PARLAMENTUL ROMÂNIEI

SENATUL **CAMERA DEPUTAȚILOR**

LEGE

privind securitatea și apărarea cibernetică a României

Parlamentul României adoptă prezenta lege.

CAPITOLUL I

Dispoziții generale

Art. 1. - (1) Prezenta lege stabilește cadrul juridic și instituțional privind organizarea și desfășurarea activităților din domeniile securitate și apărare cibernetică, mecanismele de cooperare și responsabilitățile instituțiilor cu atribuții în domeniile menționate.

(2) Securitatea și apărarea cibernetică se realizează prin adoptarea și implementarea de politici și măsuri în scopul cunoașterii, prevenirii și contracarării riscurilor și amenințărilor în spațiul cibernetic.

Art. 2. - În sensul prezentei legi, termenii și expresiile de mai jos au următoarea semnificație:

a) apărare cibernetică - totalitatea activităților, mijloacelor și măsurilor utilizate pentru a contracara amenințările provenite din spațiul cibernetic și a atenua efectele acestora asupra sistemelor de comunicații și tehnologia informației, sistemelor de armament și rețelelor și sistemelor informatice, inclusiv cele ce susțin capabilitățile militare de apărare;

b) cyberintelligence – totalitatea activităților de culegere, procesare, prelucrare analitică și valorificare a datelor și informațiilor privind acțiuni ostile de natură a afecta interesele și obiectivele naționale de securitate pe linia tehnologiei informației și comunicațiilor, precum și identificarea, cunoașterea, prevenirea, apărarea și contracararea oricăror acțiuni din spațiul cibernetic care pot constitui amenințări la adresa securității naționale;

c) cyber counter-intelligence – totalitatea măsurilor de identificare, descurajare, neutralizare și protecție împotriva activităților de informații privind acțiuni ostile de natură a afecta interesele și obiectivele naționale de securitate, desfășurate în spațiul cibernetic în domeniul apărării;

d) furnizori de servicii de găzduire - hosting - orice persoană juridică ce desfășoară activități pe teritoriul României, care pune la dispoziție rețele și sisteme informatice, fizice sau virtuale, pentru derularea de activități și servicii informaționale;

e) furnizor de servicii de securitate cibernetică - orice persoană juridică ce realizează, în vederea protejării rețelelor și sistemelor informatice, cel puțin una dintre următoarele activități: implementare de politici, proceduri și măsuri, auditare, evaluare, testare a măsurilor implementate, management al incidentelor de securitate;

f) managementul incidentului de securitate cibernetică - ansamblul proceselor ce prevăd detectarea, raportarea, analiza și răspunsul la incidentul de securitate cibernetică;

g) rețele și sisteme informatice specifice apărării naționale - rețelele și sistemele informatice aparținând Ministerului Apărării Naționale, rețelele și sistemele informatice naționale care susțin activitățile militare ale NATO și UE, precum și rețelele și sistemele informatice de interes pentru apărarea națională date în responsabilitatea Ministerului Apărării Naționale in caz de agresiune armată, la instituirea stării de asediu, declararea stării de mobilizare, sau a stării de război;

h) serviciile publice de tip preventiv - sunt acele servicii care constau în: anunțuri privind evenimente în domeniu, anunțuri privind amenințări nou-identificate pe plan național și internațional; cercetare și informare privind noutățile tehnologice în domeniu, auditări și evaluări de securitate sau teste de penetrare; identificarea vulnerabilităților și punerea la dispoziție de situații actualizate privind încercările de intruziune și servicii de localizare a surselor atacurilor, diseminarea informațiilor de securitate cibernetică;

i) serviciile publice de tip reactiv - sunt acele servicii care constau în: alerte și atenționări, gestiunea incidentelor la nivel național, în cooperare cu celelalte echipe CSIRT, respectiv diseminarea rezultatelor investigațiilor incidentelor de securitate cibernetică;

j) serviciile publice de consultanță în contextul prezentei legi - sunt acele servicii care constau în: analize de risc aplicate la nivel local și la nivel național privind rețele și sisteme informatice de interes național; planificarea asigurării funcționării continue și a recuperării în caz de dezastre;

k) spațiul cibernetic - mediul virtual generat de rețelele și sistemele informatice , incluzând conținutul informațional, procesat, stocat sau transmis, precum și acțiunile derulate de utilizatori în acesta;

Art. 3. - (1) În domeniul securității cibernetice prezenta lege are ca obiect stabilirea cadrului general de reglementare pentru:

a) rețelele și sistemele informatice deținute, organizate, administrate, utilizate sau aflate în competenta instituțiilor din domeniul apărării, ordinii publice, securității naționale, justiției, situațiilor de urgență, Oficiului Registrului Național al Informațiilor Secrete de Stat, precum și cele puse la dispoziția beneficiarilor acestora.

b) rețelele și sistemele informatice deținute de persoanele juridice de drept privat și utilizate în vederea furnizării de servicii de comunicații electronice instituțiilor și autorităților administrației publice centrale si locale.

c) rețelele și sistemele informatice deținute, organizate, administrate sau utilizate de instituții sau autorități ale administrației publice centrale și locale, altele decât cele prevăzute la lit. a), precum și de persoane juridice care desfășoară activități industriale, de cercetare științifică sau furnizează servicii publice ori de interes public, altele decât cele de la lit. b).

(2) În domeniul apărării cibernetice prezenta lege are ca obiect stabilirea cadrului general de reglementare pentru rețelele și sistemele informatice specifice apărării naționale.

Art. 4. - Obiectivele prezentei legi sunt:

a) asigurarea rezilienței și protecției rețelelor și sistemelor informatice ce susțin funcțiile de apărare, securitate și guvernare ale statului;

b) desemnarea autorităților competente și stabilirea cadrului legal de dezvoltare a capabilităților necesare îndeplinirii responsabilităților acestora în domeniile securității și apărării cibernetice;

c) menținerea sau restabilirea climatului de securitate cibernetică la nivel național prin cooperarea între autoritățile competente și asigurarea unei reacții rapide și eficiente la amenințările provenite din spațiul cibernetic;

d) separarea responsabilităților și/sau atribuțiilor funcționale între furnizorii de rețele, sisteme și servicii informatice, autoritățile de aplicare a legii, structurile din cadrul instituțiilor cu atribuții în domeniul securității și apărării cibernetice, astfel încât să se asigure un nivel ridicat de securitate cibernetică la nivel național;

e) dezvoltarea și consolidarea unei culturi de securitate cibernetică la nivel național, prin conștientizarea riscurilor și amenințărilor, respectiv formarea unei conduite pro-active și preventive.

Art. 5. - Asigurarea securității și apărării cibernetice se realizează conform următoarelor principii:

a) principiul personalității – responsabilitatea asigurării securității cibernetice și apărării cibernetice a unui sistem, serviciu sau a unei rețele informatice revine instituției care le furnizează, respectiv le asigură managementul;

b) principiul protecției depline – instituția care furnizează sau asigură managementul unui sistem, serviciu sau rețea informatică răspunde de identificarea riscurilor și vulnerabilităților asociate acestora și de implementarea măsurilor tehnice și organizaționale necesare protecției cibernetice;

c) principiul minimizării efectelor – în cazul unui incident de securitate cibernetică instituția care furnizează sau asigură managementul sistemului, serviciului sau rețelei informatice în cauză ia măsuri de evitare a escaladării efectelor și de propagare a acestora la alte sisteme, servicii sau rețele din responsabilitatea sa sau din responsabilitatea altor instituții;

d) principiul cooperării și coordonării – constă în realizarea, în mod conjugat, a tuturor activităților care să asigure securitate serviciilor, rețelelor și sistemelor informatice care fac obiectul prezentei legi, precum și gestionarea incidentelor de securitate cibernetică, atenuarea efectelor și eliminarea situațiilor care au generat stările de alertă cibernetică instituite Ia nivel național.

CAPITOLUL II

Sistemul național de securitate cibernetică

Art. 6. - (1) La nivel național, activitățile specifice securității cibernetice se organizează și se desfășoară în mod unitar, potrivit prezentei legi.

(2) În acest scop, se definește Sistemul Național de Securitate Cibernetică, denumit în continuare SNSC, drept cadru general de cooperare care reunește autorități și instituții publice cu responsabilități și capabilități în domeniu, în vederea coordonării acțiunilor la nivel național pentru asigurarea securității cibernetice.

(3) În exercitarea competențelor, instituțiile și autoritățile publice cooperează cu sectorul privat, mediul academic, asociațiile profesionale și cu organizațiile neguvernamentale.

Art. 7. - (1) Activitățile SNSC sunt coordonate, la nivel strategic, de către Consiliul Suprem de Apărare a Țării.

(2) Activitățile SNSC sunt coordonate unitar, la nivel operațional, de către Consiliul Operativ de Securitate Cibernetică, denumit în continuare COSC.

Art. 8. - (1) COSC este un mecanism de cooperare sub autoritatea administrației prezidențiale, format din consilierul prezidențial pentru probleme de securitate națională, consilierul prim-ministrului pe probleme de securitate națională, Secretarul Consiliului Suprem de Apărare a Țării, precum și reprezentanți ai: Ministerului Apărării Naționale, Ministerului Afacerilor Interne, Ministerului Afacerilor Externe, Ministerului Cercetării, Inovării și Digitalizării, Serviciului Român de Informații, Serviciului de Informații Externe, Serviciului de Telecomunicații Speciale, Serviciului de Protecție și Pază, Oficiului Registrului Național al informațiilor Secrete de Stat, Autorității Naționale pentru Administrare și Reglementare în Comunicații și ai Directoratului Național de Securitate Cibernetică.

(2) COSC emite hotărâri, adoptate prin consens, care sunt obligatorii pentru instituțiile prevăzute la alin. (1), conform competențelor legale.

(3) Conducerea COSC este asigurată de un președinte - consilierul prezidențial pentru probleme de securitate națională și un vicepreședinte - consilierul prim-ministrului pe probleme de securitate națională.

(4) În funcție de natura și evoluția amenințărilor cibernetice sunt invitați să participe în cadrul COSC și reprezentanți ai altor entități – autorități, instituții publice, persoane juridice de drept public sau privat – care pot contribui la soluționarea problemelor de securitate cibernetică.

Art. 9. - (1) În exercitarea atribuțiilor sale, COSC analizează și evaluează securitatea cibernetică și înaintează Consiliului Suprem de Apărare a Țării, denumit în continuare CSAT, propuneri privind:

a) instituirea sau modificarea nivelurilor de alertă cibernetică la nivel național;

b) armonizarea reacției autorităților competente ale statului în situații generate de amenințări cibernetice, care necesită schimbarea nivelului de alertă cibernetică;

c) solicitarea, în caz de necesitate, de asistență din partea altor state sau organizații și organisme internaționale;

d) modalitatea de răspuns la solicitările de asistență adresate României din partea altor state sau organizații și organisme internaționale, altele decât cele din domeniul apărării naționale;

e) planuri sau direcții de acțiune, în funcție de concluziile rezultate și evoluția climatului de securitate în spațiul cibernetic;

f) direcții de dezvoltare și investiții în domeniul securității cibernetice;

g) linii de mandat referitoare la decizii şi documente de politică externă în domeniul securității cibernetice;

h) modalități de gestionare și răspuns la amenințări și atacuri cibernetice.

(2) Pentru realizarea securității cibernetice, COSC cooperează, după caz, cu organismele de coordonare sau de conducere constituite, la nivel național, pentru managementul situaţiilor de urgență, acțiuni în situații de criză în domeniul ordinii publice, prevenirea şi combaterea terorismului, securitate şi apărare națională.

CAPITOLUL III

Autorități competente și responsabilități

Art. 10. - Sunt autorități competente în sensul prezentei legi:

a) Directoratul Național de Securitate Cibernetică (DNSC), conform prevederilor Ordonanței de urgență nr. 104/2021 privind înființarea Directoratului Național de Securitate Cibernetică, aprobată prin Legea 11/2022 pentru aprobarea Ordonanței de urgență a Guvernului numărul 104/2021 privind înființarea Directoratului Național de Securitate Cibernetică;

b) Autoritatea Națională pentru Administrare și Reglementare în Comunicații (ANCOM) pentru coordonarea activităților desfășurate în vederea asigurării securității cibernetice a rețelelor și sistemelor informatice proprii și a celor prevăzute la art. 3 alin (1) lit. b);

c) Ministerul Apărării Naționale, Ministerul Afacerilor Interne, Oficiul Registrului Național al informațiilor Secrete de Stat, Serviciul Român de Informații, Serviciul de Informații Externe, Serviciul de Telecomunicații Speciale și Serviciul de Protecție și Pază pentru asigurarea securității și apărării cibernetice, respectiv pentru cunoașterea, prevenirea și contracararea amenințărilor cibernetice la adresa rețelelor și sistemelor informatice din domeniul lor de competență, activitate sau responsabilitate. În acest sens, stabilesc structuri și măsuri tehnice și organizatorice privind coordonarea și controlul activităților de securitate și apărare cibernetică.

Art. 11. - Ministerul Apărării Naționale este autoritate competentă la nivel național în domeniul apărării cibernetice, iar în sensul prezentei legi are atribuții în domeniul securității cibernetice pentru rețelele și sistemele informatice care susțin capabilitățile militare de apărare.

Art. 12. - Ministerul Afacerilor Externe:

a) sprijină și promovează colaborarea și coordonarea la nivel strategic a dialogului României in domeniul securității cibernetice cu principalii parteneri internaționali și în cadrul formatelor internaționale la care este parte, cu privire la deciziile de politica cu implicații naționale si internaționale privind spațiul cibernetic.

b) contribuie la promovarea principiilor diplomației cibernetice în concordanță cu setul de instrumente la nivel UE, normele de comportament responsabil în spațiul cibernetic la nivel ONU și dreptul internațional.

c) întreprinde acțiuni diplomatice pentru a sprijini o arhitectură cooperativă internațională care promovează stabilitatea și descurajează amenințările și atacurile în spațiul cibernetic

Art. 13. - (1) Serviciul Român de Informații este autoritate competentă la nivel național în domeniul *cyber intelligence*.

(2) Activitățile desfășurate de Serviciul Român de Informații, în sensul prezentei legi, nu se aplică rețelelor și sistemelor informatice ale autorităților prevăzute la art. 10 lit. c).

(3) În situația existenței unor amenințări cibernetice la adresa rețelelor și sistemelor informatice prevăzute la art. 3, lit. b) și lit. c), care ar aduce atingere securității naționale, securitatea cibernetică este asigurată de Serviciul Român de Informații, care va informa ANCOM și DNSC, în condițiile legii.

Art. 14. - Serviciul de Telecomunicații Speciale este autoritate competentă în domeniile securității și apărării cibernetice pentru infrastructurile, rețelele, sistemele proprii, serviciile și spectrul de frecvențe radio pe care le administrează și operează, potivit legi.

Art. 15. - Serviciul de Protecție și Pază coordonează măsuri de securitate cibernetică pentru demnitarii cărora, conform legii, le asigură protecție și acționează, independent sau în cooperare cu celelalte structuri din domeniile apărării, ordinii publice și securității naționale, pentru implementarea acestora.

Art. 16. - Autoritățile prevăzute la art. 10 au următoarele obligații:

a) să adopte planuri de acțiune corespunzătoare fiecărui nivel de alertă cibernetică;

b) să acorde sprijin, la solicitarea deținătorilor de rețele și sisteme informatice aflate în domeniul lor de competență, activitate sau responsabilitate, pentru implementarea măsurilor corespunzătoare nivelurilor de alertă cibernetică;

c) să desfășoare activități de informare și comunicare publică;

d) să organizeze sesiuni de formare și instruire în domeniul securității cibernetice;

e) să organizeze sau să participe la exerciții naționale de securitate cibernetică;

f) să își comunice reciproc date de interes referitoare la securitatea cibernetică, inclusiv către celelalte autorități și instituții publice sau deținători de rețele și sisteme informatice;

g) să solicite convocarea COSC, potrivit competențelor prevăzute în prezenta lege.

Art. 17. - Autoritățile prevăzute la art. 10 pot constitui și operaționaliza structuri specializate în realizarea de audit de securitate cibernetică și structuri specializate de securitate cibernetică pentru gestionarea amenințărilor cibernetice la adresa rețelelor și sistemelor informatice din responsabilitate.

Art. 18. - Pentru rețelele şi sistemele informatice aflate în domeniul de competență, activitate sau responsabilitate, autoritatea prevăzută la art. 10 lit. b) are şi următoarele obligații specifice:

a) să realizeze periodic evaluări ale stării de securitate cibernetică;
b) să elaboreze politici de securitate cibernetică specifice;
c) să asigure managementul incidentelor de securitate cibernetică identificate.

CAPITOLUL IV

Managementul incidentelor și reziliența în spațiul cibernetic

SECȚIUNEA 1

Managementul incidentelor de securitate cibernetică

Art. 19. - **DNSC** dezvoltă și asigură managementul *Platformei naționale pentru raportarea incidentelor de securitate cibernetică*, denumită în continuare **PNRISC**.

Art. 20. - (1) Incidentele de securitate cibernetică sunt notificate în PNRISC şi trebuie să conțină în mod obligatoriu, dar fără a se limita la:

a) elementele de identificare ale rețelelor și sistemelor informatice afectate;
b) descrierea incidentului;
c) perioada de desfășurare a incidentului;
d) impactul estimat al incidentului;
e) măsuri preliminare adoptate;
f) lista de autorități ale statului afectate de incident;
g) întinderea geografică potențială a incidentului;
h) date despre potențiale efecte transfrontaliere ale incidentului;

(2) Notificarea prevăzută la alin. (1) nu va conține:

a) informații clasificate;
b) date care pot aduce atingere drepturilor și libertăților cetățenești ori intereselor legitime ale unor terțe entități victime ale incidentului de securitate cibernetică.

(3) Accesul la informațiile din PNRISC este restricționat prin politici de confidențialitate stabilite și implementate de DNSC.

Art. 21. - (1) Persoanele juridice care au în responsabilitate rețele și sisteme informatice prevăzute la art. 3, alin. (1) lit. b) și c), au obligația de a notifica incidentele de securitate cibernetică prin intermediul PNRISC, de îndată dar nu mai târziu de 24 de ore de la constatarea incidentului.

(2) Autoritățile care au în responsabilitate rețele și sisteme informatice prevăzute la art. 3 lit. a), fără a aduce atingere normelor aplicabile în materie de raportare, confidențialitate și secret profesional, pot notifica în mod voluntar incidentele de securitate cibernetică prin intermediul PNRISC.

Art. 22. - În domeniul managementului incidentelor de securitate cibernetică, autoritățile prevăzute la art. 10 au următoarele responsabilități:

a) să colecteze notificările cu privire la incidente de securitate cibernetică din cadrul rețelelor și sistemelor informatice aflate în domeniul lor de competentă, activitate sau responsabilitate;

b) să evalueze datele și informațiile cu privire la incidentele și atacurile cibernetice la adresa rețelelor și sistemelor informatice aflate în domeniul lor de competență, activitate sau responsabilitate;

c) să notifice deținătorii de rețele și sisteme informatice aflate în domeniul lor de competență, activitate sau responsabilitate cu privire la incidente de securitate cibernetică sau vulnerabilități și atacuri cibernetice identificate la nivelul acestora;

d) să coordoneze managementul incidentelor de securitate cibernetică identificate în cadrul rețelelor și sistemelor informatice aflate în domeniul lor de competență, activitate sau responsabilitate;

e) să acorde sprijin, la solicitare sau după notificarea prevăzută la lit. c), deținătorilor de rețele și sisteme informatice aflate în domeniul lor de competență, activitate sau responsabilitate pentru adoptarea de măsuri reactive de primă urgență pentru remedierea efectelor incidentelor de securitate cibernetică.

f) să păstreze pe un termen de 5 ani datele referitoare la incidentele de securitate cibernetică și rezultatele măsurilor de contracarare a acestora.

SECȚIUNEA 2

Reziliența în spațiul cibernetic

Art. 23. - (1) Asigurarea rezilienței în spațiul cibernetic presupune implementarea de măsuri pro-active și reactive.

(2) Măsurile pro-active sunt destinate prevenirii incidentelor de securitate cibernetică și descurajării atacatorilor din spațiul cibernetic și includ:

a) constituirea și antrenarea echipelor specializate de răspuns la incidente de securitate cibernetică;

b) constituirea și operarea Centrelor Operaționale de Securitate (SOC) pentru spațiul cibernetic;

c) constituirea unei rezerve de resurse și de capabilități întrunite de securitate cibernetică care să poată fi utilizate în caz de necesitate;

d) dezvoltarea unor capabilități pro-active, care să permită cunoașterea anticipativă a amenințărilor din spațiul cibernetic;

e) cooperarea și schimbul de informații între autoritățile competente și sectorul privat pentru identificarea amenințărilor cibernetice;

f) identificarea serviciilor, rețelelor și sistemelor informatice, conform competențelor fiecărei instituții responsabile de administrare și asigurarea managementului acestora;

g) implementarea de soluții de securitate cibernetică, care să crească capacitatea de detecție și capabilitățile de prevenție la atacuri cibernetice;

h) demonstrarea nivelului de maturitate atins de capabilitățile de securitate cibernetică în cadrul exercițiilor organizate la nivel național sau internațional;

i) instruirea personalului din cadrul entităților prevăzute la art. 3 în domeniul securității cibernetice, prin realizarea periodică de campanii de informare, conștientizare și igienă cibernetică la nivel organizațional.

(3) Măsurile reactive sunt destinate reducerii efectelor atacurilor cibernetice și includ:

a) punerea în aplicare a planurilor de răspuns la incidente și de contingență în domeniul securității cibernetice;

b) utilizarea rezervei de resurse și de capabilități de securitate cibernetică;

c) restabilirea funcționalității rețelelor şi sistemelor informatice din cadrul instituțiilor afectate;

d) diseminarea informațiilor despre evenimentele cibernetice prin alerte în mediul interinstituțional pentru evaluarea riscului și diminuarea posibilităților de exploatare a vulnerabilităților;

e) descurajarea prin atribuirea publică a autorilor atacurilor cibernetice, conform atribuțiilor legale.

Art. 24. - (1) Furnizorii de servicii de securitate cibernetică ce desfășoară activități pe teritoriul României au obligația să notifice autoritățile competente, de îndată dar nu mai târziu de 24 de ore, cu privire la identificarea unor incidente, amenințări sau vulnerabilități critice a căror manifestare poate afecta o rețea sau sistem informatic a deținătorului sau a unor terți.

(2) Notificarea prevăzută la alin. (1) se realizează în scris, prin mijloace electronice sau prin orice altă modalitate stabilită de comun acord.

Art. 25. - Pentru creșterea nivelului de reziliență cibernetică și realizarea descurajării în spațiul cibernetic la nivel național, DNSC și instituțiile din domeniile apărării, ordinii publice și securității naționale iau măsuri pentru:

a) realizarea unui cadru interinstituțional de securitate cibernetică care să permită instruirea comună, transferul de cunoștințe, schimbul de informații, sprijinul de specialitate și federalizarea de resurse și capabilități de securitate cibernetică;

b) îmbunătățirea și extinderea capabilităților de protecție și detecție automată a atacurilor prin implementarea de instrumente de analiză inteligentă a amenințărilor și distribuirea oportună a indicatorilor și avertizărilor privind iminența unor atacuri cibernetice asupra rețelelor și sistemelor informatice naționale;

c) elaborarea de manuale cu tehnici, tactici și proceduri, precum și a planurilor de contingență și exersarea lor în cadrul exercițiilor de securitate cibernetică în scopul întăririi rezilienței în spațiul cibernetic;

d) constituirea de entități de tip CERT, echipe de intervenție la incidente de securitate cibernetică de tip CSIRT, echipe de protecție cibernetică și/sau alte forțe specializate în desfășurarea de acțiuni în spațiul cibernetic.

CAPITOLUL V

Sistemul național de alertă cibernetică

Art. 26. - (1) Sistemul National de Alertă Cibernetică, denumit în continuare SNAC, constă într-un ansamblu de măsuri tehnice și procedurale destinate prevenirii, descurajării și combaterii acțiunilor sau inacțiunilor ce se pot constitui în vulnerabilități sau amenințări la adresa securității cibernetice a României.

(2) SNAC asigură un serviciu de notificare publică privind nivelul de alertă cibernetică existent la nivel național, pentru o zonă geografică delimitată sau pentru un anumit domeniu de activitate, stabilit în funcție de gradul de risc asociat amenințărilor, incidentelor sau atacurilor cibernetice identificate la un anumit moment de timp.

Art. 27. - (1) Nivelurile de alertă cibernetică și modalitățile de acțiune în situații de alertă cibernetică se stabilesc printr-o metodologie elaborată de DNSC, avizată conform de COSC și aprobată prin ordin al Directorului DNSC.

(2) Instituirea nivelurilor de alertă, precum și trecerea de la un nivel la altul se decid de către Directorul DNSC, cu informarea COSC.

(3) Trecerea de la un nivel de alertă cibernetică superior la unul inferior se face după încetarea cauzelor care au generat ridicarea nivelului de alertă.

Art. 28. - (1) Entitățile care au în responsabilitate rețele și sisteme informatice prevăzute la art. 3 au obligația să elaboreze planuri proprii de acțiune pentru fiecare tip de alertă cibernetică, conform ghidurilor emise de DNSC.

(2) La declararea stărilor de alertă cibernetică, entitățile care au în responsabilitate rețele și sisteme informatice prevăzute la art. 3 pun în aplicare măsurile din planurile specificate la alin. (1).

Art. 29. - (1) Starea de criză în domeniul securității cibernetice se instituie în situația în care, din cauza unor amenințări majore sau a producerii unuia sau mai multor atacuri cibernetice asupra unor rețele și/sau sisteme informatice, sunt afectate funcțiuni critice ale statului, se aduc grave prejudicii reputației statului român, sunt cauzate pagube economice grave sau sunt puse în pericol vieți omenești.

(2) Declararea stării de criză în domeniul securității cibernetice se aprobă de către CSAT, la propunerea COSC.

Art. 30. - Responsabilitatea asigurării managementului crizei în domeniul securității cibernetice aparține DNSC, prin Centrul Național de Gestionare a Crizelor de Securitate Cibernetică, denumit în continuare CNGCSC.

CAPITOLUL VI

Apărarea cibernetică

Art. 31. - În domeniul apărării cibernetice, Ministerul Apărării Naţionale are următoarele atribuții:

a) apără și protejează sistemele și rețelele informatice aparținând Ministerului Apărării Naționale;

b) planifică și conduce operații în spațiul cibernetic prin Centrul național militar de comandă, potrivit legii;

c) planifică și execută operații defensive în spațiul cibernetic, pe timp de pace, prin Comandamentul Apărării Cibernetice;

d) dezvoltă și implementează capabilități militare de execuție a operațiilor în spațiul cibernetic prin Comandamentul Apărării Cibernetice;

e) desfășoară operații de cyber intelligence și cyber counter intelligence în spațiul cibernetic în scopul cunoașterii, monitorizării și contracarării amenințărilor la adresa securității naționale în domeniul apărării, la adresa structurilor Ministerului Apărării Naționale și a forțelor aliate;

f) dezvoltă capabilități de răspuns ofensiv, în mod individual sau ca parte dintr-o coaliție ori alianță, utilizabile în caz de atacuri cibernetice care contravin dreptului internațional.

g) participă la activități de descurajare în spațiul cibernetic;

h) asigură punctul unic de contact în relația cu NATO pentru operații militare în spațiul cibernetic;

i) elaborează și implementează politici și standarde în domeniul apărării cibernetice, în acord cu interesul național, precum și cu standardele și cerințele instituțiilor sau agențiilor NATO ori

ale Uniunii Europene.

Art. 32. - Ministerul Apărării Naționale stabilește prin lege condițiile de recrutare/selecție, modalitățile de formare și instruire periodică și măsurile de stimulare a mediului privat, precum și alte aspecte pentru asigurarea condițiilor necesare constituirii și utilizării rezervei de specialiști în domeniul apărării cibernetice.

CAPITOLUL VII

Cercetare, dezvoltare și inovare în domeniul securității cibernetice

Art. 33. - Cercetarea, dezvoltarea și inovarea în domeniul securității cibernetice sunt parte integrantă a sistemului național de cercetare, dezvoltare și inovare și se aliniază măsurilor promovate de ministerul de resort pentru încadrarea Ariei Românești a Cercetării în Aria Europeană a Cercetării.

Art. 34. - (1) Instituțiile din domeniile apărării, ordinii publice și securității naționale dezvoltă strategii și politici proprii privind cercetarea, dezvoltarea și inovarea în domeniile securității și apărării cibernetice, în funcție de potențialul științific avut la dispoziție, de competențele sau de misiunile specifice.

(2) La nivelul fiecărei instituții din domeniile apărării, ordinii publice și securității naționale se desemnează de către conducătorul instituției entitatea responsabilă pentru managementul activităților de cercetare, dezvoltare și inovare în domeniile securității și apărării cibernetice.

(3) Instituțiile din domeniile apărării, ordinii publice și securității naționale cooperează cu mediul academic și industria națională de profil pentru implementarea următoarelor linii de efort în domeniul cercetării, dezvoltării și inovării:

a) menținerea unei poziții avansate în rândul instituțiilor ce investesc și valorifică rezultatele activităților de cercetare, dezvoltare și inovare desfășurate în domeniul securității cibernetice;

b) dezvoltarea și menținerea de parteneriate eficiente în domeniul cercetării, dezvoltării și inovării;

c) promovarea de prototipuri și demonstratoare tehnologice în domeniile securității și apărării cibernetice;

d) dezvoltarea rețelelor de experți în domeniu la nivel național și interinstituțional.

CAPITOLUL VIII

Cooperare în domeniul securității și apărării cibernetice

SECȚIUNEA 1

La nivel național

Art. 35. - (1) Cooperarea în domeniul securității și apărării cibernetice la nivel național are următoarele obiective:

a) realizarea unui răspuns dinamic și eficient la incidentele de securitate cibernetică;

b) valorificarea experienței și bunelor practici în domeniile securității și apărării cibernetice;

c) implementarea unui mediu deschis, transparent, colaborativ și de încredere între instituțiile cu responsabilități în domeniile securității și apărării cibernetice la nivel național;

d) acceptarea și promovarea standardelor de securitate cibernetică în parteneriat cu industria națională de profil;

e) dezvoltarea și implementarea de soluții de securitate cibernetică;

f) dezvoltarea unei culturi de securitate cibernetică și implementarea bunelor practici de igienă cibernetică la nivel național.

(2) Activitățile de cooperare la nivel național includ, fără a se limita la acestea:

a) proiecte de dezvoltare capabilități;
b) programe de cercetare-inovare;
c) cursuri de formare profesională sau de specializare;
d) exerciții;
e) conferințe și alte manifestări științifice;
f) alte tipuri de activități.

SECȚIUNEA 2

La nivel internațional

Art. 36. - (1) Cooperarea internațională în domeniile securității și apărării cibernetice are următoarele obiective:

a) informarea reciprocă privind amenințările din spațiul cibernetic;

b) creșterea capacității de reacție la amenințările cibernetice și formarea coeziunii de acțiune a echipelor specializate, în cadrul exercițiilor multinaționale de securitate și apărare cibernetică;

c) verificarea și validarea nivelului de maturitate atins de capabilitățile de apărare și securitate cibernetică implementate la nivel național;

d) realizarea interoperabilității tehnice și procedurale a forțelor de apărare cibernetică;

e) dezvoltarea și exersarea mecanismelor de avertizare și schimb de informații privind amenințările de natură cibernetică, precum și a celor de descurajare;

f) dezvoltarea de proiecte comune de cercetare, dezvoltare și inovare în domeniile securității și apărării cibernetice;

g) evaluarea și implementarea de soluții revoluționare de securitate cibernetică, precum și adoptarea de concepte noi de proiectare și utilizare a tehnologiilor emergente în spațiul cibernetic;

h) creșterea contribuției naționale la activități de transfer de cunoștințe, de creștere a încrederii și de dezvoltare a capacității în domeniul securității și apărării cibernetice;

i) dezvoltarea domeniului diplomației cibernetice;

Art. 37. - (1) Instituțiile din domeniile apărării, ordinii publice și securității naționale cooperează cu statele membre, cu organismele, agențiile și instituțiile Uniunii Europene și ale NATO cu atribuții în domeniul securității și apărării cibernetice, conform domeniilor de competență.

(2) Cooperarea în domeniul apărării cibernetice cu instituțiile NATO, cu armatele țărilor membre UE și ale statelor aliate se realizează prin Ministerul Apărării Naționale.

CAPITOLUL IX

Politici și reglementări în domeniul securității cibernetice

Art. 38. - DNSC, în domeniul elaborării de politici și reglementări, îndeplinește atribuțiile prevăzute în Ordonanța de urgență 104/2021 privind înființarea Directoratului Național de Securitate Cibernetică, aprobată prin Legea 11/2022 pentru aprobarea Ordonanței de urgență a Guvernului numărul 104/2021 privind înființarea Directoratului Național de Securitate Cibernetică.

Art. 39. - Instituțiile din domeniile apărării, ordinii publice și securității naționale pot elabora norme proprii pentru reglementarea activităților în domeniul securității cibernetice la nivel instituțional;

CAPITOLUL X

Formarea profesională, educația, instruirea

Art. 40. - Procesul de instruire în domeniile securității și apărării cibernetice se realizează prin cursuri, exerciții, conferințe, seminarii, precum și alte tipuri de activități organizate la nivel național sau internațional.

Art. 41. - Instituțiile din domeniile apărării, ordinii publice și securității naționale pot organiza~~,~~ la nivel instituțional sau interinstituțional, exerciții de securitate și apărare cibernetică.

Art. 42. - (1) Instituțiile din domeniile apărării, ordinii publice și securității naționale participă la exerciții de apărare și securitate cibernetică organizate în mediul internațional, la nivel UE, NATO sau multinațional.

(2) Participarea la exercițiile de apărare cibernetică organizate în cadrul NATO se realizează sub coordonarea Ministerului Apărării Naționale.

Art. 43. - În domeniul prevenirii și conștientizării, DNSC și instituțiile din domeniile apărării, ordinii publice și securității naționale:

a) asigură informarea și pregătirea la nivel național a populației precum și a tuturor entităților care acționează în spațiul cibernetic național, inclusiv a operatorilor economici din sectoarele stabilite în baza Legii nr. 362/2018 și din sectorul public cu privire la riscurile de securitate cibernetică identificate;

b) promovează dezvoltarea unui comportament adecvat în spațiul cibernetic pentru persoanele fizice și juridice prin conștientizarea efectelor atacurilor cibernetice și a modalității de semnalare a acestora;

c) emite informări privind obligațiile care derivă din calitate de administrator, furnizor sau utilizator al rețelelor și sistemelor informatice, privind atitudinea în fața unor posibile atacuri cibernetice, privind conștientizarea cetățenilor și instituțiilor publice și private, despre necesitatea semnalării/notificării atacurilor cibernetice;

d) dezvoltă cadrul național de conștientizare a populației în cooperare cu mediul public, privat și academic în scopul asigurării unei abordări eficiente a pregătirii populației privind modalitățile de comportament, reacție și apărare în mediul online;

e) desfășoară și participă la campanii/acțiuni de prevenire și conștientizare a cauzelor și consecințelor atacurilor cibernetice asupra rețelelor și sistemelor informatice civile, la nivel internațional, național și regional.

CAPITOLUL XI

Securitatea lanțului de aprovizionare

Art. 44. - (1) Instituțiile din domeniile apărării, ordinii publice și securității naționale implementează procesele de management a riscurilor de securitate cibernetică specifice lanțului de aprovizionare;

(2) Riscurile lanțului de aprovizionare includ: livrarea de echipamente contrafăcute, producție neautorizată, manipulare frauduloasă, inserarea de componente software și hardware periculoase, spionaj, compromiteri neintenționate, practici deficitare de fabricație și dezvoltare de produse.

Art. 45. - La nivelul fiecărei instituții din domeniile apărării, ordinii publice și securității naționale se desemnează de către conducătorul instituției una sau mai multe entități responsabile pentru:

a) stabilirea politicilor, strategiilor și proceselor de management al riscurilor de securitate cibernetică specifice lanțului de aprovizionare;

b) includerea în conținutul politicilor, strategiilor și proceselor existente a cerințelor noi și emergente privind managementul riscurilor cibernetice specifice lanțului de aprovizionare;

c) stabilirea standardelor de management al riscurilor de securitate cibernetică obligatorii pentru autoritățile contractante în cadrul procedurilor de achiziții;

d) stabilirea măsurilor de stimulare a potențialilor furnizori în cadrul proceselor de achiziții, raportat la nivelul de implementare a practicilor de securitate cibernetică ale acestora;

e) stabilirea metodologiilor și aplicațiilor folosite în evaluarea riscurilor de securitate cibernetică specifice lanțului de aprovizionare;

f) schimbul de informații cu celelalte instituții referitoare la amenințările de natură cibernetică specifice lanțului de aprovizionare;

g) elaborarea metodologiei de evaluare a nivelului de maturitate și a capacității operatorilor de pe lanțurile de aprovizionare de a realiza managementul riscurilor de securitate cibernetică;

h) colectarea și actualizarea datelor referitoare la eficiența furnizorilor în eliminarea sau diminuarea riscurilor de securitate cibernetică.

Art. 46. - Instituțiile din domeniile apărării, ordinii publice și securității naționale dispun măsurile necesare pentru organizarea de cursuri de instruire în domeniul managementului riscurilor de securitate cibernetică specifice lanțului de aprovizionare, respectiv introducerea de teme noi în cadrul cursurilor și programelor de instruire existente.

Art. 47. - Instituțiile din domeniile apărării, ordinii publice și securității naționale pot dezvolta capabilități avansate de testare și evaluare a riscurilor de securitate cibernetică în scopul identificării vulnerabilităților cibernetice ale echipamentelor, produselor software sau pieselor componente achiziționate sau dezvoltate la nivel instituțional.

CAPITOLUL XII

Dispoziții tranzitorii și finale

Art. 48. - În termen de 6 luni de la intrarea în vigoare a prezentei legi DNSC elaborează metodologia prevăzută la art. 27 din prezenta lege.

Art. 49. - Prezenta lege intră în vigoare la 30 zile de la data publicării ei în Monitorul Oficial al României, Partea I.