

Guvernul României

Hotărârea nr. 271/2013 pentru aprobarea Strategiei de securitate cibernetică a României și a Planului de acțiune la nivel național privind implementarea Sistemului național de securitate cibernetică

Publicat în Monitorul Oficial, Partea I nr. 296 din 23.05.2013.

Hotărâre pentru aprobarea Strategiei de securitate cibernetică a României și a Planului de acțiune la nivel național privind implementarea Sistemului național de securitate cibernetică

În temeiul art. 108 din Constituția României, republicată, și al art. 11 lit. f) din Legea nr. 90/2001 privind organizarea și funcționarea Guvernului României și a ministerelor, cu modificările și completările ulterioare,

Guvernul României adoptă prezenta hotărâre.

Art. 1. - Se aprobă Strategia de securitate cibernetică a României, prevăzută în anexa nr. 1.

Art. 2. - Se aprobă Planul de acțiune la nivel național privind implementarea Sistemului național de securitate cibernetică prevăzut în anexa nr. 2^{1*)}.

Art. 3. - Ministerul pentru Societatea Informațională și celelalte autorități publice responsabile au obligația de a duce la îndeplinire obiectivele și direcțiile de acțiune prevăzute în Strategia de securitate cibernetică a României și în Planul de acțiune la nivel național privind implementarea Sistemului național de securitate cibernetică, cu respectarea prevederilor legale în vigoare.

Art. 4. - Anexele nr. 1 și 2 fac parte integrantă din prezenta hotărâre.

PRIM-MINISTRU

VICTOR-VIOREL PONTA

Contrasemnează:

Viceprim-ministru,

Gabriel Oprea

Ministrul pentru societatea informațională,

¹ *) Anexa nr. 2 se comunică instituțiilor interesate, fiind clasificată potrivit legii.

Dan Nica

Viceprim-ministru,

ministrul finanțelor publice,

Daniel Chițoiu

Ministrul delegat pentru buget,

Liviu Voinea

Ministrul apărării naționale,

Mircea Dușa

Ministrul afacerilor interne,

Radu Stroe

Ministrul educației naționale,

Remus Pricopie

Ministrul afacerilor externe,

Titus Corlățean

Ministrul delegat pentru învățământ superior,

cercetare științifică și dezvoltare tehnologică,

Mihnea Cosmin Costoiu

Directorul Serviciului Român de Informații,

George-Cristian Maior

Directorul Serviciului de Informații Externe,

Teodor Viorel Meleşcanu

Directorul Serviciului de Protecție și Pază,

Lucian-Silvan Pahonțu

Directorul Serviciului de Telecomunicații Speciale,

Marcel Opreș

Directorul Oficiului Registrului Național
al Informațiilor Secrete de Stat,
Marius Petrescu

București, 15 mai 2013.

Nr. 271.

STRATEGIA de securitate cibernetică a României

I. Introducere

1. Context

Dezvoltarea rapidă a tehnologiilor moderne de informații și comunicații - condiție sine qua non a edificării societății informaționale - a avut un impact major asupra ansamblului social, marcând adevărate mutații în filozofia de funcționare a economicului, politicului și culturalului, dar și asupra vieții de zi cu zi a individului. Practic, în prezent, accesul facil la tehnologia informației și comunicațiilor reprezintă una dintre premisele bunei funcționări a societății moderne.

Spațiul cibernetic se caracterizează prin lipsa frontierelor, dinamism și anonimat, generând deopotrivă oportunități de dezvoltare a societății informaționale bazate pe cunoaștere, dar și riscuri la adresa funcționării acesteia (la nivel individual, statal și chiar cu manifestare transfrontalieră).

Alături de beneficiile incontestabile pe care informatizarea le induce la nivelul societății moderne, aceasta introduce și vulnerabilități, astfel că asigurarea securității spațiului cibernetic trebuie să constituie o preocupare majoră a tuturor actorilor implicați, mai ales la nivel instituțional, unde se concentrează responsabilitatea elaborării și aplicării de politici coerente în domeniu.

România urmărește atât dezvoltarea unui mediu informațional dinamic bazat pe interoperabilitate și servicii specifice societății informaționale, cât și asigurarea respectării drepturilor și libertăților fundamentale ale cetățenilor și a intereselor de securitate națională, într-un cadru legal adecvat. Din această perspectivă se resimte necesitatea dezvoltării culturii de securitate cibernetică a utilizatorilor sistemelor informatice și de comunicații, adesea insuficient informați în legătură cu potențialele riscuri, dar și cu soluțiile de contracarare a acestora. Cunoașterea pe scară largă a riscurilor și amenințărilor derivate din activitățile desfășurate în spațiul cibernetic, precum și a modului de prevenire și contracarare a acestora necesită o comunicare și cooperare eficiente între actorii specifici în acest domeniu.

Statul român își asumă rolul de coordonator al activităților desfășurate la nivel național pentru asigurarea securității cibernetică, în concordanță cu demersurile inițiate la nivelul UE și NATO. Problematika securității cibernetică a devenit prioritară pentru aceste organisme, care derulează demersuri reglementare necesare dezvoltării mecanismelor de apărare cibernetică.

Incidentele de securitate cibernetică și atacurile cibernetice majore cu care s-au confruntat în ultimii ani unele state și organizații internaționale au determinat conștientizarea, la nivel internațional, a necesității adoptării unor strategii și politici în domeniul securității cibernetice. Astfel, există în prezent strategii naționale de securitate cibernetică, precum cele ale Estoniei, Statelor Unite ale Americii, Marii Britanii, Germaniei și Franței, care fundamentează necesitatea demersurilor pentru dezvoltarea capabilităților proprii de contracarare a atacurilor cibernetice și stabilesc cadrul de acțiune și cooperare între diverse entități guvernamentale și nonguvernamentale pentru limitarea consecințelor. Conform acestor strategii, eforturile națiunilor vizează implementarea unor măsuri de securitate care să conducă la creșterea nivelului de protecție a infrastructurilor cibernetice, în special a celor care susțin infrastructurile critice naționale.

Evoluția rapidă a naturii amenințărilor cibernetice a necesitat adoptarea, și de către Organizația Nord-Atlantică, a unui nou concept și a unei noi politici în domeniul apărării cibernetice. În acest sens, NATO și-a redefinit rolul și perimetrul de acțiune în domeniu și a elaborat un plan de acțiune pentru dezvoltarea unor capabilități necesare protejării infrastructurilor cibernetice proprii, precum și a unor mecanisme de consultare a statelor membre și de asigurare a asistenței în cazul unor atacuri cibernetice majore.

La nivelul UE sunt întreprinse demersuri în privința adoptării unei strategii europene pentru securitatea cibernetică, care să armonizeze eforturile statelor membre în abordarea provocărilor de securitate din spațiul cibernetic și protecția infrastructurilor informatice critice.

Totodată, la nivelul UE, s-a conturat necesitatea adoptării unei politici privind lupta împotriva criminalității informatice. Inițiativele subsecvente au pornit de la constatarea creșterii numărului de infracțiuni informatice, a tot mai amplei implicări a grupurilor de criminalitate organizată în criminalitatea informatică, precum și a necesității unei coordonări a eforturilor europene în direcția combaterii acestor acte. Având în vedere că atacurile cibernetice pe scară largă, bine coordonate și direcționate către infrastructurile cibernetice critice ale statelor membre, constituie o preocupare crescândă a UE, întreprinderea de acțiuni pentru combaterea tuturor formelor de criminalitate informatică, atât la nivel european, cât și la nivel național, a devenit o necesitate stringentă.

Creșterea capacității de luptă împotriva criminalității informatice la nivel național, european și internațional implică, printre altele:

- creșterea gradului de cooperare și coordonare între unitățile responsabile cu combaterea criminalității informatice, alte autorități și experți din cadrul Uniunii Europene;

- dezvoltarea unui cadru de reglementare coerent, la nivelul UE, privind lupta împotriva criminalității informatice, în coordonare cu statele membre, precum și cu autoritățile europene și internaționale cu relevanță în domeniu;

- creșterea nivelului de conștientizare a costurilor și pericolelor pe care le implică criminalitatea informatică.

În acest context, România recunoaște existența unor astfel de amenințări și susține o abordare comună, integrată și coordonată, atât la nivelul NATO, cât și la nivelul UE, pentru a putea oferi un răspuns oportun la atacurile cibernetice.

2. Scop și obiective

Scopul Strategiei de securitate cibernetică a României este de a defini și de a menține un mediu virtual sigur, cu un înalt grad de reziliență și de încredere, bazat pe infrastructurile cibernetice naționale, care să constituie un important suport pentru securitatea națională și buna guvernare, pentru maximizarea beneficiilor cetățenilor, mediului de afaceri și ale societății românești, în ansamblul ei.

Strategia de securitate cibernetică a României prezintă obiectivele, principiile și direcțiile majore de acțiune pentru cunoașterea, prevenirea și contracararea amenințărilor, vulnerabilităților și riscurilor la adresa securității cibernetice a României și pentru promovarea intereselor, valorilor și obiectivelor naționale în spațiul cibernetic.

În scopul asigurării coerenței și eficienței acțiunilor, Strategia de securitate cibernetică a României, denumită în continuare strategie, urmărește îndeplinirea obiectivului național de securitate privind "asigurarea securității cibernetice", cu respectarea principiilor și caracteristicilor Strategiei naționale de apărare și Strategiei naționale de protecție a infrastructurilor critice.

Pentru asigurarea securității cibernetice a României, strategia stabilește următoarele obiective:

a) adaptarea cadrului normativ și instituțional la dinamica amenințărilor specifice spațiului cibernetic;

b) stabilirea și aplicarea unor profile și cerințe minime de securitate pentru infrastructurile cibernetice naționale, relevante din punct de vedere al funcționării corecte a infrastructurilor critice;

c) asigurarea rezilienței infrastructurilor cibernetice;

d) asigurarea stării de securitate prin cunoașterea, prevenirea și contracararea vulnerabilităților, riscurilor și amenințărilor la adresa securității cibernetice a României;

e) valorificarea oportunităților spațiului cibernetic pentru promovarea intereselor, valorilor și obiectivelor naționale în spațiul cibernetic;

f) promovarea și dezvoltarea cooperării între sectorul public și cel privat în plan național, precum și a cooperării internaționale în domeniul securității cibernetice;

g) dezvoltarea culturii de securitate a populației prin conștientizarea față de vulnerabilitățile, riscurile și amenințările provenite din spațiul cibernetic și necesitatea asigurării protecției sistemelor informatice proprii;

h) participarea activă la inițiativele organizațiilor internaționale din care România face parte în domeniul definirii și stabilirii unui set de măsuri destinate creșterii încrederii la nivel internațional privind utilizarea spațiului cibernetic.

3. Concepte, definiții și termeni

În înțelesul prezentei strategii, termenii și expresiile de mai jos au următoarea semnificație:

infrastructuri cibernetic - infrastructuri de tehnologia informației și comunicații, constând în sisteme informatice, aplicații aferente, rețele și servicii de comunicații electronice;

spațiul cibernetic - mediul virtual, generat de infrastructurile cibernetic, incluzând conținutul informațional procesat, stocat sau transmis, precum și acțiunile derulate de utilizatori în acesta;

securitate cibernetică - starea de normalitate rezultată în urma aplicării unui ansamblu de măsuri proactive și reactive prin care se asigură confidențialitatea, integritatea, disponibilitatea, autenticitatea și nonrepudierea informațiilor în format electronic, a resurselor și serviciilor publice sau private, din spațiul cibernetic. Măsurile proactive și reactive pot include politici, concepte, standarde și ghiduri de securitate, managementul riscului, activități de instruire și conștientizare, implementarea de soluții tehnice de protejare a infrastructurilor cibernetic, managementul identității, managementul consecințelor;

apărare cibernetică - acțiuni desfășurate în spațiul cibernetic în scopul protejării, monitorizării, analizării, detectării, contracarării agresiunilor și asigurării răspunsului oportun împotriva amenințărilor asupra infrastructurilor cibernetic specifice apărării naționale;

operații în rețele de calculatoare - procesul complex de planificare, coordonare, sincronizare, armonizare și desfășurare a acțiunilor în spațiul cibernetic pentru protecția, controlul și utilizarea rețelelor de calculatoare în scopul obținerii superiorității informaționale, concomitent cu neutralizarea capabilităților adversarului;

amenințare cibernetică - circumstanță sau eveniment care constituie un pericol potențial la adresa securității cibernetic;

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

incident cibernetic - eveniment survenit în spațiul cibernetic ale cărui consecințe afectează securitatea cibernetică;

terorism cibernetic - activitățile premeditate desfășurate în spațiul cibernetic de către persoane, grupări sau organizații motivate politic, ideologic ori religios ce pot determina distrugeri materiale sau victime, de natură să determine panică ori teroare;

spionaj cibernetic - acțiuni desfășurate în spațiul cibernetic, cu scopul de a obține neautorizat informații confidențiale în interesul unei entități statale sau nonstatale;

criminalitatea informatică - totalitatea faptelor prevăzute de legea penală sau de alte legi speciale care prezintă pericol social și sunt săvârșite cu vinovăție, prin intermediul ori asupra infrastructurilor cibernetic;

vulnerabilitatea în spațiul cibernetic - slăbiciune în proiectarea și implementarea infrastructurilor cibernetic sau a măsurilor de securitate aferente care poate fi exploatată de către o amenințare;

riscul de securitate în spațiul cibernetic - probabilitatea ca o amenințare să se materializeze, exploatând o anumită vulnerabilitate specifică infrastructurilor cibernetic;

managementul riscului - un proces complex, continuu și flexibil de identificare, evaluare și contracarare a riscurilor la adresa securității cibernetic, bazat pe utilizarea unor tehnici și instrumente complexe, pentru prevenirea pierderilor de orice natură;

managementul identității - metode de validare a identității persoanelor când acestea accesează anumite infrastructuri cibernetic;

reziliența infrastructurilor cibernetic - capacitatea componentelor infrastructurilor cibernetic de a rezista unui incident sau atac cibernetic și de a reveni la starea de normalitate;

entități de tip CERT - structuri specializate în înțelesul art. 2 lit. a) din Hotărârea Guvernului nr. 494/2011 privind înființarea Centrului Național de Răspuns la Incidente de Securitate Cibernetică - CERT-RO.

4. Principii

Asigurarea securității cibernetic trebuie să constituie rezultatul unor abordări bazate pe evaluarea riscurilor, prioritizarea resurselor, implementarea și monitorizarea eficienței măsurilor de securitate identificate prin aplicarea managementului de risc și respectarea următoarelor principii:

- coordonarea - activitățile se realizează într-o concepție unitară, pe baza unor planuri de acțiune convergente destinate asigurării securității cibernetic, în conformitate cu atribuțiile și responsabilitățile fiecărei entități;

- cooperarea - toate entitățile implicate (din mediul public sau privat) colaborează, la nivel național și internațional, pentru asigurarea unui răspuns adecvat la amenințările din spațiul cibernetic;

- eficiența - demersurile întreprinse vizează managementul optim al resurselor disponibile;

- prioritizarea - eforturile se vor concentra asupra securizării infrastructurilor ciberneticice ce susțin infrastructurile critice naționale și europene;

- diseminarea - asigurarea transferului de informații, expertiză și bune practici în scopul protejării infrastructurilor ciberneticice;

- protejarea valorilor - politicile de securitate cibernetică vor asigura echilibrul între nevoia de creștere a securității în spațiul cibernetic și prezervarea dreptului la intimitate și alte valori și libertăți fundamentale ale cetățeanului;

- asumarea responsabilității - toți deținătorii și utilizatorii de infrastructuri ciberneticice trebuie să întreprindă măsurile necesare pentru securizarea infrastructurilor proprii și să nu afecteze securitatea infrastructurilor celorlalți deținători sau utilizatori;

- separarea rețelelor - reducerea probabilității de manifestare a atacurilor ciberneticice, specifice rețelei internet, asupra infrastructurilor ciberneticice care asigură funcțiile vitale ale statului, prin utilizarea unor rețele dedicate, separate de internet.

II. Provocări și oportunități

1. Amenințări, vulnerabilități și riscuri

Amenințările specifice spațiului cibernetic se caracterizează prin asimetrie și dinamică accentuată și caracter global, ceea ce le face dificil de identificat și de contracarat prin măsuri proporționale cu impactul materializării riscurilor.

România se confruntă, în prezent, cu amenințări provenite din spațiul cibernetic, la adresa infrastructurilor critice, având în vedere interdependența din ce în ce mai ridicată între infrastructuri ciberneticice și infrastructuri precum cele din sectoarele financiar-bancar, transport, energie și apărare națională. Globalitatea spațiului cibernetic este de natură să amplifice riscurile la adresa acestora, afectând deopotrivă cetățenii, mediul de afaceri și cel guvernamental.

În general, infrastructurile ciberneticice pot fi afectate de amenințări de natură tehnică (de exemplu deficiențe sau defecțiuni tehnice), umană (de exemplu erori de operare, acțiuni voluntare) ori naturale (de exemplu fenomene meteo extreme, catastrofe naturale).

Amenințările la adresa spațiului cibernetic se pot clasifica în mai multe moduri, dar cele mai frecvent utilizate sunt cele bazate pe factorii motivaționali și impactul asupra societății. În acest sens, pot fi avute în vedere criminalitatea informatică, terorismul cibernetic și războiul cibernetic, având ca sursă atât actori statali, cât și actori nonstatali.

Amenințările din spațiul cibernetic se materializează - prin exploatarea vulnerabilităților de natură umană, tehnică și procedurală - cel mai adesea în:

- atacurile ciberneticе împotriva infrastructurilor care susțin funcții de utilitate publică ori servicii ale societății informaționale a căror întrerupere/afectare ar putea constitui un pericol la adresa securității naționale;

- accesarea neautorizată a infrastructurilor ciberneticе;

- modificarea, ștergerea sau deteriorarea neautorizată de date informatice ori restricționarea ilegală a accesului la aceste date;

- spionajul cibernetic;

- cauzarea unui prejudiciu patrimonial, hărțuirea și șantajul persoanelor fizice și juridice, de drept public și privat.

Principalii actori care generează amenințări în spațiul cibernetic sunt:

- persoane sau grupări de criminalitate organizată care exploatează vulnerabilitățile spațiului cibernetic în scopul obținerii de avantaje patrimoniale sau nepatrimoniale;

- teroriști sau extremiști care utilizează spațiul cibernetic pentru desfășurarea și coordonarea unor atacuri teroriste, activități de comunicare, propagandă, recrutare și instruire, colectare de fonduri etc., în scopuri teroriste;

- state sau actori nonstatali care inițiază sau derulează operațiuni în spațiul cibernetic, în scopul culegerii de informații din domeniile guvernamental, militar, economic ori al materializării altor amenințări la adresa securității naționale.

2. Oportunități

În același timp, spațiul cibernetic, devenit un nou domeniu de interacțiune în cadrul societății moderne, oferă o serie de oportunități generate de însăși specificitatea acestuia. Astfel, au fost identificate următoarele oportunități pe care România le poate exploata prin intermediul spațiului cibernetic:

- susținerea politicilor și promovarea intereselor naționale;

- dezvoltarea și susținerea mediului de afaceri;

- creșterea calității vieții prin dezvoltarea serviciilor oferite de societatea informațională;
- îmbunătățirea cunoașterii și susținerea deciziilor strategice naționale în era informațională prin asigurarea capacităților și instrumentelor cibernetice adecvate;
- creșterea nivelului de cunoaștere și a capacității de predicție în scopul avertizării timpurii privind riscurile și amenințările la adresa securității naționale;
- creșterea capacităților tehnice și a competențelor resursei umane pentru realizarea obiectivelor de securitate națională.

III. Direcții de acțiune

România își propune asigurarea stării de normalitate în spațiul cibernetic reducând riscurile și valorificând oportunitățile, prin îmbunătățirea cunoștințelor, a capabilităților și a mecanismelor de decizie. În acest sens, eforturile se vor focaliza pe următoarele direcții de acțiune:

1. Stabilirea cadrului conceptual, organizatoric și acțional necesar asigurării securității cibernetice

- constituirea și operaționalizarea unui sistem național de securitate cibernetică;
- completarea și armonizarea cadrului legislativ național în domeniu, inclusiv stabilirea și aplicarea unor cerințe minimale de securitate pentru infrastructurile cibernetice naționale;
- dezvoltarea cooperării între sectorul public și cel privat, inclusiv prin stimularea schimbului reciproc de informații, privind amenințări, vulnerabilități, riscuri, precum și cele referitoare la incidente și atacuri cibernetice.

2. Dezvoltarea capacităților naționale de management al riscului în domeniul securității cibernetice și de reacție la incidente cibernetice în baza unui program național, vizând:

- consolidarea, la nivelul autorităților competente potrivit legii, a potențialului de cunoaștere, prevenire și contracarare a amenințărilor și minimizarea riscurilor asociate utilizării spațiului cibernetic;
- asigurarea unor instrumente de dezvoltare a cooperării dintre sectorul public și cel privat, în domeniul securității cibernetice, inclusiv pentru crearea unui mecanism eficient de avertizare și alertă, respectiv de reacție la incidentele cibernetice;
- stimularea capabilităților naționale de cercetaredezvoltare și inovare în domeniul securității cibernetice;
- creșterea nivelului de reziliență a infrastructurilor cibernetice;

- dezvoltarea entităților de tip CERT, atât în cadrul sectorului public, cât și în sectorul privat.

3. Promovarea și consolidarea culturii de securitate în domeniul cibernetic

- derularea unor programe de conștientizare a populației, a administrației publice și a sectorului privat, cu privire la amenințările, vulnerabilitățile și riscurile specifice utilizării spațiului cibernetic;

- dezvoltarea de programe educaționale, în cadrul formelor obligatorii de învățământ, privind utilizarea sigură a internetului și a echipamentelor de calcul;

- formarea profesională adecvată a persoanelor care își desfășoară activitatea în domeniul securității cibernetice și promovarea pe scară largă a certificărilor profesionale în domeniu;

- includerea unor elemente referitoare la securitatea cibernetică în programele de formare și perfecționare profesională a managerilor din domeniul public și privat.

4. Dezvoltarea cooperării internaționale în domeniul securității cibernetice

- încheierea unor acorduri de cooperare la nivel internațional pentru îmbunătățirea capacității de răspuns în cazul unor atacuri cibernetice majore;

- participarea la programe internaționale care vizează domeniul securității cibernetice;

- promovarea intereselor naționale de securitate cibernetică în formatele de cooperare internațională la care România este parte.

IV. Sistemul național de securitate cibernetică

Sistemul național de securitate cibernetică (SNSC) reprezintă cadrul 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 spațiului cibernetic, inclusiv prin cooperarea cu mediul academic și cel de afaceri, asociațiile profesionale și organizațiile neguvernamentale.

Misiunea SNSC constă în asigurarea elementelor de cunoaștere, prevenire și contracarare a amenințărilor, vulnerabilităților și riscurilor specifice spațiului cibernetic care pot afecta securitatea infrastructurilor cibernetice naționale, inclusiv managementul consecințelor.

Pentru îndeplinirea obiectivelor prezentei strategii, SNSC funcționează ca un mecanism unitar și eficient de relaționare și cooperare interinstituțională, în vederea adoptării și aplicării cu celeritate a deciziilor.

SNSC acționează pe următoarele componente:

Componenta de cunoaștere - furnizează suportul informațional necesar elaborării măsurilor proactive și reactive în vederea asigurării securității cibernetice.

Componenta de prevenire - este principalul mijloc de asigurare a securității cibernetice prin crearea și dezvoltarea capacităților necesare analizei și prognozei evoluției stării acesteia.

Componenta de cooperare și coordonare - asigură mecanismul unitar și eficient de relaționare în cadrul SNSC.

Componenta de contracarare - asigură reacția eficientă la amenințările sau atacurile cibernetice, prin identificarea și blocarea manifestării acestora. Aceasta se realizează în scopul menținerii sau restabilirii securității infrastructurilor cibernetice vizate, precum și pentru identificarea și sancționarea autorilor, potrivit legii.

Funcțiile principale ale SNSC se realizează prin informare, monitorizare, diseminare, analizare, avertizare, coordonare, decizie, reacție, refacere și conștientizare, precum și prin adoptarea de măsuri proactive și reactive.

Măsurile proactive vizează:

- actualizarea și armonizarea cadrului național de reglementare în domeniul securității cibernetice în concordanță cu evoluțiile mediului de referință;

- implementarea de politici, concepte, standarde și ghiduri de securitate;

- colectarea de date și informații referitoare la amenințări, vulnerabilități și riscuri identificate în spațiul cibernetic;

- analiza, anticiparea și prognoza evoluției stării de securitate cibernetică;

- realizarea și eficientizarea cooperării între sectorul public și cel privat între deținătorii infrastructurilor cibernetice și autoritățile statului abilitate să întreprindă măsuri de prevenire și contracarare a amenințărilor, precum și de minimizare a efectelor unui atac cibernetic;

- ridicarea nivelului de instruire și conștientizare a populației asupra riscurilor derivate din utilizarea spațiului cibernetic;

- interoperabilitatea cu alte sisteme naționale și internaționale cu atribuții în domeniul securității;

- protejarea infrastructurilor cibernetice naționale și a celor aparținând NATO sau UE aflate în administrarea unor instituții ori autorități publice;

- implementarea unui mecanism de management al riscului;

- asigurarea unui grad ridicat de autoadaptabilitate, în funcție de evoluțiile spațiului cibernetic;
- asigurarea confidențialității, integrității, disponibilității, autenticității și nonrepudierii informațiilor din spațiul cibernetic;
- asigurarea managementului identității în spațiul cibernetic;
- operaționalizarea capacităților destinate managementului incidentelor de securitate cibernetică, inclusiv managementul consecințelor;
- dezvoltarea mecanismelor pentru creșterea nivelului de cultură de securitate.

Măsurile reactive urmăresc:

- aplicarea planurilor de contingență în vederea minimizării efectelor unui atac cibernetic;
- aplicarea măsurilor cu privire la asigurarea continuității fluxurilor informaționale și decizionale;
- aplicarea unui plan de măsuri cu privire la asigurarea funcționalității sistemelor în condiții de securitate a serviciilor publice sau private;
- recuperarea și restaurarea datelor;
- identificarea și implementarea lecțiilor învățate, rezultate în urma aplicării procedurilor de management al incidentelor, management al consecințelor unui atac cibernetic, precum și de continuitate a activităților.

Eficiența activităților desfășurate în SNSC depinde în mod esențial de cooperarea, inclusiv între sectorul public și cel privat, între deținătorii infrastructurilor cibernetică și autoritățile statului abilitate să întreprindă măsuri de prevenire și contracarare a amenințărilor, de investigare a atacurilor cibernetică, precum și de minimizare a efectelor acestora.

Consiliul Suprem de Apărare a Țării este autoritatea ce coordonează, la nivel strategic, activitatea SNSC. Consiliul Suprem de Apărare a Țării avizează Strategia de securitate cibernetică a României și aprobă Regulamentul de organizare și funcționare al Consiliului operativ de securitate cibernetică.

Consiliul operativ de securitate cibernetică (COSC) reprezintă organismul prin care se realizează coordonarea unitară a SNSC. Din COSC fac parte, în calitate de membri permanenți, reprezentanți ai Ministerului Apărării Naționale, Ministerului Afacerilor Interne, Ministerului Afacerilor Externe, Ministerului pentru Societatea Informațională, Serviciului Român de Informații, Serviciului de Telecomunicații Speciale, Serviciului de Informații Externe, Serviciului

de Protecție și Pază, Oficiului Registrului Național pentru Informații Secrete de Stat, precum și secretarul Consiliului Suprem de Apărare a Țării. Conducerea COSC este asigurată de un președinte (consilierul prezidențial pe probleme de securitate națională) și un vicepreședinte (consilierul prim-ministrului pe probleme de securitate națională). Coordonatorul tehnic al COSC este Serviciul Român de Informații, în condițiile legii.

Guvernul României, prin Ministerul pentru Societatea Informațională, asigură coordonarea celorlalte autorități publice care nu sunt reprezentate în COSC, în vederea realizării coerenței politicilor și implementarea strategiilor guvernamentale în domeniul comunicațiilor electronice, tehnologiei informației și al serviciilor societății informaționale și societății bazate pe cunoaștere, iar prin Centrul Național de Răspuns la Incidente de Securitate Cibernetică - CERT-RO - asigură elaborarea și diseminarea politicilor publice de prevenire și contracarare a incidentelor din cadrul infrastructurilor cibernetice, potrivit ariei de competență.

Guvernul României va elabora proiectul legii privind securitatea cibernetică, pe care îl va supune aprobării Parlamentului, potrivit legii.

Fiecare dintre instituțiile reprezentate în COSC cooperează cu organismele internaționale ale UE, NATO, OSCE etc., fiecare pe domeniul său de competență.

V. Cooperarea între sectorul public și cel privat

Dezvoltarea cooperării dintre mediul public și cel privat, în scopul asigurării securității cibernetice, reprezintă o direcție prioritară de acțiune la nivelul organismelor internaționale sau alianțelor la care România este parte, având în vedere că spațiul cibernetic reunește deopotrivă infrastructuri cibernetice deținute și administrate de stat, precum și de entități private.

Principalele linii directoare de asigurare a securității cibernetice, în cadrul cooperării între sectorul public și cel privat, trebuie să urmărească:

- cooperarea bazată pe încredere între stat și mediul de afaceri, la toate nivelurile;
- creșterea nivelului de protecție al infrastructurilor cibernetice prin corelarea măsurilor întreprinse cu resursele disponibile în sectorul public și privat.

Responsabilitatea asigurării securității cibernetice revine tuturor actorilor implicați, ținând cont de interesele complementare în acest domeniu pentru asigurarea legalității operațiunilor desfășurate, combaterea fenomenului criminalității informatice și protecția infrastructurilor critice interconectate cu spațiul cibernetic și se bazează pe sporirea încrederii reciproce.

Principalele obiective ale cooperării între sectorul public și cel privat vizează:

- schimbul de informații privind amenințări, vulnerabilități și riscuri specifice;

- dezvoltarea capacităților de avertizare timpurie și de răspuns la incidente și atacuri cibernetice;
- desfășurarea de exerciții comune privind securitatea spațiului cibernetic;
- dezvoltarea de programe educaționale și de cercetare în domeniu;
- dezvoltarea culturii de securitate;
- reacția comună în cazul unor atacuri cibernetice majore.

Realizarea obiectivelor menționate presupune conlucrarea dintre sectorul public și sectorul privat, inclusiv prin măsuri de prevenție, conștientizare și promovare a oportunităților în domeniul cibernetic.

VI. Concluzii

Asigurarea securității cibernetice se bazează pe cooperarea la nivel național și internațional pentru protejarea spațiului cibernetic, prin coordonarea demersurilor naționale cu orientările și măsurile adoptate la nivel internațional, în formatele de cooperare la care România este parte.

Având în vedere dinamismul evoluțiilor globale în spațiul cibernetic, precum și obiectivele României în procesul de dezvoltare a societății informaționale și implementare pe scară largă a serviciilor electronice este necesară elaborarea unui program național detaliat, care - pe baza reperelor oferite de prezenta strategie - să asigure elaborarea și punerea în practică a unor proiecte concrete de securitate cibernetică.

Măsurile destinate operaționalizării SNSC trebuie armonizate cu eforturile pe dimensiunea protecției infrastructurilor critice, respectiv cu evoluția procesului de dezvoltare a capacităților de tip CERT. În varianta optimă, SNSC trebuie să dispună de o structură flexibilă și adaptivă care să înglobeze capacități de identificare și anticipare, resurse și proceduri operaționale de prevenire, reacție și contracarare, precum și instrumente pentru documentare și sancționare a autorilor atacurilor cibernetice.

Este necesară implementarea, la nivel național, a unor standarde minimale procedurale și de securitate pentru infrastructurile cibernetice, care să fundamenteze eficiența demersurilor de protejare față de atacuri cibernetice și să limiteze riscurile producerii unor incidente cu potențial impact semnificativ.

Autoritățile publice cu responsabilități în acest domeniu vor aloca resursele financiare necesare asigurării securității cibernetice prin intermediul politicilor de planificare. Pentru asigurarea unei capacități sporite de identificare, evaluare și proiectare a măsurilor adecvate de management al riscului sau de răspuns la incidente și atacuri cibernetice este prioritară dezvoltarea schimburilor

de informații și transferului de expertiză între autoritățile cu responsabilități în domeniu, dezvoltarea cooperării între sectorul public și cel privat și extinderea cooperării cu mediile neguvernamentale și comunitatea academică.

SNSC va constitui platforma de cooperare și armonizare a capacităților de tip CERT existente la nivel național, valorificând instrumentele oferite de acestea, și va acționa pentru consolidarea expertizei în domeniul riscurilor cibernetice, prin stimularea sinergiilor între diferitele planuri de acțiune în domeniul securității cibernetice (militar-civil, public-privat, guvernamental-negvernamental).

Dat fiind ritmul rapid de evoluție a problematicii, prezenta strategie va fi testată și revizuită permanent, inclusiv în contextul mai larg al Strategiei de apărare, în vederea adaptării continue la provocările și oportunitățile generate de un mediu de securitate în permanentă schimbare.

În termen de 90 de zile de la intrarea în vigoare a prezentei strategii, COSC va elabora Programul național destinat managementului riscului în domeniul securității cibernetice.