DIRECTORATUL NAȚIONAL
DE SECURITATE CIBERNETICĂ

Raport anual de activitate
2025

(aprobat prin HCSAT nr. 117/07.08.2026)

DOCUMENT DESTINAT PUBLICĂRII

TLP:CLEAR

Cuprins

1 CUVÂNTUL DIRECTORULUI

Pentru un domeniu eminamente tehnic, de nișă, extrem de avansat și dinamic precum securitatea cibernetică, este esențial ca România să proiecteze o viziune clară, o ambiție susținută și un pragmatism strategic, atent calibrat.

De la înființarea sa în 2021, până la finalul lui 2023 când s-a reușit recrutarea primilor noi angajați și apoi până în 2025 când am accelerat semnificativ activitatea și am crescut vizibil rezultatele concrete ale activității, Directoratul a urmărit și a implementat constant viziunea de a deveni o instituție de clasă internațională care poziționează ferm România ca lider recunoscut în domeniul securității cibernetice. În contextul geopolitic, tehnologic și de reglementare actual este esențial să acționăm rapid, decisiv și vizibil în această direcție.

Cred că noua Strategie Națională de Securitate Cibernetică, pe care o (re)definim în 2026, prin aliniere cu Strategia Națională de Apărare a Țării pentru perioada 2025-2030, va oferi direcția și cadrul necesar pentru ca instituțiile statului, sectorul privat și mediul academic să acționeze coordonat în vederea consolidării poziției României ca actor capabil și influent în domeniul cibernetic. Aceasta va valorifica resursele, expertiza și soluțiile pe care România le deține și le dezvoltă, contribuind la afirmarea sa ca furnizor de competență și inovare în spațiul digital. În același timp, securitatea cibernetică va rămâne, în anii care urmează, un pilon strategic și un catalizator esențial pentru accelerarea inovării, stimularea creșterii economice și aprofundarea procesului de digitalizare de care avem nevoie.

Într-o perioadă în care observăm evoluții majore, rapide, și cu impact global asupra securității cibernetice, când Uniunea Europeană regândește reglementările și cadrul normativ (ex. propunerea de regulament Digital Omnibus), iar Statele Unite ale Americii și-au publicat în martie 2026 noua strategie națională cyber ce definește un nivel de coordonare fără precedent între actorii guvernamentali și mediul privat, Directoratul va avea parte de multă acțiune, presiune și responsabilitate, și va avea un rol esențial în efortul interinstituțional de urmărire a intereselor României în formatele bilatetale și multilaterale din domeniul securității cibernetice.

Este evident că în 2026 va trebui și să continuăm să poziționăm, să sprijinim și să apărăm interesele României în contextul actual. Dar, precizez că se vor putea înțelege, anticipa și influența aceste trenduri complexe doar printr-o prezență bine pregătită, activă și vizibilă în grupurile tehnice de lucru și de decizie la nivel UE, la Bruxelles, Washington, etc. Desigur, o prezență bine coordonată cu celelalte instituții dar și cu mediul privat, pentru a utiliza efectiv puterea și impactul calitativ superior al ecosistemului nostru cibernetic.

Vom sprijini și asista în domeniul cibernetic atât Republica Moldova cât și Ucraina, în parcursul lor către statutul de membri ai Uniunii Europene. Alianța Cibernetică pentru Reziliență Regională înființată recent, cu DNSC ca unul dintre instituțiile semnatare, va fi un vector major în acest sens. Vom consolida reziliența împotriva amenințărilor cibernetice și hibride facilitate de mijloace cyber, prin cooperare, schimb de cunoștințe, tehnologii avansate, răspuns coordonat și asistență reciprocă.

Nu am niciun dubiu că și în 2026, activitatea operațională a Directoratului va continua trendul din 2025 și va fi una intensă, pe toate palierele: tehnic și operațional, de reglementare, de definire de strategii, sau de cooperare națională și internațională. O vom realiza cu succes împreună cu partenerii instituționali și experții noștri. În domeniul securității cibernetice, poate cea mai importantă dar greu de atras resursă este resursa umană: una competentă, motivată și calificată. Dacă în 2024, Directoratul a reușit (nu fără eforturi substanțiale) recrutarea de 18 noi experți, necesari pentru a demara activitatea unor compartimente cheie în care erau încadrate zero persoane, în 2025 am realizat atât o schimbare de strategie cât și un salt calitativ. Sprijinul continuu din partea Guvernului României s-a materializat în atragerea prin concurs a 81 noi angajați (din care 37 debutanți cu studii medii, majoritatea încă studenți) care au generat o vizibilitate și un impact semnificativ al activităților DNSC. Mai mult, au adus cu ei un val de inovare și expertiză în noi tehnologii digitale și au compensat cu succes pentru plecarea a 27 angajați (prin pensionare, demisie, încetarea detașării, etc.).

Livrăm deja rezultate semnificative cu un buget absolut rezonabil și cu un nivel de încadrare cu personal de doar 17,69%. Estimez că atingerea unui procent de 25% aproape va dubla numărul de inițiative naționale și internaționale, de exerciții, notificări și alerte, de măsuri proactive împotriva actorilor cibernetici malițioși, de intervenții la incidente cibernetice, precum și acoperirea cu servicii specializate pe care DNSC o oferă cetățenilor, firmelor și partenerilor instituționali. Iar AI-ul va amplifica în mod pozitiv acest efort și impactul său.

Vă rog și vă invit să aveți încredere în viziunea mea și viitorul acestei instituții competente pentru spațiul cibernetic național civil; și în nivelul de performanță și rezultatele pe care Directoratul le va putea livra dacă abordarea, evoluția pozitivă și substanțială a acestuia vor continua în același ritm.

Dan Cîmpean - Directorul Directoratului Național de Securitate Cibernetică (DNSC)

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 2025, a fost unul ridicat:

Nivelul amenințării cibernetice în România ↑

Avansul tehnologic accelerat și dependența crescândă de infrastructura digitală au amplificat riscurile cibernetice, transformându-le într-o preocupare semnificativă la nivel global. Anul 2025 a marcat o intensificare a acestor amenințări, conturând un peisaj digital volatil și imprevizibil.

Peisajul global al atacurilor cibernetice în 2025 a fost marcat de operațiuni derulate atât de grupări de criminalitate informatică, de hacktiviști pro-ruși, cât și de grupări de tip Advanced Persistent Threat (APT) statale și non-statale, vizând nu doar România, Ucraina, Republica Moldova, ci și numeroase țări ale Uniunii Europene, SUA, Israel etc. La nivelul României, țintele au inclus atât instituții guvernamentale, cât și operatori din sectoare critice, precum cel energetic, financiar, transporturi, telecomunicații și sănătate.

Intensificarea acțiunilor hibride desfășurate de Federația Rusă în contextul războiului de agresiune declanșat asupra Ucrainei în 2022, al alegerilor parlamentare din Germania, Portugalia și Republica Moldova, dar și a celor prezidențiale din România și Polonia, a continuat să influențeze peisajul cibernetic românesc și în 2025. Acest conflict a consolidat rolul hacktivismului și al grupărilor de tip APT sprijinite de Federația Rusă ca instrumente strategice, demonstrând capacitatea acestora de a influența și derula atacuri cibernetice complexe asupra infrastructurilor IT&C din spațiul cibernetic național civil.

Directoratul a monitorizat constant activitatea acestor grupări și a beneficiat constant de date și informări pe acest subiect, provenind în principal din partea Serviciului Român de Informații (SRI), a Ministerului Afacerilor Interne (MAI), precum și a partenerilor instituționali internaționali:

APT28 FANCY BEAR

Gruparea APT28, cunoscută și sub numele de **Fancy Bear**, **Sofacy**, **Sednit**, **Strontium** sau **Pawn Storm**, este sponsorizată de Federația Rusă. APT28 este recunoscută pentru activitățile sale continue de spionaj cibernetic și operațiuni disruptive, reprezentând o amenințare semnificativă la nivel internațional prin atacuri țintite asupra guvernelor, organizațiilor militare, mass-media și infrastructurii critice.

APT29 COZY BEAR

Gruparea APT29, cunoscută și sub denumirile **Cozy Bear**, **Midnight Blizzard**, **The Dukes**, **Dark Halo** sau **NobleBaron**, este sponsorizată de Federația Rusă și este asociată cu **Serviciul de Informații Externe al Rusiei (SVR)**. Gruparea este implicată în operațiuni de spionaj cibernetic de lungă durată, vizând în special instituții guvernamentale, organizații internaționale și entități din domeniul cercetării și securității.

În paralel, evoluția peisajului malware a adus în prim-plan noi tipuri de software malițios, iar ingineria socială a rămas o metodă preferată de atac, cu un focus deosebit pe phishing și utilizarea tehnologiilor avansate, precum **Inteligența Artificială (AI) și Deepfake**. De asemenea, atacurile de tip vishing, care utilizează tehnologia phone spoofing, au înregistrat o creștere îngrijorătoare, iar compromiterea conturilor de social media, în special prin campanii ca ***Votează pe Adeline***, a devenit o practică tot mai răspândită.

Aceste tendințe subliniază necesitatea unei vigilențe sporite și a unor măsuri de protecție mai eficiente pentru a face față provocărilor tot mai complexe din domeniul securității cibernetice.

În cursul anului 2025 Directoratul a detectat și monitorizat, cu precădere, următoarele tipuri de atacuri:

- **Ransomware**: comparativ cu 2024, acest tip de atac a înregistrat o creștere de peste 153%, și a impactat 22 de instituții publice, 115 persoane fizice și 119 persoane juridice, ce au fost sprijinite de DNSC. Datele disponibile indică o diversificare a actorilor implicați și menținerea unui interes constant al grupărilor ransomware pentru organizațiile din România. Modelul operațional predominant rămâne cel de tip **Ransomware-as-a-Service (RaaS)**, caracterizat prin infrastructuri distribuite și afiliere

descentralizată. Totodată, atacurile de tip ransomware au înregistrat o creștere semnificativă, inclusiv în sectorul financiar-contabil, fiind asociate și cu o grupare de atacatori de origine română.

Tabel 1 - Principalele grupări ransomware monitorizate active în România și sectoarele vizate de atacuri în perioada 2023-2025

Nr.	Grupare	Localizare / Afinitate	Limbă	Sectoare afectate în România	Note
1.	**LockBit 3.0**	Federația Rusă (localizare declarată Olanda)	Engleză și Rusă	Transport/Logistică, Servicii Financiare, Servicii Juridice, Alimentar/Producție	Au fost confirmate 4 victime în România în anul 2023. Operațiunea a fost de tip takedown și s-a desfășurat în februarie 2024
2.	**RansomHub**	Aliniat Federației Ruse (origine neconfirmată)	Rusă	Administrație publică, Agricultură, Tehnologie, Producție industrială	Au fost confirmate 6 victime în România. Gruparea a fost cea mai activă la nivel global în anul 2024
3.	**KillSec**	Neconfirmat (posibil Federația Rusă)	Engleză și Rusă	Administrație publică (Poliție, Administrație), Transport urban	În perioada 2024-2025 au fost confirmate 5 victime în România
4.	**Benzona**	Neconfirmat	Necunoscut	Servicii auto (dealeri), Producție industrială	Au fost înregistrate 4 victime simultan în România, în noiembrie 2025. Gruparea este considerată emergentă
5.	**Akira**	Probabil Federația Rusă / CIS	Engleză	Producție industrială, Agricultură/Alimentar, Echipamente	În perioada 2024-2025 au fost confirmate 3 victime în România
6.	**Qilin**	Neconfirmat (posibil Federația Rusă)	Engleză	Alimentar, Agricultură, Producție	În perioada 2023-2025 au fost confirmate 2 victime în România
7.	**Safepay**	Neconfirmat	Engleză	Retail/Modă, Consumer Services, Tehnologie/IT	Au fost confirmate 3 victime în România în anul 2025
8.	**Fog**	Neconfirmat	Engleză	Educație, Tehnologie/Software	În România au fost confirmate 2 victime: UPB și Acqua Development
9.	**APT73**	Neconfirmat	Engleză	Tehnologie/Software, Servicii Auto	Au fost confirmate 2 victime în România în perioada 2024-2025
10.	**Lynx**	Neconfirmat (posibil Federația Rusă)	Engleză	Energie electrică (distribuție)	În februarie 2025 a fost confirmată o victimă în România - Electrica S.A. - sector critic

- **Aplicații software de tip infostealer**, preponderent: **pseudo-manuscrypt, vipersoftx și ramnit**. De asemenea, a fost observată și utilizarea unor aplicații software de tip **Remote Access Trojan (RAT)**, preponderent: **m0vy, toxicpanda și andromeda**. Tacticile de distribuție s-au menținut, atacatorii utilizând metode precum arhive protejate prin parolă, ceea ce implică dificultate crescută în detectare sau prevenire.
- **Ingineria socială**: atacurile de tip phishing reprezintă, în continuare, un vector preferat. Utilizarea IA pentru crearea de mesaje mai convingătoare și a tehnologiei Deepfake menține un nivel de complexitate ridicat, al atacurilor, acestea fiind tot mai dificil de detectat.
- **Atacuri de tip vishing, cu utilizarea tehnicilor preponderente de phone spoofing**: numărul atacurilor în care este folosită tehnologia de tip phone spoofing a înregistrat o creștere semnificativă, atât din punct de vedere al numărului de incidente cibernetice, cât și din punct de vedere al complexității modului de operare. Aceste atacuri au vizat în principal persoanele fizice prin impersonarea, atât a instituțiilor statului, cât și a instituțiilor bancare.
- **Compromiterea conturilor de social media:** acest tip de atac a înregistrat creșteri majore cauzate în principal de campaniile derulate sub denumirea ***Votează pe Adeline*** prin care se prelua accesul la conturile de WhatsApp ale victimelor, dar și de tradiționalele compromiteri ale conturilor Meta Platforms (Instagram, Facebook).

2.2 Atacuri și incidente cibernetice notabile

2.2.1 Situația de ansamblu a atacurilor și incidentelor raportate către Directorat

În cursul anului 2025 la nivelul Directoratului au fost raportate, investigate și analizate următoarele categorii principale de atacuri și incidente cibernetice:

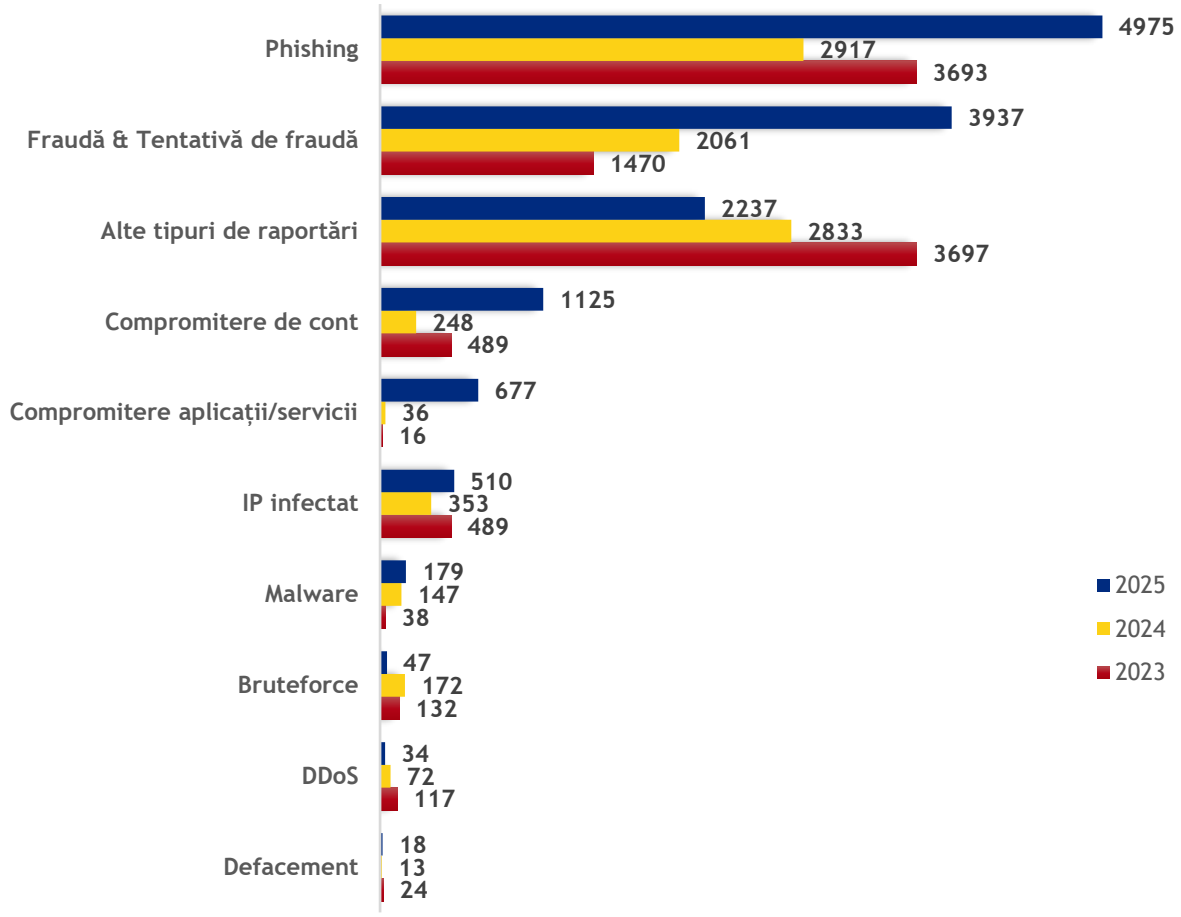


Figura 1 - Situația numerică comparativă a datelor 2023-2024-2025 pe tip de incident

Creșteri semnificative în 2025

Analiza comparativă a datelor aferente anilor 2024 și 2025 evidențiază creșteri relevante în categoriile de incidente cibernetice asociate identității digitale, fraudei și compromiterii serviciilor, indicând o schimbare clară a tacticilor utilizate de atacatori, de la atacuri volumetrice către atacuri țintite, cu impact direct asupra utilizatorilor și organizațiilor.

- **Phishing (+70,60%)**: Numărul incidentelor de tip phishing a crescut de la 2.917 (32,95% din total) în 2024 la 4.975 (36,09% din total) în 2025, consolidând această categorie drept principal vector de atac. Această creștere a fost determinată, în principal, de:
    - Profesionalizarea campaniilor de phishing, inclusiv utilizarea de mesaje redactate corect în limba română, cu elemente grafice ce reproduc fidel identitatea vizuală a entităților legitime.
    - Diversificarea canalelor de livrare prin combinarea emailului cu aplicații de mesagerie și platforme de social media.
    - Utilizarea phishing-ului ca etapă inițială în lanțuri de atac mai complexe, ce conduc ulterior la fraude sau la compromiterea conturilor de utilizator.
    - Utilizarea pe scară largă a mecanismelor de inteligență artificială precum și a pregătirii atacurilor cu ajutorul AI.

- **Fraude (+91%)**: Incidentele de fraudă și tentativă de fraudă au crescut de la 2.061 (23,28% din total) în 2024 la 3.937 (28,56% din total) în 2025, reprezentând una dintre cele mai consistente creșteri procentuale. Factorii principali care au contribuit la această evoluție includ:
  - Îmbunătățirea capacității de identificare și raportare, care conduce la o creștere a numărului de incidente documentate, inclusiv tentative nereușite.
  - Intensificarea atacurilor ce utilizează tehnici de spoofing telefonic.
  - Corelarea directă cu creșterea phishing-ului, fraudele fiind adesea rezultatul exploatării credențialelor sau informațiilor obținute în faza inițială.
  - Creșterea atractivității fraudelor financiare, în special în zone precum comerțul electronic, investițiile false și schemele de tip impersonare.
- **Compromitere de cont (+353%)**: Incidentele de compromitere a conturilor au înregistrat o creștere majoră, de la 248 (2,80% din total) în 2024 la 1.125 (8,16% din total) în 2025, indicând o schimbare strategică majoră în modul de operare al atacatorilor. Această categorie reprezintă un risc critic, întrucât compromiterea unui cont poate facilita accesul la date sensibile, propagarea atacurilor și escaladarea privilegiilor. Evoluția poate fi explicată prin:
  - O parte relevantă a acestor incidente a fost generată de campanii de inginerie socială, desfășurate prin intermediul aplicațiilor de mesagerie, în special WhatsApp, care au vizat preluarea conturilor utilizatorilor prin mesaje de tipul ***voteaz-o pe fiica mea la concurs***, urmate de redirecționarea victimei către pagini frauduloase sau solicitarea introducerii unor coduri de autentificare.
  - Reutilizarea parolelor și exploatarea bazelor de date cu credențiale compromise anterior.
  - Lipsa sau configurarea deficitară a autentificării multifactor (MFA) pentru conturile personale și organizaționale.
  - Creșterea atacurilor de tip ***credential stuffing***, care permit accesarea conturilor fără exploatarea unor vulnerabilități tehnice propriu-zise.

Scăderi semnificative în 2025

Datele DNSC indică și scăderi notabile pentru anumite categorii de incidente, în special cele asociate atacurilor volumetrice sau oportuniste, ceea ce sugerează o îmbunătățire a măsurilor de protecție implementate la nivel național.

- **Bruteforce (-72,7%)**: Incidentele de tip bruteforce au scăzut de la 172 (1,94% din total) în 2024 la 47 (0,34% din total) în 2025. Această scădere poate fi atribuită:
  - Implementării diverselor mecanisme de protecție, precum rate-limiting și CAPTCHA.
  - Scăderii atractivității acestui tip de atac, în contextul în care atacatorii obțin rezultate mai rapide și mai eficiente prin compromiterea credențialelor existente.
- **DDoS (-52,8%)**: Numărul incidentelor DDoS a scăzut de la 72 (0,81% din total) în 2024 la 34 (0,25% din total) în 2025. Această tendință reflectă:
  - Îmbunătățirea protecțiilor la nivel de rețea, inclusiv utilizarea serviciilor de protecție DDoS oferite de furnizori specializați.
  - Reorientarea atacatorilor către metode cu impact financiar și operațional mai mare.
- **Alte tipuri de raportări (-21%)**: Categoria a scăzut de la 2.833 (32,00% din total) în 2024 la 2.237 (16,23% din total) în 2025. Această scădere este interpretată ca:
  - Un semn de maturizare a procesului de raportare, incidentele fiind clasificate mai precis în categoriile consacrate.
  - Reducerea raportărilor generice sau neclare, ca urmare a standardizării procedurilor și a unei mai bune înțelegeri a tipologiilor de incidente.

În vederea creșterii capacității de analiză și valorificare a datelor operaționale disponibile la nivelul DNSC, **a fost dezvoltată și implementată, prin resurse proprii, o aplicație statistică dedicată,** prin intermediul căreia datele brute colectate din activitatea curentă au fost transformate în informații structurate, relevante și ușor de utilizat de către utilizatorul standard.

Această abordare permite fundamentarea de statistici detaliate, identificarea de trenduri și tipare recurente, precum și sprijinirea procesului decizional și elaborarea de strategii operaționale, contribuind astfel la creșterea nivelului de predictibilitate, eficiență și maturitate analitică la nivelul DNSC:

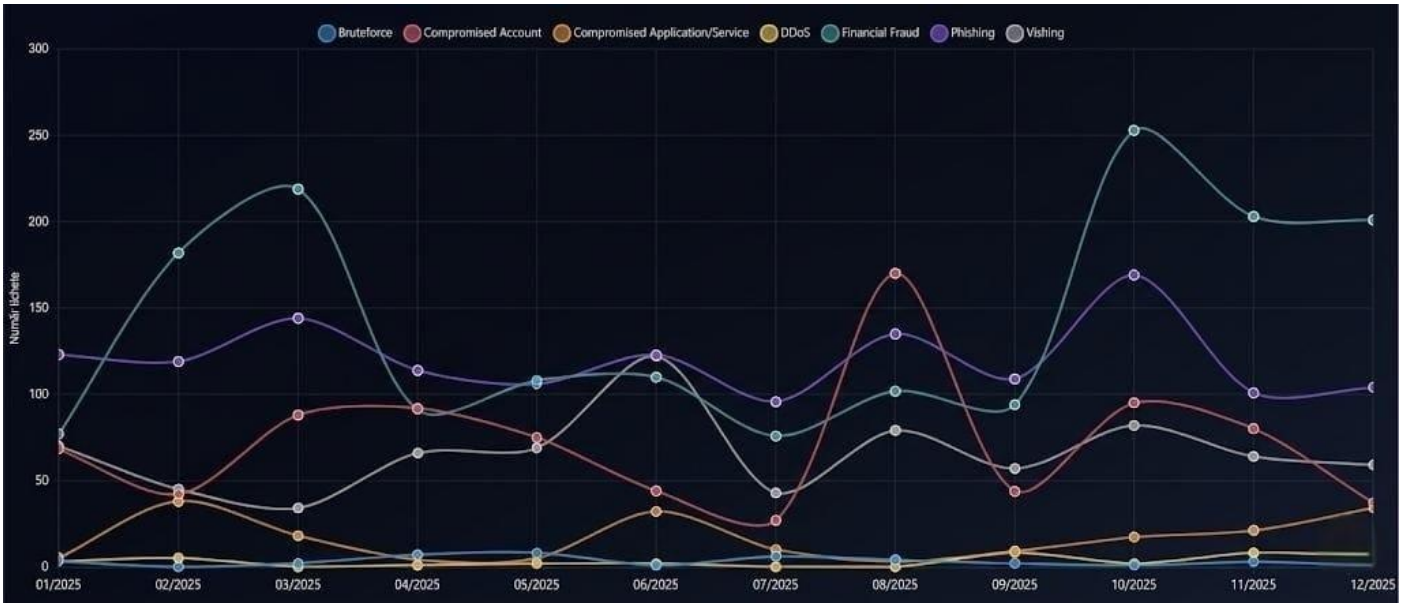


Figura 2 - Evoluția principalelor categorii de incidente cibernetice înregistrate în anul 2025

Nu au fost identificate corelații directe între volumul atacurilor și evenimente specifice naționale sau la nivel european.

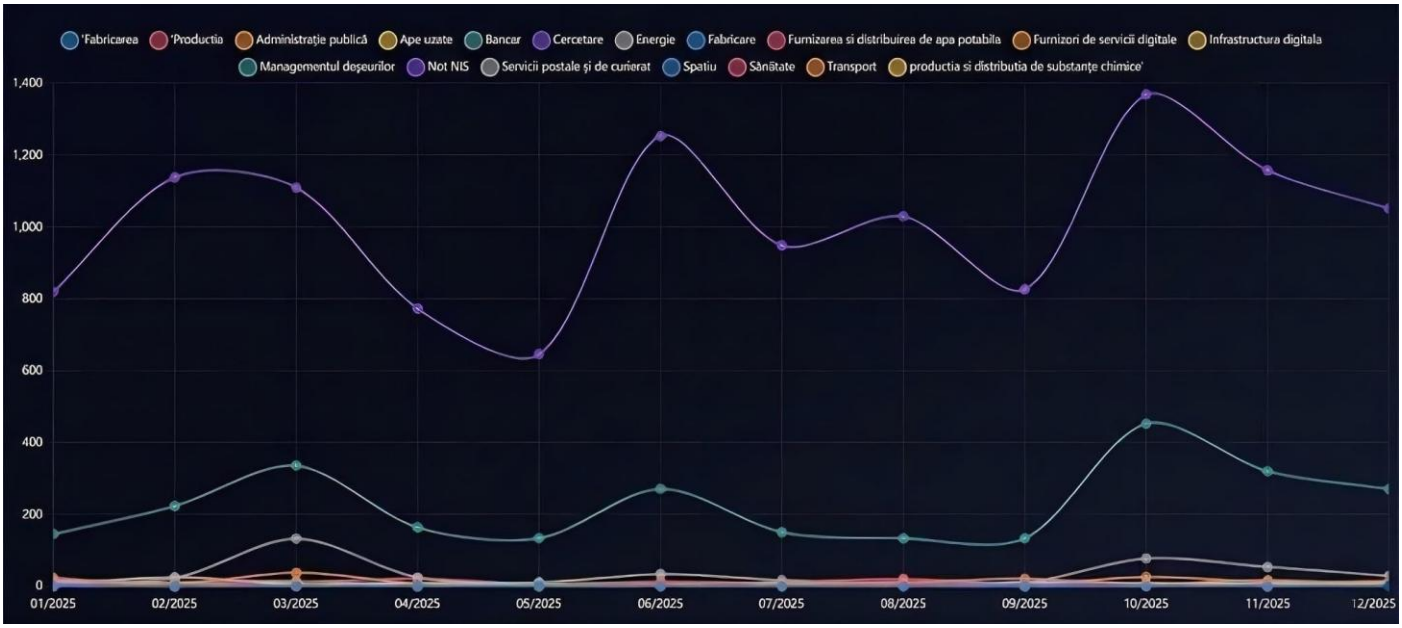


Figura 3 - Evoluția incidentelor înregistrate în anul 2025 defalcate pe sectorul NIS vizat

Din punct de vedere al incidentelor raportate în funcție de sectorul de activitate, anul 2025 a evidențiat o concentrare semnificativă asupra anumitor domenii critice.

Sectorul bancar, serviciile poștale și de curierat, precum și infrastructurile pieței financiare au fost cele mai vizate, cumulând 3.326 incidente – respectiv 88,23% din totalul raportărilor.

2.2.2 Evenimente de securitate cibernetică detectate de senzorii Directoratului

De asemenea, în 2025 au fost înregistrate **25.033.446** de evenimente de securitate cibernetică relevante, extrase din senzorii de detecție instalați/configurați de către DNSC, defalcate după cum urmează:

Tabel 2 - Situația evenimentelor colectate de senzorii DNSC în 2023-2024-2025

Eveniment	2023	2024	2025	Trend 2025 vs. 2024
Evenimente de securitate cibernetică cu sursă rețele de botnet	828.877	1.880.886	241.721	↘↘↘
Scanări ce urmăresc colectarea de informații	11.234.472	6.549.076	5.315.696	↘
Evenimente legate de trafic provenind de la adrese IP cu reputație îndoielnică	1.000.781	860.790	1.034.700	↗
Încercări de penetrare a infrastructurilor prin exploatarea unor vulnerabilități	30.620	14.590	292.117	↗↗↗
Evenimente legate de volume de trafic nejustificate cu scopul identificării vulnerabilităților și colectării de informații	7.885.887	6.170.245	4.282.152	↘
Încercări de penetrare a infrastructurilor prin campanii de tip phishing	8.405.259	941.076	7.251.708	↗↗↗
Încercări de penetrare a infrastructurilor prin atacuri de tip brute force	20.385.302	7.960.959	5.879.193	↘
Software malițios - malware	491.364	284.888	267.867	↘
Posibile atacuri DDoS prin cereri DNS suspecte	1.530.805	904.831	741.874	↘
Total	**51.793.367**	**25.567.341**	**25.307.028**	→

Această evoluție reflectă atât optimizarea mecanismelor de detecție și filtrare a alertelor în prima parte a anului 2025, cât și intensificarea activităților malițioase în a doua parte a anului, incluzând atacuri automatizate, campanii coordonate și utilizarea unor vectori de atac mai sofisticați, capabili să genereze un volum ridicat de alerte din partea senzorilor.

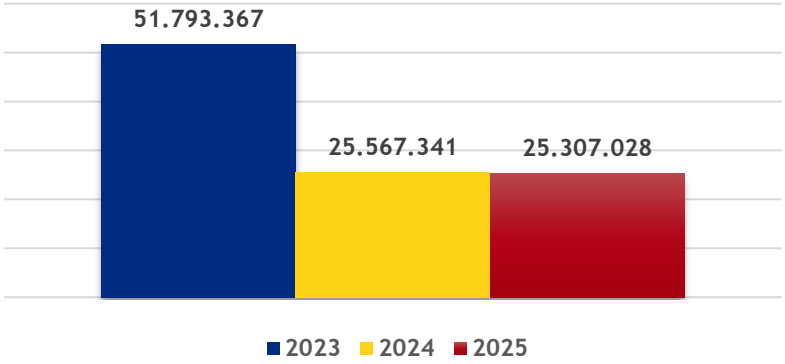


Figura 4 - Total evenimente colectate de senzorii DNSC

În ansamblu, datele evidențiază o schimbare în distribuția temporală a amenințărilor cibernetice, cu o concentrare mai pronunțată a acestora în ultima parte a anului 2025, subliniind necesitatea menținerii unui nivel ridicat de vigilență operațională și a adaptării continue a capacităților de detecție și răspuns.

De asemenea, în anul 2025, DNSC a colectat și soluționat alerte de securitate cibernetică provenite din mai multe surse, respectiv: raportările cetățenilor și organizațiilor (din sectorul public sau privat) transmise prin **Platforma Națională pentru Raportarea Incidentelor de Securitate Cibernetică (PNRISC)**, sesizările primite prin numărul unic național de urgență cibernetică 1911, datele furnizate de senzorii

instalați și configurați în infrastructurile IT&C naționale, activitățile de monitorizare a darknetului, precum și cooperarea cu parteneri instituționali naționali și internaționali.

2.2.3 Situația incidentelor gestionate la nivelul Directoratului în 2025 pe sector economic

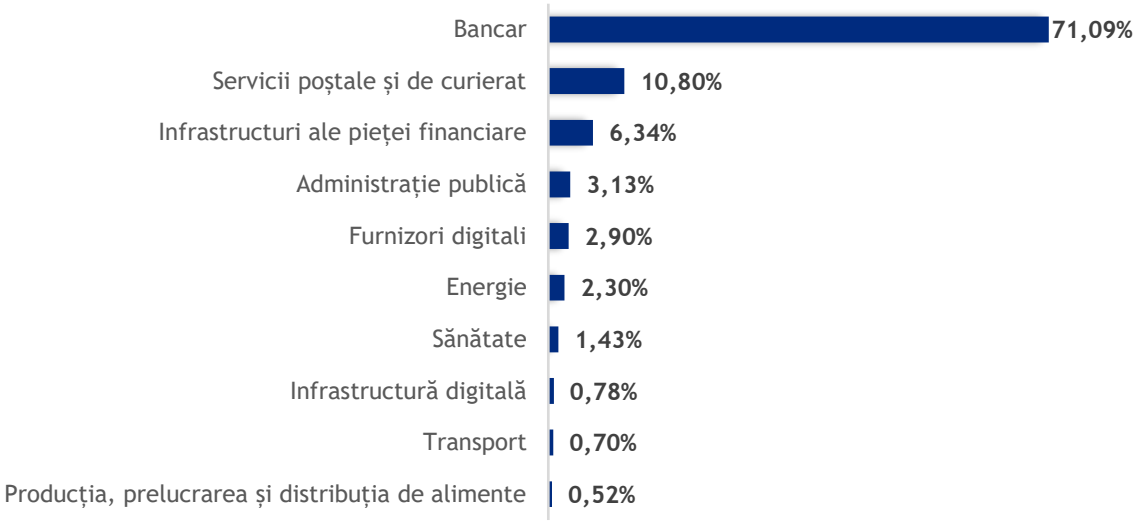


Figura 5 – Procent incidente cibernetice raportate către DNSC în funcție de sector

Sectorul bancar a fost (procentual) cel mai afectat, majoritatea incidentelor fiind de **tip phishing** și vizând în general utilizatorii serviciilor financiar-bancare.

Serviciile poștale și de curierat a fost al doilea sector ca număr de incidente, predominând, de asemenea, atacurile de tip phishing.

Sectorul energetic a înregistrat incidente mai puține, dar relevante din punct de vedere al impactului.

Sectorul sănătății a fost vizat și el de o serie de incidente de securitate, dintre care cele mai relevante au implicat atacuri de tip ransomware și SQL Injection. În afară de acestea, sectorul sănătății a fost vizat și de alte incidente cu impact mai redus, care au fost gestionate conform procedurilor standard de securitate cibernetică.

În ceea ce privește natura tehnică a incidentelor, pe lângă phishing și ransomware, s-au înregistrat atacuri de tip DDoS cu impact asupra unor entități din sectoarele bancar și transporturi, precum și identificarea de vulnerabilități și credențiale expuse, în special în sectorul sănătății, pentru care DNSC a transmis măsuri și recomandări concrete de remediere către 129 de organizații.

Aceste incidente evidențiază importanța unei monitorizări continue, a implementării măsurilor de securitate proactivă și a colaborării între autorități și operatorii de infrastructură critică, pentru reducerea riscurilor și protecția utilizatorilor finali.

2.2.4 Situația incidentelor de tip ransomware gestionate la nivelul Directoratului în 2025

Fenomenul ransomware este unul dintre cele mai persistente și grave. În cursul anului 2025, DNSC a detectat și gestionat 256 de incidente majore, remarcându-se, sub aspectul impactului generat, al datelor și al infrastructurii vizate, următoarele atacuri relevante:

- **Atac cibernetic de tip ransomware**, efectuat de gruparea Akira, care a vizat societatea Aaylex ONE SA (CocoRico), ce reprezintă grupul integrat din industria alimentară, cu peste 2.000 angajați și activitate în 36 de locații, din 9 județe din România, care include fluxul complet de producție a produselor din carne de pui, și care a afectat servicii critice precum contabilitate, producție, operațiuni, servere de fișiere. Atacul a fost inițiat, cel mai probabil, prin exploatarea vulnerabilității CVE-2020-3259, care afectează interfața de servicii web a aplicațiilor Cisco Adaptive Security Appliance (ASA) și Cisco Firepower Threat Defense (FTD). Specialiștii DNSC au întocmit un raport tehnic detaliat de investigații digitale, în baza artefactelor disponibile, și au reușit recuperarea a peste 66% din

fișierele criptate, printre care s-au regăsit baze de date critice, necesare pentru continuitatea serviciilor operaționale.

- **Atac cibernetic de tip ransomware la nivelul Primăriei Municipiului București (PMB),** vectorul de atac fiind o vulnerabilitate de tip SQL injection, concretizat prin exploatarea serverului GIS expus public și a bazei de date specifică acestuia. Atacatorii au reușit să facă mișcare laterală și astfel au ajuns în serverul de Active Directory al organizației și au creat un cont de administrator, asigurându-și persistența. Acest cont a fost utilizat ulterior pentru accesarea serverului Microsoft Exchange și implantarea Sliver.exe, utilitar folosit de obicei pentru exfiltrare. Specialiștii DNSC au identificat programul malițios, l-au eliminat și au fost oferite, prin intermediul unui raport tehnic, recomandări cu privire la securizarea sistemelor și a adreselor de email.
- **Atac cibernetic de tip ransomware la nivelul Institutului Național de Cercetare-Dezvoltare pentru Ecologie Industrială (INCD ECOIND)**, atacatorii folosind tehnici avansate de infiltrare și persistență, care le-au permis accesul în rețeaua internă și extinderea rapidă către alte sisteme din infrastructură. Specialiștii DNSC au sprijinit specialiștii din cadrul INCD ECOIND, în scopul izolării și colectării probelor digitale, precum și restaurării serverelor afectate, folosind copii de siguranță disponibile.
- **Atac de tip ransomware care a vizat Administrația Națională Apele Române (ANAR).** În urma atacului, aproape întreaga activitate a instituției a fost blocată, inclusiv cea a structurilor teritoriale, instituția aflându-se în imposibilitatea de a-și desfășura activitatea pentru o perioadă de aproximativ o săptămână. Prin intervenția sa, DNSC a reușit recuperarea integrală a datelor aflate pe un server al ABA Jiu, precum și a bazei de date SQL – Hidrolog, utilizată de dispeceri. Activitatea de analiză de tip ***digital forensics*** a incidentului și a artefactelor colectate a fost documentată într-un raport.
- **Atac de tip ransomware asupra Junior Group SRL - Constanța.** În urma sesizării incidentului, la sediul societății din mun. Constanța, jud. Constanța, s-a deplasat o echipă DNSC care a colectat date de la un număr de 3 servere afectate, fiind ulterior supuse unei analize de tip forensics din care au rezultat artefacte ce au condus la concluzia că atacatorii sunt gruparea LockBit. Datele criptate nu au putut fi recuperate. De asemenea, s-a mai stabilit că societatea atacată utiliza anterior atacului programe software piratate, dintre care menționăm Windows Server, ESET NOD 32, aspecte ce au facilitat accesul atacatorilor în infrastructură.
- Compania **Energobit SA** a raportat un incident de tip ransomware asupra unui sistem de tip Domain Controller, utilizat drept punct central pentru mișcări laterale în rețea. Accesul neautorizat a permis conexiuni la distanță către stații de lucru și servere prin PowerShell, WinRM și sesiuni RDP, iar atacatorii au efectuat mai întâi două valuri de atacuri brute-force asupra conturilor pentru a obține acces. În cadrul acestui incident, au fost identificate artefacte asociate suitei Jetico BestCypt, utilizată pentru criptarea sau mascarea activităților malițioase. Acțiunile de răspuns au permis izolarea sistemelor afectate și limitarea impactului asupra operațiunilor.
- **Complexul Energetic Oltenia (CEO)** a raportat un incident ransomware care a afectat parțial infrastructura IT internă. Incidentul a fost izolat, iar măsurile de remediere au inclus restaurarea sistemelor din copii de siguranță, reinstalarea dispozitivelor afectate, resetarea parolelor și aplicarea actualizărilor de securitate. Atacatorii nu au fost contactați și nu a fost efectuată nicio plată de răscumpărare. În urma incidentului, aproximativ 20 de stații de lucru și 45 de servere au fost afectate, fără impact asupra rețelei operaționale sau prejudicii financiare semnificative, iar activitatea de producție nu a fost perturbată. Organizația a planificat implementarea autentificării multifactor (MFA), îmbunătățirea filtrării mesajelor e-mail, monitorizare continuă prin SOC și audit de securitate pentru prevenirea incidentelor viitoare.
- Compania **DASCO GRUP SRL,** care are ca obiect de activitate lucrări de instalații electrice, a raportat criptarea unui dispozitiv al companiei cu BitLocker, ca urmare a accesării unui fișier atașat unui e-mail malițios primit de la un presupus membru CECCAR. Atacatorul a solicitat o răscumpărare inițială de 12.000 LEI, majorată ulterior la 15.000 LEI, însă compania nu a efectuat plata, restabilind sistemul de operare și datele dintr-un backup realizat cu aproximativ două luni înainte. Recomandările transmise pentru prevenirea unor incidente similare au vizat activarea autentificării multifactor (MFA), limitarea

utilizării conturilor cu privilegii administrative, adoptarea unor soluții de securitate adecvate și instruirea periodică a personalului în recunoașterea tentativelor de phishing.

- **Centrele de transfuzie sanguină Maramureș și respectiv Craiova** au fost compromise prin atacuri Lockbit 4.0, accesul inițial fiind realizat prin brute-force asupra conexiunilor VPN externe, ceea ce a condus la criptarea completă a fișierelor.

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.

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.

Cooperarea internațională în acest domeniu se face atât prin **Inițiativa de Combatere a Ransomware (Counter Ransomware Initiative - CRI)**, propusă de Statele Unite ale Americii, cât și printr-o serie de inițiative ale Uniunii Europene și Europol. Directoratul este una dintre entitățile responsabile pentru combaterea atacurilor cibernetice de tip ransomware și derulează constant inițiative menite să ajute victimele acestor tipuri de atacuri sau să prevină derularea de campanii ransomware.

2.2.5 Alte evoluții și activități relevante

În anul 2025, **DNSC a intervenit în mod activ și a gestionat mai multe incidente majore**, remarcându-se, sub aspectul impactului generat, al datelor compromise și al infrastructurilor vizate, următoarele atacuri:

- **Atac de tip infostealer la nivelul societății Tohan SA - parte din grupul industrial ROMARM**, ce activează în producția de armament, muniție și echipamente pentru sectorul militar, având un număr de 375 angajați. Atacul a constat în compromiterea adreselor de email office@tohan.ro și achizitii@tohan.ro. Atacatorii au reușit să configureze redirecționări ale email-urilor, facilitând astfel atacuri de tip **Man-In-The-Middle (MitM)**. Acest lucru le-a permis să modifice documente în cadrul conversațiilor de email, conducând la efectuarea unor transferuri bancare neautorizate, în valoare totală de 20.148 euro, de la victimă către atacatori. În urma analizei datelor colectate, DNSC a identificat numeroase programe malițioase de tip spyware/infostealer și au fost oferite recomandări cu privire la securizarea sistemelor și adreselor email, fiind întocmit un raport tehnic în acest sens.
- **Atac de tip implementare webshell care a vizat aplicația web a Autorității de Supraveghere Financiară (ASF),** afectând confidențialitatea și integritatea serverului găzduitor. DNSC a identificat faptul că accesul a fost efectuat prin exploatarea componentei Symfony Profiler, prin intermediul căreia au putut fi extrase date cu privire la numele contului și parola administratorului, în text clar, cât și date referitoare la cookies și sesiuni. A fost întocmit un raport tehnic de investigații digitale, în baza artefactelor disponibile și au fost înaintate recomandările de securitate cibernetică necesare.
- **Atac cibernetic ce a vizat infrastructura IT&C a SC Informatică Feroviară SA,** respectiv pe trei stații aflate în punctele de lucru din Gurahonț, Ineu și Sebiș, toate din județul Arad. Au fost identificați indicatori ai unui acces provenind de la mai multe adrese IP neautorizate, fără a fi afectată disponibilitatea serviciilor.
- **Atac de tip phishing la nivelul CN ROMARM** prin care au fost distribuite programe malițioase. Din datele prezentate inițial în rețeaua locală au fost identificate două stații de lucru suspecte de a fi infectate cu un malware de tip RAT (Remote Access Trojan). În urma sesizării incidentului, la sediul din București al societății, s-a deplasat o echipă DNSC care a efectuat două clone bit-by-bit ale mediilor de stocare din stațiile de lucru pe care s-a executat fișierul malițios. Din analiza de tip ***digital forensics*** efectuată pe artefactele colectate a rezultat că malware-ul final a fost un Remcos RAT. Din acest incident nu au rezultat pierderi sau date criptate.
- **Blind SQL Injection, la nivelul Spitalului Județean Clinic de Urgență Sf. Apostol Andrei din Constanța,** atac care a vizat serverului pentru programări online și a permis maparea bazei de date fără extragerea de informații concrete, vectorul de atac fiind lipsa verificării și curățării inputului în formularele web. Pentru aceste incidente, DNSC a transmis recomandări pentru prevenirea unor situații

similare, printre care utilizarea query-urilor parametrizate și aplicarea principiilor de zero trust asupra tuturor datelor clientului.

- Unul dintre incidentele notabile ce a fost raportat a implicat activități malițioase de tip scanare automatizată asupra unei aplicații web ce aparține **Poștei Române**. Atacatorii au generat un volum ridicat de cereri automate, utilizând instrumente de tip scaner/spider, pentru a identifica vulnerabilități precum SQL Injection (inclusiv blind SQLi), path traversal, Local File Inclusion (LFI), Remote Code Execution și Server-Side Request Forgery. Analiza jurnalelor de acces nu a indicat compromiterea aplicației sau divulgarea datelor sensibile, însă amploarea și diversitatea tehnicilor utilizate au evidențiat un nivel ridicat de risc, subliniind necesitatea monitorizării continue și a aplicării stricte a politicilor de securitate.
- Incidentul sesizat de **Autoritatea de Supraveghere Financiară (ASF)** cu privire la compromiterea site-ului web prin YANZ Webshell, vectorul de atac fiind inițial un cont de administrare al unei companii terțe. Persistența atacatorului a fost asigurată prin aproximativ 800 de fișiere .php dispersate în întreaga structură a site-ului ASF. Ulterior, website-ul a fost curățat de fișierele malițioase și restaurat.
- Un alt incident a vizat o instituție de credit, care a raportat crearea unui domeniu malițios similar cu domeniul oficial, utilizat într-o campanie de phishing. Mesajele au fost detectate de mecanismele de securitate, fără compromiterea sistemelor interne, iar domeniul fraudulos a fost rapid dezactivat.
- **Spoofing-ul telefonic**: este una dintre cele mai utilizate tehnici în atacurile de tip inginerie socială și constă în falsificarea numărului de telefon afișat destinatarului pentru a copia/clona numere de telefon 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.

  Modul de operare este unul hibrid, care combină vishing-ul cu ingineria socială prin impersonarea autorităților și a instituțiilor financiare, utilizarea de canale digitale (e-mail cu documente false) și mecanisme de plată greu de recuperat (transferuri prin cod QR către portofele de criptomonede accesate prin terminale ATM).
- **Analiza campaniilor de phishing** a evidențiat un nivel ridicat de organizare și automatizare, fiind identificate elemente care pot indica utilizarea unor ecosisteme avansate de tip **Phishing-as-a-Service**, deși această ipoteză nu poate fi confirmată cu certitudine pe baza datelor disponibile.
    - Au fost observate domenii de tip ***typosquatting*** atent alese pentru a imita domeniile legitime ale entităților vizate, precum și mecanisme de camuflare a conținutului malițios, livrat sub forma unor secvențe de date codate și activat doar în momentul îndeplinirii unor condiții specifice, precum locația geografică, tipul de dispozitiv sau parametrii de tip user-agent.
    - Din analiza comportamentului acestor mecanisme au rezultat indicii privind existența unui panou de control centralizat, utilizat pentru monitorizarea în timp real a interacțiunilor și pentru restricționarea accesului anumitor adrese IP sau categorii de utilizatori, în scopul evitării activităților de analiză. De asemenea, a fost observată transmiterea în timp real a datelor introduse de utilizatori, fără a fi necesară finalizarea completă a formularelor, ceea ce permite compromiterea informațiilor chiar și în situațiile în care procesul este abandonat.
    - În intervalul de timp de referință, DNSC a observat o intensificare a atacurilor cibernetice care au vizat în mod specific firmele și angajații din domeniul serviciilor de contabilitate. 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 companiile din acest sector.

      Pentru a face față acestei provocări, **DNSC a transmis 1.799 informări specifice** către companii de servicii de contabilitate, cu recomandări concrete și măsuri tehnice specifice necesar a fi implementate pentru a evita astfel de incidente.

- Totodată, DNSC a investigat și analizat în anul 2025 peste 40 de medii de stocare, **totalizând un volum de peste 35 TB de date**, în scopul identificării și procesării de mostre de malware. Activitatea a vizat înțelegerea comportamentului acestora, a metodelor de propagare și a vectorilor de atac utilizați.

  Pe baza rezultatelor obținute, au fost elaborate și implementate măsuri de protecție**, inclusiv reguli YARA**, și au fost distribuiți Indicatori de Compromitere (IOC) prin platforma MISP către organizațiile relevante. Aceste activități au contribuit la creșterea capacității instituționale de apărare proactivă, la consolidarea mecanismelor de detecție și la reducerea riscurilor asociate incidentelor cibernetice pentru infrastructurile critice, facilitând schimbul de bune practici și cooperarea interinstituțională.

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

2.2.6 Activități tehnice pro-active

În 2025, Directoratul a efectuat, la cerere, și o serie de **activități tehnice pro-active de tip penetration testing**, pentru verificarea și îmbunătățirea securității cibernetice, după cum urmează:

- **La Primăria Sectorului 5 București** DNSC a efectuat o evaluare a posturii de securitate cibernetică, în urma căreia au fost identificate mai multe deficiențe de securitate în infrastructura informatică internă. Au fost transmise un raport tehnic și recomandările aferente.
- **La Institutul Național de Sănătate Publică (INSP)** a fost efectuată o evaluare a posturii de securitate cibernetică de către specialiști din cadrul DNSC, în urma căreia au fost identificate deficiențe de securitate în infrastructura informatică externă, respectiv asupra **aplicației web a Registrului Electronic Național de Vaccinări.** Au fost transmise raportul tehnic și recomandările aferente.
- **La Secretariatul General al Guvernului (SGG)** a fost efectuată o evaluare de securitate cibernetică a aplicației https://te-comunicare.gov.ro, în urma căreia au fost evidențiate o serie de vulnerabilități și probleme de funcționalitate cu impact asupra confidențialității, integrității și disponibilității datelor. Testarea a fost realizată folosind conturi corespunzătoare rolurilor Administrator Instituții, Funcționar, Superadmin și Cetățean, ceea ce a permis o verificare completă a mecanismelor de autentificare, autorizare și gestionare a accesului.

Suplimentar Directoratul a dezvoltat și a implementat un mecanism tehnic de **monitorizare continuă a resurselor web de importanță la nivel național pentru 111 entități din România.** Prin intermediul acestuia, entitățile sunt monitorizate, iar **25 dintre ele au fost notificate în timp real** în legătură cu problemele identificate la site-urile web ale acestora.

În cadrul acestui mecanism, entităților li s-au furnizat recomandări privind modul de identificare a posibilelor incidente de securitate cibernetică, precum și pașii de remediere pentru limitarea impactului.

Această abordare proactivă a contribuit la creșterea rezilienței infrastructurii critice, la reducerea timpilor de reacție și la consolidarea nivelului de conștientizare și maturitate cibernetică al organizațiilor vizate.

2.2.7 Operaționalizarea de capabilități tehnice cu instituțiile naționale competente - protocol de cooperare între DNSC – PICCJ – IGPR – ANCOM – ICI

Pentru îndeplinirea funcției de cooperare prevăzută de OUG nr. 104/2021, Directoratul a încheiat un protocol de cooperare împreună cu **Parchetul de pe lângă Înalta Curte de Casație și Justiție (PÎCCJ), Inspectoratul General al Poliției Române (IGPR), Autoritatea Națională pentru Administrare și Reglementare în Comunicații (ANCOM) precum și cu Institutul Național de Cercetare-Dezvoltare în Informatică (ICI București).**

Protocolul are ca obiect principal cooperarea în realizarea atribuțiilor legale care le revin părților, în materie de prevenire și de combatere a criminalității informatice, inclusiv a atacurilor împotriva sistemelor informatice, derulată în scopul creării unui cadru formal, necesar pentru asumarea implementării unor măsuri de prevenire și de răspuns la atacurile informatice și de îmbunătățire a securității sistemelor informatice.

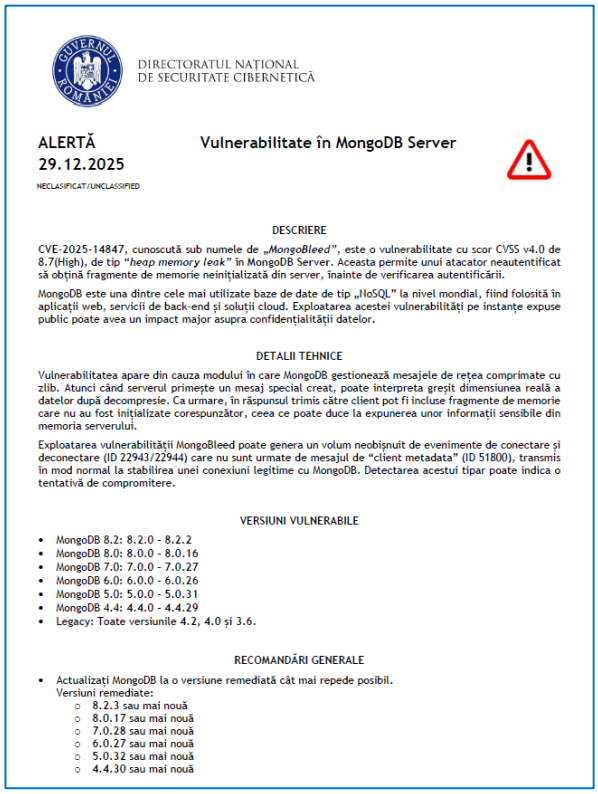
2.3 Vulnerabilități critice și riscuri de securitate cibernetică

În exercitarea rolului său de autoritate competentă la nivel național pentru spațiul cibernetic național civil, Directoratul efectuează multiple acțiuni și activități tehnice specifice de identificare a vulnerabilităților critice ale infrastructurilor. DNSC monitorizează în mod constant evoluțiile, alertele și datele tehnice publicate în cadrul programului **Common Vulnerabilities and Exposures (CVE)** derulat de către **MITRE Corporation** și de către **Cybersecurity and Infrastructure Security Agency (CISA)** din Statele Unite ale Americii și transmite informări și alerte către entitățile impactate din România.

În același timp, DNSC are în vedere și mecanismele tehnice promovate de către **Agenția Uniunii Europene pentru Securitate Cibernetică (ENISA)** privind **Coordinated Vulnerability Disclosure (CVD)**, care completează ecosistemul CVE printr-un cadru structurat de raportare și gestionare responsabilă a vulnerabilităților. Interacțiunea dintre programul CVE (standardizarea și identificarea vulnerabilităților) și mecanismele CVD (raportarea și coordonarea remedierii) este esențială pentru consolidarea rezilienței cibernetice a României și a Uniunii Europene, iar DNSC urmărește activ aceste două programe pentru a asigura alinierea la bunele practici internaționale și europene.

La nivelul anului 2025, **DNSC a monitorizat un număr de 317.000 de înregistrări disponibile prin intermediul programului CVE**, iar identificarea și gestionarea vulnerabilităților critice a reprezentat un element central de activitate al Directoratului, pentru protejarea infrastructurilor naționale, din punct de vedere al securității cibernetice.

Cu titlu de măsură proactivă, în 2025 DNSC **a informat un total de 2.020 de instituții publice și operatori de servicii esențiale cu privire la peste 43.000 de vulnerabilități exploatabile identificate asupra infrastructurii IT&C expuse public** și privind **scurgeri de date confidențiale sau sensibile,** care au fost diseminate de către atacatori prin diverse canale de comunicare, inclusiv platforme populare de comunicare precum Telegram, WhatsApp, Signal, Threema 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.



DIRECTORATUL NAȚIONAL DE SECURITATE CIBERNETICĂ

ALERTĂ 29.12.2025

Vulnerabilitate în MongoDB Server

NECLASIFICAT/UNCLASSIFIED

DESCRIERE

CVE-2025-14847, cunoscută sub numele de *„MongoBleed”*, este o vulnerabilitate cu scor CVSS v4.0 de 8.7(High), de tip *“heap memory leak”* în MongoDB Server. Aceasta permite unui atacator neautentificat să obțină fragmente de memorie neinițializată din server, înainte de verificarea autentificării.

MongoDB este una dintre cele mai utilizate baze de date de tip „NoSQL” la nivel mondial, fiind folosită în aplicații web, servicii de back-end și soluții cloud. Exploatarea acestei vulnerabilități pe instanțe expuse public poate avea un impact major asupra confidențialității datelor.

DETALII TEHNICE

Vulnerabilitatea apare din cauza modului în care MongoDB gestionează mesajele de rețea comprimate cu zlib. Atunci când serverul primește un mesaj special creat, poate interpreta greșit dimensiunea reală a datelor după decompresie. Ca urmare, în răspunsul trimis către client pot fi incluse fragmente de memorie care nu au fost inițializate corespunzător, ceea ce poate duce la expunerea unor informații sensibile din memoria serverului.

Exploatarea vulnerabilității MongoBleed poate genera un volum neobișnuit de evenimente de conectare și deconectare (ID 22943/22944) care nu sunt urmate de mesajul de “client metadata” (ID 51800), transmis în mod normal la stabilirea unei conexiuni legitime cu MongoDB. Detectarea acestui tipar poate indica o tentativă de compromitere.

VERSIUNI VULNERABILE

- MongoDB 8.2: 8.2.0 - 8.2.2
- MongoDB 8.0: 8.0.0 - 8.0.16
- MongoDB 7.0: 7.0.0 - 7.0.27
- MongoDB 6.0: 6.0.0 - 6.0.26
- MongoDB 5.0: 5.0.0 - 5.0.31
- MongoDB 4.4: 4.4.0 - 4.4.29
- Legacy: Toate versiunile 4.2, 4.0 și 3.6.

RECOMANDĂRI GENERALE

- Actualizați MongoDB la o versiune remediată cât mai repede posibil.
  Versiuni remediate:
  - 8.2.3 sau mai nouă
  - 8.0.17 sau mai nouă
  - 7.0.28 sau mai nouă
  - 6.0.27 sau mai nouă
  - 5.0.32 sau mai nouă
  - 4.4.30 sau mai nouă

În anul 2025 au fost elaborate și publicate **43 de alerte și buletine de informare** pe platforma www.dnsc.ro având ca obiect vulnerabilități cunoscute cu potențial impact semnificativ asupra infrastructurilor informatice. Aceste materiale au avut rolul de a informa și îndruma organizațiile vizate în ceea ce privește riscurile asociate, oferind recomandări și măsuri clare, aplicabile pentru prevenirea și remedierea acestora. Diseminarea buletinelor a contribuit la creșterea nivelului de conștientizare, la consolidarea capacității de răspuns proactiv la amenințările cibernetice și la uniformizarea practicilor de securitate la nivelul ecosistemului național.

În cadrul activităților continue de monitorizare, evaluare și analiză a amenințărilor cibernetice efectuate de către Directorat, au fost analizate în detaliu **121 de vulnerabilități CVE, imediat după ce acestea au fost publicate**, toate fiind încadrate în categorii de **severitate ridicată sau critică**. Acest demers a permis limitarea timpurie a riscurilor cu potențial semnificativ de impact asupra sistemelor informatice, facilitând adoptarea măsurilor preventive necesare și contribuind în mod direct la reducerea expunerii infrastructurilor și a serviciilor esențiale la nivel național.

Ca rezultat al acestor analize, **Directoratul a emis și transmis 253 de informări către entitățile relevante** din sectorul public și privat. Această activitate a asigurat diseminarea rapidă și structurată a informațiilor privind vulnerabilitățile identificate, a sprijinit un răspuns coordonat și eficient la nivel organizațional și

a contribuit la aplicarea unitară a măsurilor de securitate, limitând riscul de exploatare și prevenind escaladarea incidentelor cibernetice.

De asemenea, **Directoratul a** identificat un număr de **734 de adrese IP vulnerabile sau caracterizate printr-un nivel de risc foarte ridicat**. Notificarea promptă a entităților afectate și, după caz, a furnizorilor de servicii de hosting a permis inițierea în timp util a acțiunilor de remediere, conducând la diminuarea suprafeței de atac, la creșterea nivelului general de reziliență cibernetică și la consolidarea securității și stabilității ecosistemului digital la nivel național.

Scurgerile de date detectate sau raportate către DNSC au vizat, în majoritatea cazurilor, 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.

Principalele vulnerabilități critice identificate în 2025 în infrastructura cibernetică din spațiul cibernetic național civil au constat în:

- **CVE-2025-37164**, este o vulnerabilitate cu scor de 10.0 (maxim) conform **Common Vulnerability Scoring System (CVSS)**, de tip executare de cod de la distanță (Remote Code Execution - RCE) în Hewlett Packard Enterprise OneView, o platformă de management centralizat pentru infrastructuri IT (servere, stocare, rețele) folosită în medii ***enterprise*** și ***data center***. Vulnerabilitatea este cauzată de procesarea necorespunzătoare a datelor de intrare, permițând unui atacator fără autentificare să obțină execuție de cod arbitrar pe sistemul afectat.
- **CVE-2025-20393**, reprezintă o vulnerabilitate cu scor CVSS de 10.0 (maxim) în componenta AsyncOS folosită de produsele Cisco pentru securitatea mesageriei electronice. Produsele afectate sunt Cisco Secure Email Gateway (SEG) și Cisco Secure Email and Web Manager (SEWM). Vulnerabilitatea este cauzată de validarea incorectă a input-ului (CWE-20) în AsyncOS, atunci când funcția ***Spam Quarantine*** este expusă la Internet. Un atacator neautentificat poate trimite de la distanță cereri special construite care conduc la execuția de comenzi arbitrare, cu privilegii de tip root (RCE). Impactul este critic și poate include instalarea de backdoor-uri, ștergerea sau alterarea loguri-lor, exfiltrarea de date și mișcare laterală în rețea, fiind raportată utilizarea de unelte pentru menținerea persistenței și ștergerea urmelor după compromitere.
- **CVE-2025-24865** este o vulnerabilitate de securitate critică, cu scor CVSS de 10 (maxim), clasificată drept Authentication Bypass, care afectează sistemele ce rulează software-ul mySCADA myPRO Manager. Aceasta permite atacatorilor neautentificați să acceseze interfața de administrare fără a necesita credențiale valide, oferindu-le posibilitatea de a accesa informații sensibile și de a încărca fișiere în sistem.
- **CVE-2025-55182** este o vulnerabilitate critică cu scor CVSS de 10.0 (maxim), de tip remote code execution în implementarea React Server Components (RSC), care permite unui atacator neautentificat să execute cod arbitrar pe server prin deserializarea nesigură a unor obiecte interne speciale (denumite Chunks) transmise prin intermediul protocolului Flight în cadrul componentelor RSC.
- **CVE-2025-13780,** este o vulnerabilitate cu scor CVSS de 9.9 de tip Remote Code Execution (RCE) descoperită în pgAdmin 4, un instrument open-source folosit pe scară largă pentru administrarea bazelor de date PostgreSQL. Exploatarea acestei vulnerabilități permite unui atacator să execute comenzi arbitrare pe serverul gazdă unde rulează pgAdmin, punând în pericol integritatea, confidențialitatea și disponibilitatea sistemului afectat.
- **CVE-2025-24016** este o vulnerabilitate critică ce afectează componenta server (Manager) a soluției Wazuh și permite execuția de cod de la distanță (Remote Code Execution – RCE) prin exploatarea unui mecanism de deserializare nesecurizat. Aceasta are un scor CVSS de 9.9, reflectând severitatea ridicată a impactului. Exploatarea activă a vulnerabilității a fost confirmată, fiind utilizată în scopuri malițioase precum compromiterea completă a serverului, exfiltrarea de date sensibile și includerea sistemelor afectate în infrastructuri de tip botnet.

- **CVE-2025-20286** este o vulnerabilitate critică cu scor CVSS de 9.9, ce afectează instanțele Cisco Identity Services Engine (ISE) implementate în Amazon Web Services (AWS), Azure și Oracle Cloud Infrastructure (OCI). Aceasta permite unui atacator neautentificat, cu acces la rețea, să compromită alte instanțe ISE din cloud folosind date de autentificare generate identic în anumite versiuni și platforme.
- **CVE-2025-2945** este o vulnerabilitate critică la nivelul pgAdmin, cu un scor CVSS de 9.9. Aceasta afectează mai multe versiuni de pgAdmin 4 și poate permite unui atacator autentificat să exploateze anumite API-uri pentru a executa cod arbitrar pe serverul afectat. Atacatorii pot exploata acest punct slab pentru a instala backdoor-uri, a fura date sensibile sau a prelua controlul complet asupra mediului afectat. Exploatarea nu necesită interacțiune din partea utilizatorului și poate fi realizată de la distanță, ceea ce crește considerabil riscul pentru organizațiile care folosesc versiuni vulnerabile.
- **CVE-2025-59718** și **CVE-2025-59719** sunt 2 vulnerabilități critice cu scor CVSS de 9.8, care afectează mecanismul FortiCloud Single Sign-On (SSO) și pot permite atacatorilor neautentificați să ocolească autentificarea, trimițând mesaje SAML manipulate și să obțină astfel acces complet cu rol de administrator pe dispozitive precum FortiOS, FortiProxy, FortiSwitchManager și FortiWeb, compromițând securitatea întregului sistem.
- **CVE-2025-61757** este o vulnerabilitate critică, evaluată cu un scor CVSS de 9.8, identificată în Oracle Identity Manager, care permite unui atacator neautentificat să realizeze Remote Code Execution (RCE) pe serverele afectate. Odată exploatată, vulnerabilitatea permite manipularea mecanismelor interne de gestionare a conturilor, oferind atacatorului acces extins la operațiuni cu drepturi de administrator și posibilitatea de a modifica sau crea conturi noi în sistem.
- **CVE-2025-64446**, clasificată ca ***path traversal***, este o vulnerabilitate critică în produsul FortiWeb cu scor CVSS de 9.8. Exploatarea acestei vulnerabilități permite unui atacator neautentificat să evite mecanismele de control al accesului, să acceseze resurse și să execute comenzi cu privilegii de administrator direct pe dispozitivul afectat, fără a necesita un cont sau o parolă.
- **CVE-2025-53770** este o vulnerabilitate de tip Remote Code Execution (RCE), cu un scor CVSS de 9.8, ce afectează mai multe versiuni de Microsoft SharePoint Server instalate local. Vulnerabilitatea poate fi exploatată fără autentificare de către un potențial atacator și poate avea ca impact compromiterea completă a sistemului afectat, permițând executarea de cod arbitrar cu privilegii ridicate, accesul neautorizat la date sensibile, modificarea sau ștergerea informațiilor, precum și utilizarea serverului ca punct de lansare pentru atacuri ulterioare în infrastructura internă.
- **CVE-2025-32756** este o vulnerabilitate critică de tip stack-based buffer overflow identificată în mai multe produse Fortinet, inclusiv FortiVoice, FortiMail, FortiRecorder, FortiNDR și FortiCamera. Această vulnerabilitate permite unui atacator neautentificat să execute cod arbitrar sau comenzi pe sistemul afectat prin trimiterea unui cookie hash, special construit, într-o cerere HTTP către o interfață API vulnerabilă.
- **CVE-2025-20188** reprezintă o vulnerabilitate critică de securitate, cauzată de utilizarea unor credențiale hard-codate sub forma unui JSON Web Token (JWT) în Cisco IOS XE pentru controlere Wireless LAN, având un scor CVSS de 10.0 (maxim), care poate fi exploatată de la distanță, fără autentificare sau interacțiune cu utilizatorul, permițând unui atacator să încarce fișiere arbitrare și să execute comenzi cu privilegii de root, ceea ce poate conduce la compromiterea completă a dispozitivului și la afectarea confidențialității, integrității și disponibilității sistemului.
- **CVE-2024-20439** este o vulnerabilitate de tip ***Static Credential Vulnerability***, cu un scor de severitate CVSS de 9.8. Această vulnerabilitate apare din cauza existenței unor date de log-are statice administrative în Cisco Smart Licensing Utility (CSLU). În versiunile afectate, există un cont predefinit (nedocumentat) care permite unui atacator să obțină acces complet la interfața CSLU fără autentificare.
- **CVE-2024-20440** este o vulnerabilitate de tip ***Information Disclosure Vulnerability***, cu un scor de severitate CVSS de 9.8. Problema constă în faptul că Cisco Smart Licensing Utility generează fișiere de

log care conțin date sensibile în format text. Un atacator poate trimite o cerere HTTP special creată către interfața CSLU pentru a obține acces la aceste fișiere de log.

- **CVE-2025-25015** este o vulnerabilitate critică de tip Remote Code Execution (RCE), cu scor CVSS de 9.9, care afectează platforma Kibana, utilizată pentru analiza și vizualizarea datelor Elasticsearch. Exploatarea acestei vulnerabilități permite unui atacator autentificat să ruleze cod arbitrar pe serverul vulnerabil, ceea ce poate duce la compromiterea completă a instanței Kibana și la acces neautorizat la date importante.
- **CVE-2024-55591** este o vulnerabilitate de securitate critică, clasificată drept Authentication Bypass, ce afectează produsele FortiOS și FortiProxy utilizate la scară largă pentru securitatea rețelelor. Aceasta permite atacatorilor să obțină privilegii de administrator, exploatând o gestiune defectuoasă a sesiunilor de autentificare în modulul Node.js websocket al dispozitivelor afectate. Exploatarea cu succes oferă atacatorului acces de tip super-administrator (super_admin) pe dispozitivul vizat, acesta obținând astfel control complet asupra sistemului și capacitatea de a modifica setări critice sau de a compromite alte părți ale infrastructurii.

Față de 2024, în 2025 a crescut semnificativ numărul de vulnerabilități raportate pentru care Directoratul a emis alerte tehnice, reflectând atât creșterea complexității sistemelor IT&C, cât și numărul ridicat de noi tehnologii, platforme și sisteme informatice utilizate la nivel național.

Exemplele includ creșterea numărului de CVE-uri legate de tehnologii emergente, cum ar fi containerele, mediile cloud hibride și aplicațiile IoT.

De asemenea, vulnerabilitățile de tip CVE din 2025 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 de tip RCE fiind mai frecvente.

Figura 6 - Statistică informări DNSC pe sector de activitate sau tip de entitate

Creșterea numărului de alerte emise de DNSC pentru vulnerabilități este o ilustrare concretă și obiectivă a impactului pozitiv pe care l-au avut capacitățile tehnice nou dezvoltate dar și resursele umane specializate atrase în Directorat în anul 2025.

2.4 Managementul riscurilor cibernetice

În anul 2025, Directoratul a consolidat procesul național de **evaluare și prioritizare a riscurilor cibernetice** prin organizarea a 10 workshop-uri sectoriale dedicate sectoarelor esențiale și importante, în creștere semnificativă față de anul precedent. Evaluările au acoperit sectoare esențiale și importante, respectiv transport rutier, sănătate, administrație publică centrală și locală, apă potabilă, educație, energie, infrastructură digitală (centre de date), servicii poștale și de curierat, precum și producția, prelucrarea și distribuția de alimente.

Procesul de analiză a fost realizat prin aplicarea unor chestionare privind postura de securitate cibernetică și prin organizarea de sesiuni structurate cu manageri de risc, responsabili IT/OT și specialiști în domeniu, în urma cărora au fost elaborate rapoarte sectoriale ce includ riscuri prioritizate și recomandări specifice fiecărui domeniu analizat. Analiza agregată la nivel național evidențiază un profil de risc predominant mediu, cu vulnerabilități recurente și expunere semnificativă la:

- **Atacuri ransomware/wiper** cu impact asupra disponibilității serviciilor.
- **Phishing și inginerie socială.**
- **Exploatarea vulnerabilităților** software/firmware.
- **Compromiterea conturilor privilegiate.**
- **Deficiențe** în guvernanță, alocare de resurse și capacitate de reacție la incidente.
- **Segmentare insuficientă** a mediilor IT/OT și **gestionare incompletă** a furnizorilor critici.

Evaluările DNSC au evidențiat o serie de provocări structurale persistente ce stau la baza unora dintre riscuri, precum deficitul de personal specializat, dependențele de furnizori IT&C, inventarul incomplet al activelor și testarea insuficientă a scenariilor de criză.

Percepția asupra nivelului de securitate cibernetică organizațională indică faptul că majoritatea entităților își evaluează postura ca fiind ***bună*** sau ***foarte bună*** 68%, în timp ce 29% o consideră ***medie***. În schimb, la nivel sectorial, percepția este mai rezervată: 52% apreciază nivelul drept ***mediu***, iar 37% ***bun***, sugerând existența unor vulnerabilități sistemice și diferențe de maturitate între entități.

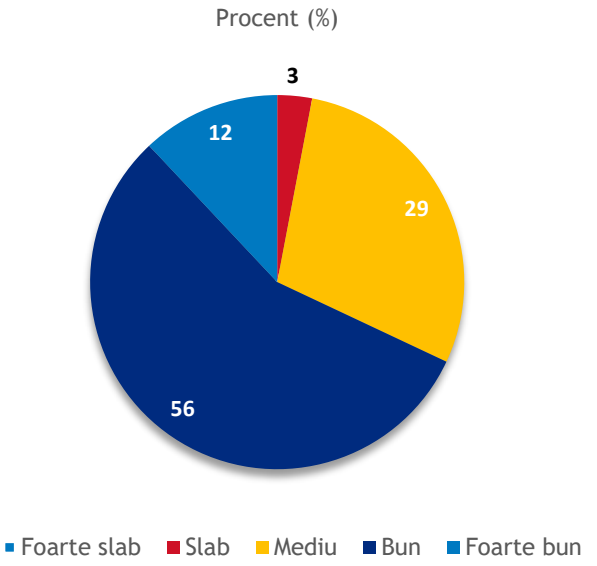


Figura 7 - Perspectiva privind starea actuală de securitate cibernetică organizațională

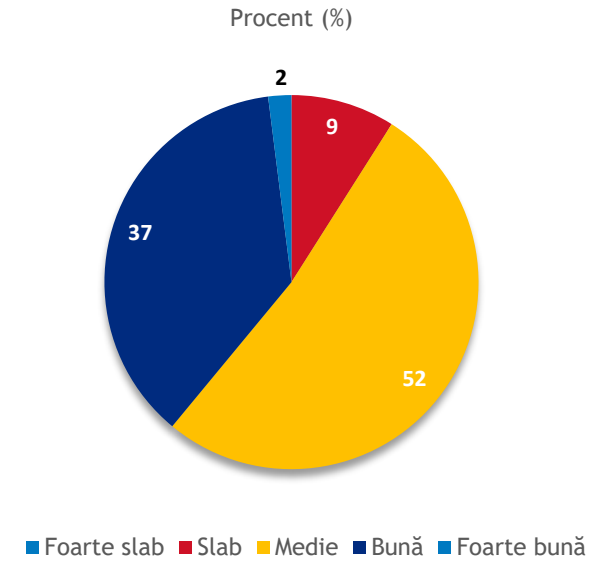


Figura 8 - Perspectiva privind starea curentă a securității cibernetice sectoriale

Analiza principalelor amenințări percepute confirmă predominanța atacurilor ransomware, urmate de phishing/spear-phishing și exploatarea vulnerabilităților software/firmware, cu relevanță transversală în toate sectoarele analizate.

Rezultatele evaluărilor riscurilor cibernetice din 2025 indică necesitatea consolidării guvernanței, creșterii capacității de reacție la incidente și accelerării măsurilor de reziliență operațională, în special în sectoarele cu toleranță redusă la întrerupere. Activitatea Directoratului a contribuit la dezvoltarea unei imagini coerente asupra profilului de risc al spațiului cibernetic național civil și la fundamentarea unor decizii strategice orientate spre creșterea nivelului de securitate cibernetică la nivel național.

Concluziile principale ale evaluării riscurilor de securitate cibernetică pe următoarele sectoare au fost:

Sector	Profil de risc la nivelul anului 2025	Principalele riscuri confirmate de sector
Transport rutier 	MEDIU mai multe riscuri peste linia mediană necesită măsuri suplimentare	Compromiterea operațiunilor pe fondul pregătirii insuficiente a personalului Guvernanță și resurse insuficiente, postură de securitate deficitară Ransomware/wiper cu impact ridicat asupra continuității
Sănătate 	**MEDIU** măsuri parțial implementate, expunere semnificativă	Lipsă de resurse umane specializate și control incomplet al infrastructurii IT Ransomware și blocarea operațiunilor medicale Inginerie socială și erori umane
Administrație publică centrală 	**MEDIU**	Lipsa unei reacții coordonate la incidente, din cauza absenței unui plan de răspuns și notificare în caz de atac Întrerupere a operațiunilor din cauza insuficienței măsurilor fizice de securitate Infectare cu malware și ransomware ca urmare a unor atacuri de tip phishing
Administrație publică locală 	**MEDIU** vulnerabilități structurale de bază precum absența planurilor de răspuns la incidente, protecție fizică insuficientă și expunere la phishing/ransomware	Resurse și control IT insuficiente în infrastructură Cultură de securitate deficitară, risc de acces neautorizat Afectarea disponibilității serviciilor prin atacuri cibernetice
Apă potabilă 	**MEDIU** prioritățile reflectă deficiențe în resurse, protecții tehnice și pregătirea personalului	Resurse financiare insuficiente pentru capabilități tehnice și personal Conștientizare și instruire insuficiente, risc de compromitere a datelor și sistemelor Phishing și inginerie socială asupra personalului Reacție întârziată la incidente din lipsa planurilor de răspuns/continuitate Acces neautorizat din cauza parolelor implicite/slabe/partajate
Centre de date 	**MEDIU**	Exfiltrare și divulgare neautorizată a datelor sensibile, inclusiv date ale clienților, ca urmare a compromiterii infrastructurii Întreruperea operațiunilor ca urmare a unui atac ransomware care criptează servere de management sau sisteme partajate între clienți Compromitere extinsă a infrastructurii din cauza lipsei segmentării între rețele de producție, rețele de management și rețele de clienți

Sector	Profil de risc la nivelul anului 2025	Principalele riscuri confirmate de sector
Servicii poștale și de curierat 	**MEDIU** amenințări pe două axe: fraudă pe canalul clientului și compromiterea operatorului cu maturitate neuniformă între operatori și necesitate de consolidare	Compromitere a datelor și sistemelor din cauza nivelului redus de conștientizare/instruire a personalului Gestionare inadecvată a infrastructurii în caz de atac, din cauza insuficienței personalului IT/cyber specializat Indisponibilitate a aplicațiilor de livrare, cauzată de atacuri cibernetice, cu impact operațional
Producție, prelucrare și distribuție alimentară 	**MEDIU** amenințări cu impact operațional major într-un sector cu toleranță foarte scăzută la întrerupere și maturitate neuniformă între operatori	Blocarea operațiunilor în urma unui atac ransomware, cu impact direct asupra producției, depozitării și distribuției Compromiterea prin furnizori terți (supply chain), cu potențial de propagare a incidentelor în sistemele interne Perturbarea operațiunilor cauzată de activități malițioase sau accidentale din interior (insider threat)

Analizele de risc efectuate de Directorat în 2025, coroborate cu istoricul incidentelor cibernetice, relevă că sectorul energetic, sectorul sănătății precum și administrația publică (centrală și locală) sunt în continuare printre cele mai expuse la riscurile și amenințările cibernetice. Sectorul sănătății se confruntă în continuare cu amenințări semnificative din cauza volumului mare de date personale, a lipsei de personal de specialitate și a infrastructurii IT&C subfinanțate.

Administrația publică este ținta sistematică a 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. Fenomenul este agravat de atacurile tot mai complexe desfășurate de actori malițioși cu capacități avansate.

Lipsa personalului specializat în domeniul securității cibernetice, în special pentru răspuns la incidente cibernetice, rămâne unul dintre cele mai relevante riscuri cu care se confruntă organizațiile din România. Concomitent, nivelul încă redus de conștientizare din partea publicului larg și interesul limitat al managementului privind riscurile și amenințările cibernetice amplifică vulnerabilitățile existente.

Având în vedere aceste riscuri și sectoarele cu cel mai mare nivel de expunere, au fost planificate și implementate o serie de măsuri ce vizează atât consolidarea capacităților de securitate cibernetică, cât și îmbunătățirea gradului de conștientizare la nivel național cu privire la riscurile implicate. Acțiunile desfășurate au urmărit colaborarea strânsă între instituții publice, mediul privat și parteneri internaționali, pentru a asigura o abordare unitară și eficientă în limitarea și diminuarea riscurilor cibernetice.

2.5 Demersuri în contextul securității cibernetice a alegerilor prezidențiale din mai 2025 din România

În perioada preelectorală și electorală aferentă alegerilor prezidențiale din 2025, Directoratul a avut un rol esențial în sprijinirea autorităților statului pentru protejarea integrității procesului democratic în spațiul digital. Activitatea DNSC s-a desfășurat în baza unui cadru legal dedicat și a fost orientată către asigurarea securității cibernetice și a transparenței în mediul online, într-un context marcat de provocări complexe, volum ridicat de conținut electoral și presiune instituțională.

Directoratul a participat activ în cadrul **Echipei Lucrări Campanie Online (ELCO)** constituită la **Biroul Electoral Central (BEC)**, unde a mobilizat 10 experți care au contribuit la procesarea a peste 5.800 de decizii privind conținutul electoral online. Aceștia au elaborat o metodologie de analiză a comportamentului neautentic pe platformele Very Large Online Platforms (VLOPs), reușind să creeze o bază de date cu peste 1.400 de conturi verificate, context în care DNSC propune soluții de suport precum automatizarea redactării deciziilor și digitalizarea fluxurilor de lucru.

În paralel, task-force-ul intern al DNSC a analizat peste 1.600 de conturi suspecte de pe platformele TikTok, Facebook și Instagram, dintre care 103 au fost identificate cu comportament posibil automatizat. Aceste conturi au fost raportate oficial către platformele respective, ca măsură de protecție a ecosistemului electoral online.

În zilele critice ale scrutinului electoral și în particular în 4 și 18 mai 2025, echipa CSIRT național din cadrul DNSC a asigurat capabilități de răspuns la incidente cibernetice și supravegherea infrastructurii digitale în regim 24/24, colaborând permanent cu autoritățile naționale relevante implicate (AEP, STS, MAI).

Prin platformele tehnice OSAVUL și EXOLYT, Directoratul a monitorizat și analizat conținuturi electorale suspecte, campanii de dezinformare și comportamente artificiale din jurul conturilor candidaților. De asemenea, în ziua turului doi, DNSC a gestionat în regim de criză comunicarea oficială a AEP pe platforma X (fostă Twitter), contribuind la diseminarea rapidă și corectă a informațiilor către cetățeni.

DNSC a formulat recomandări concrete către BEC privind digitalizarea completă a fluxului de soluționare a sesizărilor, implementarea unor instrumente de analiză automatizată bazate pe AI, asigurarea unei infrastructuri IT licențiate și securizate, stabilirea unui cadru clar de coordonare interinstituțională și profesionalizarea echipelor mixte prin ghiduri operaționale și protocoale de lucru comune.

Pe tot procesul de desfășurare al alegerilor prezidențiale, în cadrul grupului de lucru intern de la nivelul DNSC, s-a acordat asistență tehnică și juridică prin întocmirea a 30 de adrese de răspuns către BEC, în urma solicitărilor instituției privind verificarea conturilor de utilizatori pe platformele de socializare suspectate de propagandă electorală și centralizarea acestor conturi. Această activitate s-a desfășurat într-un mod neutru, obiectiv și independent, în baza unei metodologii complet noi, concepută de către DNSC. Metodologia a fost elaborată pentru a răspunde la solicitările oficiale primite din partea BEC, fără a exista un cadru preexistent pentru acest tip de analiză.

DNSC a colaborat cu **ENISA în publicarea unui raport special de avertizare privind riscurile cibernetice în contextul alegerilor din România** și a participat la exerciții de simulare, coordonate de către ANCOM și Comisia Europeană, vizând scenarii hibride precum deepfake, atacuri asupra conturilor oficiale și manipulare algoritmică a tendințelor online.

Pe ansamblu, efortul Directoratului în sprijinul autorităților competente s-a tradus astfel:

Formatul de sprijin din partea DNSC	Persoane din DNSC implicate
În cadrul Echipei Lucrări Campanie Online (ELCO) la BEC (100% la BEC)	10
Task force intern DNSC	11
Task force intern DNSC – platformele OSAVUL și EXOLYT	2
Echipa CSIRT națională și număr unic 1911 lucru în schimburi 12h+12h în preziua și ziua alegerilor)	14
Comunicare, media și marketing	5
Juridic	7
Participare în STRATCOM	1
Participare în grupul de coordonare inter-instituțional hibrid	3
Coordonare cu instituții ale UE și State Membre UE	2
TOTAL	**55**

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

3 STADIUL DE ÎNDEPLINIRE A OBIECTIVELOR DIRECTORATULUI

Cadrul normativ existent la nivel național, în special Legea nr. 58/2023 privind securitatea și apărarea cibernetică a României, art. 67 alin. (1) din OUG nr. 155/2024 privind instituirea unui cadru pentru securitatea cibernetică a rețelelor și sistemelor informatice din spațiul cibernetic național civil, respectiv HG nr. 1321/2021 privind aprobarea Strategiei de securitate cibernetică a României pentru 2022-2027, stabilește sarcini precise ale DNSC pentru domeniul securității cibernetice la nivel național, pe care DNSC le-a îndeplinit cu succes în 2025 și pentru care a realizat progrese semnificative, dintre care:

- Dezvoltarea și asigurarea managementului Platformei Naționale pentru Raportarea Incidentelor de Securitate Cibernetică (PNRISC).
- Identificarea, evaluarea și gestionarea riscurilor asociate vulnerabilităților de securitate cibernetică din produsele, soluțiile, componentele și/sau serviciile informatice ale sectorului guvernamental.
- Informarea și pregătirea, la nivel național, a populației, precum și a tuturor persoanelor fizice și juridice care acționează în spațiul cibernetic național, inclusiv a operatorilor economici din sectoarele stabilite potrivit dispozițiilor OUG nr.155/2024 și din sectorul public, cu privire la riscurile, amenințările și vulnerabilitățile de securitate cibernetică identificate.
- Stabilirea și instituirea nivelurilor de alertă cibernetică și a modalităților de acțiune la nivel național.
- Întreprinderea măsurilor pentru dezvoltarea unui comportament responsabil în spațiul cibernetic pentru persoanele fizice și juridice prin conștientizarea efectelor atacurilor cibernetice și a modalității de semnalare a acestora.
- Dezvoltarea cadrului național de conștientizare a populației în cooperare cu mediul public, privat și academic, în scopul pregătirii populației privind modalitățile de comportament, reacție și apărare în mediul online.
- Desfășurarea de campanii/acțiuni de prevenire și conștientizare a cauzelor și consecințelor atacurilor cibernetice asupra rețelelor și sistemelor informatice civile, la nivel internațional, național și regional.
- Crearea cadrului național de cooperare între instituții din domeniul public, privat, de educație și cercetare, pentru asigurarea unei viziuni și abordări realiste, comune și coerente privitor la securitatea cibernetică a României.
- Crearea cadrului național de certificare în domeniul securității cibernetice, în cooperare cu instituțiile care au competențe și atribuții în domeniu.
- Asigurarea cadrului de strategii, politici și reglementări care să susțină implementarea viziunii naționale în domeniul securității cibernetice.
- Crearea cadrului național destinat evaluării noilor tehnologii și impactului acestora asupra securității cibernetice a României.
- Crearea și operarea unei platforme naționale de colaborare care să permită schimbul de informații între constituenți, instituții ale statului, mediul academic și mediul privat în domeniul incidentelor, vulnerabilităților și crizelor de natură cibernetică.

3.1 Întărirea cadrului legislativ și de reglementare

Pe parcursul anului 2025, 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, norme metodologice și ordine emise

OUG nr. 155/2024 privind instituirea unui cadru pentru securitatea cibernetică a rețelelor și sistemelor informatice din spațiul cibernetic național civil, act normativ prin care a fost realizată transpunerea în legislația națională a Directivei NIS 2 [Directiva (UE) nr. 2022/2555], a fost modificată și completată prin **Legea nr. 124/2025**, DNSC fiind angrenat atât în elaborarea, cât și în susținerea activă a proiectului de

lege în cadrul comisiilor parlamentare. DNSC a inițiat elaborarea cadrului normativ de punere în aplicare a dispozițiilor OUG nr. 155/2024, după cum urmează:

- **Ordinul Directorului DNSC nr. 1/2025** pentru aprobarea Cerințelor privind procesul de notificare în vederea înregistrării și metoda de transmitere a informațiilor, prin intermediul căruia DNSC a realizat implementarea prevederilor art. 18 alin. (9) din OUG nr. 155/2024, normând cerințele privind procesul de notificare în vederea înregistrării și metoda de transmitere a informațiilor.
- **Ordinul Directorului DNSC nr. 2/2025** pentru aprobarea Criteriilor și pragurilor de determinare a gradului de perturbare a unui serviciu și a **Metodologiei privind evaluarea nivelului de risc al entităților**, prin intermediul căruia DNSC a realizat implementarea prevederilor art. 10 alin. (2) și ale art. 18 din OUG nr. 155/2024, reglementând criteriile și pragurile de determinare a gradului de perturbare a unui serviciu, elemente procedurale privind evaluarea nivelului de risc al entităților, inclusiv valorile sectoriale pentru stabilirea nivelului de risc utilizate în evaluarea acestuia.
- **Ordinul Directorului DNSC nr. 3/2025** pentru aprobarea Normelor de aplicare a dispozițiilor privind supravegherea, verificarea și controlul respectării prevederilor OUG nr. 155/2024 și a **Metodologiei de prioritizare pe bază de risc a activităților de supraveghere, verificare și control**.

În plus, în decembrie 2025, Directoratul a finalizat etapa de elaborare a proiectului de Ordin al Directorului DNSC pentru aprobarea **Măsurilor de gestionare a riscurilor de securitate cibernetică aferente rețelelor și sistemelor informatice utilizate de entitățile esențiale și importante** și a **Metodologiei de auto-evaluare a maturității măsurilor** și pentru modificarea **Metodologiei privind evaluarea nivelului de risc al entităților**, aprobată prin Ordinul Directorului DNSC nr. 2/2025.

De asemenea, în decembrie 2025, DNSC a finalizat etapa de elaborare a proiectului de Decizie a Directorului DNSC pentru aprobarea **Standardului de pregătire a membrilor organelor de conducere ale entităților esențiale și importante** și a **Listei de certificări de securitate cibernetică**.

În vederea facilitării procesului de identificare și calificare a entităților drept esențiale sau importante conform prevederilor OUG nr. 155/2024, a notificării și înscrierii lor în **Registrul entităților esențiale sau importante**, precum și a îndeplinirii de către acestea a unor obligații subsecvente emiterii deciziei de înscriere în registru, DNSC a creat, testat și pus la dispoziția entităților următoarele mecanisme:

- Un instrument digital de evaluare și generare a datelor de notificare, denumit **Instrumentul NIS2@RO**.
- Un instrument de evaluare a nivelului de risc al unei entități, denumit **Instrumentul ENIRE@RO**.
- Un instrument suport reprezentat de **Ghidul pentru realizarea analizei privind efectul perturbator**, elaborat pentru a sprijini entitățile în procesul de autoevaluare reglementat de OUG nr.155/2024.

În cadrul proiectului ***Implementarea Directivei NIS în sectorul producția, prelucrarea și distribuția de alimente în România și Bulgaria – INFORB***, finanțat prin programul UE Europa Digitală (Digital Europe) a fost, de asemenea, dezvoltată o aplicație de înregistrare a entităților esențiale și importante. Platforma INFORB este în proces de operaționalizare și va constitui un instrument de facilitare a interacțiunii dintre DNSC și entitățile esențiale și importante, precum și a îndeplinirii obligațiilor reglementate de dispozițiile OUG nr. 155/2024 de către entitățile care intră în domeniul de aplicare al acesteia.

De la momentul declanșării procesului de înregistrare a entităților esențiale și importante în temeiul dispozițiilor OUG nr. 155/2024, DNSC a gestionat un număr de 2.410 formulare de notificare, fiind emise 644 de decizii de înscriere a unor entități esențiale și 34 de decizii de înscriere a unor entități importante.

3.1.2 Suport legislativ și colaborare inter-instituțională

Directoratul a furnizat puncte de vedere pe domeniul său de competență cu privire la proiectele de acte normative în dezbatere atât la nivel național, spre exemplu, cu privire la proiectul de act normativ de înființare a **Centrului de Răspuns la Incidente de Securitate Cibernetică în Energie (CRISCE).**

În calitatea sa de autoritate competentă la nivel național de reglementare, supraveghere și control – care asigură reglementarea și gestionarea securității cibernetice a României și a spațiului cibernetic național, Directoratul a avut în 2025 ca prioritate pregătirea de puncte de vedere asupra proiectelor de acte

normative în dezbatere la nivelul Uniunii Europene, spre exemplu, punctele de vedere cu privire la **Digital Omnibus Regulation Proposal**.

În contextul pregătirii acestui ultim punct de vedere, DNSC s-a consultat și coordonat în mod transparent organizând inclusiv sesiuni de consultare inter-instituțională cu alte instituții interesate, precum: **Banca Națională a României (BNR), Autoritatea de Supraveghere Financiară (ASF), Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP), Centrul Național de Coordonare a Protecției Infrastructurilor Critice (CNCPIC), Ministerul Afacerilor Externe (MAE).**

DNSC a furnizat puncte de vedere relevante cu privire la proiecte de acte normative în dezbatere la nivelul Uniunii Europene, organizând inclusiv sesiuni de consultare inter-instituțională privind subiectele comune de interes cu actorii naționali interesați.

S-a realizat și inițierea dialogului cu Ministerul Educației, reprezentanți ai altor instituții, ai mediului academic și ai mediului privat pentru elaborarea unei strategii naționale de educație și formare în domeniul securității cibernetice.

În 2025, Directoratul a continuat lucrul la sprijinirea directă a armonizării legislației Republicii Moldova cu cea a Uniunii Europene și a României privind securitatea cibernetică, inclusiv prin acordarea de sprijin concret pentru dezvoltarea cadrului normativ în domeniul securității cibernetice, prin consultări bilaterale cu **Agenția pentru Securitate Cibernetică (ASC)**. În acest sens au fost formulate 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.

3.1.3 Activități de supraveghere și control

În vederea asigurării respectării dispozițiilor legale, începând cu luna septembrie 2025, s-a procedat la analizarea, identificarea și notificarea entităților care nu și-au îndeplinit obligația de a se supune procesului de identificare în vederea înscrierii în **Registrul entităților esențiale sau importante**.

Din 1.869 de entități analizate conform criteriilor stabilite de OUG nr. 155/2024, au fost notificate 341 de entități, dintre care un procent de peste 50% a inițiat procedura de identificare și înscriere.

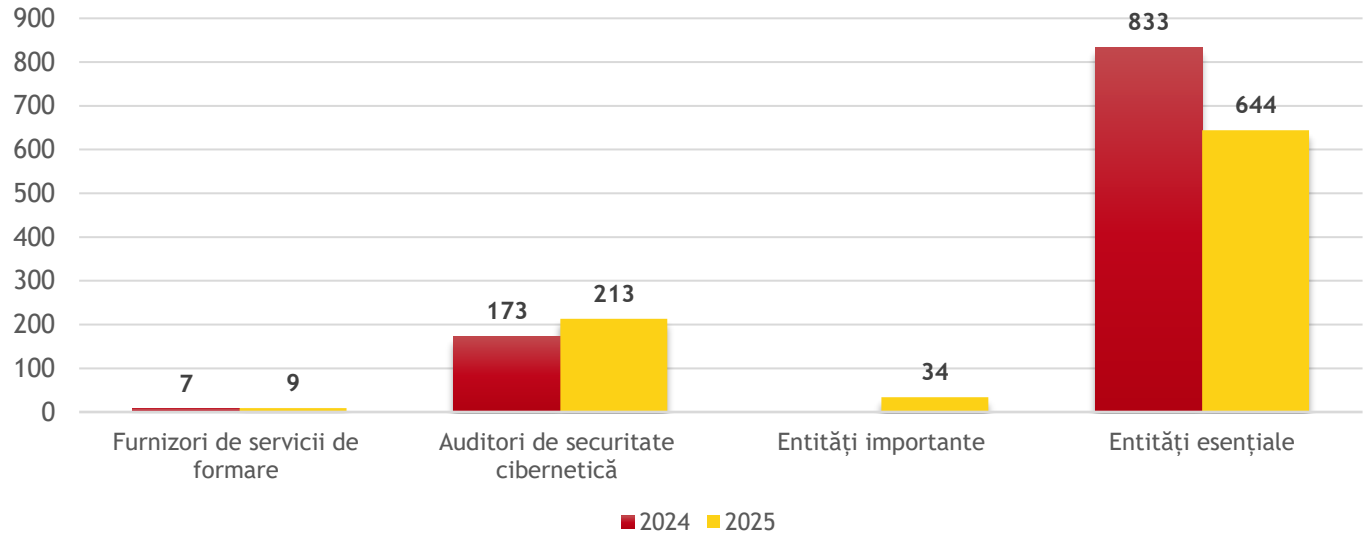


Figura 9 - Situația numerică a actorilor reglementați de DNSC după reclasificarea impusă de OUG nr. 155/2024

La sfârșitul anului 2025, DNSC avea în supraveghere 644 de entități esențiale și 34 de entități importante, 213 auditori de securitate cibernetică și 9 furnizori de servicii de formare pentru securitate cibernetică.

În anul 2026, numărul total al entităților esențiale și importante va depăși pragul de 3.000.

3.2 Capacități operaționale și tehnice consolidate în 2025

3.2.1 Încadrarea cu personal calificat la nivelul DNSC

Din punctul de vedere al capacităților operaționale, în anul 2025, similar cu 2024, Directoratul a avut o serie de provocări majore în ceea ce privește încadrarea cu personal de specialitate în securitate cibernetică. Creșterea numărului de posturi ocupate s-a menținut ca o prioritate și a rezultat din obligativitatea îndeplinirii atribuțiilor stabilite prin OUG 104/2021 privind înființarea DNSC, care conferă noii instituții atribuțiile de autoritate de securitate cibernetică la nivel național, cu un număr de 18 atribuții și funcții instituționale distincte, majoritatea acestora fiind complet noi la nivel național.

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. 156/2024, **a fost necesară aprobarea organizării în anul 2025** de noi concursuri de recrutare pentru continuarea demersurilor de ocupare a posturilor din cadrul DNSC (execuție/conducere).

Suplimentar, în scopul urmăririi priorităților stabilite pentru 2025, privind continuarea operaționalizării structurilor Directoratului prin atragerea resursei umane, în contextul provocărilor asociate lipsei acute a încadrării statului de funcții cu personal înalt calificat necesar îndeplinirii atribuțiilor instituționale, Guvernul României a aprobat HG nr. 672/2025 privind suplimentarea bugetului SGG pentru DNSC din Fondul de rezervă bugetară la dispoziția Guvernului, prevăzut în bugetul de stat pe anul 2025.

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

Gradul de ocupare a posturilor Directoratului la sfârșitul anului 2025 a fost de 17,69%, în ușoară creștere față de sfârșitul anului 2024, când gradul de ocupare a fost de doar 13,07%.

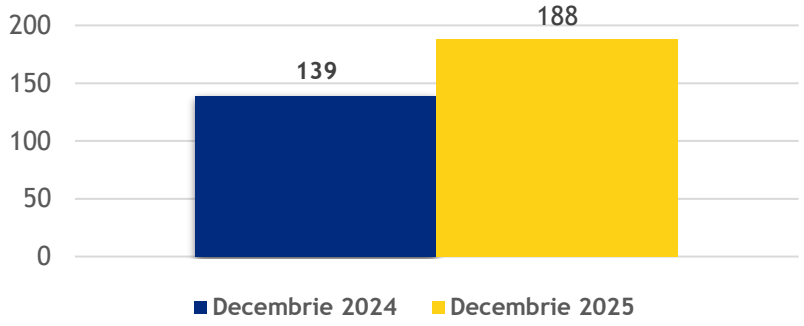


Figura 10 - Posturi ocupate în cadrul DNSC

În anul 2025, Directoratul a intensificat efortul de recrutare, organizând un număr de 45 concursuri pentru ocuparea posturilor vacante. Rata de succes a efortului de recrutare a crescut de la o medie de 0,5 persoane angajate pe concurs la 1,8 persoane angajate pe concurs derulat.

Tip acțiune pentru atragerea de personal calificat	2024	2025
Concursuri angajare derulate	36	45
Persoane angajate prin concurs	18	81
Rata de succes (persoane angajate / concurs)	0,50	1,80

O explicație a creșterii ratei de succes a efortului de recrutare al DNSC a reprezentat-o organizarea de concursuri de angajare dedicate studenților din an terminal de facultate (funcții specifice cu studii medii). În anul 2025, în cadrul Directoratului au fost angajați cu contract de muncă **25 de studenți (reprezentând 45,68% din întregul personal angajat)**.

Această abordare este o practică strategică pentru atragerea talentelor emergente în domeniul securității cibernetice și asigură un flux continuu de competențe noi, tinere și aliniate cu nevoile instituției, contribuind la obiectivele naționale de securitate digitală.

Strategia DNSC de a investi masiv în studenți și debutanți promovează meritocrația și incluziunea în sectorul public, prevenind blocajele de angajare și susținând retenția absolvenților în România, în contextul cererii crescute de specialiști în domeniul securității cibernetice. Procesul de recrutare dedicat studenților permite identificarea proactivă a profilelor tehnice cu potențial ridicat în domeniul securității cibernetice, reducând timpul de recrutare și costurile asociate formării inițiale.

În anul 2025, **81 persoane** au fost angajate prin concurs, iar **27 persoane** au părăsit DNSC (prin demisie, încetarea detașării, pensionare, desfacere disciplinară a contractului individual de muncă).

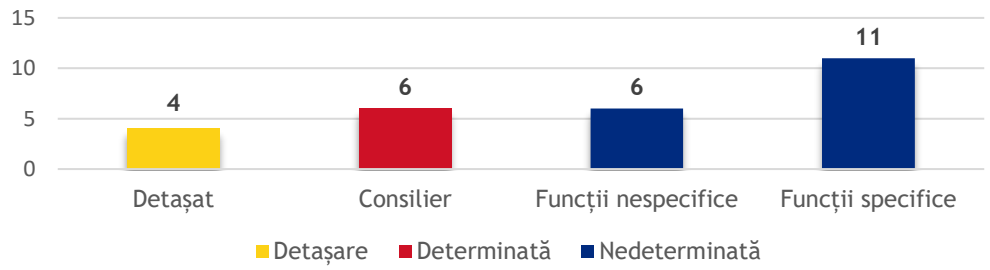


Figura 11 - Plecări de personal din instituție în 2025

De menționat că una dintre prioritățile Directoratului este asigurarea unei bune împărțiri pe sexe a ocupării posturilor de execuție și de conducere. Situația curentă este următoarea și implică o **creștere cu 2,36%** a procentului de femei în DNSC, comparativ cu 2024:

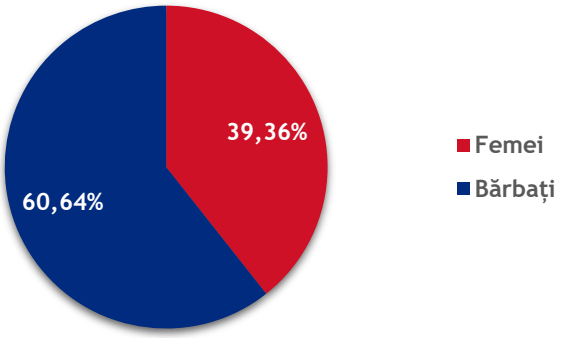


Figura 12 - Distribuția pe gen a ocupării posturilor DNSC

Un număr de **28 studenți** din următoarele facultăți au participat în anul 2025 la stagiile de practică organizate în cadrul Directoratului:

- Facultatea de Electronică, Telecomunicații și Tehnologia Informației (ETTI) din cadrul Universității Naționale de Știință și Tehnologie Politehnica București.
- Facultatea de Istorie și Filosofie din cadrul Universității Babeș-Bolyai.
- Facultatea de Drept din cadrul Universității București.
- Facultatea de Drept din cadrul Universității Babeș-Bolyai.

3.2.2 Operaționalizarea compartimentelor funcționale cheie ale Directoratului

Similar cu anii 2023 și 2024, continuarea recrutării de personal specializat și calificat a fost și în 2025 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.

La începutul anului 2025, un număr de structuri cheie ale Directoratului aveau zero (0) poziții ocupate:

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

În 2025, Directoratul a reușit recrutarea sau detașarea de 10 persoane în trei dintre compartimentele funcționale care în 2024 aveau încadrate zero (0) persoane:

- Serviciul Dezvoltare și Implementare Strategii și Politici de Securitate Cibernetică - **4 posturi nou ocupate în 2025**
- Serviciul PSIRT (Product Security Incident Response Team) - **1 post nou ocupat în 2025**
- Direcția Evaluare și Certificare Securitate Cibernetică Noi Tehnologii, Produse și Servicii - **5 posturi nou ocupate în 2025**

Pentru ocuparea acestora au fost absolut necesare aptitudini, atitudini și un mod de lucru care impun profiluri profesionale care, la acest moment, nu există în sistemul public național și trebuie să fie 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.

3.2.3 Optimizarea proceselor privind raportarea incidentelor de securitate cibernetică

Numărul unic 1911, destinat raportării incidentelor de securitate cibernetică la nivel național, a fost reorganizat și permanentizat pentru a funcționa în **regim 24/7**. Directoratul a efectuat migrarea serviciului de centrală telefonică aferent numărului unic 1911 către o soluție de tip cloud, pentru creșterea eficienței, disponibilității, scalabilității și reziliență serviciului.

Prin intermediul acestui canal au fost înregistrate peste **4.357 de apeluri,** raportorilor (cetățeni și beneficiari) fiindu-le furnizate recomandări și îndrumări în timp real, în vederea limitării impactului incidentelor și a adoptării unor măsuri imediate de protecție. Această reorganizare a contribuit la creșterea accesibilității și a capacității de reacție a instituției, asigurând un mecanism eficient de comunicare rapidă și intervenție timpurie în gestionarea incidentelor de securitate cibernetică.

În vederea menținerii și îmbunătățirii continue a nivelului calitativ al răspunsurilor la incidentele cibernetice gestionate la nivelul DNSC, a fost dezvoltat și implementat un mecanism de feedback. În cadrul acestuia **a fost primit un număr de 845 de recenzii**, nivelul mediu de satisfacție înregistrat fiind de 4,59/5, ceea ce reflectă un grad ridicat de apreciere din partea persoanelor care au raportat incidente. Rezultatele obținute relevă un grad de încredere ridicat față de instituție, față de răspunsurile și recomandările oferite, precum și față de nivelul de maturitate operațională atins. Aceste rezultate sunt datorate, în principal, controlului eficient impus asupra procesului de transmitere a răspunsurilor și informărilor către raportori, prin implementarea unui nivel superior de asigurare a calității (Layer 2).

Din analiza cazurilor izolate în care a fost primit feedback negativ s-a constatat că majoritatea recenziilor de acest tip au fost generate de percepții subiective ale raportorilor, precum: un nivel insuficient de cunoaștere a cadrului legal aplicabil, a competențelor și atribuțiilor instituționale, respectiv în materie de securitate cibernetică. Totodată, în anumite situații, nivelul de satisfacție scăzut a fost determinat de neîndeplinirea așteptărilor privind rezultatul scontat, acesta depășind sfera de responsabilitate și intervenție a instituției.

Au fost elaborate și implementate instrucțiuni de lucru clare și standardizate, care au condus la o reducere semnificativă a timpului de răspuns la incidente de securitate cibernetică gestionate de către DNSC. Aceste instrucțiuni definesc etapele procesului de gestionare a incidentelor, responsabilitățile fiecărui nivel de suport și fluxurile de comunicare interne și externe, asigurând o abordare coerentă și rapidă. Ca urmare,

s-a înregistrat o creștere a eficienței operaționale, o îmbunătățire a calității soluțiilor oferite și consolidarea nivelului de încredere raportat la capacitatea instituției de a gestiona incidentele într-un mod profesionist și predictibil.

3.2.4 Modernizarea infrastructurii proprii de rețea a DNSC

În anul 2025, ca urmare a creșterii semnificative a mobilității personalului instituției și a nevoilor de comunicații și conectivitate ale DNSC, au fost realizate modernizări ale infrastructurii de rețea, în vederea creșterii performanței și a nivelului de securitate și reziliență al acesteia:

- Creșterea capacității conexiunii la internet de la 1 Gbps la 10 Gbps, inclusiv implementarea rutării și a configurărilor necesare.
- Implementarea, administrarea și operaționalizarea unui sistem de conectivitate satelitară Starlink, ca soluție alternativă și mobilă de comunicații, în vederea asigurării continuității operaționale și a rezilienței infrastructurii de rețea în scenarii de indisponibilitate a legăturilor terestre.
- Implementarea și reconfigurarea clasei de adrese IP ale DNSC.
- Configurarea și administrarea segmentării infrastructurii interne - Virtual Local Area Network (VLAN).
- Configurarea și administrarea tunelurilor pentru acces securizat la resursele interne ale DNSC prin utilizarea unor tehnologii de tip VPN reziliente la atacuri cibernetice.
- Definirea, implementarea și administrarea permanentă de noi politici pentru echipamentele de tip firewall, în scopul protejării rețelei și a serviciilor critice ale DNSC, pe fondul creșterii numărului de atacuri cibernetice îndreptate asupra infrastructurii proprii.

3.2.5 Virtualizarea infrastructurii IT&C a DNSC pentru creșterea rezilienței și scăderea costurilor

La nivelul Directoratului, a fost asigurată exploatarea și dezvoltarea infrastructurii de virtualizare bazată pe tehnologia VMware ESXi, necesară creșterii rezilienței și performanței aplicațiilor și serviciilor critice operaționale ale instituției. Aceasta a implicat:

- Administrarea și menținerea funcționalității pentru aproximativ 200 de mașini virtuale simultan.
- Configurarea și punerea în producție a 15 mașini virtuale noi, pentru implementarea soluțiilor software utilizate în vederea îmbunătățirii activităților de capital uman ale DNSC; a celor aferente proiectelor cu finanțare din partea Uniunii Europene (în principal proiectele ENSOC, DYNABIC); instalarea, migrarea și actualizarea aplicațiilor utilizate pentru înregistrarea incidentelor cibernetice și monitorizarea indicatorilor de compromis (Indicators of Compromise – IOC), precum și instalarea și testarea soluțiilor tehnice interne.
- Migrarea și reconfigurarea mașinilor virtuale găzduite anterior pentru DNSC în sediul Institutului Național de Cercetare-Dezvoltare în Informatică (ICI București).

3.2.6 Creșterea nivelului de apărare juridică a drepturilor și intereselor Directoratului

Anul 2025 a adus față de anul 2024 un element de noutate cu privire la litigiile în care Directoratul este parte. Astfel, în exercitarea rolului său de autoritate națională de reglementare în domeniul securității cibernetice și în derularea activităților de înregistrare a entităților importante și esențiale, conform OUG nr. 155/2024 a fost înregistrat pe rolul instanței de judecată de către o societate cu obiect de activitate în industria farmaceutică, **primul dosar având ca obiect anularea deciziei emise de către DNSC privind înscrierea SANOFI ROMANIA SRL ca entitate esențială în sectorul sănătății.**

Directoratul estimează că acest caz singular din 2025 este unul relevant pentru a ilustra un trend din partea entităților supuse înscrierii în **Registrul entităților esențiale sau importante**. Pentru gestionarea corespunzătoare a acestui trend și pentru exercitarea rolului său de autoritate de reglementare în domeniul securității cibernetice, DNSC are nevoie de atragerea și consolidarea de personal cu expertiză și resurse juridice adecvate.

În anul 2025, în mod inerent creșterii volumului și complexității activităților desfășurate de către DNSC, acesta și-a apărat interesele într-un **număr de litigii mai ridicat față de 2024**, aflate pe rolul instanțelor

inclusiv a celor civile, de contencios administrativ și de dreptul muncii, precum și a organelor de urmărire penală. Ca atare, apărarea juridică a drepturilor și intereselor Directoratului a implicat un efort ridicat precum și alocarea de resurse umane substanțiale.

În anul 2025, DNSC a avut **calitatea de reclamant în 5 cauze** care au avut ca obiect contestarea unor acte administrative sau constatarea nulității unor documente.

În aceeași perioadă, DNSC a avut **calitatea de pârât/intimat în 9 cauze** având ca obiect exercitarea de către persoane fizice și/sau persoane juridice a dreptului legal de a contesta acte administrative emise de către DNSC, inclusiv privind desfășurarea examenelor de promovare în grad superior, măsuri de încetare a raporturilor de muncă ori măsuri de sancționare pentru săvârșirea abaterilor disciplinare de către personalul contractual.

Nu au fost înregistrate dosare în faza executării silite cu DNSC având calitatea de debitor și/sau creditor.

În anul 2025 Directoratul a emis 1.225 decizii, această evoluție fiind determinată de **optimizarea și adaptarea activității instituționale la noile priorități și mecanisme de lucru**, comparativ cu anul 2024. Deciziile emise au vizat domenii esențiale precum: înscrierea entităților esențiale și importante (conform OUG nr. 155/2024), organizarea internă, resursele umane, fonduri europene rambursabile și nerambursabile, delegarea competențelor, digitalizarea proceselor administrative, guvernanța și operaționalizarea instituțională.

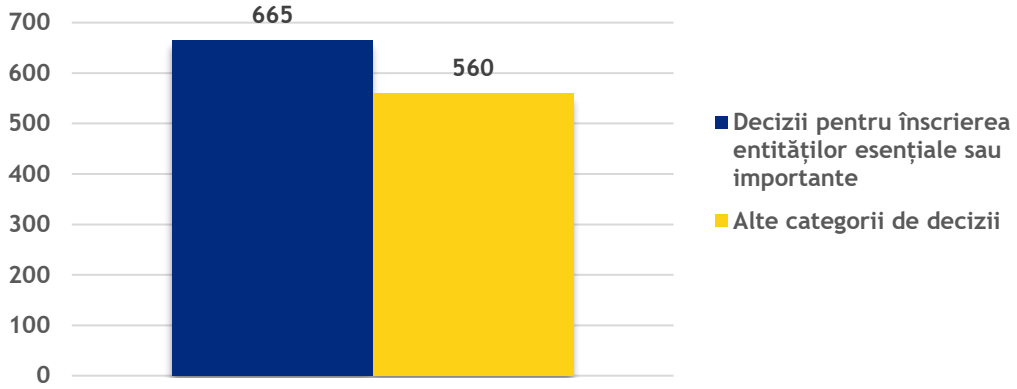


Figura 13 - Decizii emise la nivelul DNSC în 2025

În cursul anului 2025 Directoratul a primit și a soluționat **un număr ridicat de petiții/solicitări de informații de interes** public și solicitări pe diferite alte problematici de ordin juridic provenind din partea unor petenți (persoane fizice și/sau juridice), respectiv a unor entități de drept public și privat, având o rată semnificativă de **creștere de 150%**, comparativ cu anul 2024, dintre acestea:

- Un număr de **127 de petiții/alte solicitări** au fost soluționate în baza OG nr. 27/2002 privind reglementarea activității de soluționare a petițiilor.
- Un număr de **36 de cereri de informații de interes public/alte solicitări** au fost soluționate în baza Legii nr. 544/2001 privind liberul acces la informațiile de interes public.

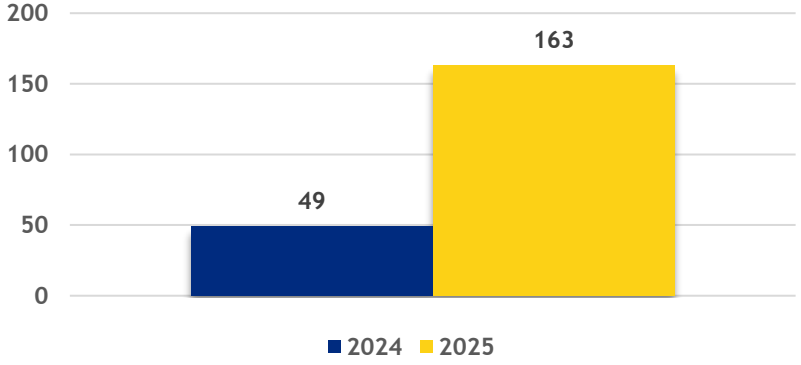


Figura 14 - Numărul de petiții/solicitări/cereri de informații de interes public soluționate în anul 2025 comparativ cu anul 2024

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 OUG nr. 104/2021 aplicându-se în mod corespunzător.

3.2.7 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

Având în vedere bugetul alocat în anul 2025 către DNSC prin ordonatorul principal de credite (Secretariatul General al Guvernului - SGG) și corelarea obiectivelor asumate cu resursele disponibile, au fost necesare virări de credite bugetare și de angajament pentru a asigura nevoile urgente de întreținere și funcționare ale instituției și pentru finanțarea proiectelor europene aprobate în buget.

Pentru a asigura acoperirea nevoilor instituționale și a cheltuielilor de personal în anul 2025 a fost necesară solicitarea suplimentării cu 13.855 mii lei din Fondul de rezervă bugetară la dispoziția Guvernului, prevăzut în bugetul de stat pe anul 2025, care s-a materializat prin HG nr. 672/2025.

Directoratul a asigurat evidențele contabile atât pentru activitatea curentă, cât și pentru toate proiectele finanțate din fonduri externe nerambursabile pe care instituția le-a avut în derulare în anul 2025, în conformitate cu reglementările legale în vigoare, facilitând astfel transparența și responsabilitatea în activitățile economice ale instituției.

DNSC a susținut implementarea proiectelor cu finanțare europeană și internațională prin asigurarea cadrului financiar necesar, monitorizarea cheltuielilor și gestionarea eficientă a resurselor alocate. Prin implicarea activă în toate etapele de derulare, a contribuit la respectarea termenelor și asigurarea transparenței în utilizarea fondurilor de la bugetul de stat.

Tabel 3 - Centralizare virări credite bugetare și de angajament

Nr.	Denumire indicator	Nr. adresă
1.	Titlul XII Cheltuieli de capital	E258/31.03.2025
2.	Titlul II Bunuri si servicii	E280/03.04.2025
3.	Titlul XII Cheltuieli de capital	E283/07.04.2025
4.	Titlul I Cheltuieli de personal	E462/23.05.2025
5.	Titlul X Alte cheltuieli	E519/10.06.2025
6.	Titlul I Cheltuieli de personal	E658/31.07.2025
7.	Titlul VIII Proiecte cu finanțare din fonduri externe nerambursabile aferente cadrului financiar 2021-2027	E690/11.08.2025
8.	Titlul X Proiecte cu finanțare din fonduri externe nerambursabile aferente cadrului financiar 2014-2020	E694/11.08.2025
9.	Titlul XII Cheltuieli de capital	E798/10.09.2025
10.	Titlul II Bunuri si servicii	E953/23.10.2025
11.	Titlul XII Cheltuieli de capital	E954/23.10.2025

Situațiile financiare periodice au fost întocmite și transmise cu rigurozitate, asigurând informații corecte și complete, respectând cu strictețe termenele legale pentru raportările lunare, trimestriale și anuale.

Directoratul a răspuns solicitărilor venite din partea structurilor de control și audit cu promptitudine, asigurându-se că toate informațiile și documentele necesare au fost furnizate în timp util și a oferit explicații detaliate privind procesele contabile și gestionarea resurselor. Prin această abordare, a asigurat transparență și conformitate, facilitând o evaluare corectă a activităților sale și contribuind la

îmbunătățirea continuă a practicilor financiare și la identificarea oportunităților de optimizare a proceselor interne. Directoratul a respectat toate termenele de depunere a situațiilor financiare conform prevederilor legale în vigoare.

Gradul de execuție bugetară al DNSC în 2025 a fost unul ridicat și constituie un indicator este esențial pentru evaluarea eficienței utilizării resurselor financiare, pentru monitorizarea respectării planificării bugetare a DNSC, contribuind la transparența și responsabilitatea în gestionarea fondurilor publice.

Tabel 4 - Execuție bugetară la data de 31.12.2025

Denumire indicator	Cod clasificație	Buget DNSC 2025 (mii lei)	Execuție bugetara la data de 31.12.2025 (mii lei)	Procent de realizare (%)
TOTAL GENERAL	**8500**	**59.463**	**43.057**	**72,41%**
TOTAL CHELTUIELI, din care:		**47.616**	**39.073**	**82,06%**
Titlul I Cheltuieli de personal	*10*	*32.087*	*31.240*	97,36%
Titlul II Bunuri si servicii	*20*	*1.539*	*1.251*	81,29%
Titlul VII Transferuri	*55*	*100*	*14*	14,00%
Titlul VIII Proiecte cu finanțare din fonduri externe nerambursabile aferente cadrului financiar 2021-2027	*56*	*6.850*	*1.967*	28,72%
Titlul X Proiecte cu finanțare din fonduri externe nerambursabile aferente cadrului financiar 2014-2020	*58*	*4.683*	*2.599*	55,50%
Titlul X Alte cheltuieli	*59*	*307*	*278*	90,55%
Titlul XII Cheltuieli de capital	*70*	*2.050*	*1.724*	84,10%
Fonduri externe nerambursabile -Sursa D	**5008**	**11.847**	**3.984**	**33,63%**
Titlul VIII Proiecte cu finanțare din fonduri externe nerambursabile aferente cadrului financiar 2021-2027	56	8.941	2.645	29,58%
Titlul X Proiecte cu finanțare din fonduri externe nerambursabile aferente cadrului financiar 2014-2020	58	2.906	1.339	46,08%

Situația prezentată oferă o imagine detaliată a execuției bugetare pentru anul 2025, evidențiind astfel realizările financiare pe categorii de cheltuieli la data de 31 decembrie 2025.

Bugetul total alocat a fost de 59.463 mii LEI, din care s-au executat 43.057 mii LEI, rezultând un procent de realizare de 72,41%.

În anul 2025, DNSC a încasat venituri în valoare de 626.500 LEI, din taxe de atestare pentru auditorii de securitate cibernetică și operatori de servicii esențiale.

Directoratul a avut în vedere permanent continuitatea activităților economice, asigurându-se că toate procesele administrative și operaționale se desfășoară într-un mod fluid și eficient. Prin coordonarea eficientă a resurselor umane și materiale s-a reușit menținerea unui flux constant de informații și posibilitatea de a răspunde prompt la solicitările interne și externe.

Prin activitatea derulată pe parcursul anului 2025, DNSC a menținut nevoile instituționale prin gestionarea resurselor financiare și prin monitorizarea constantă a cheltuielilor. Aceasta a inclus elaborarea și respectarea bugetului, care a fost adaptat în funcție de necesitățile instituției.

3.2.8 Implementarea platformei OpenProject pentru managementul portofoliului de proiecte

Una dintre activitățile majore operaționalizate în 2025 a fost consolidarea managementului de portofoliu, ca nivel distinct față de managementul individual al proiectelor, cu sprijinul platformei software OpenProject, de tip open-source, fără costuri de licență. Prin aceasta, Directoratul a asigurat:

- O viziune de ansamblu asupra tuturor proiectelor aflate în derulare.
- Corelarea calendarului proiectelor cu prioritățile interne ale DNSC.

- Identificarea timpurie a suprapunerilor, riscurilor și dependențelor.
- Prioritizarea resurselor în funcție de impact și urgență.

Utilizarea platformei OpenProject a generat economii directe anuale de aproximativ 12.000 EUR și a eliminat eforturile recurente asociate licențierii și achiziției publice aferente, fără a compromite funcționalitățile esențiale de securitate a informației, de management al proiectelor și bună guvernanță.

3.2.9 Implementarea platformelor pentru managementul resurselor umane

În contextul actual al evoluțiilor tehnologice și al creșterii complexității activităților organizaționale, eficientizarea managementului resurselor umane a devenit o prioritate pentru DNSC, care a implementat în 2025 sistemul integrat **One** care este un sistem profesional și modern pentru gestionarea resurselor umane și pentru îmbunătățirea eficienței operaționale, optimizarea resurselor și creșterea performanței.

Suplimentar, pentru consilierea eficientă în carieră, pentru creșterea nivelului de randament al personalului din cadrul DNSC și în vederea asigurării unui nivel optim de competență în ceea ce privește îndeplinirea obiectivelor individuale și instituționale, Directoratul a implementat și platforma computerizată de evaluare psihologică **Cognitrom Assessment System (CAS++)**. CAS++ reprezintă o platformă software de teste psihologice offline, de evaluare psihologică a adulților, cu posibilitatea utilizării pentru evaluări individualizate, pentru selecție și recrutare de personal sau pentru consiliere în carieră. CAS++ este acreditat de Colegiul Psihologilor din România (COPSI) pe o perioadă nedeterminată și sistemul de evaluare CAS++ conține peste 50 de teste psihologice adaptate și etalonate pe populația din România, grupate în cinci categorii principale: aptitudini cognitive, aptitudini non-cognitive, personalitate și atitudini, emoții și comportamente, interese și valori.

3.2.10 Alte activități strategice și de bună guvernanță proprie a DNSC

Pe parcursul anului 2025, experții din cadrul Directoratului au contribuit în mod activ la consolidarea cadrului de guvernanță internă, la susținerea proceselor instituționale și la fundamentarea deciziilor strategice în domeniul tehnologiei informației, prin următoarele activități:

- Inițierea, elaborarea și contribuția substanțială la definirea și actualizarea politicilor interne privind utilizarea dispozitivelor personale în regim BYOD, precum și a politicii de casare a patrimoniului și a echipamentelor DNSC, în vederea alinierii la cerințele de securitate, conformitate și bune practici.
- Furnizarea de expertiză tehnică și consultanță de specialitate în procesul de armonizare a politicilor IT cu obiectivele strategice ale instituției.
- Participarea activă, în calitate de membri sau experți tehnici, în comisiile de concurs, asigurând suport tehnic și operațional pentru desfășurarea corectă și transparentă a procedurilor de selecție.
- Participarea în comisiile de recepție a bunurilor, echipamentelor IT, soluțiilor software și licențelor, cu rol în verificarea conformității tehnice și a respectării cerințelor contractuale.
- Coordonarea și realizarea procesului de mutare, reinstalare și operaționalizare a infrastructurii IT&C din sediul vechi în sediul nou, incluzând echipamentele de rețea, serverele și sistemele de stocare, cu asigurarea continuității serviciilor critice și minimizarea timpilor de indisponibilitate.
- Stabilirea și operaționalizarea de grupuri de lucru ale DNSC în vederea derulării de activități de sprijin tehnic și non-tehnic către Republica Moldova și Ucraina.
- Gestionarea a peste 400 de documente clasificate, cu nivel de clasificare maximum Strict Secret, cu respectarea normelor de protecție și confidențialitate în vigoare.

3.2.11 Programul intern „Train the Cyber Security Expert to become a Cyber Security Leader”

Începând cu anul 2024, în cadrul Directoratului s-a implementat programul intern de training **„Train the Cyber Security Expert to become a Cyber Security Leader”** adresat personalului instituției. Scopul acestuia vizează îmbunătățirea performanțelor profesionale ale angajaților, dezvoltarea de noi competențe corelate cu evoluția domeniului securității cibernetice, facilitarea accesului personalului DNSC la perfecționare continuă, precum și menținerea unui climat optim în cadrul echipei.

Pe parcursul anului 2025 au avut loc **zece sesiuni de pregătire** pentru personalul DNSC, cu o **participare medie de 90 de persoane (în format fizic și online),** pe teme precum: Directiva NIS2, Open Source Intelligence - OSINT, programul de conștientizare AR-in-a-Box al ENISA, penetration testing, utilizarea de aplicații/platforme pentru gestionarea documentelor, comunicare cu impact în spațiul public, GDPR, Inteligența artificială, ransomware și impactul atacurilor cibernetice.

Sesiunile de pregătire au fost susținute atât de lectori din cadrul Directoratului dar și de experți în securitate cibernetică din afara instituției, invitați din partea mediului de afaceri, din alte instituții publice ori din mediul academic. Abordarea DNSC este că investiția în perfecționarea continuă a propriului personal este imperios necesară pentru obiectivelor instituției.

3.2.12 Testarea și implementarea soluțiilor de Inteligență Artificială (AI) la nivelul DNSC

Înființată în a doua jumătate a anului 2025, echipa multidisciplinară de Inteligență Artificială (AI) a Directoratului a desfășurat activități de cercetare, evaluare și implementare a soluțiilor bazate pe modele lingvistice mari **(Large Language Model - LLM)** în infrastructura internă a instituției. A fost elaborat un raport tehnic privind integrarea LLM-urilor de tip open-source pe serverul intern echipat cu GPU NVIDIA L40S (48 GB VRAM), cu o foaie de parcurs etapizată pentru implementare, validare și securizare.

Pe latura operațională, DNSC a configurat o infrastructură locală proprie pe care rulează o serie de modele open-source selectate în funcție de cazurile de utilizare identificate, printre care:

- Modele de uz general (Llama 3.1, Llama 3, Mistral, Mixtral 8x7B, Qwen 2.5 și Qwen 3).
- Modele specializate pentru generarea de cod (CodeLlama, Yi-Coder, DeepSeek-R1 32B).
- Modele de embeddings și similaritate semantică (BGE-M3, Nomic-Embed-Text, All-MiniLM).
- Un model de traducere (TranslateGemma).
- Un model de extracție structurată (nuextract:latest 3.8B).
- Un model cu capabilități de procesare vizuală (Granite 3.2 Vision).

Au fost configurate două medii distincte, dezvoltare și respectiv producție, cu roluri diferențiate pe direcții și structuri interne ale DNSC.

În urma elaborării unor analize SWOT comparative pentru platformele Dify și n8n, echipa AI a Directoratului a optat pentru tehnologia n8n ca soluție principală de automatizare a fluxurilor de lucru interne.

Ca rezultat concret al activității de automatizare, echipa a implementat două fluxuri operaționale funcționale în n8n, care rulează în mod independent și livrează zilnic, prin e-mail, la ora 07:01, un raport consolidat către destinatarii relevanți din cadrul instituției: primul constă într-un raport automat de threat intelligence care agregă și prioritizează vulnerabilitățile critice din sursele NIST NVD, ENISA EUVD și CWE Database, semnalând inclusiv vulnerabilitățile confirmate ca exploatate activ (CISA KEV).

Al doilea flux operațional implementat constă într-un buletin informativ generat prin monitorizarea automată a comunităților de specialitate, din care un LLM local extrage și sintetizează punctele cheie relevante pentru DNSC, precum noi vulnerabilități publicate, instrumente open-source emergente și tendințe în domeniul inteligenței artificiale și al automatizării.

Implementarea acestor soluții de inteligență artificială (AI) reprezintă un pas concret în direcția reducerii costurilor, a modernizării și eficientizării activității operaționale a DNSC.

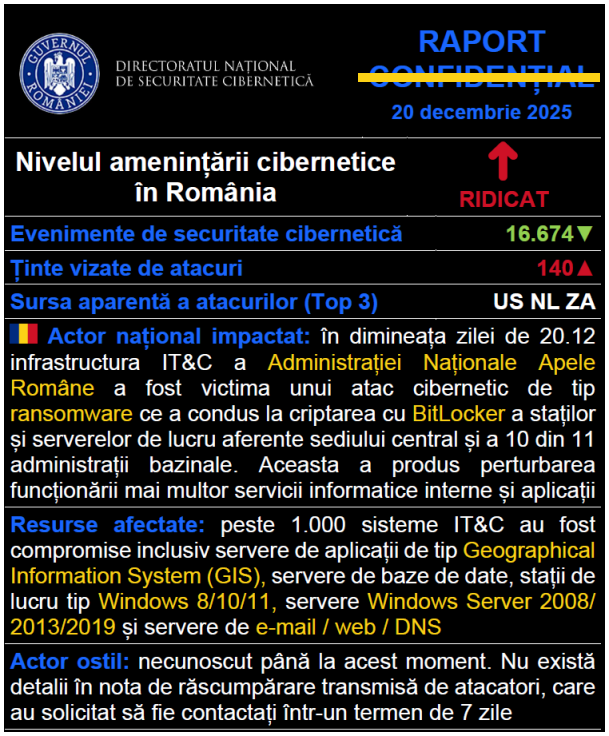
3.2.13 Acord cu ADR pentru migrarea, integrarea și interconectare în Cloud-ul Privat Guvernamental a platformei PNRISC

În decembrie 2025, Directoratul a semnat cu Autoritatea pentru Digitalizarea României (ADR) un acord în vederea migrării, integrării și interconectării în cloudul privat guvernamental a **Platformei Naționale pentru Raportarea Incidentelor de Securitate Cibernetică (PNRISC).**

Această inițiativă comună a DNSC și ADR va conduce la optimizarea costurilor de operare ale platformei, dar și la creșterea nivelului de performanță tehnică, al rezilienței acesteia în fața atacurilor cibernetice, precum și sporirea masurilor sale de securitate (confidențialitate, integritate, disponibilitate).

3.2.14 Buletine de informare (cyber dashboard) destinate factorilor de decizie naționali

Similar anului 2024, în vederea consolidării și actualizării nivelului de conștientizare la nivel înalt privind starea de securitate cibernetică, **au fost întocmite 248 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 2025, a fost astfel:


DIRECTORATUL NAȚIONAL DE SECURITATE CIBERNETICĂ

RAPORT CONFIDENȚIAL

20 decembrie 2025

Nivelul amenințării cibernetice în România	↑ RIDICAT
Evenimente de securitate cibernetică	16.674▼
Ținte vizate de atacuri	140▲
Sursa aparentă a atacurilor (Top 3)	US NL ZA

Actor național impactat: în dimineața zilei de 20.12 infrastructura IT&C a Administrației Naționale Apele Române a fost victima unui atac cibernetic de tip ransomware ce a condus la criptarea cu BitLocker a stațiilor și serverelor de lucru aferente sediului central și a 10 din 11 administrații bazinale. Aceasta a produs perturbarea funcționării mai multor servicii informatice interne și aplicații

Resurse afectate: peste 1.000 sisteme IT&C au fost compromise inclusiv servere de aplicații de tip Geographical Information System (GIS), servere de baze de date, stații de lucru tip Windows 8/10/11, servere Windows Server 2008/ 2013/2019 și servere de e-mail / web / DNS

Actor ostil: necunoscut până la acest moment. Nu există detalii în nota de răscumpărare transmisă de atacatori, care au solicitat să fie contactați într-un termen de 7 zile

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

Notă: raportul ilustrativ din figură nu mai are un caracter confidențial. Informațiile din acesta au devenit publice între timp.

3.2.15 Menținerea și gestionarea capacitaților tehnice proprii

Din punctul de vedere al infrastructurii tehnice proprii, Directoratul a depus toate diligențele pentru asigurarea funcționării optime și cu costuri scăzute a infrastructurii IT&C din 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 optimizarea arhitecturii, managementul și dezvoltarea rețelelor, platformelor informatice și sistemelor de comunicații la nivel instituțional. 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 2025 au fost instalate, configurate și administrate un număr de aproximativ 248 de servere dintre care 216 de servere virtuale, 204 calculatoare și laptop-uri, respectiv 60 de alte tipuri de echipamente (tablete, telefoane) utilizate în mod curent de către personalul DNSC.

3.2.16 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.

3.3 Implementarea de proiecte în domeniul securității cibernetice

3.3.1 Dezvoltarea de capabilități cibernetice naționale prin implementarea de proiecte

În 2025, prin implementarea unui portofoliu diversificat de proiecte finanțate prin programe, instrumente, mecanisme, fonduri naționale, europene sau internaționale, precum și a celor finanțate prin Planul Național de Redresare și Reziliență (PNRR) al României, DNSC a contribuit la dezvoltarea de capabilități și competențe cibernetice, la creșterea rezilienței, la adoptarea de soluții și tehnologii inovatoare pentru răspunsul la incidente, protecția infrastructurilor critice și a societății digitale.

DNSC a continuat implementarea strategiei sale privind proiectele din domeniul securității cibernetice și a accentuat trecerea de la gestionarea unui set de inițiative punctuale la dezvoltarea unui portofoliu robust și coerent de proiecte, orientat către impact, sustenabilitate și valoare publică. Comparativ cu anul 2024, în 2025 Directoratul a acționat ca **inițiator, arhitect și catalizator** de inițiative strategice cu impact direct asupra securității cibernetice naționale și s-a concentrat pe:

- Creșterea ponderii proiectelor în care DNSC are roluri de coordonare, leadership sau influență decizională în pachetele de lucru, activitățile proiectelor, rezultatele scontate, diseminare etc.
- Orientarea către proiecte multi-anuale, multi-partener și multi-stat, precum și către proiecte cu impact de nivel național sau regional.
- Consolidarea portofoliului de proiecte în jurul unor axe tematice prioritare (reziliență, capacități operaționale, educație cibernetică, politici europene, infrastructuri critice).
- Integrarea proiectelor în obiectivele instituționale și selectarea acestora în funcție de nevoile operaționale ale DNSC, de obiectivele strategice asumate la nivel instituțional precum și de contribuția la dezvoltarea de capabilități cibernetice sustenabile.

Un pilon important al activității din 2025 a fost **gestionarea relației cu finanțatorii, agențiile europene și consorțiile internaționale**. DNSC este prezent în 24 de consorții cu proiecte în curs de implementare, alături de 170 de parteneri din România și Europa. Directoratul a asigurat:

- Respectarea cerințelor contractuale și a regulilor de implementare.
- Comunicarea constantă și predictibilă cu finanțatorii.
- Gestionarea modificărilor, clarificărilor și situațiilor neprevăzute.
- Reprezentarea coerentă și profesionistă a intereselor DNSC în cadrul proiectelor.

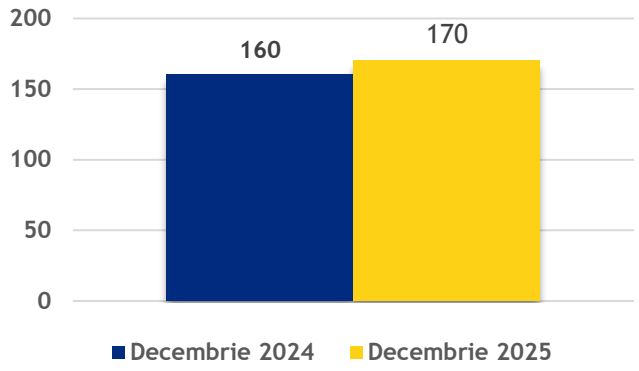


Figura 15 - Număr parteneri în proiectele DNSC

Această activitate a consolidat reputația DNSC ca **partener de încredere**, capabil să gestioneze proiecte complexe și să livreze rezultate conforme și relevante. Comparativ cu anul 2024, un indicator-cheie îl reprezintă rolul asumat de DNSC în cadrul proiectelor, prin creșterea ponderii proiectelor în care Directoratul a avut rol de lider de pachete de lucru sau partener strategic și diminuarea îndeplinirii de către Directorat a unor roluri eminamente tehnice sau secundare.

3.3.2 Proiecte de securitate cibernetică cu finanțare națională

În 2025, Directoratul a continuat proiectul pentru implementarea **Măsurii 184 - PNRR, Crearea de noi competențe de securitate cibernetică pentru societate și economie** – finanțat din cadrul Investiției I15, Componenta C7, Pilonul II transformare digitală din PNRR. Proiectul intenționează să genereze următoarele rezultate:

- Evaluarea nivelului de maturitate cibernetică pentru 1.000 de entități publice și private.
- Dezvoltarea unui set coerent de instrumente de sprijin pentru îmbunătățirea securității.
- Crearea unui model replicabil de formare și evaluare, aliniat practicilor europene.

Un element definitoriu al anului 2025 a fost **pregătirea propunerilor de proiecte**, cu o valoare cumulată a bugetului DNSC de **34.501.623 LEI**.

Proiecte precum **SmartGovEdu** și **SmartNIS** reflectă o schimbare de paradigmă:

- De la proiecte punctuale la ecosisteme digitale și cibernetice integrate.
- De la inițiative izolate la platforme naționale cu impact sistemic.

În anul 2025, DNSC a pregătit **propunerile de finanțare pentru proiectele SmartGovEdu și SmartNIS**, care sunt în curs de evaluare / aprobare a finanțării și a căror implementare poate începe în anul 2026.

Proiectul SmartGovEdu: Educația ca serviciu public esențial – cu un buget total de 71.601.754 LEI, din care finanțarea solicitată de către DNSC este de 11.618.608 LEI (cofinanțarea este 0 LEI). Consorțiul este format din DNSC, Palatul Național al Copiilor (subordonat Ministerului Educației și Cercetării) și Centrul Proedus (instituție subordonată Primăriei Municipiului București). Obiectivul general al proiectului este de a crea și implementa o platformă integrată de e-guvernare dedicată educației ca serviciu public esențial.

Proiectul SmartNIS: Digitalizarea proceselor pentru implementarea Directivei NIS2 și consolidarea spațiului cibernetic național – finanțarea solicitată de către DNSC este de 22.883.015 LEI (cofinanțarea este 0 LEI). DNSC este unic solicitant. Obiectivul general al proiectului SmartNIS constă în digitalizarea proceselor pentru implementarea Directivei NIS2 (implementată în România prin OUG nr. 155/2024).

În aceste propuneri, DNSC a acționat **ca inițiator** prin definirea unor concepte de proiect care nu existau anterior în peisajul instituțional național. Propunerile de proiect **SmartGovEdu și SmartNIS** nu au fost simple răspunsuri la apeluri de finanțare, ci au pornit de la **identificarea unor lacune sistemice** – lipsa unei infrastructuri digitale integrate pentru implementarea Directivei NIS2 sau absența unei platforme naționale care să trateze educația digitală ca serviciu public esențial.

DNSC a identificat problema, a construit viziunea și a transpus-o în obiective, arhitecturi funcționale și mecanisme de implementare, asumând rolul de promotor al schimbării. Aceste activități au consolidat poziția DNSC ca **instituție capabilă să atragă și să gestioneze fonduri semnificative**, într-un mod inovator, pentru domeniul de competență al instituției. 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.

3.3.3 Proiecte de securitate cibernetică cu finanțare internațională

Prin activitatea sa, Directoratul a contribuit decisiv la **transformarea abordării proiectelor cu finanțare din fonduri europene și internaționale dintr-un obiectiv în sine într-un mijloc de consolidare a securității cibernetice la nivel național**, poziționând DNSC ca instituție activă, matură, credibilă și relevantă în plan european.

Dacă anul 2024 a fost caracterizat drept un an de acumulare accelerată de proiecte, de experiență și de stabilire de parteneriate și mecanisme de lucru în mod proiect, **anul 2025 marchează o schimbare de paradigmă** în modul în care DNSC a abordat managementul acestor proiecte.

Diferența esențială dintre cele două perioade nu constă exclusiv în numărul sau bugetele proiectelor realizate, ci în modul de **integrare strategică a proiectelor în arhitectura instituțională a DNSC și în sprijinirea obiectivelor de securitate cibernetică la nivel național.**

Criteriu	Trend 2025 vs. 2024
Creștere portofoliu / expansiune	↘
Acumulare experiență	↗
Integrare strategică	↗
Leadership și roluri	↗
Orientare către impact	↗
Maturitatea proceselor și a cadrului de guvernanță	↗

În anul 2025 Directoratul s-a concentrat pe o poziționare mult mai competitivă în cadrul consorțiilor europene, și și-a atins obiectivul de a nu a fi perceput numai ca beneficiar sau participant tehnic, ci și ca un partener strategic, cu contribuție la:

- Definirea obiectivelor generale și a celor specifice ale proiectelor.
- Definirea arhitecturii și guvernanței proiectelor.
- Dezvoltarea și implementarea de soluții și tehnologii cu relevanță la nivel european.

Această evoluție reflectă nu doar maturizarea Directoratului, ci și creșterea capitalului de încredere al acestuia în relația cu partenerii europeni și instituțiile UE.

La finalul anului 2025, în portofoliul DNSC figurau 25 de proiecte cu finanțare din fonduri europene și internaționale (dintre care 24 în format de consorțiu). Toate aceste proiecte au fost inițiate, derulate și gestionate nu doar din perspectiva conformității contractuale, ci și a impactului instituțional, a relevanței pentru spațiul cibernetic național civil și a valorii adăugate pentru ecosistemul național.

Tabel 5 - Proiecte cu finanțare internațională aflate în derulare la nivelul DNSC în 2025

Nr.	Acronim	Denumire proiect	Buget total EUR	Buget DNSC EUR
1.	SIEMBIOT	Modular, open, research platform integrating SIEM, NOC, SOC, CTI and Vulnerability Management	3.358.195	538.210
2.	CYRESRANGE	Cyber Ranges Resiliency Networks	1.746.240	65.912
3.	CYDERCO	CYber DEtection, Response and COllaboration	2.881.082	819.192
4.	5G-TACTIC	5G Trusted And seCure network servICes	5.211.184	241.606
5.	SECUR-EU	Enhancing Security of European SMEs in Response to Cybersecurity Threats	3.777.100	230.585
6.	INTERSOC	INTERconnected Security OperatIon Centres	6.566.561	475.080
7.	ENSOC	ENSOC-CROSSBORDER PLATFORM	10.360.557	1.165.230
8.	ECYBRIDGE	Strengthening Synergies in Defence and Civilian Cybersecurity	2.493.118	165.208
9.	CYSSDE	CyberSecurity Deplopyment Preparedness Support, Capacity & Capabilities	6.984.087	228.445
10.	aSIEMmetry	Employ entropy models to pre-emptively detect novel risks for monitored SIEM assets and enhance SOC processes and analysts leveraging AI capabilities	1.461.299	370.434
11.	ACSOC	Advanced Cooperative Security Operation Centres	3.037.730	400.608
12.	CYBERGUARD	Fortifying SOCs Against Evolving Cyber Threats	7.690.250	481.500
13.	EU-INSPIRE	INnovative multi-diSciPlinary Industry-focused cybersecurity education for upskilling and ReskIlling the EU workforcE	19.477.569	289.756

Nr.	Acronim	Denumire proiect	Buget total EUR	Buget DNSC EUR
14.	SAFE	Security AI for Enhanced SOC	7.998.210	692.504
15.	CONFIRMATE	CONFormIty assessment, metRics and compliance autoMATion for the cyber resiliencE act	1.934.132	447.902
16.	CRA-AI	The CRA-AI - 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	2.873.164	177.834
17.	ENDURANCE	Strategies and Services for Enhanced Disruption Resilience and Cooperation in Europe	4.999.776	119.250
18.	TRUSTBOOST	Unifying & Upgrading Certification Capabilities Across Europe	3.169.019	243.960
19.	CYBERFORT	Strengthening Cyber Defenses of SMEs for Cyber Resilience Act (CRA) Compliance	3.728.629	315.008
20.	CTIS4NIS	CyberThreat Information Sharing enabling Network and Information systems Security in the EU	5.087.315	390.764
21.	CYBER-BRIDGE	Building Cross-Border Cybersecurity and Compliance for a Safer Digital Europe	5.839.899	702.348
22.	DYNABIC	Dynamic business continuity of critical infrastructures on top of adaptive multi-level cybersecurity	4.999.695	151.000
23.	RO-CCH	Romanian Cyber Care Health	578.870	578.870
24.	DNS4EU	The DNS4EU and European DNS Shield	6.173.310	203.600
25.	INFORB	Implementation of the NIS Directive in the sector production, processing and distribution of Food in Romania and Bulgaria	1.105.598	455.820

Proiectele în implementare în 2025 la nivelul DNSC se concentrează, în principal, pe:

- Creșterea rezilienței serviciilor critice europene în urma atacurilor cibernetice și fizice avansate.
- Sprijinirea rezilienței securității cibernetice în sistemul de sănătate din România.
- Consolidarea suveranității tehnologice europene prin oferirea unei alternative îmbunătățite pentru serverele DNS în Europa.
- Consolidarea funcției de autoritate competentă a DNSC în sectorul producției, prelucrării și distribuției alimentelor în România și Bulgaria.
- Creșterea rezistenței naționale și regionale împotriva atacurilor cibernetice prin integrarea evaluării continue a vulnerabilității în procesele tehnice de tip SIEM, NOC și SOC.
- Consolidarea capacităților poligoanelor cibernetice existente și crearea unei rețele de Centre de Excelență în Securitate Cibernetică.
- Dezvoltarea unei platforme pentru îmbunătățirea capacităților de detectare și răspuns la amenințările cibernetice.
- Dezvoltarea de soluții 5G sigure și interoperabile, cu accent pe securitate cibernetică și încredere.
- Crearea unui punct central pentru informațiile despre amenințările cibernetice la scară largă.
- Îmbunătățirea securității cibernetice a IMM-urilor și a infrastructurilor critice, promovând o cultură de conștientizare și dezvoltând soluții open-source.
- Îmbunătățirea pregătirii pentru perturbări, reziliența infrastructurilor digitale și consolidarea capacităților prin previziunea amenințărilor, detectarea și răspunsul la incidente cibernetice.

- Crearea unui cadru și implementarea unei rețele comune pentru sprijinirea echipelor de tip CERT/CSIRT europene în detectarea, partajarea, răspunsul și recuperarea în urma amenințărilor de securitate cibernetică și a vulnerabilităților sistemelor informatice.
- Consolidarea securității cibernetice și a confidențialității prin oferirea unui cadru holistic pentru evaluarea riscurilor de securitate cibernetică.
- Dezvoltarea competențelor în securitate cibernetică pentru elevi, studenți și actori publici și privați.
- Abordarea provocărilor vulnerabilităților cibernetice cunoscute și sprijinirea îmbunătățirii rezilienței cibernetice a operatorilor de servicii esențiale și IMM-urilor.
- Sprijinirea conformării producătorilor, în special a IMM-urilor, cu cerințele Cyber Resilience Act (CRA), prin dezvoltarea unei platforme software automatizate, bazate pe inteligență artificială, care să acopere integral procesul de evaluare, certificare, monitorizare și menținere a marcajului CE pentru securitate cibernetică.
- Consolidarea sinergiilor în domeniul apărării și al securității cibernetice civile.

În anul 2025, Directoratul a elaborat, depus și coordonat un număr de 16 propuneri de proiecte - cu un buget total al DNSC de 5.600.000 EUR și implicând 230 de parteneri unici - în cadrul programelor **Digital Europe Programme (DEP)** și respectiv **Horizon Europe (HE)** – aceste propuneri sunt aflate în prezent în etapa de evaluare la nivelul Comisiei Europene.

Cu titlu de exemplu ilustrativ, **proiectul ECYBRIDGE** www.ecybridge.eu își propune să consolideze coordonarea și sinergia dintre sectoarele civil și de apărare din domeniul securității cibernetice, sporind rezistența Europei împotriva amenințărilor emergente.

Proiectul ECYBRIDGE reunește 17 parteneri din țări membre UE, din sectorul public, privat și din mediul academic, având o durată de implementare de 24 luni, iar principalele activități ale proiectului sunt concentrate pe crearea de capabilități prin: exerciții de tip Table Top Exercise (TTX), rapoarte de tip whitepaper, mese rotunde, conferințe specializate și ateliere de lucru, crearea unei rețele de beneficiari specializați, sesiuni de training cu lectori specializați internaționali, precum și diseminare, exploatare și inovare în managementul securității cibernetice.

Figura 16 – Conferința de la Constanța a proiectului ECYBRIDGE

În plus, ca parte a proiectului **ECYBRIDGE** ce urmărește crearea de sinergii între sectoarele civil și militar, DNSC a participat în 2025 la organizarea unui exercițiu de tip **Table Top Exercise (TTX)** pentru evaluarea eficacității măsurilor actuale de securitate cibernetică, dar și pentru identificarea lacunelor și a

oportunităților de inovare, contribuind astfel semnificativ la reziliența securității cibernetice a Uniunii Europene.

Nu în ultimul rând, ca efort susținut pe care DNSC îl realizează în îndeplinirea funcției de cercetare-dezvoltare, precum și a celei de educație și pregătire în domeniul securității cibernetice, Directoratul a coordonat prin proiectul **ECYBRIDGE** activitatea de scriere a unui ***White Paper*** de importanță strategică la nivel european, intitulat ***Perspective cuprinzătoare privind securitatea cibernetică: Reflecții și recomandări privind dinamica actuală a securității cibernetice în Uniunea Europeană***.

Documentul își propune să ofere un cadru strategic și îndrumări practice pentru a consolida cooperarea în domeniul securității cibernetice între sectoarele civil și de apărare din UE.

White Paper-ul urmărește să ofere factorilor de decizie o viziune practică și o foaie de parcurs structurată pentru realizarea unei Europe digitale sigure și unificate. Aceste inițiative servesc nu numai la consolidarea securității infrastructurilor critice, ci și la promovarea autonomiei strategice a UE în spațiul cibernetic, protejând în același timp drepturile, interesele și securitatea digitală a cetățenilor europeni.

3.3.4 Participarea experților DNSC în proiecte prin formatul TAIEX

Asistența tehnică și schimbul de informații (TAIEX) este un instrument de consolidare a instituțiilor Uniunii Europene, gestionat de **Direcția Generală pentru Extindere și Vecinătate Estică (DG ENEST),** care este o entitate a Comisiei Europene, înființată la 1 februarie 2025, responsabilă pentru gestionarea proceselor de aderare la UE și consolidarea relațiilor cu vecinii estici.

Programul TAIEX oferă asistență specifică pe termen scurt administrațiilor publice prin schimburi inter partes. Instrumentul completează înfrățirea instituțională care sprijină cooperarea instituțională pe termen mai lung prin parteneriate structurate între administrațiile statelor membre și țările beneficiare.

Directoratul furnizează personal propriu în calitate de experți TAIEX în domeniul securității cibernetice și în alte domenii conexe acestuia. În această calitate, experții DNSC își împărtășesc experiența cu omologii lor din țările partenere TAIEX (ex. Republica Moldova, Albania, Bosnia și Herțegovina, Ucraina, Armenia, Azerbaidjan, Macedonia de Nord, Muntenegru, Turcia). Suplimentar, DNSC încurajează și sprijină activ specialiștii români pentru a se înscrie și a participa ca experți în programul TAIEX.

Această contribuție a Directoratului la programul TAIEX contribuie, de asemenea, la o reformă mai amplă a sectorului public în domenii precum securitatea cibernetică, Inteligența Artificială, transformarea digitală, reziliența la schimbările climatice, sănătatea publică, guvernanța economică și îmbunătățirea mediului de afaceri.

3.4 Conștientizare, cultură și educație în domeniul securității cibernetice

3.4.1 Campanii, evenimente și proiecte de conștientizare

Pe parcursul anului 2025, DNSC a implementat o serie de activități de comunicare strategică și conștientizare, desfășurate în colaborare cu entități relevante din sectorul public, privat și mediul academic. Demersurile au vizat direcții prioritare precum derularea de campanii tematice pe rețelele de socializare și inițiative dedicate educării publicului, participarea la evenimente de profil, precum și apariții în cadrul emisiunilor TV, radio, podcasturi audio sau video.

Pentru creșterea nivelului de pregătire a publicului larg pe domeniul securității cibernetice, au fost implementate o serie de campanii tematice de conștientizare, care au abordat, în mod integrat, principalele riscuri și tendințe din mediul online care afectau, la acel moment, spațiul cibernetic național civil, după cum urmează:

- **Principalele tipologii de fraude și amenințări online:** fraude asociate cumpărăturilor online prin utilizarea site-urilor false și a mesajelor de phishing, fraude care vizează compromiterea și deturnarea conturilor utilizatorilor (**account takeover**), fraude cu specific romantic bazate pe inginerie socială (**romance scam**), amenințări facilitate de instrumente bazate pe AI, cu accent sporit pe materiale audio-video falsificate (**deepfake**), fraude propagate prin concursuri și promoții false în mediul online, fraude specifice perioadei vacanțelor, realizarea de materiale audio-video dedicate fraudelor de tip **vishing** și **spoofing**, riscurile cibernetice asociate perioadei Black Friday, metodele de fraudă specifice sezonului sărbătorilor de iarnă.
- **Campanii de conștientizare cibernetică și educație digitală:**
    - Bune practici de securitate online, inclusiv verificarea regulată a securității dispozitivelor și a conturilor de utilizator.
    - Conștientizare de tip ***Mit vs. Realitate*** pentru combaterea informațiilor eronate din domeniul securității cibernetice.
    - Transmiterea de mesaje de interes public difuzate de televiziuni din România.
    - Privind fenomenul **fake news**, utilizarea site-urilor false și metode de recunoaștere a dezinformării, folosite cu scopul propagării atacurilor.
    - Măsuri de igienă cibernetică dedicate elevilor și studenților.
    - Securitatea dispozitivelor mobile.
    - Protecția și recuperarea conturilor de social media.
    - Dezvoltarea și promovarea campaniei naționale de conștientizare ***Siguranța Online*** împreună cu **Poliția Română și Asociația Română a Băncilor (ARB)**.

Pe parcursul anului 2025 DNSC a emis comunicări publice către cetățeni, entități de presă, parteneri instituționali și alte autorități relevante, în vederea informării corecte a acestora în cazul unor incidente de securitate cibernetică semnificative. Directoratul a oferit și sprijin entităților afectate pentru gestionarea comunicării în cazul incidentelor de securitate cibernetică, spre exemplu către: **Orange România SA, Aaylex One SA (CocoRico) și Administrația Națională Apele Române (ANAR)**.

În paralel, pentru întărirea cooperării interinstituționale și extinderea parteneriatelor strategice în domeniul comunicării publice în domeniul securității cibernetice, au fost desfășurate o serie de activități menite să sprijine coordonarea mesajelor, creșterea coerenței comunicării publice și susținerea inițiativelor comune de informare și conștientizare.

Un exemplu este sprijinul oferit în procesul de comunicare publică și conștientizare pentru **Agenția de Securitate Cibernetică (ASC)** din Republica Moldova, în context electoral, în vederea susținerii unui demers instituțional coerent și credibil. În acest sens, au fost formulate recomandări privind structura și calendarul comunicării, precum și sprijin pentru elaborarea materialelor de conștientizare axate pe igienă cibernetică, phishing, tentative de fraudă și utilizarea responsabilă a platformelor online, dar și combaterea dezinformării.

Directoratul a planificat și organizat în 2025 o serie de evenimente, vizite, ateliere și dezbateri, având scopul de a crește nivelul de conștientizare asupra riscurilor și pericolelor existente în mediul online, diseminarea de bune practici și prezentarea oportunităților de carieră în domeniul securității cibernetice:

- DNSC a organizat 10 workshop-uri sectoriale pentru evaluarea riscurilor cibernetice cu participarea reprezentanților din sectoarele prevăzute în OUG nr. 155/2024: transport rutier, administrație publică centrală și locală, educație, sănătate, apă potabilă, energie, infrastructură digitală, servicii poștale și producție alimentară. Rezultatele au inclus liste de riscuri prioritizate, rapoarte de evaluare și recomandări sectoriale specifice. În cadrul acestor sesiuni au fost prezentate:
    - Rezultatele evaluărilor sectoriale privind riscurile cibernetice.
    - Aspecte specifice managementului riscurilor cibernetice, inclusiv metodologii și bune practici.
    - Platforme și instrumente de management al riscurilor cibernetice, menite să sprijine implementarea măsurilor de securitate la nivelul entităților vizate.
    - Strategii regionale de reziliență cibernetică și modalitățile de implementare practică a politicilor publice în domeniul securității cibernetice.
- DNSC a desfășurat în cursul anului o serie de prezentări și activități de diseminare la nivel național, având ca obiective principale promovarea aliniamentului la standardele internaționale și la cele mai bune practici din industrie în domeniul managementului riscurilor de securitate cibernetică, precum și asigurarea informării și pregătirii populației și a entităților din spațiul cibernetic civil național, inclusiv a operatorilor economici din sectoarele prevăzute de OUG nr. 155/2024 și din sectorul public.
- DNSC a găzduit întâlniri și sesiuni de lucru cu instituții publice și organizații din sectoarele prevăzute în Directiva NIS2, în cadrul cărora au fost discutate aspecte privind cooperarea în gestionarea incidentelor de securitate cibernetică. În baza acestor interacțiuni au fost formulate și transmise recomandări specifice, adaptate particularităților fiecărei entități, având ca obiectiv creșterea nivelului de conștientizare în domeniul securității cibernetice, înțelegerea obligațiilor și responsabilităților legale, precum și evaluarea și îmbunătățirea nivelului de maturitate cibernetică.
- În 2025 s-au efectuat demersuri susținute ce au facilitat stabilirea și consolidarea canalelor de comunicare operațională, inclusiv desemnarea punctelor de contact, contribuind la eficientizarea cooperării și la asigurarea unui răspuns coordonat în cazul producerii unor incidente de securitate cibernetică. În total, au fost implicate **7 instituții** și **23 organizații**, consolidând astfel rețeaua de colaborare și schimb de bune practici.
- Urmare a demersurilor inițiate în 2024 pentru includerea României în proiectul pilot **AR-in-a-Box+** organizat de ENISA, Directoratul a implementat efectiv, la nivel intern, metodologia dezvoltată de ENISA și a adaptat-o la specificul României. DNSC a organizat și livrat în 2025 sesiuni de training în sectoarele energie, transporturi și justiție. Directoratul a susținut workshopuri pentru dezvoltarea de programe de conștientizare adaptate organizațiilor lor pentru **Ministerul Energiei, Autoritatea Aeronautică Civilă Română (AACR), Administrația Națională a Penitenciarelor (ANP) și Autoritatea pentru Reformă Feroviară (ARF)**. Acest demers a avut ca obiectiv sprijinirea organizațiilor implicate în definirea și implementarea de programe interne de conștientizare în domeniul securității cibernetice - activitate ce va fi continuată și pe parcursul anului 2026.
- În 2025, DNSC a organizat **două webinarii naționale de referință dedicate administrației publice centrale și locale**, cu impact direct asupra creșterii rezilienței cibernetice instituționale. **Primul webinar *De la Zero la Rezilient* (septembrie 2025)** a reunit aproximativ 700 de instituții publice, oferind o abordare practică și unitară pentru aplicarea cerințelor NIS2/OUG nr. 155/2024 și pentru dezvoltarea capacităților operaționale de securitate cibernetică**. Al doilea webinar, *Securitate cibernetică în instituțiile publice – NIS2* (decembrie 2025)** a înregistrat participarea a circa 1.000 de instituții publice, contribuind la alinierea la nivel național a interpretării obligațiilor legale, la consolidarea guvernanței în domeniu și la promovarea unor soluții tehnice eficiente. Prin aceste acțiuni, DNSC a facilitat tranziția de la conformitate formală la consolidarea efectivă a capacităților de securitate cibernetică în sectorul public din România.

- De asemenea, DNSC a organizat sesiuni de consultare săptămânale cu scopul de a facilita aplicarea OUG nr. 155/2024. Astfel, în cadrul sesiunilor organizate (12) conform cererilor înregistrate din partea beneficiarilor, au participat un număr de aproximativ 90 de persoane din cadrul societății civile.
- În plus, menționăm inițierea, sub egida programului Support Action, a unei serii naționale de workshop-uri, dedicate implementării Directivei NIS2 destinate entităților din domeniile public și privat, primele 9 fiind organizate în anul 2025.
- Conferința CyberMed 2025 – Securitatea Cibernetică în Era Digitalizării Sănătății.
- Conferința Națională a Personalului din Sistemul Sanitar (C.N.P.S.S.), Ediția a XIV-a.
- Zilele Securității Cibernetice – impactul Directivei NIS2 în mediul academic.
- Directoratul a coordonat la nivel național campania ***Luna Europeană a Securității Cibernetice 2025***, activitate de conștientizare desfășurată în fiecare an la nivelul statelor membre ale Uniunii Europene.
- Co-organizarea fazei naționale a Campionatului European de Securitate Cibernetică ROCSC / ECSC ediția 2025, în parteneriat cu Centrul Național Cyberint din cadrul SRI, Asociația Națională pentru Securitatea Sistemelor Informatice (ANSSI), Orange România, Bit Sentinel și Ministerul Educației.
- Co-organizarea Olimpiadei de Securitate Cibernetică (OSC), în parteneriat cu Universitatea Politehnică București (UPB), Centrul Național Cyberint din cadrul SRI, Asociația Națională pentru Securitatea Sistemelor Informatice (ANSSI), Orange România, Bit Sentinel și Ministerul Educației.
- Efectuarea demersurilor pentru organizarea participării echipei României la Olimpiada Internațională de Securitate Cibernetică.
- Găzduirea la București și organizarea împreună cu ENISA a celei de-a 10-a ediții a Conferinței e-health și a Work Streamului pe sănătate 2025.
- Găzduirea la București și coorganizarea ENISA Market and Resilience Conference (Cyber Resilience Act Conference) – 2025.
- Organizarea în cadrul dialogului pe tema strategiei de educație cibernetică a unei mese rotunde cu titlul ***Forging a Whole-of-System Approach: A Strategic Dialogue on Integrating Cybersecurity into the National Education Ecosystem,*** în cadrul BCC2025, cu participarea Ministerului Educației și Cercetării (MEC) și a altor instituții partenere, precum și a partenerilor din mediul privat.
- Organizarea unei mese rotunde pe tema rezilienței în sănătate ***Connected, Exposed, Essential: Rethinking Cyber Resilience in Healthcare,*** în cadrul BCC2025.
- Dezvoltarea de materiale de conștientizare (clipuri video, ghiduri etc) pentru diverse categorii de public (IMM-uri, angajați, publicul larg etc).
- Dezvoltarea de standarde și metodologii pentru activitățile de pregătire în domeniile conștientizării și igienei de securitate cibernetică.
- Elaborarea unui chestionar pentru organizațiile din administrația publică centrală, cu scopul de a fundamenta și calibra măsurile de sprijin oferite autorităților.
- Activități de instruire și conștientizare adresate unor entități din sectoare critice din domeniul sănătății, elaborarea de materiale și suport de prezentare axate pe riscurile și provocările actuale de securitate cibernetică.
- Implicarea în dezvoltarea unor programe educaționale în cadrul formelor obligatorii de învățământ pentru utilizarea sigură a internetului și a echipamentelor de calcul, prin asigurarea de lectori și livrarea materialelor de instruire către aceste categorii de public țintă. Exemple includ Colegiul Economic Virgil Madgearu din București și Colegiul Național Spiru Haret din București.
- Aceste activități au contribuit la creșterea gradului de conștientizare și la consolidarea capacității de prevenire și gestionare a riscurilor și incidentelor cibernetice, atât în sectorul public, cât și în cel privat, consolidând parteneriatele cu actorii relevanți din spațiul cibernetic național civil.

3.4.2 Educație și formare

Totodată, pentru extinderea impactului activităților de conștientizare la nivelul comunităților relevante pentru activitatea DNSC, au fost organizate **sesiuni de educație și formare**, astfel:

- În cooperare cu **Autoritatea Aeronautică Civilă Română (AACR)**, atât în vederea unei bune implementări a prevederilor OUG nr. 155/2024, precum și a cerințelor specifice din domeniul aeronautic, cât și pentru promovarea colaborării inter-instituționale, DNSC a elaborat un program de tip ***formare de formatori*** în domeniul conștientizare și igienă cibernetică și a organizat o sesiune pilot de training pentru entitățile esențiale și importante din sectorul aviației civile.
- Sesiune de pregătire a seniorilor prin intermediul programului Siguranța Online – workshop organizat cu aproximativ 100 de administratori de bloc.
- Sesiuni de pregătire dedicate funcționarilor publici, unde echipa DNSC a oferit recomandări esențiale din zona igienei de securitate cibernetică.
- Sesiuni dedicate elevilor și studenților – licee, Școala de vară de la Galați, Universitatea Catolică, Universitatea Maritimă, Academia de Studii Economice (ASE), Universitatea Politehnică din Timișoara (UPT), Academia Forțelor Terestre, Universitatea Națională de Apărare și Academia Tehnică Militară.
- Organizarea unei sesiuni de educație, formare și conștientizare pentru personalul Hidroelectrica.
- Sesiuni de pregătire profesională dedicate echipei de comunicare din cadrul **Agenției de Securitate Cibernetică (ASC)** din Republica Moldova, axate pe consolidarea vizibilității instituției în social media și oferirea de bune practici din partea DNSC.
- În vederea pregătirii societății civile pentru implementarea actului normativ de transpunere a Directivei NIS2, DNSC a participat la sau a coorganizat peste 15 sesiuni de training și awareness în domeniu împreună cu entități din domeniul privat.
- Au fost organizate întâlniri de lucru cu instituții partenere - în principal cu **Ministerul Apărării Naționale (MApN)** și cu **Serviciul de Pază și Protecție (SPP)** - pentru a facilita schimbul de experiență între experți, formarea acestora și explorarea oportunităților de colaborare în domeniul inteligenței artificiale aplicate în domeniul securității cibernetice.

3.4.3 Platforma educațională CyberSea Festival

DNSC, în parteneriat cu **Women4Cyber Romania**, a lansat platforma educațională **CyberSea Festival**, un concept inovator la nivel național, dedicat formării, orientării și inspirării noii generații către domeniul securității cibernetice. Desfășurat pe parcursul a două zile la Constanța, evenimentul a reunit 450 de participanți, preponderent tineri, care au beneficiat de activități practice, workshop-uri aplicate, sesiuni interactive și competiții tehnice, menite să faciliteze contactul direct cu specialiștii din industrie și cu realitățile operaționale ale domeniului. Prin acest demers, DNSC a contribuit la consolidarea ecosistemului național de competențe cibernetice și la creșterea interesului tinerilor pentru cariere în domeniu, într-un format educațional modern, orientat spre experiență și aplicabilitate practică.

3.4.4 Publicarea de materiale pentru conștientizare și informarea despre securitatea cibernetică

În scopul îndeplinirii funcției DNSC de alertare, prevenire, conștientizare și instruire, precum și în vederea creșterii nivelului de conștientizare a publicului larg cu privire la riscurile de securitate cibernetică și la principalele tipologii de amenințări manifestate în spațiul digital, pe website-ul instituției au fost publicate un total de **20 de ghiduri, analize și materiale informative de actualitate**.

Acestea au avut rolul de a sprijini informarea corectă, prevenirea incidentelor și promovarea bunelor practici de securitate online, având ca tematică:

- Analiza pieței DevSecOps în România.
- Protecția brandului în era digitală.
- Managementul riscurilor de securitate cibernetică.
- Reglementarea platformelor de social media.
- Recomandări pentru securitatea dispozitivelor mobile.
- Analiza incidentului Lazarus – ByBit.
- Analiză blockchain din perspectiva securității cibernetice.
- Securitatea lanțului de aprovizionare software pentru IMM-uri.
- Bune practici pentru politica privind utilizarea rețelelor sociale.
- Ghidul pentru prevenirea și gestionarea amenințărilor din interiorul organizației – transmis către 2.862 primării.
- Ghidul de igienă cibernetică pentru instituțiile publice locale – transmis către 2.862 primării.
- Ghidul de protejare și recuperare a conturilor de social media (actualizat în 2025).
- Integrarea inteligenței artificiale în infrastructura organizațiilor.

În 2025, pe baza experienței tehnice acumulate în perioada alegerilor prezidențiale din România și a celor parlamentare din Republica Moldova, Directoratul a întocmit un raport specializat de identificare și analiză privind o rețea coordonată de **1.188 conturi cu comportament neautentic pe platforma TikTok,** care au manifestat tipare tehnice identice pe parcursul a cinci campanii distincte:

- **Moldova** - 1.088 conturi TikTok - alegerile parlamentare
- **Ucraina** - 95 conturi TikTok – campania #повернітьнашихдодому și alte două extensii regionale
- **Germania -** 5 conturi TikTok - campania Steinmeier

DNSC a detectat, documentat și analizat utilizarea acestor capabilități tehnice și metode similare de serializare și a demonstrat că acestea indică o operațiune centralizată cu resurse substanțiale și capacitate operațională complexă pentru amplificarea artificială a mesajelor politice, în multiple contexte geografice și lingvistice, pe platformele sociale.

3.4.5 Interacțiunea cu mass-media pe subiectul securității cibernetice

În cadrul activității media și social media, pe parcursul anului 2025, Directoratul a înregistrat un număr de **252 de intervenții media** (incluzând materiale în presa scrisă, intervenții radio și TV, participări live și prezențe în format podcast) și 180 de alerte, comunicate de presă, articole și știri. Aceste demersuri au contribuit la creșterea vizibilității instituției și la consolidarea rolului său ca sursă de referință în domeniul securității cibernetice la nivel național și internațional.

Audiența totală a DNSC în 2025, estimată de un operator extern independent, a fost de **389.258.756 de persoane**: 119.671.000 la TV, 252.939.000 la radio, 10.940.756 în online și 5.708.000 în presa centrală.

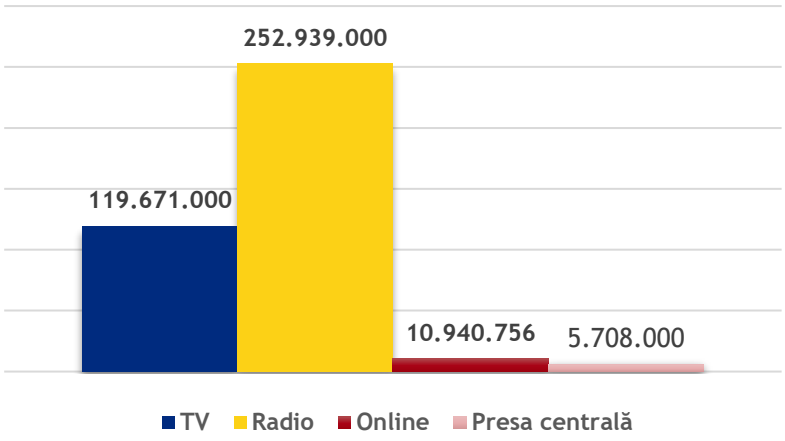


Figura 17 - Audiența DNSC în 2025, pe diferite canale media (număr de persoane)

Valoarea aproximativă estimată 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, ar fi fost de **19.353.791 EUR,** calculată pe baza rate card-urilor specifice fiecărui canal media.

În ceea ce privește împărțirea știrilor în funcție de sentimentul generat de anumite sintagme, negative sau pozitive prezente în articolele monitorizate, **imaginea DNSC în 2025 poate fi evaluată ca fiind majoritar pozitivă** (cu 9.367 de articole pozitive) spre neutră (cu 7.167 de articole neutre).

În anul 2025 au fost înregistrate **doar 7 articole care pot fi considerate negative** la adresa DNSC.

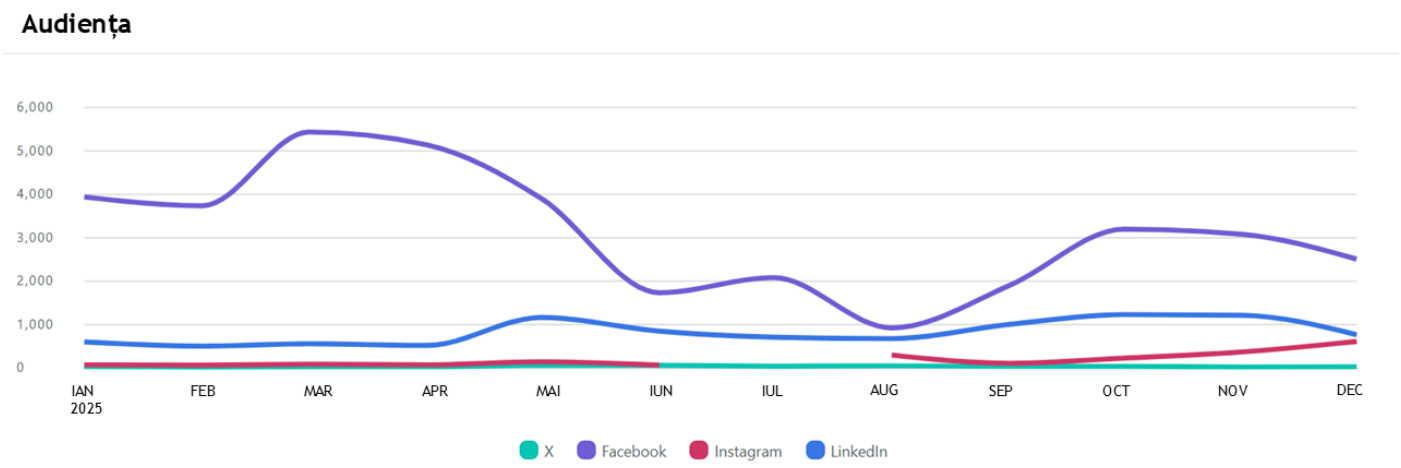


Figura 18 - Evoluția creșterii audienței pe canalele DNSC în 2025

Audiența totală a canalelor DNSC de social media de **Facebook, Instagram, LinkedIn și X** a înregistrat o creștere de 49.087 utilizatori față de anul 2024.

Pe parcursul anului 2025, Directoratul a publicat pe platformele de socializare **Facebook, Instagram, LinkedIn și X un total de 1.581 de materiale** inclusiv cele de comunicare generală, alertare sau privind inițiativele sale de conștientizare și prevenție.

Acestea au generat **29.135.511** de vizualizări, precum și **1.255.739** de reacții, comentarii sau distribuiri.

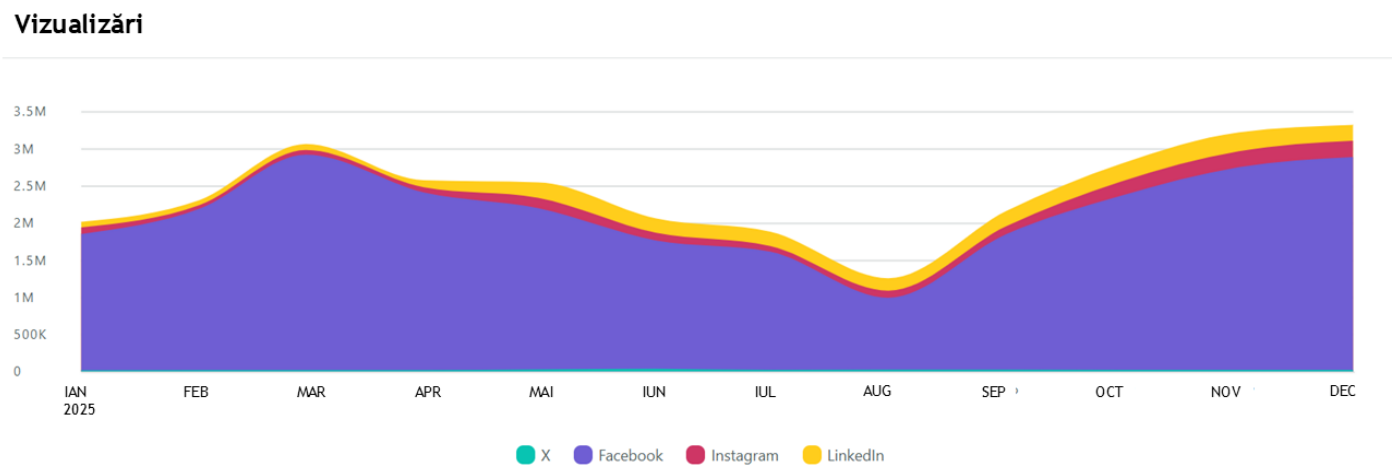


Figura 19 - Evoluția vizualizărilor pe canalele DNSC în 2025

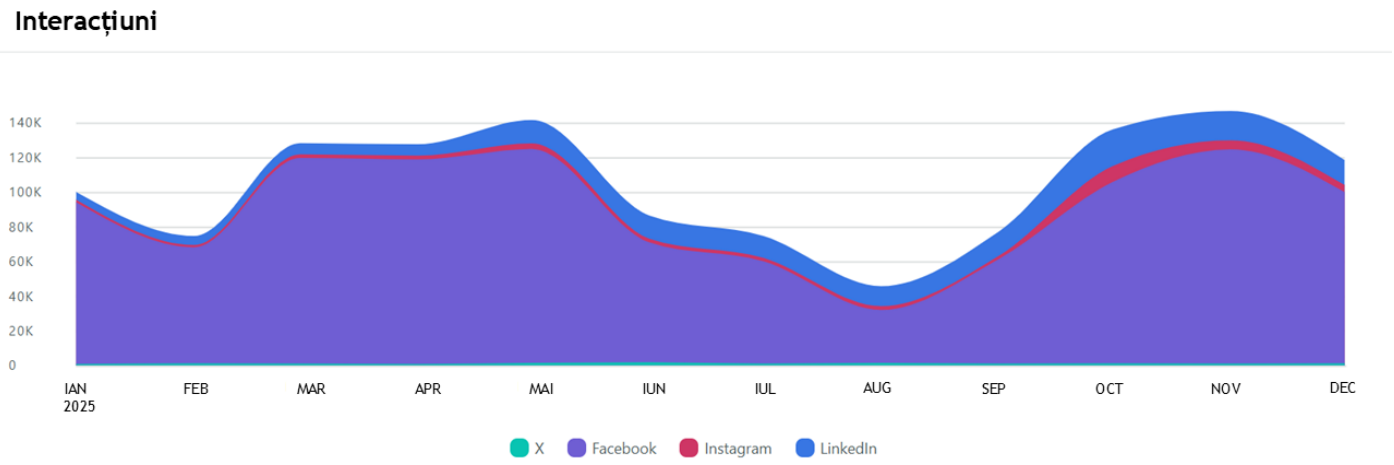


Figura 20 - Evoluția interacțiunilor cu utilizatorii pe canalele DNSC în 2025

În 2025, **10.925.816** din **29.135.511** (37,49% din total) vizualizări aferente postărilor DNSC au fost legate de materialele de creștere a conștientizării în domeniul securității, amenințărilor și riscurilor cibernetice.

Cele mai performante postări de conștientizare pe 2025, din punctul de vedere al impactului realizat, au fost:

- Alerta ***CVE-2025-29824*** (839.803)
- Promovarea Ghidului ***Deepfake*** (571.773)
- Alerta ***WhatsApp Zero-Click*** (524.033)
- ***Porcu' PIN*** – Timișoara (73.428 vizualizări)
- Video de conștientizare privind dezinformarea (61.955)
- Avertizarea privind scam-ul cu credit fals (60.190)

Directoratul a publicat, în 2025, pe canalul său de YouTube **89 de videoclipuri** (dintre care 63 de videoclipuri și 26 de shorts) pe diverse teme din domeniul securității cibernetice.

Însumat, acestea au înregistrat 77.800 de vizualizări (cu 415% mai mult față de 2024) și 1.900 de ore de timp de vizualizare (cu 308% mai mult decât în 2024).

În 2025 canalul de YouTube al Directoratului a înregistrat o creștere de 214% comparativ cu anul 2024 (reprezentând 566 de abonați noi).

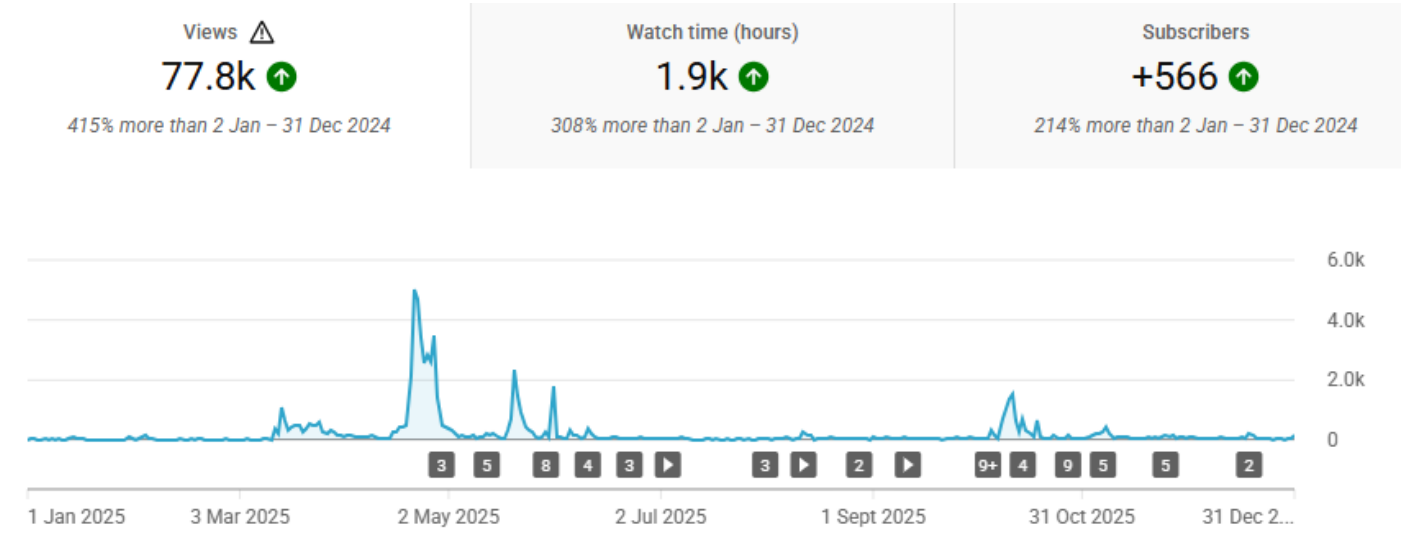
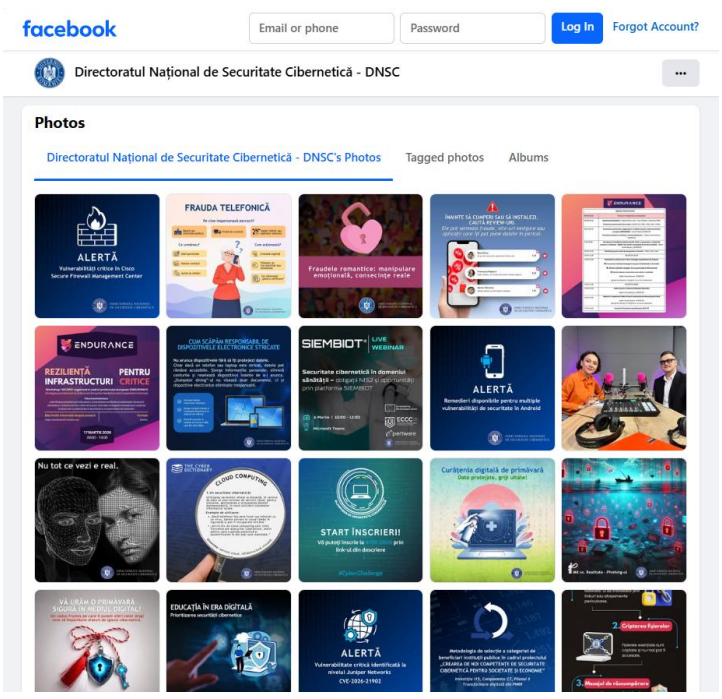


Figura 21 - Performanța canalului de YouTube al DNSC în 2025

Un element important de menționat cu privire la analiza performanței inițiativelor pe platformele de social media este faptul că Directoratul a reușit atingerea acestor cifre cu **zero costuri de promovare**.



3.5 Cooperarea la nivel național și internațional în domeniul securității cibernetice

Pentru a-și calibra corespunzător prioritățile de cooperare, strategia Directoratului a fost una de transparență și coordonare constantă cu instituțiile competente din România și cu partenerii internaționali, pentru a se asigura eficientă, rezultate concrete și a se evita potențiale redundanțe.

Eforturile DNSC au vizat constituirea de capabilități, cunoștințe tehnice și consolidarea resurselor disponibile, prin facilitarea cooperării la nivel de ecosisteme, acționând ca un hub pentru organizații din domeniile public și privat din România și din statele partenere.

3.5.1 Parteneriate naționale în domeniul securității cibernetice

Directoratul a înființat, coordonează și gestionează Platforma Națională de Cooperare în Domeniul Securității Cibernetice (PNCDSC), între instituțiile de stat, mediul privat, mediul academic și organizații non-guvernamentale, în scopul asigurării unui cadru național unitar de expertiză, cercetare, informare și alte acțiuni conexe domeniului de competență, conform OUG nr. 104/2021 Art. 5. În acest sens, în anul 2025 principalele categorii de acțiuni ale DNSC au constat în:

- Inițierea de dialoguri, ateliere de lucru, seminare și schimb de experiență în format 1-1 cu partenerii instituționali naționali.
- Negocierea și semnarea de acorduri de parteneriat și cooperare.
- Realizarea unor acțiuni și evenimente comune care să sprijine demersurile de consolidare a capacităților și capabilităților naționale de securitate cibernetică, inclusiv prin armonizarea cadrului legislativ național în domeniu.

În 2025, Directoratul a realizat pregătirea, finalizarea și semnarea de acorduri de parteneriat strategic și cooperare cu o serie de **entități naționale relevante**, contribuind la îndeplinirea obiectivelor generale și specifice ale DNSC pentru întărirea capacităților și capabilităților naționale de securitate cibernetică:

1. Asociația InfoCons – Organizație pentru Protecția Consumatorilor (InfoCons)
2. Agenția Națională a Funcționarilor Publici (ANFP)
3. Asociația Patronală a Industriei de Software și Servicii (ANIS)
4. Autoritatea Națională pentru Administrare și Reglementare în Comunicații (ANCOM)
5. Autoritatea Națională de Management al Calității în Sănătate (ANMC)
6. Autoritatea de Supraveghere Financiară (ASF)
7. Casa Națională de Asigurări de Sănătate (CNAS)
8. ENEVO Group
9. Institutul de Cercetare-Dezvoltare în Genomică
10. Institutul Național de Cercetare-Dezvoltare în Informatică București (ICI)
11. Inspectoratul General al Poliției Române (IGPR)
12. Institutul Aspen România
13. Institutul Național pentru Pregătirea și Perfecționarea Avocaților (INPPA)
14. Oficiul de Stat pentru Invenții și Mărci (OSIM)
15. Parchetul de pe lângă Înalta Curte de Casație și Justiție (PICCJ)
16. Patronatul Furnizorilor de Servicii Medicale Private (PALMED)
17. Uniunea Națională a Barourilor din România (UNBR)
18. Universitatea Babeș-Bolyai (UBB)

19. Secretariatul General al Guvernului (SGG), privind Gala Inovării în Sectorul Public
20. Secretariatul General al Guvernului (SGG), privind Programul Oficial de Internship al Guvernului

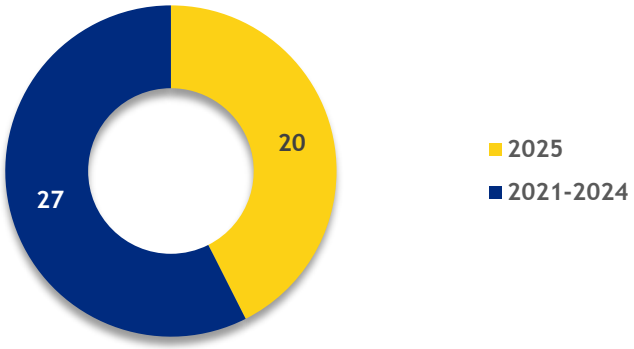


Figura 22 - Parteneriate naționale în domeniul securității cibernetice

3.5.2 Parteneriate internaționale în domeniul securității cibernetice

În 2025, DNSC a realizat pregătirea, finalizarea și semnarea de acorduri de parteneriat strategic și cooperare cu o serie de **entități internaționale relevante**, contribuind la consolidarea rolului Directoratului ca instituție relevantă la nivel internațional, care să poziționeze România ca un lider recunoscut în securitatea cibernetică:

1. National Computer and Cybercrimes Coordination Committee (NC4) Kenya
2. Centrul Național de Securitate Cibernetică din Regatul Hașemit al Iordaniei
3. Sierra Nevada Corporation (SNC)
4. NetCentrics
5. Microsoft
6. Amazon Web Services EMEA

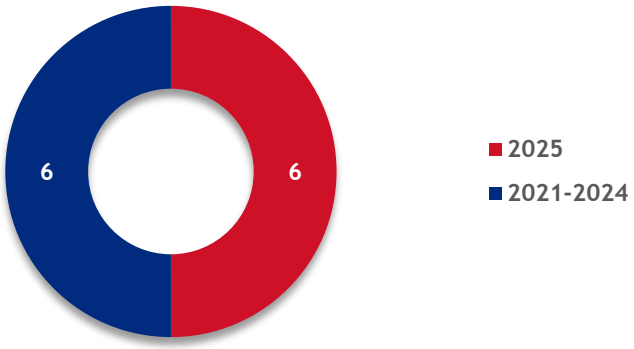


Figura 23 - Parteneriate internaționale în domeniul securității cibernetice

3.5.3 Relația bilaterală cu autoritățile din SUA

Anul 2025 a fost caracterizat de o stagnare a cooperării bilaterale între Directorat și **Cybersecurity and Infrastructure Security Agency (CISA)**, cauzată de schimbarea managementului Agenției americane, pe fondul schimbărilor politice ale Administrației SUA. Concomitent, în 2025, volumul și calitatea contactelor și interacțiunilor în domeniul securității cibernetice, prin intermediul Ambasadei SUA la București, au avut de suferit în principal ca urmare a rotației experților tehnici din cadrul Ambasadei, a întârzierilor în numirea Ambasadorului și a constrângerilor bugetare ale părții americane.

3.5.4 Sprijin acordat Republicii Moldova în domeniul securității cibernetice

În 2025 un obiectiv major al DNSC a privit creșterea rolului României ca principal furnizor de consultanță în domeniul securității cibernetice pentru instituțiile din Republica Moldova, inclusiv prin sprijin direct în materie de consolidare a capacității instituționale pentru **Agenția pentru Securitate Cibernetică (ASC)** dar și pentru **Serviciul Tehnologia Informației și Securitate Cibernetică (STISC).** Pe parcursul anului 2025, 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. Principalele acțiuni în acest sens au inclus:

- **Reiterarea constantă și vizibilă a sprijinului pentru parcursul european al Republicii Moldova**, inclusiv prin susținerea integrării rapide a instituțiilor sale naționale competente în mecanismele și formatele UE în domeniul securității cibernetice.
- Coordonarea activă cu **State Membre ale UE, Marea Britanie, Misiunea de parteneriat a UE în Republica Moldova (EU Partnership Mission in the Republic of Moldova - EUPM)** pentru a oferi sprijin operațional autorităților moldovene în domeniul securității cibernetice.
- Creșterea semnificativă în 2025 a prezenței Directoratului în Republica Moldova prin participarea la conferințe și grupuri de lucru, atât de nivel înalt, cât și la nivel de expert, la Chișinău și București.
- Organizarea de seminare și training-uri dedicate instituțiilor din Republica Moldova în cooperare cu organizații internaționale – precum Marea Britanie și OSCE (workshop în octombrie 2025 axat pe cooperare pentru schimbul de informații, protecția infrastructurii critice și pe divulgarea coordonată a vulnerabilităților - CVD).
- Facilitarea și sprijinirea semnării unui memorandum de înțelegere (MoU) între **ASC și Centrul european de competențe în domeniul industrial, tehnologic și de cercetare în materie de securitate cibernetică (European Cybersecurity Competence Center - ECCC).**
- Facilitarea participării **ASC** la formate de cooperare internațională în materie de securitate cibernetică (ex: participarea la ECCC Governing Board).
- Sprijin al DNSC pentru operaționalizarea **ASC**, inclusiv pentru consolidarea capabilităților tehnice ale instituției, a definirii și îmbunătățirii cadrului legal și pregătirea resurselor umane.
- Includerea unui panel regional în cadrul Conferinței ***ENISA eHealth - The evolving threat landscape and regional approaches***, care a permis ASC să prezinte abordarea și provocările Republicii Moldova privind amenințările cibernetice specifice sectorului sănătate.
- Includerea unui panel specific pe tema ***Closing the gaps and building cyber capacity for a resilient future*** în cadrul BCC2025, care a permis **ASC** prezentarea perspectivei naționale privind importanța dezvoltării capacităților cibernetice pentru consolidarea rezilienței instituționale, reducerea vulnerabilităților și întărirea cooperării regionale în contextul amenințărilor hibride și al provocărilor de securitate din regiune.
- Operaționalizarea și menținerea de canale de comunicare în regim 24/7 pentru acordarea de sprijin operațional următoarelor autorități din Republica Moldova: ASC, STISC, Ministerul Dezvoltării Economice și Digitalizării, **Centrul pentru Comunicare Strategică și Contracarare a Dezinformării (STRATCOM)**.
- Misiuni de experți DNSC pe segment tehnic, reglementare, cooperare cu entități externe și comunicare - în cooperare cu EUPM și cu mecanismul UE de asistență tehnică și schimbul de informații (TAIEX).

SPRIJN CĂTRE REPUBLICA MOLDOVA ÎN CONTEXTUL ALEGERILOR PARLAMENTARE DIN SEPTEMBRIE 2025

Având în vedere buna cooperare dintre DNSC și autoritățile naționale competente din Republica Moldova respectiv **ASC și STISC** pentru asigurarea securității cibernetice a proceselor electorale în cazul alegerilor prezidențiale și a referendumului privind integrarea în UE din octombrie-noiembrie 2024, demersuri similare au fost efectuate și pentru alegerile parlamentare derulate în septembrie 2025.

Având în vedere arhitectura instituțională și responsabilitățile stabilite prin lege pentru instituțiile partenere din Republica Moldova, Directoratul a cooperat inclusiv cu **STRATCOM**. Sprijinirea **ASC, STISC și STRATCOM** a fost efectuată prin prisma activităților malițioase online cu impact și asupra țării noastre prin prisma riscurilor și amenințărilor cibernetice asociate.

DNSC a furnizat sprijin pentru instituțiile din Republica Moldova pe următoarele componente cheie:

1

Monitorizarea spațiului cibernetic în contextul campaniei electorale și alegerilor parlamentare din Republica Moldova și identificarea vulnerabilităților exploatabile asociate cu resursele IT&C expuse public aparținând principalelor entități publice:

- Activități proactive de identificare a vulnerabilităților pentru 171 de entități relevante
- 99 de informări privind 1.655 credențiale expuse asociate un număr de 77 entități
- 27 de informări privind 1.976 vulnerabilități identificate pentru un număr de 27 entități

2

Identificarea, analiza și raportarea de conturi de social media care au aparent un comportament neautentic, posibil de tip BOT, parte a unei rețele automatizate, pe platformele TikTok, Instagram și Facebook, cu următoarele rezultate:

- 903 de conturi TikTok raportate către platforma de social media, din care 728 închise,
- 128 conturi Facebook raportate către platforma de social media, din care 7 închise

3

Sprijinirea eforturilor autorităților din Republica Moldova pentru comunicare publică eficientă și pentru creșterea nivelului de conștientizare privind amenințările cibernetice, cu următoarele rezultate:

- Planificarea și derularea campaniilor de conștientizare derulate de către ASC în perioada premergătoare alegerilor parlamentare din Republica Moldova
- Configurarea și utilizarea unui canal adițional de comunicare și a unui grup de lucru dedicat acesteia, care a permis schimbul rapid de informații și validarea conținutului destinat comunicării în mediul online

4

Creșterea conștientizării la nivelul UE și internațional privind amenințările cibernetice din Republica Moldova și consolidarea poziției instituțiilor acesteia în formate multilaterale relevante pentru securitatea cibernetică, cu următoarele rezultate:

- Sprijinirea ASC și STISC în întocmirea și transmiterea periodică de analize privind incidentele și atacurile cibernetice înregistrate în Republica Moldova către ENISA și Serviciul European de Acțiune Externă (SEAE), dar și către beneficiari din România

5

Facilitarea implementării de bune practici în asigurarea securității cibernetice a proceselor electorale, identificate în state *like-minded*, cu următoarele rezultate:

- Diseminarea către instituțiile din Republica Moldova a unui material comun realizat de DNSC și instituțiile din Marea Britanie *Joint UK-Romania note: lessons learned on cyber threats to elections*, dedicat lecțiilor învățate din demersurile de asigurare a securității cibernetice a proceselor electorale din România și Regatul Unit
- La invitația Ambasadei României la Chișinău și a EUPM, realizarea unei prezentări și transfer de expertiză către ASC, STISC și alte instituții din Republica Moldova privind lecții învățate și bune practici de cooperare inter-instituțională în efortul de asigurare a securității cibernetice a proceselor electorale din România

6

Operaționalizarea și menținerea de canale de comunicare specializate, în regim 24/7, pentru a asigura un schimb rapid și efectiv de informații tehnice relevante în contextul securității cibernetice a alegerilor parlamentare din republica Moldova

- DNSC s-a coordonat și a comunicat în timp real cu autoritățile din Republica Moldova în perioada alegerilor, inclusiv pentru sprijin în gestionarea incidentelor cibernetice

3.5.5 Sprijin acordat Ucrainei în domeniul securității cibernetice

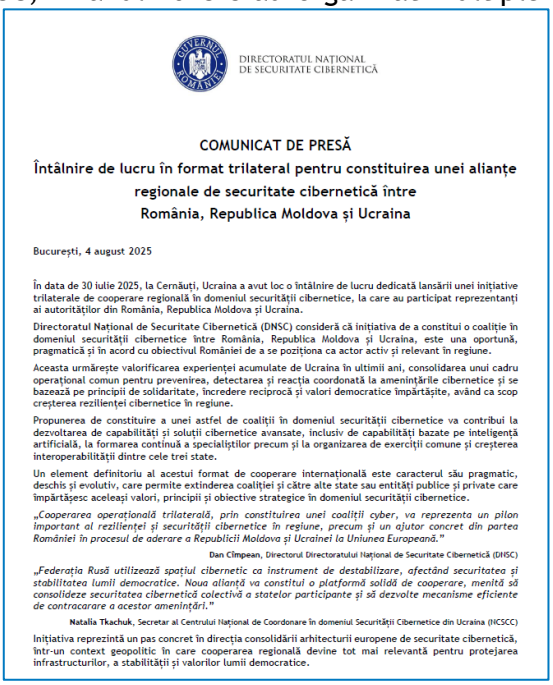
În 2025, principalii parteneri ai DNSC în Ucraina au fost **Centrul Național de Coordonare a Securității Cibernetice din cadrul Consiliului Național de Securitate și Apărare al Ucrainei (NCSCC)** și **Serviciul de Stat pentru Comunicații Speciale și Protecția Informației din Ucraina (SSSCIP)**. Directoratul a cooperat cu aceștia prin:

- Coordonarea și susținerea prezenței României în Ucraina prin participarea unei delegații inter-instituționale la Forumul internațional în domeniul rezilienței cibernetice (Kiev 11-12 martie 2025).
- Organizarea de training-uri dedicate instituțiilor din Ucraina (și Republica Moldova) în cooperare cu organizații internaționale – OSCE, EGA, **European Union Advisory Mission (EUAM) Ukraine** etc.
- Organizarea cu sprijinul EUAM a unui workshop dedicat administrației regionale și operatorilor de infrastructuri critice din regiunea Cernăuți (27-28 august 2025).
- Organizarea, cu sprijinul EUAM, a unor workshop-uri online de specialitate pentru reprezentanți ai instituțiilor din Ucraina (Kiev 19 iunie, Donetsk 20 noiembrie 2025).
- Invitarea instituțiilor din Ucraina la conferințele și evenimentele internaționale organizate de DNSC în parteneriat cu ENISA și ECCC (ex. ENISA Health, BCC 2025). DNSC a inclus unui panel regional în cadrul Conferinței ***ENISA eHealth - The evolving threat landscape and regional approaches***, care a permis specialiștilor NCSCC să prezinte abordarea Ucrainei privind amenințările cibernetice specifice sectorului sănătate, în contextul războiului de agresiune din partea Federației Ruse.
- De asemenea, în cadrul BCC2025 a fost organizat panelul ***Cyber resilience in wartime: Lessons learned from Ukraine***, dedicat analizării experienței Ucrainei în gestionarea atacurilor cibernetice. Discuțiile au evidențiat modul în care Ucraina a reușit să își consolideze reziliența cibernetică prin răspuns rapid la incidente, utilizarea inovatoare a tehnologiilor și cooperarea extinsă cu parteneri internaționali, precum și lecțiile învățate privind consolidarea cooperării civil-militare, crearea redundanței în sistemele critice și rolul domeniului cibernetic în conflictele moderne.
- Facilitarea participării NCSCC și SSSCIP la formate de cooperare internațională în materie de securitate cibernetică (ex: participarea la ECCC Governing Board, Cyber Security Director's meeting).

3.5.6 Pregătirea înființării Alianței Cibernetice pentru Reziliență Regională cu implicarea Ucrainei, României și Republicii Moldova

În vederea pregătirii înființării **Alianței Cibernetice pentru Reziliență Regională** dintre DNSC, NCSCC și ASC, în anul 2025 s-au organizat multiple contacte inter-instituționale, dar și o serie de întâlniri de lucru formale în vederea alinierii și consultării trilaterale:

- Martie 2025, Kiev
- Aprilie 2025, Ivano Frankivsk
- Aprilie 2025, Chișinău (în marja conferinței anuale a ASC)
- Iunie 2025, Roma (în marja ECCC Governing Board)
- Iulie 2025, Cernăuți
- Octombrie 2025, București (în marja Bucharest Cybersecurity Conference 2025)



DIRECTORATUL NAȚIONAL DE SECURITATE CIBERNETICĂ

COMUNICAT DE PRESĂ

Întâlnire de lucru în format trilateral pentru constituirea unei alianțe regionale de securitate cibernetică între România, Republica Moldova și Ucraina

București, 4 august 2025

În data de 30 iulie 2025, la Cernăuți, Ucraina a avut loc o întâlnire de lucru dedicată lansării unei inițiative trilaterale de cooperare regională în domeniul securității cibernetice, la care au participat reprezentanți ai autorităților din România, Republica Moldova și Ucraina.

Directoratul Național de Securitate Cibernetică (DNSC) consideră că inițiativa de a constitui o coaliție în domeniul securității cibernetice între România, Republica Moldova și Ucraina, este una oportună, pragmatică și în acord cu obiectivul României de a se poziționa ca actor activ și relevant în regiune.

Aceasta urmărește valorificarea experienței acumulate de Ucraina în ultimii ani, consolidarea unui cadru operațional comun pentru prevenirea, detectarea și reacția coordonată la amenințările cibernetice și se bazează pe principii de solidaritate, încredere reciprocă și valori democratice împărtășite, având ca scop creșterea rezilienței cibernetice în regiune.

Propunerea de constituire a unei astfel de coaliții în domeniul securității cibernetice va contribui la dezvoltarea de capabilități și soluții cibernetice avansate, inclusiv de capabilități bazate pe inteligență artificială, la formarea continuă a specialiștilor precum și la organizarea de exerciții comune și creșterea interoperabilității dintre cele trei state.

Un element definitoriu al acestui format de cooperare internațională este caracterul său pragmatic, deschis și evolutiv, care permite extinderea coaliției și către alte state sau entități publice și private care împărtășesc aceleași valori, principii și obiective strategice în domeniul securității cibernetice.

„Cooperarea operațională trilaterală, prin constituirea unei coaliții cyber, va reprezenta un pilon important al rezilienței și securității cibernetice în regiune, precum și un ajutor concret din partea României în procesul de aderare a Republicii Moldova și Ucrainei la Uniunea Europeană."

Dan Cîmpean, Directorul Directoratului Național de Securitate Cibernetică (DNSC)

„Federația Rusă utilizează spațiul cibernetic ca instrument de destabilizare, afectând securitatea și stabilitatea lumii democratice. Noua alianță va constitui o platformă solidă de cooperare, menită să consolideze securitatea cibernetică colectivă a statelor participante și să dezvolte mecanisme eficiente de contracarare a acestor amenințări."

Natalia Tkachuk, Secretar al Centrului Național de Coordonare în domeniul Securității Cibernetice din Ucraina (NCSCC)

Inițiativa reprezintă un pas concret în direcția consolidării arhitecturii europene de securitate cibernetică, într-un context geopolitic în care cooperarea regională devine tot mai relevantă pentru protejarea infrastructurilor, a stabilității și valorilor lumii democratice.

În paralel, Directoratul a realizat demersurile pentru informarea și consultarea instituțiilor membre ale Consiliul Operativ de Securitate Cibernetică (COSC) privind obiectivele **Alianței Cibernetice pentru Reziliență Regională** și proiectul de text al memorandumului de înțelegere (MoU) planificat a se semna între DNSC, ASC și NCSCC în acest sens.

Simultan, în linie cu viziunea comună a preconizatei alianței cibernetice, pe parcursul anului 2025, Directoratul s-a implicat activ în:

- Organizarea cu sprijinul EUAM în aprilie 2025 la Ivano Frankivsk, Ucraina, a primei ediții a exercițiului în format trilateral cu componentă tehnică și la nivel de factori de decizie. Exercițiul a fost mixt: Capture The Flag (CTF) și Table-Top Exercise (TTX) cu participarea a 16 instituții din cele trei state.
- Efectuarea unui exercițiu comun la nivel expert în format trilateral la Chișinău, iulie 2025 - Strategic Cybersecurity Tabletop Exercise, găzduit în comun de Agenția de Securitate Cibernetică și Consiliul Suprem de Securitate din Republica Moldova, cu participarea reprezentanților agențiilor de securitate cibernetică din cele trei state.
- Coordonarea participării echipelor din România și Republica Moldova la un exercițiu online de tip Capture The Flag (CTF) dedicat securității cibernetice a sectorului bancar (iulie 2025), la invitația NCSCC, în format trilateral. Echipa României a fost formată din reprezentanți de la instituțiilor din COSC și reprezentanți ai BNR.
- Organizarea mesei rotunde trilaterale, cu tema ***Forging a Cyber Resilience Arc: Strengthening Trilateral Cooperation between Romania, Republic of Moldova and Ukraine*** în cadrul Bucharest Cybersecurity Conference 2025.

3.5.7 Cooperarea cu instituții ale Uniunii Europene și internaționale

ORGANIZAȚII ȘI FORMATE ALE UNIUNII EUROPENE

- La nivelul Uniunii Europene, Directoratul reprezintă România pe aria sa de competență într-o serie de organisme specializate privind securitatea cibernetică, precum:
    - Management Board al Agenției Uniunii Europene pentru Securitate Cibernetică (ENISA)
    - Consiliul de Conducere (Governing Board) al European Cybersecurity Competence Centre (ECCC)
    - Board of Directors of the European Cyber Security Organisation (ECSO)
    - Grupul de Cooperare NIS (și sub-grupurile tematice ale acestuia)
    - Rețeaua echipelor de răspuns la incidente cibernetice (CSIRT Network)
    - Rețeaua Europeană de legătură în domeniul crizelor cibernetice (EU-CyCLONe)
    - ENISA National Liaison Officers' Network, plus Grupul de experți pentru Regulamentul privind reziliența cibernetică (Cyber Resilience Act – CRA) și sub-grupurile tematice ale acestuia
    - EU Cyber Directors' Meeting

În acest context, DNSC coordonează activitățile la nivel național privind aceste formate de cooperare ale UE și are rolul de a gestiona contribuția activă a autorităților române la analiza, elaborarea și transmiterea de contribuții și puncte de vedere naționale pe problematicile aferente securității cibernetice.

În acest context, s-au derulat o serie de activități concrete:

- Directoratul a participat la toate întâlnirile aferente formatelor de lucru UE, în care a susținut poziția și interesele României și a prezentat date și elemente menite să vină în sprijinul dezvoltării ecosistemului național de securitate cibernetică. Suplimentar, în mod constant și deschis DNSC a argumentat în favoarea sprijiniri aderării Republicii Moldova și Ucrainei la mecanismele și formatele UE din domeniul securității cibernetice.
- La nivelul Consiliului de Conducere (Governing Board) al European Cybersecurity Competence Centre (ECCC), Directoratul a susținut invitarea ca observatori permanenți a reprezentanților Republicii Moldova și ai Ucrainei.
- DNSC a participat în mod activ la aceste formate de lucru, ceea ce a condus atât la organizarea a două conferințe ENISA la București (ENISA e-Health și ENISA Market and Resilience Conference), precum și a reuniunii NIS Cooperation Group Work Stream on Health.

- Co-prezidarea Work Stream Health și susținerea punctelor de vedere naționale în domeniul securității cibernetice a organizațiilor din domeniul sănătății, prin diseminarea de informații publicului larg și instituțiilor interesate. Precizăm că în urma campaniei DNSC România este printre statele care transmis cel mai mare număr de răspunsuri la consultarea publică organizată de Comisia Europeană pe tema Planului de acțiune al UE pentru securitatea cibernetică a spitalelor și furnizorilor de servicii medicale.
- DNSC a coordonat și transmis răspunsul național pentru EU Cyber Security Index 2026, cu sprijinul instituțiilor cu competențe specifice din România.
- DNSC a analizat și elaborat împreună cu celelalte instituții cu atribuții în domeniu puncte de vedere naționale pe problematicile aferente securității cibernetice de la nivelul UE (ex: pentru propunerea UE de regulament *Digital Omnibus*).
- În urma implicării active a Directoratului a fost planificată, negociată și obținută valorificarea adaptată nevoilor naționale a resurselor oferite statelor membre UE prin **ENISA Cybersecurity Support Action**. Datorită acestui demers, România se numără printre primele state care au utilizat integral bugetul alocat prin programul Cybersecurity Support Action, demonstrând o implementare eficientă și un angajament solid pentru consolidarea capacităților naționale în domeniul securității cibernetice:
    - Directoratul și consorțiul de furnizori români de servicii selectat de ENISA au coorganizat în 2025 un set de workshop-uri tematice dedicate implementării NIS2 și a cadrului legislativ național de transpunere, reprezentat de OUG nr. 155/2024:
        - Nouă workshopuri în patru orașe (București, Craiova, Constanța și Iași), care au acoperit patru sectoare esențiale Sănătate, Transport, Energie și Administrație Publică, și la care au participat 102 persoane.
        - S-au planificat pentru 2026 un număr de 22 de workshop-uri precum și două exerciții practice cu o acoperire extinsă în București, Timișoara, Cluj, Brașov și Iași. Activitățile planificate vor acoperi sectoarele: sănătate, transport, energie, administrație publică, fabricare, apă potabilă și ape uzate, infrastructură digitală și IT&C, poștă și curierat.
    - S-a elaborat ghidul de implementare al CyberFundamentals (CyFUN), cadrul de măsuri de securitate dezvoltat de Centre for Cybersecurity Belgium (CCB) și transpus în România de către DNSC, pentru a ajuta organizațiile să-și îmbunătățească nivelul de securitate cibernetică.
    - S-a elaborat un ghid pentru implementarea unui plan de management al crizelor cibernetice.
    - DNSC a utilizat, în cadrul programului, licențe ale unor platforme de training de securitate cibernetică – necesare pregătirii personalului de specialitate propriu.
- În abordarea propunerilor UE privind măsuri pe segmentul securității cibernetice sau a provocărilor întâmpinate la nivel național, Directoratul a efectuat discuții și consultări bilaterale cu autorități din state ale Uniunii Europene (Germania, Franța, Belgia, Slovenia, Spania, Austria, Cehia, Polonia etc.), dar și cu Moldova, Ucraina, Marea Britanie, Elveția, Bosnia Herțegovina.

CYBERCRIME PROGRAMME OFFICE OF THE COUNCIL OF EUROPE (C-PROC)

- Continuarea cooperării DNSC-C-PROC și organizarea de activități comune, cum ar fi exercițiul regional dedicat combaterii criminalității informatice din aprilie 2025 la București.
- Participarea în premieră a DNSC la Octopus Conference 2025, Strasbourg.

ORGANIZAȚIA PENTRU COOPERARE ȘI DEZVOLTARE ECONOMICĂ (OCDE)

Directoratul a sprijinit reprezentarea României în formatele de lucru relevante ale OCDE și a contribuit la monitorizarea și implementarea recomandărilor comitetelor OCDE, inclusiv prin actualizări privind progresele naționale și participarea la grupuri de lucru tematice:

- Asigurarea contribuției și reprezentării României (în cooperare cu MAE și MEDAT) la formatele de lucru ale OCDE în domeniul securității cibernetice.

- Participare a DNSC la Working Party on Digital Economics, Measurement, and Analysis și Guidance for Vulnerability Researchers Workshop.
- Elaborare și transmitere de puncte de vedere ale Directoratului cu privire la instrumentul legal 0380 - Recommendation of the Council on Digital Technologies and the Environment și instrumentul legal privind integritatea informațiilor OCDE.
- Contribuții din partea DNSC privind implementarea recomandărilor prioritare ale Comitetului pentru Politică Digitală (DPC) al OCDE.
- DNSC a elaborat poziții și răspunsuri instituționale pe teme prioritare, precum integritatea informațiilor, impactul tehnologiilor digitale asupra mediului și securitatea digitală și a contribuit la exerciții de analiză și raportare strategică, inclusiv la materialul Digital Economy Outlook 2026 al OCDE.

NATO

În cooperare cu alte autorități competente, Directoratul a contribuit la întărirea cooperării cu NATO prin:

- Participarea la reuniunea Grupului Interinstituțional pentru Implementarea Deciziilor Strategice în Domeniul Securității Naționale a României (GIDeS).
- Participarea DNSC la Techcelerator Investors Day on Dual Use & NATO DIANA și elaborarea de mesaje către organizații private din domeniul securității cibernetice privind oportunitățile de finanțare a proiectelor prin mecanismul **NATO Defence Innovation Accelerator for the North Atlantic (DIANA).**
- Participarea DNSC la masa rotundă Consolidarea rezilienței: *Răspunsul strategic al României la Cerințele de bază ale NATO în contextul proiectului noii Strategii Naționale de Apărare*.

ONU

- Directoratul a asigurat puncte de contact pentru United Nations Global Intergovernmental Points of Contact Directory on the Use of ICTs in the Context of International Security.
- Directoratul a furnizat puncte de vedere cu privire la proiectul revizuit al raportului Grupului de lucru deschis al ONU (OEWG) dedicat securității și utilizării tehnologiilor de informații și telecomunicații.

OSCE

- Directoratul a participat la reuniunile **Organizației pentru Securitate și Cooperare în Europa (OSCE)** Informal Working Group Cyber, respectiv la Reuniunea Anuală a Punctelor de Contact Naționale pentru OSCE Confidence-Building Measure (CBM) No. 8, Conferința privind securitatea cibernetică organizată de Președinția finlandeză a OSCE/Helsinki.
- Directoratul a participat și a furnizat clarificări și puncte de vedere pe domeniul său de competență, pe parcursul procesului de colectare de date din cadrul ***Limited Election Observation Mission*** a OSCE privind alegerile prezidențiale din România din anul 2025.
- S-a efectuat transmiterea de actualizări naționale privind implementarea Confidence-Building Measures (CBMs), iar experții DNSC au realizat activități de coordonare cu statele participante co-adoptatoare ale CBM15 și CBM16 din cadrul OSCE IWG.
- DNSC a furnizat expertiză de specialitate la evenimentul OSCE ***Sub-regional workshop on cyber/ICT security focusing on threat information sharing, critical infrastructure protection and sharing vulnerability information / Coordinated Vulnerability Disclosure***, organizat la Chișinău în octombrie 2025, pentru reprezentanți ai instituțiilor din Republica Moldova și Ucraina.
- DNSC a participat la workshop-ul OSCE derulat în ianuarie 2025 la Varșovia și dedicat reprezentanților autorităților ucrainene pe tema clasificării incidentelor de securitate cibernetică.

REGIUNEA BALCANII DE VEST

- Organizarea și susținerea de către experții DNSC a unui program de training de 3 zile la **Western Balkans Cyber Capacity Centre (WB3C)** din Podgorița, Muntenegru (noiembrie 2025), dedicat reprezentanților agențiilor de securitate cibernetică din regiune, cu sprijinul URSIV - Slovenia.

- Organizarea și desfășurarea vizitei la DNSC a unui grup de experți cyber din Bosnia și Herțegovina.
- În cooperare cu Geneva Centre for Security Sector Governance (DCAF), Directoratul a pregătit și susținut prezentări de specialitate în cadrul ***Seminar on Cybersecurity Legislation***, pentru reprezentanți ai autorităților naționale competente în domeniul securității cibernetice din Balcanii de Vest și Republica Moldova (februarie 2025).

3.5.8 Organizarea conferinței anuale Bucharest Cybersecurity Conference 2025 - principalul eveniment național dedicat securității cibernetice

În perioada 6-9 octombrie 2025, Directoratul a organizat **Bucharest Cybersecurity Conference 2025 (BCC2025)**, unul dintre cele mai mari și relevante evenimente strategice dedicate securității cibernetice la nivel regional și european. Conferința a fost organizată în colaborare cu **Agenția Uniunii Europene pentru Securitate Cibernetică (ENISA)** și **Centrul European de Competențe în materie de Securitate Cibernetică (ECCC)**, cu sprijinul **Centrului Național de Coordonare (NCC-RO)** și al **Asociației Naționale pentru Securitatea Sistemelor Informatice (ANSSI).**

Evenimentul a avut tema ***Working together on cybersecurity in a time of global uncertainty*** și s-a desfășurat într-un context geopolitic marcat de intensificarea amenințărilor hibride, accelerarea transformării digitale și creșterea dependenței societății de infrastructuri digitale critice.

Scopul principal al BCC2025 a fost explorarea strategiilor și soluțiilor pentru asigurarea viitorului digital al Uniunii Europene în fața amenințărilor cibernetice și hibride.

Evenimentul a reunit peste **1.200 de experți din 45 de țări** din domeniul securității cibernetice din sectorul privat, public și academic și a avut o structură multi-format desfășurată pe parcursul a patru zile, reunind keynote speeches, paneluri strategice și intervenții speciale, sesiuni tematice și tehnice organizate în paralel, precum și workshop-uri și exerciții aplicate. Agenda a inclus intervenții la nivel înalt privind evoluțiile cadrului european în materie de securitate cibernetică, securitatea produselor cu elemente digitale și mecanismele de implementare sectorială, precum și dezbateri dedicate supravegherii pieței, evaluării maturității în domeniul securității cibernetice și provocărilor asociate aplicării cadrului normativ, oferind atât perspective de politică publică, cât și abordări operaționale.

BCC2025 a găzduit și **41 de paneluri** deschise**,** dar și un număr de **18 mese rotunde** și **7 workshop-uri**, desfășurate sub principiile Chatham House, creând un cadru de reflecție strategică și schimb de expertiză și de bune practici între experți și reprezentanți ai autorităților, mediului privat, academic și partenerilor internaționali, contribuind la dezvoltarea unei abordări integrate pentru întărirea rezilienței cibernetice la nivel național, regional și european. Discuțiile au inclus: arhitectura capabilităților cibernetice, coordonarea public-privat în gestionarea vulnerabilităților, guvernanța datelor și a inteligenței artificiale, controlul accesului în ecosisteme digitale complexe, reziliența și continuitatea serviciilor esențiale.

Au fost abordate și dimensiuni regionale și transfrontaliere ale cooperării, provocările specifice infrastructurilor critice, precum și implicațiile noilor forme de influență informațională asupra securității și stabilității societale. Un mesaj central al conferinței a fost că amenințările cibernetice au devenit permanente și tot mai complexe, fiind susținute de actori statali, de grupări infracționale și prin utilizarea tehnologiilor emergente. În acest context, securitatea cibernetică este esențială pentru funcționarea serviciilor publice, protejarea datelor și menținerea încrederii cetățenilor în instituțiile statului.

În cadrul dezbaterilor s-a evidențiat că, deși Uniunea Europeană dispune de un cadru de reglementare avansat, precum **Directiva NIS2, Cyber Resilience Act, Cyber Solidarity Act și DORA - Regulamentul privind reziliența operațională digitală a sectorului financiar**, aplicarea acestor cerințe ridică provocări practice, în special pentru organizațiile cu resurse limitate.

De asemenea, a fost evidențiat rolul României ca actor strategic în arhitectura europeană de securitate cibernetică, având în vedere poziționarea geografică la frontiera estică a Uniunii Europene și a NATO, expunerea la amenințări hibride și găzduirea ECCC în București. Această poziționare la intersecția dintre riscurile operaționale și procesele de inovare în materie de tehnologii digitale, soluții și servicii cibernetice și politici publice, oferă României oportunitatea de a contribui activ la definirea politicilor europene și la furnizarea de expertiză practică relevantă.

BCC2025 a găzduit și masa rotundă cu tema ***Forging a Cyber Resilience Arc: Strengthening Trilateral Cooperation between Romania, Republic of Moldova and Ukraine***, care a reunit actori din mediul public și privat din Republica Moldova, România, Ucraina și state partenere, cu discuții centrate pe amenințările și provocările cibernetice comune, dar și pe mecanismele și formatele disponibile pentru a sprijini demersurile de cooperare în format trilateral.

Un mesaj recurent al intervențiilor în cadrul BCC2025 a fost că reziliența cibernetică nu poate fi asigurată exclusiv prin soluții tehnologice, ci depinde de guvernanță eficientă, personal calificat, cooperare interinstituțională și încredere între actorii implicați. Discuțiile au indicat că tehnologiile emergente pot îmbunătăți semnificativ capacitățile de apărare, dar pot fi utilizate în egală măsură și pentru dezvoltarea unor amenințări mai dificil de contracarat.

Un alt element important identificat a fost necesitatea trecerii de la planificare la pregătire practică. Reziliența reală poate fi obținută prin exerciții, simulări, cooperare public-privată și mecanisme de răspuns testate în condiții reale. În contextul crizelor hibride, consolidarea cooperării interinstituționale și a parteneriatelor public-private devine esențială pentru gestionarea eficientă a incidentelor majore.

Componenta practică a fost susținută la BCC2025 prin organizarea unor exerciții și competiții tehnice, inclusiv de tip Capture The Flag (CTF), un workshop dedicat evaluării maturității organizaționale în contextul implementării directivei NIS2, o competiție intitulată ***Cybersecurity Project Challenge: From Submission to Admission***, precum și un eveniment dedicat promovării instrumentelor UE de finanțare pentru intitulat ***NIS2 Toolbox: Funding & Solutions from EU Projects***.

BCC2025 a evidențiat că reziliența cibernetică nu poate fi realizată exclusiv de autorități publice, iar cooperarea public-privată reprezintă un factor de succes esențial. Consolidarea mecanismelor de partajare a informațiilor, exercițiile comune, dezvoltarea încrederii precum și îmbunătățirea procedurilor și a capabilităților operaționale sunt condiții necesare pentru un răspuns eficient la amenințările emergente. Discuțiile din cadrul conferinței au evidențiat faptul că securitatea cibernetică depășește dimensiunea tehnică, devenind un element esențial pentru funcționarea instituțiilor democratice, protejarea economiei și consolidarea capacității Uniunii Europene de a răspunde amenințărilor cibernetice și hibride.

Sprijinită de parteneri instituționali și sponsori de prestigiu, conferința BCC2025 a consolidat poziția României ca hub regional de dialog strategic în domeniul securității cibernetice și a contribuit la dezvoltarea unui cadru european de cooperare orientat spre reziliență și sustenabilitate digitală.

3.5.9 Organizarea sau participarea la exerciții și simulări de securitate cibernetică

În anul 2025 DNSC a participat la pregătirea și realizarea unui număr semnificativ de exerciții și simulări naționale și internaționale de securitate cibernetică, având ca obiective principale creșterea nivelului de pregătire a personalului și testarea echipelor în situații de incidente, atacuri și crize cibernetice:

- Cyber Europe 2026 organizat de către **Agenția Uniunii Europene pentru Securitate Cibernetică (ENISA)** – exercițiu în care DNSC a fost implicat în întâlniri și sesiuni de planificare, contribuind la definirea scenariilor, coordonarea logistică și stabilirea obiectivelor strategice ale acestuia
- CYDEX25 organizat de **Centrul Național Cyberint din cadrul Serviciului Român de Informații (SRI)**
- NATO Locked Shields 2025, la care DNSC a condus sub-echipa STRATCOM; NATO Cyber Coalition 2025
- Co-organizarea, la invitația **Cybercrime Programme Office of the Council of Europe (C-PROC)**, a Regional Cybercrime Cooperation Exercise, la București în 7-11 aprilie 2025
- Coordonarea participării unei delegații a instituțiilor relevante din COSC, alături de BNR, la un exercițiu online de tip Capture The Flag (CTF) dedicat sectorului bancar la invitația **Centrului Național de Coordonare a Securității Cibernetice din cadrul Consiliului Național de Securitate și Apărare al Ucrainei (NCSCC)** și a **Agenției pentru Securitate Cibernetică a Republicii Moldova (ASC)**
- Exercițiul în format trilateral România - Republica Moldova – România – Ucraina de la Ivano Frankivsk
- Participarea la exerciții de securitate cibernetică prin Centrul Euro-Atlantic pentru Reziliență (E-ARC)
- Exercițiile: CONVEX, Neptun Alert, Neptun Protect, Cyber Drill 2025 Dubai, CyberSOPex25
- Pregătirea pentru exercițiul Histria 2026

Aceste participări au permis consolidarea competențelor operaționale, testarea capacităților de răspuns la incidente și atacuri cibernetice, în scenarii realiste, precum și schimbul de bune practici cu partenerii naționali sau internaționali implicați. În același context, în 2025 reprezentanții DNSC au fost prezenți la întâlnirile periodice ale CSIRT Network și EU-CyCLONe, facilitând schimbul de informații, bune practici și coordonarea operațională între echipele de răspuns la incidente cibernetice din diferite state membre. Toate aceste activități au contribuit la consolidarea capacității instituționale de reacție rapidă, la alinierea procedurilor interne la standardele europene și la creșterea nivelului de cooperare transnațională în domeniul securității cibernetice.

3.5.10 Participarea în cadrul Programului Oficial de Internship al Guvernului României

DNSC și-a continuat participarea, pentru al doilea an consecutiv în calitate de organizație gazdă, în cadrul Programului Oficial de Internship al **Guvernului României**. Directoratul a coordonat activitatea pentru trei dintre cei 150 de stagiari care au luat parte la program și i-a implicat în activitatea structurilor instituției, pentru a contribui activ la proiectele și inițiativele DNSC.

Suplimentar, în coordonare cu **Secretariatul General al Guvernului (SGG)**, DNSC a organizat un eveniment de conștientizare în domeniul securității cibernetice dedicat celor 150 de participanți la Program, având ca obiectiv creșterea rezilienței individuale la amenințările cibernetice, dar și diseminarea informațiilor privind contextul actual de securitate cibernetică și recomandările în domeniul igienei cibernetice și în cadrul celorlalte instituții ale administrației publice centrale participante la program cu efect de multiplicare prin implicarea stagiarilor ca ambasadori de securitate cibernetică în instituțiile gazdă.

4 PRIORITĂȚI ALE DIRECTORATULUI PENTRU 2026

Pentru anul 2026, Directoratul se va concentra pe următoarele aspecte prioritare:

- **Directoratul va continua operaționalizarea structurilor sale** din București și din principalele orașe ale țării, **prin atragerea resursei umane (cu organizarea de concursuri și examene).** Similar cu strategia de recrutare pentru anul 2025, accentul va fi pus pe atragerea și integrarea rapidă a unui grup semnificativ de debutanți și studenți, simultan **cu** participarea la programul guvernamental de internship, prin parteneriate cu actori instituționali și echipe de voluntari.
- Demararea procesului de actualizare a **Strategiei de Securitate Cibernetică a Românei**, în linie cu **Strategia Națională** de Apărare a Țării pentru perioada 2025-2030, cu sprijinul membrilor permanenți ai Consiliului Operativ de Securitate Cibernetică (COSC). Aceasta va lua în considerare și evoluțiile strategiilor cyber actualizate ale unor state partenere sau relevante pentru România.
- Actualizarea cadrului legislativ prin elaborarea, adoptarea și aplicarea actelor normative subsecvente OUG nr. 155/2024. DNSC se va concentra pe operaționalizarea **autorității naționale de certificare** și a **autorității naționale de notificare și supraveghere a pieței** pentru securitatea cibernetică a produselor cu componentă IT&C; pe operaționalizarea funcțiilor-cheie de **supraveghere și control**, respectiv de **evaluare și certificare** în domeniul securității cibernetice; pe continuarea înscrierii organizațiilor în **Registrul entităților esențiale sau importante.**
- Continuarea și accelerarea în 2026 a sprijinului instituțional operațional către autoritățile naționale competente din domeniul securității cibernetice din Republica Moldova, în vederea susținerii parcursului european al acestui stat.
- Operaționalizarea și creșterea nivelului de activități trilaterale în formatul stabilit de **Alianța Cibernetică pentru Reziliență Regională**, cu implicarea autorităților, experților și a ecosistemelor cibernetice din România, Ucraina și Republica Moldova.
- **Relansarea cooperării bilaterale** cu **CISA**, instituția omoloagă din **SUA**.
- Efectuarea, conform planificării, a programelor de formare profesională, training-uri și cursuri de specializare tehnică, necesare menținerii și dezvoltării competențelor personalului de specialitate al DNSC, ca element-cheie pentru asigurarea capacității operaționale a instituției.
- Creșterea nivelului de participare activă 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.
- **Inițierea implementării de noi proiecte în domeniul securității cibernetice** cu impact național și regional, centrate pe soluții, servicii, produse și tehnologii cu utilizare mixtă civil-militară (dual use), în parteneriat cu alte instituții publice, mediul privat și academic. Furnizarea de expertiză tehnică și transferul de cunoștințe în domeniul securității cibernetice către entitățile din România active în Programul SAFE (Security Action for Europe).
- Permanentizarea realizării de analize de risc cibernetic la nivel național și sectorial, cu sprijinul unei soluții tehnice specifice pentru managementul riscurilor de securitate cibernetică.
- Continuarea investițiilor în infrastructura proprie IT&C, adoptarea de noi soluții digitale și a celor bazate pe Inteligență Artificială (AI) pentru creșterea eficienței și acoperirii serviciilor publice oferite de către DNSC către cetățeni și organizații, simultan cu optimizarea costurilor proceselor interne.
- Susținerea consolidării la nivel național a funcției de monitorizare a trendurilor și pieței de securitate cibernetică (***Cyber Market Intelligence***) ca instrument de sprijin de reziliență națională, sub coordonarea DNSC. Securitatea spațiului cibernetic național sectorului civil nu este determinată doar de amenințări și atacatori, ci și de calitatea tehnologiilor, serviciilor, soluțiilor, produselor și capacităților defensive disponibile în piață. Înțelegerea pieței devine element de securitate națională
- Lansarea pe baze comerciale a unor soluții, produse și servicii proprii ale DNSC, precum și promovarea acestora în vederea exportului, în vederea atragerii de venituri suplimentare la bugetul de stat.