe securitatea cibernetică în domeniul maritim.

### 3.4.4 Proiecte de securitate cibernetică finalizate

În anul 2024, au fost finalizate următoarele proiecte:

- SECurity And privacy protectioN in Internet of Things devices – SECANT
- Artificial Intelligence Threat Reporting and Incident Response System – IRIS
- Joint Threat Analysis Network – JTAN

Valoarea totală a proiectelor a fost de: 639.768 €, respectiv 3.198.840 LEI.

## 3.5 Conștientizare, cultură și educație în domeniul securității cibernetice

### 3.5.1 Campanii, evenimente și proiecte de conștientizare

Directoratul a efectuat în 2024 o serie de evenimente, vizite, ateliere și dezbateri, având scopul de a crește nivelul de conștientizare asupra pericolelor existente în mediul online și prezentarea oportunităților de carieră în domeniul securității cibernetice:

- Elaborarea și susținerea prezentări educaționale în diferite instituții de învățământ preuniversitar și universitar, precum: Școala de Vară Ovidius Constanța; Școala Gimnazială Olga Gudynn; Școala nr.79 București; Autoliv - Brașov; Liceul Teoretic Internațional de Informatică București (ICHB), Colegiului Național I.L. Caragiale; Școala Gimnazială Șeica Mare; Liceul Teoretic “Ioan Petruș” Otopeni, licee din Buzău , Universitatea Constantin Brâncoveanu, filiala RM Vâlcea.
- Participarea cu prezentări educaționale la evenimente precum: CodeKIDS (București), PatriotFest (București); Conferința “Bune practici de securitate cibernetică pentru oameni și companii” (Sibiu).
- Implicarea împreună cu Poliția Română, Asociația Română a Băncilor și compania Ascendia în organizarea și desfășurarea Campaniei "Protecție prin educație: Securitate digitală".
- Realizarea de materiale și broșuri de prezentare a Directivei NIS 2.0.
- **5 (cinci) workshop-uri pentru analiza riscurilor de securitate cibernetică** din sectoarele: sănătate, energie, transport naval, transport aerian și transport feroviar. În urma acestor activități au fost identificate principalele riscuri cibernetice din sectoarele respective și au fost elaborate recomandări pentru diminuarea sau eliminarea acestora.
- Directoratul a coordonat la nivel național campania “Luna Europeană a Securității Cibernetice 2024”, activitate de conștientizare desfășurată în fiecare an la nivelul statelor membre UE.
- Campania de informare și educație cibernetică la nivel național Siguranța Online: 6 (șase) cursuri online de tip e-learning, dedicate elevilor, părinților și profesorilor; variate cursuri derulate fizic sau online (webinar) în școli și licee la nivel național; 3 evenimente de presă organizate pe diferite tematici de conștientizare; participare la Bucharest Gaming Week; 2 campanii de conștientizare pe social media.
- Alte activități desfășurate în sprijinul procesului de informare corectă a populației privind amenințările curente din spațiul cibernetic:
    - 2 (două) workshop-uri cu presa din România pe subiectul deepfake, respectiv scam-uri cu investiții;
    - 2 (două) campanii de conștientizare a pericolelor din mediul online, în parteneriat cu Google România (cu focus pe fraudele online și pe dezinformare);

- Diseminarea și promovarea continuă pe social media, TV și radio a materialelor de informare privind riscurile de securitate cibernetică.
- Organizarea periodică a unor evenimente dedicate securității cibernetice:
    - Dialog cu instituțiile omoloage din Belgia și Franța pentru obținerea de know-how și bune practici în ceea ce privește implementarea Directivei NIS2 și pentru crearea cadrului național în domeniul politicilor CVD
    - Dialog cu instituțiile omoloage din Cipru privind implementarea AR-in-a-Box+
    - Co-organizarea și participarea la conferințe, seminarii și mese rotunde pe teme de securitate cibernetică, cu participarea actorilor din mediul public, privat și din cel academic, în țară și în străinătate
    - Organizarea de workshop-uri precum:
        - Workshop Cyber Citizen Initiative, la sediul Reprezentanței Comisiei Europene în România București
        - Worskshop "Tehnologie de criptare pentru sistemele IoT utilizabilă în infrastructurile critice"
        - BOX2M Engineering la sediul DNSC

### 3.5.2 Educație și formare

Activitățile de educare și formare derulate de Directorat în domeniul securității cibernetice au fost foarte variate și complexe, incluzând, printre altele:

- Participarea DNSC în cadrul Programului Oficial de Internship al Guvernului României.
- Elaborarea unui chestionar adresat unităților de învățământ liceal, pentru evaluarea nivelului de maturitate în materie de securitate cibernetică al unităților de învățământ liceal de pe raza Municipiului București.
- Realizarea și diseminarea unui chestionar privind nivelul de maturitate al politicilor de securitate cibernetică în administrația publică locală. Analiza inițiată de Directorat a avut ca obiectiv înțelegerea nivelului de maturitate al politicilor de securitate cibernetică implementate sau avute în vedere de autoritățile administrației publice locale.
- Susținerea de prezentări privind activitatea, prioritățile și oportunitățile de carieră în DNSC: Cyber Awareness Webinar (organizat de Chenist), Gala Internship (organizată de Guvernul României), activitate de conștientizare în domeniul securității cibernetice în cadrul Programului Oficial de Internship al Guvernului României (organizată la sediul DNSC pentru stagiarii din Program).
- Co-organizarea fazei naționale a Campionatului European de Securitate Cibernetică ROCSC / ECSC ediția 2024, în parteneriat cu Centrul Național Cyberint/SRI, ANSSI, Orange România și Bit Sentinel și Ministerul Educației.
- Co-organizarea primei ediții a Olimpiadei de Securitate Cibernetică (OSC), în parteneriat cu Centrul Național Cyberint/SRI, ANSSI, Orange România și Bit Sentinel și Ministerul Educației.
- Gestionarea grupului de lucru (EduCorner) ce vizează maparea tuturor inițiativelor din mediul privat în domeniul educației cibernetice pentru copii.
- Elaborarea bazei de date a inițiativelor educaționale din sectorul preuniversitar în domeniul securității cibernetice în România, – pentru ENISA, plecând de la inițiativele partenerilor din grupul EDU Corner și alte inițiative demarate în colaborare cu DNSC.

### 3.5.3 Publicarea de materiale pentru conștientizare și informarea despre securitatea cibernetică

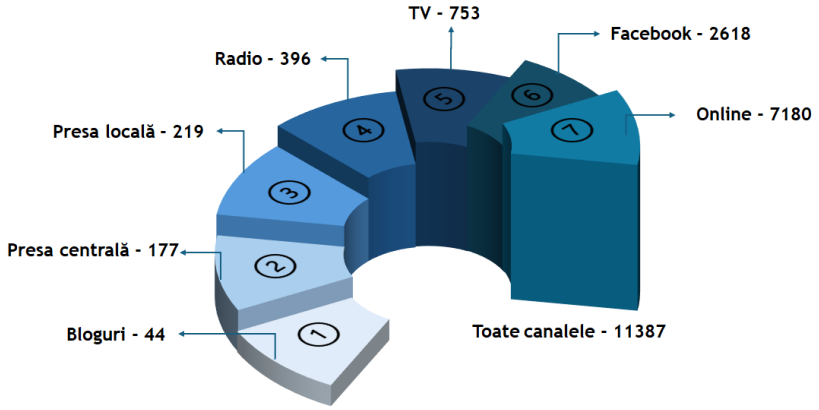
În scopul îndeplinirii funcției de alertare, prevenire, conștientizare și instruire, DNSC a lansat și promovat o serie de evenimente, acțiuni și materiale menite a crește gradul de conștientizare a publicului cu privire la riscurile de securitate cibernetică:

- **9 (nouă) ghiduri de securitate cibernetică** pentru creșterea nivelului de conștientizare a publicului cu privire la riscurile de securitate cibernetică, având ca tematică:
  - Protejare si recuperare conturi social media (RO, EN, UA);
  - Bune practici pentru utilizarea aplicațiilor de acces la distanță;
  - Deepfake – Manipulat sau informat?;
  - Conștientizarea importanței protecției datelor cu caracter personal și a securității cibernetice pentru copii, părinți, profesori;
  - Deepfake - ghid pentru organizații;
  - Inginerie Socială;
  - Considerații etice ale IA;
  - Blockchain și securitatea cibernetică;
  - 7 principii strategice de securitate cibernetica pentru managementul companiilor.
- **6 (șase) analize pe subiecte de actualitate din domeniul securității cibernetice**: Riscuri cibernetice asociate platformei TikTok; Ransomware Backmydata; Malware Rafel RAT; Atac DDOS; Incident Crowdstrike; Gruparea Sandworm.
- O altă prioritate în anul 2024 a constat în elaborarea de documente aferente proiectului pilot al Agenției pentru Securitate Cibernetică a Uniunii Europene (ENISA) – Awareness Raising (AR)-in-a-Box+ pentru definirea programului intern de conștientizare față de amenințările cibernetice.

### 3.5.4 Interacțiunea cu mass-media pe subiectul securității cibernetice

În 2024, Directoratul a acordat o atenție deosebită comunicării cu mass-media în vederea distribuirii de materiale și mesaje menite să contribuie la creșterea nivelului de conștientizare în domeniul securității cibernetice. În acest sens, conducerea DNSC și specialiștii în comunicare, media și marketing ai institutiei au avut un total de **315 intervenții de presă** (**240 TV, 37 radio, 14 presă centrală și 19 presă locală**) și **570 de comunicate de presă, articole și știri**.

| Toate canalele | Presă centrală | Presă locală | Radio | TV | Online | Bloguri | Facebook |
|---|---|---|---|---|---|---|---|
| **11.387** | **177** | **219** | **396** | **753** | **7.180** | **44** | **2.618** |




Audiența estimată a fost de 127.019.933 de persoane din care 83.106.000 la TV, 23.753.776 la radio, 13.960.022 în online și 6.863.109 în presa centrală. Valoarea aproximativă pe care DNSC ar fi trebuit să o plătească pentru a atinge același nivel de vizibilitate și informare a publicului prin reclame plătite, echivalent cu valoarea monetizată a aparițiilor în presă a fost de **22.076.153 EUR**.

Pe platformele de socializare (Facebook, Instagram, LinkedIn, X) au fost postate **1.581 de materiale de interes ale Directoratului,** iar feed-back-ul a fost de 207.189 de reacții și comentarii la aceste postări.

De asemenea, pentru informarea populației, au fost asigurate răspunsuri la **36 petiții și solicitări de informații de interes public** în baza Legii nr. 544/2001.

## 3.6 Cooperarea la nivel național și internațional în domeniul securității cibernetice

### 3.6.1 Încheierea de noi parteneriate instituționale naționale în domeniul securității cibernetice

În 2024, Directoratul a reușit pregătirea, finalizarea și semnarea de acorduri de parteneriat și cooperare cu o serie de entități naționale relevante, astfel:

- Universitatea Babeș-Bolyai din Cluj-Napoca
- Universitatea Națională de Apărare „Carol I” (UNAP)
- Academia Tehnică Militară „Ferdinand I”
- Școala Națională de Studii Politice și Administrative (SNSPA)
- Universitatea de Medicină și Farmacie “Carol Davila” București (UMFCD)
- Universitatea “Lucian Blaga” din Sibiu (ULBS)
- Facultatea de Drept (UNIBUC)
- Universitatea Româno-Americană (URA)
- Academia Forțelor Terestre “Nicolae Bălcescu” din Sibiu
- Universitatea Titu Maiorescu
- Universitatea Ștefan cel Mare din Suceava
- Secretariatul general al Guvernului SGG (Programul de Internship al Guvernului României, Ediția 2024)

De asemenea, au fost demarate activități de parteneriate strategice cu universități, instituții din domeniul medical, precum și cu entități din mediul academic, public și privat pentru cooperare și promovarea produselor și serviciilor DNSC în domeniu securității cibernetice:

- Academia de Studii Economice din București
- APSAP – Asociația pentru formare APSAP
- Asociația pentru Informare, Educație și Prevenție în Sănătate
- Direcția de Sănătate Publică a județului Alba
- Sanatoriul de Nevroze Predeal
- Institutul Regional de Gastroenterologie-Hepatologie prof. Dr. Octavian Fodor Cluj Napoca
- Universitatea de Medicina si Farmacie Grigore T. Popa Iași
- Serviciul de Ambulanta Județeană Covasna
- Spitalul Clinic de Recuperare Medicala Băile Felix
- Asociația Salvare București
- Sanatoriul Bușteni
- Institutul de Psihiatrie Socola
- Serviciul de Ambulanță București și Ilfov
- Spitalul de Psihiatrie "Prof. Dr. Alexandru Obregia

- Universitatea de Vest Timișoara
- Spitalului Clinic Județean de Urgență Sf. Spiridon Iași
- Direcția de Sănătate Publică a județului Brașov
- Direcția de Sănătate Publică a județului Constanța

În prezent, protocoalele bilaterale produc efecte juridice și operaționale, contribuind la îndeplinirea obiectivelor generale și specifice ale Directoratului prin întărirea capacităților naționale de securitate cibernetică și consolidarea parteneriatului strategic dintre DNSC și instituțiile partenere.

### 3.6.2 Organizarea conferinței anuale Bucharest Cybersecurity Conference 2024 - BCC2024 – evenimentul major în securitate cibernetică la nivelul României

În perioada 29-31 octombrie 2024, DNSC a organizat, într-un format complet nou, cel mai mare, relevant și vizibil eveniment de securitate cibernetică la nivel național: **Bucharest Cybersecurity Conference 2024** (**BCC2024**), cu sprijinul Centrului Național de Coordonare (NCC-RO) și al Asociației Naționale pentru Securitatea Sistemelor Informatice (ANSSI), în colaborare cu Agenția Uniunii Europene pentru Securitate Cibernetică (ENISA) și cu Centrul European de Competențe în materie de securitate cibernetică (ECCC).

**Scopul principal al conferinței** a fost explorarea strategiilor și soluțiilor pentru asigurarea viitorului digital al Uniunii Europene în fața amenințărilor cibernetice și hibride. BCC2024 a facilitat colaborarea și schimbul de experiențe și cunoștințe între experți și decidenți, având ca obiectiv consolidarea rezilienței cibernetice atât la nivel european, cât și global, într-un context marcat de riscuri în continuă schimbare.

**Evenimentul a reunit peste 1.500 de experți naționali și internaționali din domeniul securității cibernetice**, atât din sectorul privat, cât și cel public și academic. BCC2024 s-a remarcat printr-o agendă amplă, sofisticată și diversificată, incluzând 28 de sesiuni de tip masă rotundă desfășurate exclusiv pe bază de invitație, 25 de paneluri cu participarea a peste 100 de speakeri de renume internațional și 18 prezentări de tip keynote susținute de reprezentanți de top ai unor companii de tehnologie și soluții cyber.

**Sesiunile plenare** au fost dedicate implementării celor mai recente politici și reglementări europene în domeniul securității cibernetice, precum **Directiva NIS2**, Actul pentru Reziliență Cibernetică al UE (**Cyber Resilience Act**) și Actul pentru Solidaritate Cibernetică al UE (**Cyber Solidarity Act**).

În paralel s-au desfășurat sesiuni în format masă rotundă, respectând principiile Chatham House Rule, moderate de reprezentanți ai sponsorilor sau co-organizatorilor conferinței care au abordat diverse subiecte precum: reducerea decalajului de competențe din domeniu, promovarea diversității și învățarea continuă pentru adaptarea forței de muncă la provocările actuale; implementarea strategiei de dezvăluire coordonată a vulnerabilităților (CVD); soluțiile pentru consolidarea rezilienței cibernetice în industriile critice; protecția datelor și continuitatea operațională; impactul tehnologiilor emergente asupra securității cibernetice, în special rețelele 5G și protecția serviciilor de cloud; securitatea cibernetică în sectoarele critice, cum ar fi sănătatea și industria maritimă.

În plus, s-au explorat soluții pentru gestionarea riscurilor specifice acestor domenii. De asemenea, a fost organizată o discuție de tip masă rotundă dedicată subiectului „Cybersecurity Awareness Raising: The ENISA Do-It-Yourself Toolbox” susținută de reprezentanții ENISA. Evenimentul, a reunit peste 20 de participanți din autorități publice naționale în domeniul securității cibernetice, interesați să afle mai multe despre implementarea acestui proiect la nivel național.

Pe parcursul conferinței, au avut loc exerciții de tip "tabletop" privind continuitatea guvernamentală (facilitate de către AWS), exerciții tehnice de tip Red vs Blue și workshop-ul DevSecOps care s-a desfășurat pe perioada a două zile, oferind participanților oportunități de a învăța prin experiență practică în gestionarea vulnerabilităților de securitate.

Conferința a beneficiat de o acoperire mediatică amplă la nivel național cât și internațional, datorită **parteneriatelor media de prestigiu** cu lideri din industrie **incluzând Euronews, Agerpres, Financial**

**Intelligence, Kill Draper**, oferind o platformă esențială pentru abordarea provocărilor actuale și viitoare din domeniul securității cibernetice. Accentul a fost pus pe necesitatea unei acțiuni coordonate și a inovației pentru a răspunde amenințărilor emergente.


Sprijinită de sponsori și parteneri de renume, conferința BCC2024 a creat un nou standard pentru acest tip de evenimente în România și la nivel european și a deschis noi oportunități pentru construirea unui ecosistem digital sigur și sustenabil în Europa.

### 3.6.3 Organizarea/participarea la exerciții de securitate cibernetică

O preocupare majoră în anul 2024 a fost participarea DNSC la planificarea și desfășurarea exercițiilor de securitate cibernetică. Obiectivele principale pentru participarea la aceste exerciții au fost creșterea nivelului de pregătire a personalului și testarea modului de funcționarea a anumitor structuri în situații de criză cibernetică. Directoratul a fost implicat activ în **planificarea și desfășurarea** următoarelor exerciții de securitate cibernetică:

- Exercițiul UE de securitate cibernetică Cyber Europe 24;
- Exercițiul CYDEX24 organizat de Centrul Național CYBERINT
- Exercițiul NATO Locked Shields 2024
- Exercițiul NATO Cyber Coalition 2024
- Exercițiul Histria 24, organizat de MApN
- Exercițiul CyberMan 2024
- Exercițiul Național de Securitate Cibernetică pentru Sectorul Energetic din România – Energy CyberGuard, organizat împreună cu împreună cu Ministerul Energiei și companiile SANS și DragOs SUA;
- Exercițiul de tip „table top” (TTX) pe probleme de alegeri electorale împreună cu organizația GlobalFocus
- Exercițiul de tip „table top” (TTX) organizat prin proiectul ECYBRIDGE cu jucători și asistență oferită pentru elaborarea scenariului
- Hackathon-ul din cadrul Digital Innovation Summit Bucharest 2024;
- Integrated Resolve 2024, exercițiu comun UE – NATO
- Exercițiul de tip „table top” (TTX) Full Spectrum Deterrence Simulation: Consequences of a Frozen Ukrainian Conflict, Constanța
- Exercițiul CyberSpring 2024, destinat entităților din zona de energie nucleară
- Exercițiul interinstituțional de management al crizelor Neptun Watch 25

- Wargame pe tema rezilienței organizat de E-ARC și Centrul de Excelență European de Reziliență
- Exercițiul de tip capture the flag Decode and Conquer

Exercițiul cu cea mai mare amploare în care a fost implicat DNSC, cu rol de coordonator național, a fost Cyber Europe 2024. Exercițiul a fost organizat de către ENISA în vederea evaluării, consolidării și testării nivelului de pregătire al statelor membre cu privire la amenințările transfrontaliere aferente domeniului energiei. Partenerii naționali și din UE au testat planurile de criză și posibilele răspunsuri la potențiale incidente de securitate cibernetică care ar putea afecta distribuția energiei electrice la nivel european. Coordonarea națională pentru participarea României la exercițiul Cyber Europe 2024 s-a concretizat prin:

- Participarea la conferințele de planificare a exercițiului;
- Coordonarea activității echipei de planificatori din România;
- Coordonarea entităților care au avut statut de jucători;
- Testarea modului de funcționare a Centrului Național de Gestionare a Crizelor de Securitate Cibernetică (CNGCSC).

### 3.6.4 Implicarea Directoratului alături de parteneri, organizații internaționale, sectorul privat și societatea civilă în susținerea capacităților cibernetice din state terțe

Pentru a putea calibra prioritățile de cooperare cu statele partenere, Directoratul s-a coordonat constant cu instituțiile relevante din România și parteneri internaționali pentru a asigura rezultate concrete și a evita potențiale redundanțe. Eforturile DNSC au vizat schimbul de bune practici, capacity building, dar și facilitarea cooperării la nivel de ecosisteme, acționând ca un hub pentru organizații din domeniile public și privat din România și statele partenere.

**REPUBLICA MOLDOVA**

Directoratul s-a coordonat în mod activ cu partenerii europeni (Misiunea de parteneriat a UE în Republica Moldova - EUPM Moldova) și din SUA pentru a oferi sprijin operațional autorităților moldovene.

Pe parcursul anului 2024, DNSC a avut în derulare mai multe inițiative de colaborare cu autoritățile din Republica Moldova, care au vizat eforturi de consolidare instituțională și a capabilităților în domeniul securității cibernetice și transferul de bune practici:

- În contextul înființării Agenției pentru Securitate Cibernetică (ASC) din republica Moldova, Directoratul a sprijinit eforturile de consolidare a instituției, elaborare a cadrului legal și pregătire a resurselor umane. Prima acțiune de cooperare externă a ASC a fost realizarea unui memorandul de înțelegere cu DNSC.
- În contextul alegerilor prezidențiale, respectiv al referendumului privind integrarea în UE din octombrie-noiembrie 2024 din Republica Moldova, Directoratul a inițiat un proiect de creștere a nivelului de conștientizare privind amenințările cibernetice din statul vecin la nivelul UE și național.
- Directoratul a elaborat un material de analiză transmis către ENISA și Serviciul European de Acțiune Externă (SEAE), dar și către beneficiari din România. Acesta a inclus informații furnizate de Serviciului Tehnologia Informației și Securitate Cibernetică (STISC) și Agenției pentru Securitate Cibernetică (ASC) privind incidentele de securitate cibernetică identificate, rezultatele analizei OSINT și monitorizării media pe subiect, respectiv elemente de analiză și contextualizare. Directoratul s-a coordonat în timp real cu autoritățile din Republica Moldova în perioada alegerilor inclusiv pentru a oferi sprijin în gestionarea incidentelor cibernetice în desfășurare.
- Susținerea unui training facilitat de Organizației pentru Securitate și Cooperare în Europa (OSCE) privind clasificarea incidentelor cibernetice în Republica Moldova. Directoratul a contribuit la workshop cu informații privind importanța sistemelor de clasificare a incidentelor pe baza informațiilor taxonomii, prevederile legale existente în România privind clasificarea incidentelor – Legea 58/2023, Legea 362/2018, recomandări privind detaliile necesare în procesele de notificare a incidentelor conform articolului 26 din Legea 362/2018, informații generale privind Platforma Națională pentru Raportarea Incidentelor de Securitate Cibernetică, metodologia privind caracteristicile nivelurilor de

alertă cibernetică și modalitățile de acțiune în situații de alertă cibernetică conform Ordinului nr. 180 din 21 februarie 2024.

- Organizarea Roundtable The Republic of Moldova and its Path to EU Accession: Cybersecurity Chapter în cadrul Bucharest Cybersecurity Conference 2024, care a reunit stakeholderi din mediul public și privat din Republica Moldova, România și state partenere. Acest eveniment a avut ca obiectiv explorarea caracteristicilor ecosistemului de securitate cibernetică din Republica Moldova și analizarea capacității acestuia de a se adapta la provocările și amenințările specifice în domeniul securității cibernetice.
- Moderarea ședinței comune WS Elections și Comisia Europeană DG CONNECT cu invitați din cadrul ecosistemului de securitate cibernetică din Republica Moldova - Serviciul pentru Tehnologia Informației și Securitate Cibernetică (STISC).

**UCRAINA**

- Cooperarea cu autoritățile din Ucraina a vizat schimbul de bune practici și livrarea de trainiguri în domeniul securității cibernetice (ex. Workshop finanțat de Reprezentanța Fundației pentru Cercetare Civilă și Dezvoltare a Statelor Unite în Ucraina CRDF Global – Cernăuți/martie 2024, Workshop în colaborare cu E-ARC și EU AM – Ivano Frankivsk/noiembrie 2024);
- De asemenea, DNSC a organizat, în parteneriat cu Centrul Național de Coordonare în Securitate Cibernetică (NCSCC) subordonat Consiliului Național de Securitate și Apărare al Ucrainei (NSDC) și Reprezentanța Fundației pentru Cercetare Civilă și Dezvoltare a Statelor Unite în Ucraina (CRDF Global), cea de-a treia întâlnire internațională a platformei de coordonare „Dezvoltarea Parteneriatului pentru Reziliența Cibernetică a Europei de Sud-Est” (București, aprilie 2024), sub egida Cluster-ului Național de Securitate Cibernetică al Ucrainei. La reuniune au participat reprezentanți ai instituțiilor din componența COSC.
- Reprezentanții Directoratului au fost invitați să împărtășească experiența României pe teme precum reziliența în domeniul cibernetic și implementarea legislației europene la o serie de evenimente organizate de autoritățile ucrainene - Kyiv International Cyber Resilience Forum (Kiev/februarie 2024), Regional Cyber Resilience Forum (Lvov/iulie 2024), prima conferință privind diplomația cibernetică (online/iunie 2024).

**ORGANIZAȚII INTERNAȚIONALE - OCDE**

În 2024, Directoratul a furnizat puncte de vedere pe domeniul de competență pe documente de lucru și la reuniuni în formatele multilaterale ale OCDE, precum:

- Asigurarea contribuției Directoratului la evaluările OCDE în vederea sprijinirii procesului de aderare a României la organizație, prin pregătirea documentelor de background și asigurarea participării DNSC la misiunea tehnică de evaluare a Secretariatului OCDE în domeniul Politicii privind Economia Digitală și la sesiunea de evaluare a României de către Comitetul privind Politica Digitală al OCDE; realizarea rapoartelor de stadiu privind implementarea recomandărilor formulate de evaluatorii OCDE pentru alinierea cu principiile organizației, pe componenta de securitate cibernetică; elaborarea de puncte de vedere privind documentele circulate în formatele de lucru din cadrul organizației.
- În noiembrie 2024, România a primit avizul formal privind alinierea la recomandările OCDE în domeniul politicii digitale, care are o componentă importantă de securitate cibernetică. Obținea acestui aviz reprezintă un progres semnificativ în procesul de aderare a României la OCDE, care reprezintă o prioritate strategică la nivel național.
- Participarea la reuniuni de lucru online în formatele OCDE: Working Party on Security in the Digital Economy, OCDE Working Party on Measurement and Analysis of the Digital Economy, OECD 9th WPDS Session, ONE Platform training, Working Party on on Digital Security – WPDS;
- Contribuții la chestionarul pentru evaluarea nivelului de aliniere a României în domeniul Politicii Economiei Digitale al Organizației pentru Cooperare și Dezvoltare Economică (OCDE), în vederea aderării.

- Contribuția la întocmirea fișelor de autoevaluare incluse în Memorandumul Inițial al României în raport cu prevederile instrumentelor juridice ale OCDE în domeniul DEP.
- Contribuții la pregătirea Misiunii tehnice de informare și evaluare a Secretariatului OCDE-CDEP în domeniul Politicii privind economia digitală – 24 instrumente juridice OCDE, în vederea analizării și explicării cadrului legislativ național și european, a politicilor, proiectelor și a practicilor la nivel național din domeniul de activitate al DNSC evaluatorilor OCDE, corelate cu prevederile instrumentelor juridice ale OCDE.

**ORGANIZAȚII INTERNAȚIONALE - NATO**

În 2024, Directoratul a furnizat puncte de vedere pe domeniul de competență pe documente de lucru și la reuniuni în formatele multilaterale ale NATO, precum:

- Contribuția Directoratului pentru mandatul de reprezentare a României la Conferința anuală pentru apărare cibernetică a NATO.
- Elaborarea de mesaje de awareness privind Defence Innovation Accelerator for the North Atlantic (DIANA).

**ORGANIZAȚII INTERNAȚIONALE - ONU**

În 2024, Directoratul a furnizat puncte de vedere pe domeniul de competență pe documente de lucru și la reuniuni în formatele multilaterale ale ONU, precum:

- Participarea DNSC la United Nations Global Intergovernmental Points of Contact Directory on the Use of ICTs in the Context of International Security – participarea la două ping tests.
- Integrarea DNSC ca membru în cadrul Grupului Național de Implementare (GNI) al Inițiativei ONU 1325 – Femeile, Pacea și Securitatea.

**ORGANIZAȚII INTERNAȚIONALE - OSCE**

În 2024, Directoratul a furnizat puncte de vedere pe domeniul de competență pe documente de lucru și la reuniuni în formatele multilaterale ale OSCE, precum:

- Participarea DNSC la reuniunile Organizației pentru Securitate și Cooperare în Europa (OSCE) Informal Working Group Cyber (online și în format fizic), respectiv la Reuniunea Anuală a Punctelor de Contact Naționale pentru OSCE Confidence-Building Measure (CBM) No. 8; workshopul facilitat de OSCE privind clasificarea incidentelor cibernetice în Republica Moldova.

**ORGANIZAȚII INTERNAȚIONALE - UE**

În 2024, Directoratul a participat activ în și a furnizat puncte de vedere pe domeniul de competență pe documente de lucru și la reuniuni în formatele multilaterale ale Uniunii Europene, precum:

- AR-in-a-Box+: realizarea de demersuri pentru includerea României în proiectul pilot organizat de ENISA, pentru identificarea și implicarea organizațiilor beneficiare din România din sectoarele sănătate și energie. În cadrul proiectului pilot AR in a box +, care a fost implementat în perioada iulie-decembrie 2024, ENISA a oferit sprijin organizațiilor participante în dezvoltarea de campanii interne de conștientizare în domeniul securității cibernetice, adaptate specificului sectorului de activitate și nivelului de pregătire al resurselor umane.
- Gestionarea proiectului Cybersecurity Support Action, prin care DNSC a furnizat, prin intermediul ENISA, licențe în cadrul unor platforme de training pentru aproximativ 250 de operatori de servicii esențiale și organizarea a 12 workshop-uri, cinci exerciții tehnice, cinci exerciții de tip TTX, precum și a unei activități de tip pentesting, cu participarea operatorilor de servicii esențiale din sectoarele Sănătate, Energie și Furnizare de Apă. În plus, DNSC a fost implicat în negocierile pentru definirea catalogului de servicii pentru 2025 pentru ENISA Support Action, având ca obiectiv maximizarea sprijinului pe care entitățile din România (în special operatorii de servicii esențiale) îl pot primi din partea UE pentru consolidarea securității cibernetice.

- Participarea în cadrul NIS CG/WS9 - Peer Reviews and National Cybersecurity Strategies, la revizuirea metodologiei și aspectelor organizatorice ale evaluărilor inter-pares ale statelor membre, în vederea învățării din experiențele comune, consolidarea încrederii reciproce, atingerea unui nivel comun ridicat a securității cibernetice, precum și îmbunătățirea capacităților și politicilor de securitate cibernetică ale statelor membre necesare pentru punerea în aplicare a Directivei NIS 2.
- Reprezentarea DNSC în diferitele formate de la nivelul Uniunii Europene (ENISA NLO; NIS Cooperation Group; ECATS, ECASEC), având contribuții specifice.
- Participări în format ECATS și ECASEC alături de ENISA, în special pe componenta de raportare a incidentelor de securitate cibernetică (este relevantă deținerea poziției de Chair al Work Stream on incident reporting).
- Organizarea echipei internationale, la nivelul Uniunii Europene, de scriere și de promovare a unui Compendium și Checklist privind Securitatea Cibernetică și Reziliența Alegerilor PE 2024 sub NIS Cooperation Group.
- Participare la reuniunea interinstituțională desfășurată cu reprezentanții Comisiei Europena DG CONNECT la sediul MCID, format la care DNSC și-a adus contribuția prin prezentarea activităților care au implicat îndeplinirea obiectivelor subsescvente Digital Decade Programme.
- Obținerea poziției de co-chair al formatului Work Stream on Health (NIS CG).
- Directoratul a asigurat poziția de co-chair al formatului Work Stream on Incident Reporting prin organizare, coordonarea și moderarea discuțiilor și lucrărilor din cadrul formatului.

**Alte inițiative de cooperare și parteneriat ale Directoratului**

- Încheierea sau negocierea unor acorduri de cooperare la nivel internațional: AEK/MKD-CIRT Macedonia de Nord, Armenia, Azerbaidjan, Kazahstan, Iordania, Japonia, India, Singapore, CAMP, Brazilia, Qatar, AKCESK/Albania, ACN-Italia.
- Aderarea DNSC la EU CyberNet în calitate de stakeholder și promovarea opțiunilor de implicare a experților din cadrul Directoratului în activitățile de susținere a altor state partenere.
- Participarea la cea de-a treia ediție anuală a Conferinței National Cybersecurity Forum, organizată de Asociația Organizațiilor de Securitate Cibernetică din Azerbaidjan (AKTA), Baku Azerbaidjan.
- Participare în activități educaționale organizate de Departamentului Regional de Studii pentru Managementul Resurselor de Apărare (Dresmara).
- Contribuție la consultările româno-saudite.

# 4 PRIORITĂȚI ALE DIRECTORATULUI PENTRU 2025

Pentru anul 2025, Directoratul se va concentra pe următoarele aspecte:

- **Continuarea operaționalizării structurilor Directoratului prin atragerea resursei umane (organizarea de concursuri și examene),** prin participarea la programul guvernamental de internship și prin parteneriate cu actori instituționali si echipe de voluntari în cadrul unor proiecte și inițiative.
- **Implementarea OUG 155/2024** (care face transpunerea Directivei NIS 2 în legislația românească) prin elaborarea, adoptarea și aplicarea actelor normative subsecvente. Consolidarea cooperării cu autoritățile competente sectorial pentru implementarea OUG 155/2024 (ANCOM, ADR, AACR).
- **Continuarea îmbunătățirii managementului incidentelor cibernetice la nivel național.**
- Sprijin instituțional către autoritățile naționale competente din domeniul securității cibernetice din Republica Moldova.
- Continuarea îndeplinirii în mod activ și coordonat cu celelalte autorități competente la nivel național, a rolului alocat Directoratului în contextul alegerilor prezidențiale din 2025.
- **Dezvoltarea progresivă și măsurabilă a capacității operaționale a Directoratului** și implementarea măsurilor necesare pentru eficientizarea proceselor interne, în conformitate cu legislația aplicabilă.
- Operaționalizarea Autorității Naționale de Certificare de Securitate Cibernetică din cadrul **Directoratului pentru** implementarea Cyber Resilience Act.
- **Continuarea utilizării eficiente a mijloacelor de comunicare strategică ale Directoratului** pentru creșterea nivelului de informare și conștientizare privind securitatea cibernetică**.**
- Asigurarea unei participări active a Directoratului la formatele de cooperare internațională în domeniul securității cibernetice și continuarea reprezentării României la reuniunile relevante în format UE, OSCE, OCDE, ONU, NATO, în coordonare cu instituțiile relevante de la nivel național.
- **Operaționalizarea Centrului Național de Gestionare a Crizelor de Securitate Cibernetică** prin validarea ROF-ului, validarea conceptului CNGCSC într-un exercițiu major și realizarea operaționalizării structuri din cadrul Directoratului.
- **Organizarea și participarea la exerciții de securitate cibernetică**, pentru a crește coeziunea între actorii principali din domeniul public și privat.
- **Demararea procesului de actualizare a Strategiei de Securitate Cibernetică a Românei.**
- **Realizarea unei analize de risc cibernetic** la nivel național și a **două strategii sectoriale** cyber.
- Colaborarea cu start-up-uri în cadrul incubatoarelor de afaceri, facilitând integrarea tehnologiilor emergente în produsele și serviciile de securitate cibernetică existente.
- Continuarea investițiilor în infrastructura proprie IT pentru a menține standardele de calitate și pentru a asigura scalabilitate pe termen lung. Adoptarea unor soluții inovatoare pentru optimizarea proceselor interne, inclusiv implementarea de tehnologii bazate pe inteligență artificială.
- **Inițierea unor proiecte** cu impact regional și cu utilizare civil-militară (dual use), în parteneriat cu alte instituții publice, mediul privat și academic.
- **Operaționalizarea, la nivel DNSC, a platformei pentru managementul riscurilor de securitate cibernetică,** prin implementarea unei soluții tehnice specifice.