

STRATEGIA DE SECURITATE CIBERNETICĂ A ROMÂNIEI 2.0 (2021-2026)

proiect

Având la bază o viziune care ia în considerare experiența acumulată și rezultatele obținute din implementarea Strategiei de Securitate Cibernetică a României și a Planului de Acțiune la nivel național pentru implementarea Sistemului Național de Securitate Cibernetică din 2013, noul document are ca scop stabilirea principalelor linii directoare și a abordărilor generale privind domeniul securității cibernetice. Noua Strategie va promova o viziune actualizată, care să vină în ajutorul întregii societăți: instituții publice și entități private, mediul academic, cetățeni.

Implementarea și aplicarea prevederilor Strategiei de către toți actorii relevanți va sprijini pe de o parte îndeplinirea obiectivelor naționale de securitate și angajamentelor asumate de România la nivel NATO și UE, iar pe de altă parte va crea premisele necesare dezvoltării mediului de afaceri, economiei naționale și zonei educaționale și de cercetare.

Noua Strategie se înscrie în demersurile întreprinse la nivel național în scopul implementării unui cadru de securitate coerent pe toate dimensiunile vieții economice și sociale, sens în care acest document asigură complementaritatea cu documente de natură strategică asumate până în prezent.

Cuprins

1. Introducere

- 1.1. Sumar
- 1.2. Context și importanța securității cibernetice
- 1.3. Amenințarea cibernetică la adresa României
- 1.4. Factori potențatori ai amenințării cibernetice

2. Viziunea pentru 2021-2026

3. Principii

4. Obiectivele Strategiei de Securitate Cibernetică a României 2.0

- 4.1. **Rețele și sisteme informatice sigure și reziliente**
- 4.2. **Cadru normativ și instituțional consolidat**
- 4.3. **Parteneriat public-privat pragmatic**
- 4.4. **Reziliență prin abordare proactivă și descurajare**
- 4.5. **România - actor relevant în arhitectura internațională de cooperare**

5. Concepte, definiții și termeni

1. Introducere

1.1. Sumar

Evoluția rapidă a domeniului tehnologic și dinamica amenințării cibernetice sunt condiții determinante pentru actualizarea și dezvoltarea permanentă a cadrului normativ și instituțional pe componenta gestionării amenințărilor cibernetice și asigurării securității cibernetice.

România este prezentă pe harta Țintelor atacurilor cibernetice, confruntându-se permanent, atât cu atacuri complexe, care au ca scop obținerea unor avantaje strategice sau a unor beneficii financiare, cu potențial impact major la adresa securității naționale, societății și economiei, cât și cu atacuri „clasice”, care folosesc malware comun și exploatează vulnerabilități larg răspândite și cunoscute, și care, deși au un potențial redus de a aduce atingere securității naționale, afectează economia și societatea.

Un impact major asupra evoluțiilor în modul de abordare a securității cibernetice în plan național este generat și de demersurile de la nivelul ONU, NATO și UE, unde protecția spațiului cibernetic reprezintă o prioritate.

Continuând demersul în plan normativ inițiat prin Strategia de Securitate Cibernetică a României din 2013, **Strategia de Securitate Cibernetică a României 2.0** reprezintă documentul de bază pentru planificarea acțiunilor subsumate securității cibernetice a României, în acord cu documentele de natură strategică asumate până în prezent, îndeosebi Strategia Națională de Apărare a Țării.

În acest sens, **Strategia de Securitate Cibernetică a României 2.0** identifică **5 obiective de importanță națională** a căror implementare conjugată, printr-o coordonare și cooperare adecvată între instituțiile publice cu responsabilități în domeniu, sectorul privat, mediul academic și cetățeni, este menită să consolideze deopotrivă securitatea cibernetică națională și rolul României în plan regional, european și internațional și să dezvolte un ecosistem digital performant. Cele **5 obiective de importanță strategică** pentru 2021-2026 în domeniul securității cibernetice sunt:

La nivel internațional pot fi amintite:

- demersurile **UE** de implementare a prevederilor noii Strategii de securitate cibernetică a UE pentru decada digitală, Directivei UE privind măsurile de asigurare a unui nivel comun ridicat de securitate a rețelelor și a informației și Actului privind Securitatea Cibernetică, precum și inițiativele recente de revizuire a acestora;

- abordarea **NATO** care a declarat spațiul cibernetic ca spațiu operațional, a încurajat statele membre să-și dezvolte capabilitățile de apărare și descurajare și a întreprins demersuri pentru revizuirea politicii de apărare în domeniul cibernetic;

- demersurile la nivel **ONU** privind definirea și adaptarea cadrului normativ aferent comportamentului responsabil al statelor în spațiul cibernetic.

1. Rețele și sisteme informatice sigure și reziliente

2. Cadru normativ și instituțional consolidat

3. Parteneriat public-privat pragmatic

4. Reziliență prin abordare proactivă și descurajare

5. România - actor relevant în arhitectura internațională de cooperare

Măsurile concrete ce trebuie întreprinse pentru atingerea obiectivelor sunt cuprinse în **Planul de Acțiune pentru 2021-2026** și reprezintă o responsabilitate comună a tuturor actorilor implicați.

1.2. Context și importanța securității cibernetice

Dezvoltarea continuă a tehnologiilor IT&C și nivelul din ce în ce mai ridicat de interconectivitate și interoperabilitate între sisteme contribuie semnificativ la schimbarea percepției asupra riscurilor, vulnerabilităților și amenințărilor provenite din spațiul cibernetic.

Atacurile cibernetice se află într-o evoluție continuă, atât din punct de vedere al numărului, cât și al complexității metodelor specifice utilizate. Acestea vizează un număr mare și o varietate de rețele și sisteme informatice, de la cele care deservește persoane fizice, instituții publice sau entități private, până la cele care deservește entități a căror activitate se încadrează în ecuația securității naționale.

Totodată, atacurile cibernetice, în special asupra serviciilor esențiale ori a infrastructurilor critice pot avea, datorită interconectivității, impact asupra serviciilor furnizate la nivel regional sau internațional, cu efecte destabilizatoare regionale sau internaționale, în plan economic și social, și cu potențiale repercusiuni la adresa păcii și stabilității.

Un spațiu cibernetic sigur este atât responsabilitatea statului, prin autoritățile competente, cât și a sectorului privat și a societății civile. Consolidarea parteneriatelor între instituțiile statului și societatea civilă, respectiv mediul privat, precum și a celor între state și organizații internaționale este un punct esențial de atins în obținerea unui spațiu cibernetic mondial, deschis și sigur.

Dezvoltarea accelerată a tehnologiilor și lipsa unor standarde și reglementări care să impună producătorilor implementarea conceptului de securizare integrată a acestora, se transpun într-un nivel precar al securității cibernetice și într-un interes sporit al atacatorilor cibernetici. Securitatea cibernetică a tehnologiilor a devenit astfel un aspect de importanță strategică.

În același timp, noile tehnologii și implementarea rapidă a unei interconectivități sporite în domenii esențiale oferă oportunități reale de creștere economică și dezvoltare socială în România, generând evoluția securității cibernetice ca domeniu de afaceri. Tehnologiile emergente, precum internetul obiectelor (*Internet of Things*), inteligența artificială (*Artificial Intelligence*), tehnicile de învățare automată (*Machine Learning*) și tehnologii de comunicații de bandă (*5G și generații viitoare*), se pot constitui în oportunități de lansare a unor investiții în contextul dezvoltării

procesului industriei 4.0, tehnologiei medicale și mobilității 4.0, precum și al creșterii competitivității economice, atât pe plan național, cât și internațional.

De asemenea, găzduirea la București a **Centrului de competențe european industrial, tehnologic și de cercetare în materie de securitate cibernetică**, va avea un rol important în conectarea actorilor relevanți de la nivel public cu cei din cercetare și industrie. Centrul va derula investițiile viitoare ale UE în domeniul securității cibernetice, cu sprijinul unei rețele de Centre Naționale de Coordonare, ce vor fi create sau selectate ulterior de către fiecare stat membru. Mai mult, va fi un catalizator al inovării, cercetării și colaborării din domeniul securității cibernetice și va contribui decisiv la dezvoltarea ecosistemului în domeniu, atât la nivel european, cât și național.

1.3. *Amenințările cibernetice la adresa României*

Pentru a putea stabili obiective și măsuri adecvate de securitate cibernetică și de creștere a rezilienței în raport cu amenințarea cibernetică este importantă cunoașterea și înțelegerea amenințării la nivelul tuturor actorilor implicați, fie ei instituții publice, entități private sau societate civilă.

La nivel național, amenințarea cibernetică se situează în prezent pe un trend ascendent, **principala provocare la adresa securității cibernetice fiind reprezentată de atacurile cibernetice** derulate în special de trei categorii de atacatori:

- **entități asociate unor actori statali;**
- **grupări de criminalitate cibernetică;**
- **grupări de hackeri cu motivație ideologică, politică sau extremist-teroristă.**

Atacatorii cibernetici dețin capacități tehnologice și resurse diferite folosite pentru derularea de atacuri având motivații diferite.

O altă provocare la adresa securității cibernetice este reprezentată de exploatarea unor rețele și sisteme informatice de pe teritoriul României pentru utilizarea lor în atacuri cibernetice îndreptate împotriva unor entități din alte state. Astfel, atacatorii utilizează elemente de infrastructură de pe teritoriul României, în special pentru crearea de servere de comandă și control sau pentru crearea unor puncte intermediare în cadrul infrastructurii de atac, care le permit acestora o mai bună anonimizare a activităților ostile.

Entități asociate unor actori statali

Amenințarea cibernetică generată de **entități asociate unor actori statali** reprezintă cea mai importantă formă de amenințare la adresa securității cibernetice a

României și are un impact ridicat asupra securității naționale. Țintele vizate sunt rețele și sisteme informatice cu valențe critice pentru securitatea națională, îndeosebi din domeniul diplomatic, militar, economic și social.

Atacurile cibernetice derulate de actori statali sunt de regulă de tip *Advanced Persistent Threat (APT)*. Au un nivel tehnologic ridicat, atât în ceea ce privește modul de operare, cât și din punct de vedere al aplicațiilor malware folosite, actualizate permanent în vederea eludării mecanismelor de detecție și menținerii persistenței pentru o perioadă îndelungată de timp. Instrumentarul cibernetic folosit de atacatori este divers, adaptat scopurilor operaționale ale acestora.

În ceea ce privește România, atacurile cibernetice derulate de entități asociate actorilor statali au vizat rețele și sisteme informatice ale unor instituții guvernamentale, obiectivul principal fiind exfiltrarea de informații strategice din domenii de interes. Având în vedere că un astfel de atac are cel mai probabil în spate o entitate adversă României, exfiltrarea unor astfel de informații ar putea avea implicații majore pentru securitatea națională, efectele fiind multiplicat exponențial în plan operațional, strategic și de imagine într-un interval de timp ce nu poate fi stabilit.

Motivația atacurilor cibernetice derulate de entități asociate unor actori statali este una **strategică**, aceștia urmărind preluarea și menținerea sub control a rețelilor și sistemelor informatice atacate cu scopul de a:

- exfiltra sau a încerca să exfiltreze informații de interes, cu valențe strategice (*spionaj cibernetic*);
- perturba sau chiar întrerupe funcționalitatea unor infrastructuri critice de tipul unor facilități industriale sau în domeniul serviciilor publice de importanță strategică (*sabotaj cibernetic*);
- influența procese socio-politice pentru a genera dezechilibre la nivelul societății.

Grupări de criminalitate cibernetică

Amenințarea generată de atacurile cibernetice derulate de **grupările de criminalitate cibernetică** a cunoscut în ultimii ani o amploare deosebită, fapt generat atât de creșterea numărului și complexității atacurilor, cât și de diversificarea Țintelor vizate.

Motivația acestor atacuri este, de regulă, una **financiară**, obiectivul grupărilor de criminalitate cibernetică fiind reprezentat de obținerea de beneficii financiare sau de informații care să le asigure câștiguri financiare pe viitor.

Astfel de atacuri generează pe de o parte riscuri de compromitere a datelor stocate pe aceste sisteme și de afectare, cel puțin temporară, a activității entităților respective, iar pe de altă parte pot avea un impact financiar major atât la nivelul entităților vizate, cât și la nivel național.

Referitor la activitatea grupărilor de criminalitate cibernetică, se pot distinge două categorii:

- *cyber-enabled crime* - activități care presupun folosirea spațiului cibernetic pentru îndeplinirea obiectivelor;
- *cyber-dependent crime* - activități desfășurate exclusiv în spațiul cibernetic.

Peisajul autohton a fost dominat în ultimii ani de atacuri cibernetice cu aplicații malware de tip *ransomware*, *infostealer* sau *cryptojacking*, care au vizat rețele și sisteme informatice aparținând unor entități publice sau private. De asemenea, se remarcă intensificarea atacurilor cibernetice din ce în ce mai complexe, inclusiv de tip *APT*, dedicate exploatării sistemelor informatice din domeniul financiar-bancar.

Grupări de hackeri cu motivație ideologică, politică sau extremist-teroristă

Atacurile derulate de aceste tipologii de actori, a căror motivație este una ideologică, politică sau extremist-teroristă au în continuare un nivel tehnologic relativ redus și vizează sisteme cu nivel scăzut de securitate cibernetică.

Exponenții acestor categorii de atacatori derulează de regulă atacuri cibernetice de tip *defacement*, *Distributed Denial of Service (DDoS)* și *SQL Injection* pentru a indisponibiliza sau afecta funcționalitatea unor rețele și sisteme informatice. Țintele vizate sunt reprezentate îndeosebi de instituții publice, dar și de entități private sau academice.

Evoluția acestei amenințări este una **dinamică**, potențată de existența unor evenimente pe scena politică și socială, națională și internațională, care prezintă interes pe agenda grupărilor și **imprevizibilă** în cazul în care astfel de atacatori ar obține acces la capacități tehnologice ridicate pentru a putea exploata eventuale vulnerabilități ale unor rețele și sisteme informatice de interes pentru securitatea națională.

1.4. Factori potențatori ai amenințării cibernetice

Derularea de atacuri cibernetice la adresa rețelilor și sistemelor informatice este potențată de factori precum:

1. *existența unor vulnerabilități de ordin tehnologic, procedural și uman ce se manifestă la nivelul rețelilor și sistemelor informatice vizate*

Succesul unor atacuri cibernetice este asigurat și prin exploatarea unor vulnerabilități care nu au fost remediate. Deseori vulnerabilitățile sunt cunoscute, iar producătorii și firmele de securitate cibernetică publică atenționări cu privire la acestea, precum și soluții de remediere, însă, pe fondul unui nivel scăzut al culturii de securitate cibernetică a utilizatorilor și a unei pregătiri deficitare a administratorilor, atacatorii continuă să își îndeplinească scopurile prin exploatarea lor.

De asemenea, implementarea deficitară a unor politici de securitate cibernetică, precum și utilizarea în continuare a unor rețele și sisteme informatice cu versiuni vechi de software, care nu mai poate fi actualizat sau optimizat din punct de vedere al securității cibernetice, creează noi oportunități de exploatare pentru potențialii atacatori cibernetici.

2. disponibilitatea și accesibilitatea resurselor de hacking

În prezent, instrumente și cunoștințe necesare derulării de atacuri cibernetice pot fi obținute cu ușurință din mediul online (platforme de specialitate, forumuri de criminalitate cibernetică etc.). Având în vedere costul scăzut și accesul facil, de aceste resurse pot beneficia inclusiv persoane cu minime cunoștințe tehnice, generând, pe de o parte, o creștere cantitativă și calitativă a atacurilor, și accentuând, pe de altă parte, dificultatea cu care acțiunile din spațiul cibernetic pot fi atribuite.

3. nivelul scăzut de cultură de securitate cibernetică și de igienă în spațiul cibernetic

Reziliența rețelelor și sistemelor informatice și capacitatea unei organizații de a preveni și contracara atacurile cibernetice sunt dependente, într-o mare măsură, de gradul de conștientizare cu privire la amenințarea cibernetică. De asemenea, o bună igienă în spațiul cibernetic și o cultură de securitate cibernetică adecvată deținute de utilizatori se pot transpune proporțional la nivelul instituțiilor, organizațiilor sau companiilor.

4. insuficienta pregătire și specializare în domeniul securității cibernetice a angajaților și a managerilor

În contextul tehnologiilor emergente și a evoluției rapide a acestora, este dificilă consolidarea unui nivel de pregătire adecvat pentru asigurarea securității cibernetice în instituții publice și private. Elementul de noutate caracteristic spațiului cibernetic și domeniului securității cibernetice generează o nevoie constantă de pregătire a personalului. De această pregătire trebuie să beneficieze și palierul managerial, pentru buna înțelegere a riscurilor de securitate cibernetică, a impactului pe care atacurile cibernetice îl pot avea în raport cu activitatea desfășurată, dar și a măsurilor ce trebuie aplicate pentru a evita producerea unor astfel de evenimente cibernetice.

5. carențe normative și procedurale

Având în vedere toate provocările din domeniul securității cibernetice, cadrul normativ și procedural trebuie să sprijine autoritățile responsabile în prevenirea, contracararea, investigarea și diminuarea riscurilor generate prin derularea de atacuri cibernetice la adresa rețelelor și sistemelor informatice. Totodată, cadrul normativ și procedural în domeniu trebuie să asigure un mediu organizat și eficient, atât printr-o abordare cuprinzătoare la nivel guvernamental, cât și printr-o abordare multi-sectorială.

Cadrul normativ trebuie să respecte obligațiile care revin României în temeiul dreptului internațional și să ofere instrumentele necesare unui nivel ridicat de securitate cibernetică și de reprezentare adecvată și coerentă la nivel internațional.

6. extinderea gamei de dispozitive

Implementarea soluțiilor de interconectare și dezvoltarea internetului obiectelor, atât la nivel industrial, cât și la nivelul întregii societăți, conduc la creșterea și diversificarea impactului atacurilor cibernetice, care poate consta în daune fizice sau afectarea sănătății sau vieții cetățenilor.

Prin urmare, la momentul actual, trebuie avute în vedere nu numai daunele produse în spațiul cibernetic, cauzate de o securitate cibernetică inadecvată a sistemelor proprii, ci și cele cauzate de amenințări la adresa sistemelor interconectate, care sunt fundamentale pentru societate.

7. lipsa cadrului de reglementare și a politicilor de management al riscurilor de natură cibernetică ale lanțului de aprovizionare

Managementul riscurilor de natură cibernetică ale lanțului de aprovizionare trebuie să constituie o prioritate la nivel național și să fie abordat pe întreg ciclul de viață al produselor și serviciilor, începând cu faza de proiectare și continuând cu dezvoltarea, livrarea, exploatarea, mentenanța și scoaterea din funcțiune.

2. Viziunea pentru 2021-2026

România are capacitatea de a detecta atacuri cibernetice la adresa rețelelor și sistemelor informatice de pe teritoriul național și de a diminua efectele acestora. Viziunea **Strategiei de Securitate Cibernetică a României 2.0** este ca, în fața unei amenințări cibernetice din ce în ce mai complexe, România să își dezvolte și consolideze capacitățile de prevenire, descurajare și răspuns, precum și reziliența, inclusiv printr-o abordare proactivă, adecvată cadrului internațional de cooperare în domeniu.

Filosofia de protecție în spațiul cibernetic nu se rezumă numai la proceduri și **măsuri reactive**, condiție necesară, însă nu și suficientă pentru a face față evoluțiilor în domeniul amenințărilor cibernetice. Noua viziune trebuie să aibă în vedere și **abordări proactive**, care permit detectarea amenințării înainte de a ajunge în rețelele și sistemele informatice din România și dezvoltarea unor mecanisme adecvate de răspuns în acord cu respectarea dreptului internațional. Abordarea se regăsește în strategiile actuale ale mai multor state partenere și conferă un cadru mult mai larg de acțiune care să contribuie la prevenirea și descurajarea amenințărilor provenite din spațiul cibernetic și la asigurarea securității cibernetice.

Acțiunile conjugate ale actorilor implicați trebuie să vizeze:

- **prevenire și descurajare** - dezvoltarea permanentă a capacităților de detecție, investigare, combatere și atribuire a atacurilor cibernetice;

- **apărare și contracarare** - dezvoltarea și implementarea unor capacități eficiente de apărare și a unor mecanisme proactive, de răspuns la atacuri cibernetice curente și emergente;

- **dezvoltare și consolidare** - creșterea nivelului de securitate cibernetică și reziliență prin:

1. prioritizarea investițiilor în domeniul securității cibernetice;
2. dezvoltarea programelor educaționale;
3. consolidarea culturii de securitate cibernetică;
4. dezvoltarea cercetării și inovării în domeniu;
5. definirea și promovarea unui model național de reziliență cibernetică;
6. cooperarea la nivel național, european și internațional.

3. *Principii*

În vederea asigurării securității cibernetice a României trebuie respectate următoarele **principii**:

1. Securitatea cibernetică, parte integrantă a securității naționale, este responsabilitatea tuturor actorilor implicați: entități publice, private și cetățeni

Atacurile cibernetice vizează rețelele și sistemele informatice de pe teritoriul României, inclusiv cele cu impact la adresa securității naționale. Având în vedere interconectarea și interdependența dintre acestea, precum și faptul că se află atât în responsabilitatea instituțiilor publice, cât și a entităților private, securitatea cibernetică poate fi asigurată numai prin cooperare și dialog.

Gestionarea riscurilor de securitate cibernetică trebuie să devină parte integrantă a specificului organizațional al fiecărei entități, fie ea publică sau privată.

Partajarea oportună a informațiilor privind riscurile, amenințările, vulnerabilitățile sau soluțiile de securitate cibernetică, atât la nivel inter-instituțional, cât și în cadrul parteneriatului public-privat, reprezintă un element cheie al consolidării coerente a rezilienței rețelelor și sistemelor informatice naționale.

Autoritățile guvernamentale cu responsabilități în domeniul securității cibernetice au, printre altele, rolul de a:

- informa mediul public, mediul privat și societatea civilă cu privire la importanța securității cibernetice, necesitatea utilizării responsabile a noilor tehnologii sau servicii digitale și obligațiile ce revin României prin aplicarea în spațiul cibernetic a dreptului internațional existent;

- coordona asigurarea securității cibernetice la nivel național, prin crearea condițiilor necesare și facilitarea cooperării în acest sens.

Toate entitățile, publice sau private, sunt responsabile pentru asigurarea securității cibernetice a rețelelor și sistemelor informatice pe care le dețin, menținerea funcționării normale a serviciilor pe care le oferă și înglobarea unui nivel de securitate cibernetică ridicat pentru produsele pe care le proiectează și comercializează.

Nu în ultimul rând, cetățenii, în calitate de utilizatori finali, trebuie să aibă o responsabilitate civică individuală de asigurare a securității cibernetice, în sensul aplicării unei igiene în spațiul cibernetic, prin promovarea unui comportament responsabil în utilizarea tehnologiilor, a rețelelor și sistemelor informatice.

2. Securitatea cibernetică sprijină funcționarea statului și a societății, creșterea competitivității economiei naționale, dezvoltarea capacităților naționale de cercetare-dezvoltare și inovare

În ultimii ani, domeniul IT&C are o componentă din ce în ce mai consistentă de securitate cibernetică. Trebuie susținute inițiativele de cercetare, inovare și dezvoltare

în domeniul securității cibernetice, care se pot constitui în oportunități de creștere a competitivității economiei naționale și de recuperare a unor decalaje economice față de alte state, de creare și menținere în România a unei resurse umane înalt specializată în domeniul securității cibernetice, precum și de creștere a capabilităților naționale de cercetare-dezvoltare și inovare.

Se va urmări asigurarea coerenței între aceste inițiative și eforturile de consolidare a rezilienței cibernetice printr-o coordonare eficientă a politicilor în domeniu.

3. Securitatea cibernetică se bazează pe stabilirea unui cadru normativ adecvat

Actualizarea și adaptarea constantă a cadrului normativ și procedural sunt necesare pentru îndeplinirea obiectivelor de securitate cibernetică, având în vedere evoluția permanentă a tehnologiei și reglementărilor în materie, de la nivel internațional.

Dezvoltarea cadrului normativ se va realiza în baza acquis-ului european și cu luarea în considerare a obligațiilor ce revin României în temeiul dreptului internațional, inclusiv în materie de drepturi și libertăți ale omului.

4. Securitatea cibernetică este consolidată printr-o cooperare pragmatică la nivel internațional

Spațiul cibernetic nu este limitat de granițe, astfel încât securitatea cibernetică trebuie gândită și asigurată la nivel internațional. În acest sens, atingerea obiectivelor naționale, europene și internaționale necesită cooperarea tuturor actorilor implicați.

Cadrul normativ la nivel internațional oferă un set de norme, reguli, principii și obligații de drept internațional, care stabilesc limitele unui comportament responsabil statal în relațiile internaționale.

România trebuie să continue să joace un rol activ și relevant în structurile și inițiativele majore pe plan internațional legate de acțiunile din domeniul digital și al securității cibernetice și să își consolideze poziția de centru de excelență și actor relevant pentru securitatea cibernetică europeană și internațională.

5. În asigurarea securității cibernetice este garantată menținerea unui spațiu cibernetic deschis, liber, stabil și sigur, cu aplicarea deplină a drepturilor omului și libertăților fundamentale și a statului de drept, precum și protejarea libertăților individuale și a datelor cu caracter personal.

Asigurarea securității cibernetice presupune aplicarea în spațiul cibernetic a acelorași norme și valori ca în spațiul fizic și trebuie să se bazeze pe respectarea, promovarea și protejarea exercițiului drepturilor omului și a libertăților fundamentale, în special în ceea ce privește libertatea de opinie, libertatea de exprimare, dreptul de

a accesa și de a primi informații, precum și pe protejarea datelor cu caracter personal și a dreptului la viață privată, atât în mediul online, cât și offline.

Eforturile României în domeniul asigurării și gestionării securității cibernetice vor fi definite în acord cu obligațiile care decurg din aplicarea în spațiul cibernetic a dreptului internațional existent, inclusiv Carta ONU și dreptul internațional umanitar și a normelor vizând un comportament responsabil la nivel de stat în spațiul cibernetic aferente dezbaterilor la nivelul ONU pentru menținerea unui spațiu cibernetic și al tehnologiei informațiilor și comunicațiilor care să fie deschis, sigur, stabil și accesibil.

Totodată, o atenție particulară va fi acordată de către România dezbaterilor la nivel UE în ceea ce privește „mediul digital și drepturile omului” și „inteligenta artificială și drepturile omului”.

4.1. Rețele și sisteme informatice sigure și reziliente

Pentru România este prioritară securitatea cibernetică a rețelilor și sistemelor informatice, îndeosebi a celor din domenii esențiale și importante, precum și a celor cu valențe critice pentru securitatea națională. Menținerea în parametri optimi a disponibilității, continuității și integrității și asigurarea rezilienței acestora contribuie la susținerea în condiții optime a tuturor domeniilor vieții economice și sociale.

Entitățile publice și private trebuie să implementeze și să operaționalizeze politici de securitate cibernetică adecvate. Acest deziderat presupune inclusiv realizarea de investiții în domeniul tehnologic și alocarea de resursă umană cu pregătire de specialitate. Totodată este necesară impunerea și respectarea unui set de standarde calitative pentru produsele și serviciile utilizate în cadrul acestor rețele și sisteme.

Măsuri:

4.1.1. Implementarea de politici și măsuri de securitate cibernetică

Pentru a putea avea rețele și sisteme informatice sigure este dezirabilă crearea și implementarea corectă, de către întregul personal al unei entități, a unui set minim de politici și măsuri de securitate cibernetică. Acestea trebuie să fie adaptabile, permanent corelate cu nivelul amenințării cibernetică și cu trendul rapid de dezvoltare al tehnologiilor.

De asemenea, aceste politici trebuie să fie însoțite de implementarea unor planuri de recuperare în caz de atac cibernetic și de măsuri tehnice și organizaționale, menite să contribuie la creșterea atât a capacității de reacție la atacuri și incidente de securitate cibernetică, cât și a rezilienței infrastructurilor.

În plus, este necesar ca fiecare operator de rețele și sisteme cu impact la adresa securității naționale, inclusiv cei desemnați prin legislația de transpunere a Directivelor NIS, să elaboreze proceduri de testare și auditare periodică a nivelului de securitate cibernetică, ca parte integrantă a procesului de evaluare a riscurilor, și să actualizeze permanent tehnologiile hardware și software folosite în cadrul infrastructurilor.

În același timp, instituțiile statului cu responsabilități în asigurarea securității cibernetică trebuie să încurajeze și să susțină implementarea de politici și măsuri de securitate cibernetică prin crearea unui cadru de lucru unitar, oferirea pregătirii necesare și coagularea unei comunități de experți în domeniu.

4.1.2. Dezvoltarea capabilităților naționale de detectare, investigare și contracarare a atacurilor cibernetică

Pentru a avea rețele și sisteme informatice sigure și reziliente este necesară dezvoltarea și adaptarea permanentă a capabilităților de detecție și investigare. Acest lucru trebuie să fie făcut în concordanță atât cu evoluțiile tehnologice, cât și cu schimbările mediului de securitate cibernetică, printr-o cooperare între entități publice și private.

Cunoașterea obținută ca urmare a investigațiilor derulate reprezintă un element important în contracararea și, ulterior, în atribuirea atacurilor cibernetice.

4.1.3. Alocarea eficientă a resurselor financiare, tehnologice și umane

Având în vedere diversitatea domeniilor în care se regăsesc rețele și sisteme informatice și interconectarea dintre acestea, este importantă promovarea și conștientizarea în rândul operatorilor, entități publice sau private, a necesității realizării de investiții în tehnologii.

Aceste investiții trebuie să fie susținute prin demersuri de specializare a personalului din domeniu, care să fie pregătit pentru a:

- înțelege amenințarea provenită din spațiul cibernetic;
- cunoaște evoluțiile din domeniul tehnologic;
- dobândi cunoștințele necesare pentru o reacție adecvată în cazul unui atac cibernetic sau a unui incident de securitate cibernetică.

O cooperare permanentă între instituțiile statului cu responsabilități în domeniul securității cibernetice, precum și între acestea și mediul de afaceri și industrie este dezirabilă în sensul partajării cunoașterii, de exemplu prin elaborarea de ghiduri de bune practici, recomandări pe domenii de activitate, identificării celor mai bune soluții de asigurare a protecției rețelelor și sistemelor informatice, precum și alocării eficiente și complementare a resurselor.

4.1.4. Consolidarea mecanismului de raportare a incidentelor de securitate cibernetică

Un sistem de management centralizat al incidentelor de securitate cibernetică oferă imaginea de ansamblu asupra amenințării cibernetice la adresa unei infrastructuri, a unui domeniu de activitate și chiar a securității naționale. Totodată, un mecanism de raportare eficient contribuie la asigurarea unui răspuns concret la amenințările provenite din spațiul cibernetic.

Este necesară elaborarea unui set de măsuri și mecanisme de raportare a incidentelor, îndeosebi la nivelul entităților care operează rețele și sisteme informatice din domenii esențiale și importante sau cu valențe critice pentru securitatea națională. Operatorii trebuie să înțeleagă și să își asume rolul *de facto* și atribuțiile care le revin și să optimizeze fluxul subsumat mecanismului de raportare a incidentelor de securitate cibernetică, în conformitate cu recomandările și reglementările UE și cu legislația națională.

4.1.5. Crearea unor mecanisme de certificare, conformitate și standardizare în domeniul securității cibernetice

Calitatea și nivelul de securitate cibernetică al produselor hardware și software folosite sunt deosebit de importante pentru menținerea unor rețele și sisteme informatice sigure și reziliente în fața amenințărilor cibernetice și trebuie să prevaleze aspectelor restrictive de ordin bugetar.

În acest sens, este necesară crearea unor mecanisme la nivel național de certificare, conformitate și standardizare în domeniul securității cibernetice, care să aibă în vedere un set strict de criterii (tehnice, non-tehnice, inclusiv prin raportare la aspecte ce țin de securitate națională) și care să permită identificarea riscurilor și vulnerabilităților de securitate cibernetică existente la nivelul produselor hardware și software.

4.1.6. Securizarea lanțului de aprovizionare

Trebuie menținută în atenție securizarea lanțului de aprovizionare, prin impunerea implementării unor mecanisme de securitate cibernetică la toate componentele acestui ecosistem.

4.2. Cadru normativ și instituțional consolidat

Pentru diminuarea riscurilor generate de atacuri cibernetice și consolidarea nivelului de securitate cibernetică a României, este esențial să fie dezvoltate și eficientizate formate de cooperare, de nivel strategic, tactic și operațional, între toate părțile interesate relevante în domeniu. În plus, este importantă optimizarea relaționării și schimbului de informații dintre sectorul public și cel privat în vederea asigurării unei conștientizări comune a situației.

Cadrul general de cooperare, reprezentat de Sistemului Național de Securitate Cibernetică (SNSC), prin Consiliul Operativ de Securitate Cibernetică (COSC), a avut rolul de a conștientiza și cristaliza la nivelul instituțiilor statului și societății că o condiție *sine qua non* în abordarea elementelor de cunoaștere, prevenire, descurajare și răspuns la amenințările cibernetice la adresa României o reprezintă cooperarea consolidată la nivelul tuturor actorilor naționali.

Activitățile în domeniul securității cibernetice la nivelul SNSC au demonstrat utilitatea și viabilitatea acestui mecanism de cooperare la nivel strategic, însă au relevat necesitatea unei consolidări a rolului COSC și unor abordări tactic-operaționale flexibile și eficiente la nivel național prin crearea unei entități care să asigure arhitectura de cooperare necesară.

Măsuri:

4.2.1. Consolidarea cadrului normativ

Unul dintre principalele elemente care condiționează îndeplinirea obiectivelor de securitate cibernetică este reprezentat de asigurarea unui cadru normativ adaptat în permanență evoluțiilor tehnologice și armonizat cu reglementările în materie la nivel internațional. În acest sens, se va urmări modernizarea cadrului legislativ actual și asigurarea procedurilor și mecanismelor de cooperare la nivel național.

Este necesară adoptarea Legii privind Securitatea și Apărarea Cibernetică, prin care sunt stabilite: cadrul necesar privind organizarea și desfășurarea activităților din domeniile securitate și apărare cibernetică, mecanismele de cooperare și responsabilitățile instituțiilor cu atribuții în domeniile menționate.

Elaborarea politicilor, strategiilor, planurilor de acțiune legate de securitatea cibernetică și punerea lor în aplicare se va realiza de manieră compatibilă cu normele internaționale de comportament responsabil în spațiul cibernetic, cu respectarea dreptului internațional și cu minimizarea posibilului impact negativ asupra activității societății civile.

După caz, legislația ar trebui să prevadă mecanisme destinate asigurării transparenței, tragerii la răspundere a persoanelor vinovate de comiterea abuzurilor și compensării victimelor abuzurilor.

4.2.2. Consolidarea cadrului instituțional

Consolidarea rolului COSC

Consiliul Operativ de Securitate Cibernetică (COSC) rămâne mecanismul de cooperare inter-instituțională, care coordonează unitar, la nivel operațional, activitățile Sistemului Național de Securitate Cibernetică (SNSC). Activitățile, componența și responsabilitățile COSC trebuie stabilite în cadrul Legii privind Securitatea și Apărarea Cibernetică.

De la înființarea sa, COSC a avut un rol esențial în susținerea unor demersuri în domeniul securității cibernetice cu impact atât la nivel național, cât și internațional. COSC trebuie să rămână formatul în care să fie actualizate constant prioritățile, în funcție de rezultatele obținute anterior, și adoptate deciziile care să fie transpuse ulterior în măsuri concrete de nivel procedural, operațional, tactic și strategic.

În urma analizei și evaluării stării de securitate cibernetică la nivel național, COSC trebuie să adopte decizii, transpuse în propuneri înaintate Consiliului Suprem de Apărare a Țării (CSAT), privind nivelurile de alertă cibernetică naționale, planuri și direcții de acțiune, dezvoltare și investiții, precum și linii de mandat referitoare la decizii și documente de politică externă în domeniul securității cibernetice.

În acest sens, pentru o coordonare optimă între deciziile adoptate și măsurile identificate și o impulsioneare a implementării acestora, este necesar ca activitatea COSC să fie organizată după un calendar prestabilit.

Înființarea Directoratului Național de Securitate Cibernetică

În contextul actual, se impune înființarea unei instituții noi, cea a **Directoratului Național de Securitate Cibernetică (DNSC)**, care să preia atribuțiile CERT-RO și să facă față în mod dinamic provocărilor în domeniul securității cibernetice prin mecanisme, proceduri și capacități performante, flexibile și proactive.

În activitatea derulată, DNSC va avea în vedere îndeplinirea următoarelor obiective majore, precum:

- asigurarea cadrului de strategii, politici și reglementări în domeniul securității cibernetice, în colaborare sau cu avizul instituțiilor care au competențe și atribuții în domeniu;
- crearea unui centru de cooperare la nivel național și internațional între instituții din domeniul public, privat și academic;
- alinierea cu celelalte state ale UE în ceea ce privește certificarea și standardizarea domeniului securității cibernetice;
- alinierea României la procesele de implementare a noilor tehnologii;
- gestionarea crizelor de securitate cibernetică la nivel național, în cooperare cu instituțiile care au competență în domeniul managementului crizelor, sub autoritatea COSC.

De asemenea, DNSC va reprezenta o interfață a instituțiilor membre COSC pentru cooperarea cu societatea civilă, mediul privat și cel academic, constituindu-se cadrul optim pentru a crea și dezvolta parteneriate eficiente în domeniul securității cibernetice.

4.3. Parteneriat public-privat pragmatic

Un parteneriat public-privat pragmatic, între instituții publice, entități private, mediul academic și de cercetare și cetățeni reprezintă o necesitate în condițiile în care atacurile cibernetice vizează un număr mare și un spectru larg de rețele și sisteme informatice.

Pentru a putea preveni materializarea unor atacuri cibernetice este important ca subiectul securității cibernetice să fie adus în atenția întregii societăți, prin derularea unor programe de conștientizare publică, de creștere a nivelului de cultură de securitate cibernetică și de promovare a unor măsuri de igienă în spațiul cibernetic.

De asemenea, un element de interes comun îl reprezintă dezvoltarea și implementarea unor programe de învățământ și formate de pregătire în domeniul securității cibernetice.

Toate aceste măsuri generează beneficii economico-sociale majore: existența resursei umane calificate și chiar înalt specializate, capabile să răspundă provocărilor mediului de securitate cibernetică, creșterea contribuției industriei IT&C și de securitate cibernetică la PIB-ul național.

Măsuri:

4.3.1. Derularea unor programe de conștientizare publică și de creștere a nivelului de cultură de securitate cibernetică

Este importantă crearea de programe de creștere a nivelului culturii de securitate cibernetică atât la nivelul entităților publice și private, prin campanii specializate derulate de instituțiile statului cu responsabilități, cât și la nivelul publicului larg, sub forma unor campanii de informare prin programe media, broșuri, website-uri dedicate, ghiduri de igienă în spațiul cibernetic.

De asemenea, este importantă introducerea unor noțiuni de bază privind igiena în spațiul cibernetic încă din ciclul primar de învățământ și dezvoltarea unor programe educaționale în domeniul securității cibernetic.

Subiectul securității cibernetică trebuie adus în atenția a cât mai mulți utilizatori, din toate domeniile de activitate (instituții publice, entități private, mediul academic și de cercetare, cetățeni). Pentru a determina o creștere a nivelului de cultură de securitate cibernetică vor continua să fie organizate, în parteneriat public-privat, o serie de evenimente publice și dezbateri.

4.3.2. Dezvoltarea de programe educaționale în domeniul securității cibernetică

Instituțiile statului, mediul privat și cel academic trebuie să conlucreze pentru susținerea, dezvoltarea și finanțarea programelor de studii preuniversitare, universitare și postuniversitare în domeniul securității cibernetică, menite să asigure crearea unei mase critice de specialiști în acest domeniu.

Pași semnificativi au fost deja întreprinși în zona postuniversitară, iar aceștia trebuie susținuți și continuați prin:

- dezvoltarea continuă, prin adaptare și racordare la evoluțiile domeniului, a programelor de pregătire, inclusiv în etapele premergătoare - studii universitare de licență și preuniversitare;
- pregătirea și instruirea cadrelor didactice și consolidarea bazei materiale, prin accesarea de finanțare externă și prin maximizarea cooperării cu mediul privat.

4.3.3. Derularea unor programe de formare profesională pentru cei care desfășoară activități în domeniul securității cibernetică

Este necesară dezvoltarea unor programe de pregătire pentru cei care desfășoară activități în domeniul securității cibernetică, în sensul: consolidării nivelului de expertiză tehnică, în raport cu evoluția amenințării și în conformitate cu dezvoltarea tehnologică și dezvoltării unui comportament profesional eficient în prevenirea, contracararea și reacția la atacuri cibernetică și incidente de securitate cibernetică.

În cadrul *Centrului de instruire în domeniul securității cibernetică* vor fi continuate programele de pregătire continuă a specialiștilor în domeniul securității

cibernetice, cu precădere administratorii responsabili cu securitatea rețelor și sistemelor informatice, a căror afectare poate avea impact negativ la adresa securității naționale. De asemenea, Centrul oferă cadrul adecvat programelor de formare a formatorilor, asigurându-se astfel transferul de cunoștințe necesar.

4.3.4. Dezvoltarea și consolidarea cercetării și inovării în domeniul securității cibernetice

Implementarea noilor tehnologii necesită încurajarea cercetării, inovării și dezvoltării în domeniul securității cibernetice pentru a putea beneficia de expertiză și resursă umană capabilă să facă față noilor provocări ce pot apărea.

Prin expertiza și resursele deținute, mediul privat poate contribui decisiv la creșterea nivelului de securitate cibernetică la nivelul României, prin conlucrarea cu specialiștii din zona publică și academică în cadrul unor inițiative comune sau al unor platforme mixte de cercetare și inovare în domeniul securității cibernetice.

Se va avea în vedere inclusiv susținerea comunității implicate în cercetare și inovare să formeze rețele la nivel European și să participe la programe de cercetare, inclusiv la cele derulate prin Centrul de competențe european industrial, tehnologic și de cercetare în materie de securitate cibernetică.

Totodată, având în vedere că domeniul securității cibernetice este unul de interes major pentru organizațiile internaționale din care România face parte, este importantă atât creșterea gradului de alocare a resurselor din PIB către acest domeniu, cât și absorbția de finanțări pentru dezvoltarea și consolidarea cercetării și inovării în domeniul securității cibernetice.

4.3.5. Dezvoltarea industriei naționale de securitate cibernetică

O industrie de securitate cibernetică prolifică și inovativă reprezintă o necesitate pentru dezvoltarea normală a economiei naționale într-un viitor marcat din ce în ce mai mult de digitalizare și evoluții tehnologice rapide.

Instituțiile guvernamentale trebuie să impulsioneze și să susțină demersuri ale mediului de afaceri și zonei academice pentru a dezvolta incubatoare de afaceri și firme noi – *start-up* – în domeniul securității cibernetice.

În sprijinul unui parteneriat public-privat pragmatic și de succes este important să fie acordate facilități fiscale necesare impulsiei domeniului.

De asemenea, trebuie definite și asumate la nivel național mecanisme pentru motivarea, păstrarea și atragerea în țară a specialiștilor în domeniul securității cibernetice, ceea ce va determina o dezvoltare sustenabilă a acestui domeniu.

4.4. Reziliență prin abordare proactivă și descurajare

În fața amenințărilor cibernetice România trebuie:

- să fie pregătită să pună în aplicare toate măsurile proactive necesare, care au ca finalitate asigurarea rezilienței rețelor și sistemelor informatice;

- să dețină capacități și mecanisme pentru a descuraja atacurile cibernetice care afectează societatea sau interesele naționale de securitate.

Măsuri:

4.4.1. Dezvoltarea de CERT-uri și SOC-uri sectoriale

Crearea unor structuri independente, de tip CERT și SOC, în domenii esențiale, va avea un rol important pentru o mai bună cunoaștere atât a amenințării, cât și a vulnerabilităților și deficiențelor dintr-un anumit domeniu și va putea genera măsuri adecvate, a căror implementare să asigure reziliența rețelelor și sistemelor informatice.

Demersul înființării CERT-urilor și SOC-urilor sectoriale poate reprezenta atât o inițiativă națională, însă poate fi pusă în practică și în domeniul privat. Totodată, inițiativa înființării unor astfel de structuri poate face obiectul unor proiecte cu finanțare europeană.

Totodată, astfel de entități vor reprezenta un centru de expertiză cibernetică pentru un anumit domeniu și vor avea un rol important prin:

- crearea de norme și proceduri unitare în domeniul securității cibernetice pentru toți operatorii de rețele și sisteme informatice dintr-un anumit domeniu;
- transfer de expertiză și bune practici între operatorii de rețele și sisteme informatice asociați aceluiași domeniu.

4.4.2. Derularea de exerciții cu aplicabilitate practică ridicată

Exercițiile de securitate cibernetică de acest tip au un rol proactiv în asigurarea rezilienței, reprezentând cadrul în care pot fi testate și îmbunătățite: capacitățile de reziliență și răspuns, mecanismele de intervenție rapidă, procedurile de cooperare în cazul unor atacuri cibernetice sau incidente de securitate cibernetică.

În continuarea demersurilor începute la nivel național, instituțiile publice cu responsabilități în domeniul securității cibernetice sunt încurajate să organizeze și să coordoneze, în cooperare cu mediul privat și academic, exerciții naționale și internaționale de securitate cibernetică și răspuns la incidente.

4.4.3. Dezvoltarea unor capacități proactive, reactive și de descurajare

Pentru asigurarea securității și apărării cibernetice a României este important să fie dezvoltate atât capacități proactive, care să permită cunoașterea anticipativă a amenințării, cât și capacități de răspuns ofensiv, în mod individual sau ca parte dintr-o coaliție, în caz de atacuri cibernetice care contravin dreptului internațional. În acest sens, se va urmări alocarea de resurse umane și tehnologice, caracterizate prin flexibilitate și adaptabilitate, în acord cu normele aplicabile la nivel național și internațional privind comportamentul responsabil al statelor în spațiul cibernetic, prin a căror desfășurare să fie descurajată activitatea actorilor cibernetici ostili intereselor naționale, europene și aliate.

România trebuie să devină o țintă dificil de atacat în spațiul cibernetic. Acest deziderat poate fi atins inclusiv prin dezvoltarea unor capacități de securizare și descurajare care să determine costuri ridicate pentru atacatori.

4.5. România - actor relevant în arhitectura internațională de cooperare

Având în vedere că amenințarea cibernetică nu cunoaște granițe, va fi urmărită angajarea României în acțiuni coordonate și eficiente la nivel internațional pentru:

- abordarea și modelarea evoluțiilor spațiului cibernetic în vederea asigurării și promovării unui internet global, liber, deschis, stabil și sigur și a unui comportament responsabil al statelor în spațiul cibernetic;
- dezvoltarea și operaționalizarea unor mecanisme eficiente de cooperare la nivel internațional, atât în cadrul organismelor și organizațiilor internaționale din care țara noastră face parte, cât și în dialogul bilateral cu state partenere care dețin capacități pe zona securității cibernetice.

Activitatea României în cadrul organismelor și organizațiilor internaționale din care face parte, contribuția activă la promovarea și implementarea inițiativelor și politicilor în domeniul securității cibernetice, consolidarea unei participări active în dialogul cu partenerii strategici în domeniu, coroborat cu evoluțiile înregistrate în plan economic, social și tehnologic în domeniul securității cibernetice la nivel național, reprezintă **factori potențatori** pentru consolidarea rolului României de actor relevant în arhitectura internațională de cooperare în domeniul securității cibernetice.

Măsuri:

4.5.1. Consolidarea rolului României la nivel global

La nivel global, România va urmări menținerea unui angajament favorabil promovării noțiunii de spațiu cibernetic global, deschis, stabil și sigur, unde drepturile omului, libertățile fundamentale și ordinea de drept se aplică pe deplin.

În susținerea acestui rol, România va apela la instrumente de diplomatie cibernetică, în special prin:

- angajament în procesele de stabilire a normelor în organizațiile cu vocație globală, precum ONU, prin sprijinirea promovării și implementării cadrului normelor de comportament responsabil statal în spațiul cibernetic, a modului de aplicare a dreptului internațional în spațiul cibernetic, a creșterii încrederii între state și a capacității acestora;
- participarea activă la dialog și consultări cu partenerii strategici la nivel internațional și în cadrul inițiativelor internaționale;
- promovarea participării la consultări și inițiative internaționale a mai multor părți interesate și actori diferiți, inclusiv sectorul public și privat, precum și societatea civilă și mediul academic pentru a adresa acest domeniu la nivel multisectorial și multidisciplinar.

4.5.2. Consolidarea rolului României la nivel regional și pe plan bilateral

În calitate de membru al UE și al organizațiilor de tip regional (OSCE, NATO, Consiliul Europei etc.), se va urmări consolidarea poziției României de actor activ în acest domeniu prin promovarea de măsuri destinate să conducă la:

- dezvoltarea și implementarea noii Strategii de securitate cibernetică a UE pentru decada digitală și susținerea acordării unei atenții sporite securității cibernetice la nivelul Politicii Externe și de Securitate Comună a UE;

- aplicarea și implementarea măsurilor prevăzute în *EU Cyber Diplomacy Toolbox*;

- operaționalizarea măsurilor de creștere a încrederii între state („Confidence Building Measures” - CBMs) la nivel OSCE;

- dezvoltarea în continuare a politicii de apărare cibernetică a NATO, consolidarea rezilienței Alianței în întregime și a aliaților, a capabilităților cibernetice de descurajare și apărare.

România va urmări să își consolideze relațiile de cooperare cu state cu viziuni

strategice congruente și să fructifice oportunitățile de nivel strategic care să o transforme în centru european de expertiză în domeniul securității cibernetice, inclusiv prin sprijinirea activităților Centrului de competențe european industrial, tehnologic și de cercetare în materie de securitate cibernetică de la București.

În contextul promovării și implementării cadrului ONU de comportament responsabil statal în spațiul cibernetic și a EU Cyber Diplomacy Toolbox, România va urmări, de asemenea, promovarea principiului de „descurajare cibernetică” prin valorificarea oportunităților oferite de posibilitatea de raliere la inițiative de tip condamnare publică în caz de atribuire a unui atac cibernetic.

Asocierea mai multor state și organizații partenere în atribuirea unui atac și comunicarea publică a sursei sau a responsabilității atacului, îndeosebi în cazul acțiunilor ofensive coordonate sau sponsorizate de actori statali, are efecte în planul afectării reputației internaționale a atacatorului și descurajării adversarului în continuarea acestui tip de acțiuni, în sensul limitării comportamentului ofensiv al acestora și consolidării securității cibernetice colective.

4.5.3. Consolidarea rolului diplomației cibernetice

România acordă o importanță ridicată activităților subsumate **diplomației cibernetice**. Interesul național cu privire la securitatea cibernetică poate fi sprijinit și promovat la nivel internațional printr-o diplomație cibernetică proactivă și prin poziționarea rețelei diplomatice într-o manieră coordonată ce va asigura managementul optim al resurselor disponibile.

Se va urmări crearea unei poziții de reprezentare diplomatică de nivel înalt, pentru securitate cibernetică, cu rol activ în coordonarea eforturilor României de

reprezentare internațională, în probleme aferente aspectelor la nivel de strategii, reglementări, standarde, conflicte și practici de securitate cibernetică.

Activitatea va fi sprijinită de autoritățile competente în domeniul securității cibernetică pentru asigurarea coordonării și a dialogului interinstituțional în vederea asigurării unei reprezentări adecvate și a unui mesaj coerent în acțiunea externă a României, printr-o diplomatie cibernetică eficientă.

De asemenea, se va urmări consolidarea capacității de acțiune în domeniul politicilor de securitate cibernetică la nivelul misiunilor diplomatice ale României în capitalele statelor partenere și al reprezentanțelor permanente la nivelul UE, NATO și ONU.

4.5.4. Consolidarea capacității de transfer de expertiză la nivel regional

Este importantă dezvoltarea unor relații de cooperare în domeniul securității cibernetică la nivel regional în vederea consolidării nivelului de securitate cibernetică și atingerii obiectivului de a deveni un lider regional în domeniu.

În acest sens, România va avea un rol activ prin demararea unor proiecte și inițiative cu impact regional dedicate securității cibernetică, prin care instituții publice din România cu responsabilități în domeniul securității cibernetică, în parteneriat cu mediul privat și academic, să asigure transfer de cunoștințe și expertiză în acest domeniu către statele din regiune în susținerea dezvoltării strategiilor de securitate cibernetică, legislației, instituțiilor, cercetării, proiectelor și programelor de pregătire în domeniu și inițiativelor regionale în acest sens, precum și sprijin în caz de atac cibernetic.

România va urmări să servească drept punct de referință pentru consolidarea în regiunea est și sud-est europeană a cadrului normativ internațional și respectarea valorilor democratice în mediul online și offline.

5. **Concepte, definiții și termeni**

- ❖ **Amenințare cibernetică** - circumstanță sau eveniment care constituie un pericol potențial la adresa securității cibernetice;
- ❖ **Advanced Persistent Threat (APT)** - atac cibernetic complex, ce utilizează resurse importante, precum și tehnici, tactici și proceduri avansate pentru a exfiltră date de interes strategic și pentru a rămâne neobservat o perioadă îndelungată de timp;
- ❖ **Atac cibernetic** - acțiune ostilă desfășurată în spațiul cibernetic de natură să afecteze securitatea cibernetică;
- ❖ **Audit de securitate cibernetică** - activitate prin care se realizează o evaluare sistematică a tuturor politicilor, procedurilor și măsurilor de protecție implementate la nivelul unor rețele și sisteme informatice, în vederea identificării disfuncțiilor și vulnerabilităților și a furnizării unor soluții de remediere a acestora;
- ❖ **CERT (Echipă de răspuns la incidente de securitate cibernetică)** - structură independentă de expertiză în domeniul securității cibernetice, care are atribuții în ceea ce privește prevenirea, analizarea, identificarea și reacția la incidentele de securitate cibernetică;
- ❖ **Cryptojacking** - utilizarea neautorizată a resurselor unui alt dispozitiv pentru minarea de monedă virtuală;
- ❖ **Defacement** - atac asupra unui website care constă în înlocuirea neautorizată a interfeței acestuia prin exploatarea unor vulnerabilități ale serverului ce îl găzduiește;
- ❖ **Diplomație cibernetică** - acțiunile diplomatice desfășurate în scopul promovării, susținerii, apărării și protejării, prin dialog internațional și cooperare cu țările partenere și organizațiile internaționale a unui spațiu cibernetic global, deschis, liber, stabil și sigur, în care drepturile omului, libertățile fundamentale și statul de drept se aplică pe deplin pentru bunăstarea socială, creșterea economică, prosperitatea și integritatea societății libere și democratice și care contribuie la prevenirea conflictelor, atenuarea amenințărilor la adresa securității cibernetice și la o mai mare stabilitate în relațiile internaționale;
- ❖ **Distributed Denial of Service (DDoS)** - atac prin care se urmărește indisponibilizarea, blocarea sau epuizarea resurselor unui sistem informatic, rețea sau componentă a acesteia;
- ❖ **Igienă în spațiul cibernetic** – aplicarea unui set de practici și deprinderi în materie de securitate cibernetică, necesare pentru desfășurarea în siguranță a activităților zilnice întreprinse de utilizatori;
- ❖ **Incident de securitate cibernetică** - eveniment survenit în spațiul cibernetic care perturbă funcționarea uneia sau mai multor rețele și sisteme informatice și ale cărui consecințe sunt de natură a afecta securitatea cibernetică;

- ❖ **Infostealer** - aplicație *malware* utilizată pentru a fura informații (cel mai des credențiale de autentificare) dintr-un sistem informatic compromis;
- ❖ **Malware** - software realizat pentru a deteriora sau a se infiltra într-un computer sau rețea de computere, fără acordul sau cunoștința proprietarului, pentru a îndeplini scopuri nelegitime;
- ❖ **Politici de securitate cibernetică** - principii și reguli generale necesar a fi îndeplinite pentru asigurarea securității rețelelor și sistemelor informatice;
- ❖ **Ransomware** - formă de software nelegitim care restricționează accesul și utilizarea dispozitivului până când este plătită o recompensă;
- ❖ **Rețele și sisteme informatice** - infrastructuri de tehnologia informației și comunicațiilor, constând în echipamente, aplicații și rețele de comunicații digitale;
- ❖ **Reziliență în spațiul cibernetic** - capacitatea unei rețele sau sistem informatic de a rezista unui incident sau atac cibernetic și de a reveni la starea de normalitate;
- ❖ **Risc de securitate cibernetică** - probabilitatea ca o amenințare să se materializeze, exploatând o vulnerabilitate specifică rețelelor și sistemelor informatice;
- ❖ **Securitate cibernetică** - stare de normalitate rezultată în urma aplicării unui ansamblu de măsuri proactive și reactive prin care se asigură confidențialitatea, integritatea, disponibilitatea, autenticitatea și non-repudierea informațiilor în format electronic a resurselor și serviciilor publice sau private din spațiul cibernetic;
- ❖ **SOC (Centru Operațional de Securitate)** - echipă de experți în securitate cibernetică, ce are rolul de a monitoriza, analiza și răspunde la incidentele de securitate cibernetică;
- ❖ **SQL (Structured Query Language) injection** - tehnică utilizată de atacatorii cibernetici, prin care se urmărește exploatarea vulnerabilităților unui website și inserarea unui script de tip SQL;
- ❖ **Vulnerabilitate în spațiul cibernetic** - slăbiciune în proiectarea și implementarea rețelelor și sistemelor informatice sau a măsurilor de securitate aferente, care poate fi exploatată de către o amenințare.