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 vulnerabilităților, 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, rețelelor și sistemelor informatice, inclusiv cele ce susțin capabilitățile militare de apărare;

b) amenințare cibernetică - astfel cum este definită în art. 2 lit. f) din Ordonanța de Urgență a Guvernului nr. 104/2021;

c) atac cibernetic - acțiune ostilă desfășurată în spațiul cibernetic de natură să afecteze securitatea cibernetică;

d) audit de securitate cibernetică - activitate prin care se realizează o evaluare sistematică a tuturor politicilor, procedurilor și măsurilor de protecție implementate la nivelul unei rețele și sisteme informatice, în vederea identificării disfuncțiilor și vulnerabilităților și a furnizării unor soluții de remediere a acestora;

e) Advanced Persistent Threat (APT) - astfel cum este definită în art. 2 lit. a) din Ordonanța de Urgență a Guvernului nr. 89/2022 privind înființarea, administrarea și dezvoltarea infrastructurilor și serviciilor informatice de tip cloud utilizate de autoritățile și instituțiile publice;

f) criza cibernetică - astfel cum este definită în art. 2 lit. k) din Ordonanța de Urgență a Guvernului nr. 104/2021;

g) cyber intelligence – activități de culegere, procesare, prelucrare analitică și valorificare a datelor și informațiilor privind acțiuni 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 riscuri, vulnerabilități și/sau amenințări la adresa securității naționale a României;

h) 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;

i) 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 și libertățile fundamentale ale omului 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;

j) echipă de răspuns la incidente de securitate cibernetică - astfel cum este definit în art. 2 lit a) din OUG nr. 104/2021;

k) furnizor de servicii de găzduire electronică cu resurse IP - astfel cum e definit în art. 4 alin. (1), pct. 9^5din OUG nr. 111/2011 privind comunicațiile electronice;

l) furnizor de servicii de securitate cibernetică - orice persoană fizică și/sau juridică care realizează, în vederea protejării rețelelor și sistemelor informatice, cel puțin una dintre următoarele activități: implementare de politici, proceduri și măsuri, consultanță, formare, informare, cercetare-dezvoltare, inovare, auditare, evaluare, testare a măsurilor implementate, management al riscurilor și incidentelor de securitate;

m)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;

n) managementul incidentelor de securitate cibernetică - ansamblul proceselor ce prevăd detectarea, calificarea, raportarea, analiza și răspunsul la incidentele de securitate cibernetică;

o) politici de securitate cibernetică - principii și reguli generale, necesar a fi aplicate pentru asigurarea securității rețelelor și sistemelor informatice;

p) produs de securitate cibernetică - astfel cum este definit în art. 2 lit l) din OUG nr. 104/2021;

q) rețele și sisteme informatice - astfel cum sunt definite de art. 3 lit. l) din Legea nr. 362/2018 privind asigurarea unui nivel comun ridicat de securitate a reţelelor şi sistemelor informatice;

r) 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 în caz de agresiune armată, la instituirea stării de asediu, declararea stării de mobilizare, sau a stării de război;

s) reziliența 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 de dinaintea incidentului sau atacului cibernetic;

t) risc de securitate cibernetică - probabilitatea ca o amenințare să se materializeze, exploatând o vulnerabilitate specifică rețelelor și sistemelor informatice;

u) 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;

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

w) vulnerabilitate de securitate cibernetică - slăbiciune în proiectarea, implementarea, dezvoltarea, configurarea și mentenanța rețelelor și sistemelor informatice sau a măsurilor de securitate aferente, care poate fi exploatată de către o amenințare.

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 competența autorităților și instituțiilor publice din domeniul apărării, ordinii publice, securității naționale, justiției, situațiilor de urgență, Oficiului Registrului Național al Informațiilor Secrete de Stat.

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

c) rețelele și sistemele informatice deținute, organizate, administrate sau utilizate de autorități și instituții 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 națională, ordine publică și guvernare;

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 coordonării unitare de către Consiliul Operativ de Securitate Cibernetică, denumit în continuare COSC, a entităților responsabile de securitatea cibernetică proprie, și asigurarea unei reacții rapide și eficiente la amenințările provenite din spațiul cibernetic;

d) stabilirea și 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 vulnerabilităților, riscurilor și amenințărilor, respectiv formarea unei conduite proactive și preventive.

Art. 5. -

Asigurarea securității și apărării cibernetice se realizează conform următoarelor principii:

a) principiul personalității – responsabilitatea asigurării securității cibernetice și/sau apărării cibernetice a unui sistem, rețea și/sau serviciu informatic revine entității care le deține în proprietate, le organizează, administrează și/sau utilizează, după caz;

b) principiul protecției depline – entitatea responsabilă de securitatea și/sau apărarea cibernetică a unui sistem, rețea și/sau serviciu informatic răspunde de managementul riscurilor asociate acestora și conexiunilor acestora cu alte sisteme, rețele și/sau servicii informatice terțe, precum și de implementarea măsurilor tehnice și organizaționale necesare protecției cibernetice;

c) principiul minimizării efectelor – în cazul unui incident de securitate cibernetică entitatea responsabilă de securitatea și/sau apărarea cibernetică a sistemului, rețelei și/sau serviciului informatic în cauză ia măsuri de evitare a amplificării efectelor și de extindere a acestora la alte sisteme, rețele și/sau servicii informatice din responsabilitatea proprie sau din responsabilitatea altor entități;

d) principiul colaborării, cooperării și coordonării – constă în realizarea, în mod conjugat de către entitățile responsabile, a tuturor activităților care să asigure securitatea și/sau apărarea sistemelor, rețelelor și serviciilor 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 la 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 înființează 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, denumit în continuare CSAT.

(2) Activitățile SNSC sunt coordonate unitar, la nivel operațional, de către COSC.

(3) Serviciul Român de Informații asigură secretariatul tehnic al COSC, în condițiile prezentei legi.

Art. 8. -

(1) COSC este un organ consultativ, fără personalitate juridică, aflat sub autoritatea CSAT, 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 ședințelor 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 CSAT propuneri privind:

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

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

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 privind adoptarea oricăror documente la nivel internațional cu privire la securitatea cibernetică care au impact în plan național;

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 situaţii 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, denumit în continuare DNSC, pentru spațiul cibernetic național civil, conform prevederilor prezentei legi și ale Ordonanței de urgență nr. 104/2021 privind înființarea Directoratului Național de Securitate Cibernetică, aprobată, cu modificări și completări, prin Legea nr. 11/2022;

b) Ministerul Cercetării, Inovării și Digitalizării, denumit în continuare MCID, pentru elaborarea și inițierea actelor normative și politicilor publice naționale în domeniul securității cibernetice, a transformării digitale, societății informaționale, comunicațiilor, cercetării, dezvoltării și inovării.

c) Autoritatea Națională pentru Administrare și Reglementare în Comunicații, denumită în continuare, 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);

d) 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, denumit în continuare MApN, 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, denumit în continuare MAE, îndeplinește următoarele atribuții:

a) sprijină și promovează colaborarea și coordonarea la nivel strategic a dialogului României în domeniul securității și apărării cibernetice cu principalii parteneri internaționali și în cadrul formatelor internaționale la care este parte, cu privire la deciziile de politică cu implicații naționale și 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, denumit în continuare SRI, este autoritate competentă la nivel național în domeniul cyber intelligence, precum și pentru cunoașterea, analizarea, prevenirea și contracararea incidentelor și atacurilor cibernetice care reprezintă amenințări, riscuri și vulnerabilități la adresa securității naționale a României.

(2) Prevenirea și combaterea amenințărilor de tip APT la adresa rețelelor și sistemelor informatice din domeniul de competență, activitate sau responsabilitate, după caz, ale instituțiilor și autorităților prevăzute la art.10, se realizează, astfel:

a) de către SIE, MApN, MAI, SPP și STS potrivit competențelor prevăzute în prezenta lege;

b) de către SRI, în toate celelalte cazuri.

(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, SRI informează 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, serviciile și spectrul de frecvențe radio proprii, precum și pentru cele reglementate prin legi speciale.

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. -

(1) 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 proprietarilor 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 comunice reciproc date de interes referitoare la securitatea cibernetică, inclusiv către celelalte autorități și instituții publice, care dețin, organizează, administrează, utilizează sau au în competență rețele și sisteme informatice;

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

(2) Autoritățile prevăzute la art. 10 pot elabora strategii și norme proprii pentru reglementarea activităților de securitate cibernetică, la nivel instituțional.

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. c) are şi următoarele obligații specifice:

a) să realizeze periodic audit de securitate cibernetică;

b) să propună către DNSC politici de securitate cibernetică specifice;

c) să asigure coordonarea și monitorizarea gestionării incidentelor de securitate cibernetică identificate.

CAPITOLUL IV

Managementul incidentelor și reziliența în spațiul cibernetic

SECȚIUNEA 1

Managementul incidentelor de securitate cibernetică

Art. 19. -

(1) DNSC dezvoltă și asigură managementul Platformei naționale pentru raportarea incidentelor de securitate cibernetică, denumită în continuare PNRISC.

(2) Autoritățile prevăzute la art. 10 au acces garantat la PNRISC.

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

Art. 20. -

(1) Persoanele juridice care au în responsabilitate rețele și sisteme informatice prevăzute la art. 3 alin. (1) lit. b) și lit. 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) Dacă informațiile prevăzute la art. 21 nu pot fi comunicate complet în termenul prevăzut la alin. (1), acestea se transmit în cel mult 5 zile de la notificarea inițială.

(3) 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. 21. -

Incidentele de securitate cibernetică sunt notificate în PNRISC în condițiile secțiunii a 2-a din Capitolul IV al Legii nr. 362/2018 privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice.

Art. 22. -

În domeniul managementului incidentelor de securitate cibernetică, autoritățile prevăzute la art. 10 lit. c) și d) 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 competență, 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 coordoneze managementul incidentelor de securitate cibernetică identificate în cadrul rețelelor și sistemelor informatice aflate în domeniul lor de competență, activitate sau responsabilitate;

d) să acorde sprijin, la cerere, proprietarilor, administratorilor, posesorilor și/sau utilizatorilor 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;

e) 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 se realizează prin implementarea de măsuri proactive și reactive de către entitățile care dețin, organizează, administrează, și utilizează rețelele și sistemele informatice prevăzute la art. 3.

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

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

b) constituirea și operarea Centrelor Operaționale de Securitate;

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 proactive, care să permită cunoașterea anticipativă a amenințărilor din spațiul cibernetic;

e) finanțarea pentru dezvoltarea capabilităților de securitate și apărare cibernetică, inclusiv din perspectiva cercetării, dezvoltării, inovării și digitalizării în domeniu și asimilării tehnologiilor emergente;

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

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

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

i) dezvoltarea de strategii, norme, politici, proceduri, analize de risc, planuri și măsuri de control tehnic privind apărarea și securitatea cibernetică;

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

k) 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 și 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 au obligația de a pune la dispoziția autorităților prevăzute la art. 10, la cererea motivată a acestora, în termen de maximum 48 de ore de la data primirii solicitării, date și informații privind incidente, amenințări, riscuri sau vulnerabilități a căror manifestare poate afecta o rețea sau sistem informatic a deținătorului sau a unor terți.

(2) Datele și informațiile prevăzute la alin. (1) se transmit 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 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 Național 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, riscuri 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.

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) Persoanele fizice și juridice care au în responsabilitate rețelele și sistemele 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 rețelele și sistemele informatice prevăzute la art. 3 pun în aplicare măsurile din planurile prevăzute la alin. (1).

CAPITOLUL VI

Apărarea cibernetică

Art. 29. -

În domeniul apărării cibernetice, MApN are următoarele atribuții:

a) apără și protejează sistemele și rețelele informatice aparținând MApN ;

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 apărării naționale, la adresa structurilor MApN 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. 30. -

MApN 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. 31. -

(1) 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 MCID pentru încadrarea spațiului românesc al cercetării în Spațiul European al Cercetării.

(2) MCID elaborează un program multianual de finanțare a proiectelor de cercetare, dezvoltare și inovare în domeniul securității cibernetice, la care pot participa organizații de cercetare publice și private, precum și autorități și instituții publice cu atribuții în domeniul securității cibernetice.

(3) Bugetul anual alocat programului prevăzut la alin. (2) este de minimum 10% din bugetul alocat MCID pentru anul respectiv.

(4) Finanțarea pentru programul prevăzut la alin. (2) se realizează pe criterii competitive, potrivit unei metodologii de concurs adoptată prin ordin al ministrului cercetării, inovării și digitalizării.

Art. 32. -

(1) Autoritățile prevăzute la art. 10 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 autorități prevăzute la art. 10 se desemnează de către conducătorul instituției entitatea responsabilă pentru managementul activităților de cercetare, dezvoltare și inovare în domeniile securității și apărării cibernetice.

(3) Autoritățile prevăzute la art. 10 cooperează cu mediul academic, industria de profil și Centrul european de competențe în domeniul industrial, tehnologic și de cercetare în materie de securitate cibernetică, precum și cu Rețeaua de centre naționale de coordonare, pentru implementarea următoarelor linii de efort în domeniul cercetării, dezvoltării, inovării și digitalizării:

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, inovării și digitalizării;

c) promovarea de noi tehnologii, 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. 33. -

(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 cel puțin următoarele:

a) dezvoltare de capabilități de securitate și apărare cibernetică;

b) programe de cercetare, dezvoltare, inovare și digitalizare;
c) cursuri de formare profesională sau de specializare;
d) exerciții de securitate cibernetică;
e) conferințe și alte manifestări științifice.

SECȚIUNEA 2

La nivel internațional

Art. 34. -

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 securitate și apărare 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. 35. -

(1) Autoritățile și 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 MApN.

CAPITOLUL IX

Formarea profesională, educația, instruirea

Art. 36. -

Entitățile care dețin, organizează, administrează și utilizează rețelele și sistemele informatice prevăzute la art. 3 au obligația de a asigura, pentru personalul propriu, formarea profesională, educația și instruirea în domeniul securității și apărării cibernetice prin cursuri, exerciții, conferințe, seminarii, precum și alte tipuri de activități.

Art. 37. -

(1) Autoritățile și instituțiile din domeniile apărării, ordinii publice și securității naționale pot organiza~~,~~ la nivel instituțional sau interinstituțional, exerciții de securitate și apărare cibernetică.

(2) Autoritățile și instituțiile prevăzute la alin. (1) elaborează și adoptă un plan anual și multianual de exerciții de securitate și apărare cibernetică.

Art. 38. -

(1) Autoritățile și instituțiile din domeniile apărării, ordinii publice și securității naționale participă la exerciții de securitate și apărare cibernetică organizate la nivel internațional, respectiv la la nivelul UE și NATO.

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

Art. 39. -

DNSC și autoritățile și instituțiile din domeniile apărării, ordinii publice și securității naționale au următoarele atribuții:

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, amenințările și vulnerabilitățile 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) emit informări privind obligațiile care derivă din calitatea de proprietar, administrator, organizator, 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 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 X

Securitatea lanțului de aprovizionare

Art. 40. -

(1) Entitățile care dețin, organizează, administrează și utilizează rețelele și sistemele informatice prevăzute la art. 3 implementează procesele de management al riscurilor de securitate cibernetică specifice lanțului de aprovizionare.

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

Art. 41. -

La nivelul entităților care dețin, organizează, administrează și utilizează rețelele și sistemele informatice prevăzute la art. 3 se desemnează responsabili 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, riscurile și vulnerabilitățile 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. 42. -

Entitățile care dețin, organizează, administrează și utilizează rețelele și sistemele informatice prevăzute la art. 3 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. 43. -

Entitățile care dețin, organizează, administrează și utilizează rețelele și sistemele informatice prevăzute la art. 3 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 XI

Dispoziții tranzitorii și finale

Art. 44. -

(1) În vederea aplicării prevederilor art. 19 alin. (3), politicile de confidențialitate se adoptă prin ordin al directorului DNSC în maximum 90 de zile de la data intrării în vigoare a prezentei legi.

(2) În vederea aplicării prevederilor art. 23, autoritățile prevăzute la art. 10 adoptă măsuri proprii de reziliență în spațiul cibernetic în maximum 120 de zile de la data intrării în vigoare a prezentei legi.

(3) În vederea aplicării prevederilor art. 27 alin. (1), metodologia se adoptă prin ordin al directorului DNSC în maximum 6 luni de la data intrării în vigoare a prezentei legi.

(4) În vederea aplicării prevederilor art. 31 alin. (2)-(4), ministrul cercetării, inovării și digitalizării emite un ordin în maximum 120 de zile de la intrarea în vigoare a prezentei legi.

Art. 45. -

La articolul 3 din Legea nr. 51/1991 privind securitatea națională a României, republicată în Monitorul Oficial, Partea I, nr. 190 din 18 martie 2014, cu modificările și completările ulterioare, după litera m), se introduc două noi litere, literele n) și o), care vor avea următorul cuprins:

”*n) acțiuni și inacțiuni de natură a afecta interesele și obiectivele naționale de securitate pe linia infrastructurilor critice de comunicații și tehnologia informației;*

o) acțiuni, inacțiuni sau stări de fapt cu consecințe la nivel național, regional sau global care afectează reziliența statului în raport cu riscurile și amenințările de tip hibrid.”

Această lege a fost adoptată de Parlamentul României, cu respectarea prevederilor art. 75 şi ale art. 76 alin. (1) din Constituţia României, republicată.

PREȘEDINTELE CAMEREI DEPUTAȚILOR PREȘEDINTELE SENATULUI