Guvernul României

Hotărârea nr. 271/2013 pentru aprobarea Strategiei de securitate cibernetică a României şi a Planului de acţiune la nivel naţional privind implementarea Sistemului naţional de securitate cibernetică

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

Hotărâre pentru aprobarea Strategiei de securitate cibernetică a României şi a Planului de acţiune la nivel naţional privind implementarea Sistemului naţional de securitate cibernetică

În temeiul art. 108 din Constituţia României, republicată, şi al art. 11 lit. f) din Legea nr. 90/2001 privind organizarea şi funcţionarea Guvernului României şi a ministerelor, cu modificările şi 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 acţiune la nivel naţional privind implementarea Sistemului naţional de securitate cibernetică prevăzut în anexa nr. 2[1]*).

Art. 3. - Ministerul pentru Societatea Informaţională şi celelalte autorităţi publice responsabile au obligaţia de a duce la îndeplinire obiectivele şi direcţiile de acţiune prevăzute în Strategia de securitate cibernetică a României şi în Planul de acţiune la nivel naţional privind implementarea Sistemului naţional de securitate cibernetică, cu respectarea prevederilor legale în vigoare.

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

PRIM-MINISTRU

VICTOR-VIOREL PONTA

Contrasemnează:

Viceprim-ministru,

Gabriel Oprea

Ministrul pentru societatea informaţională,

[1] *) Anexa nr. 2 se comunică instituţiilor interesate, fiind clasificată potrivit legii.

Dan Nica

Viceprim-ministru,

ministrul finanţelor publice,

Daniel Chiţoiu

Ministrul delegat pentru buget,

Liviu Voinea

Ministrul apărării naţionale,

Mircea Duşa

Ministrul afacerilor interne,

Radu Stroe

Ministrul educaţiei naţionale,

Remus Pricopie

Ministrul afacerilor externe,

Titus Corlăţean

Ministrul delegat pentru învăţământ superior,

cercetare ştiinţifică şi dezvoltare tehnologică,

Mihnea Cosmin Costoiu

Directorul Serviciului Român de Informaţii,

George-Cristian Maior

Directorul Serviciului de Informaţii Externe,

Teodor Viorel Meleşcanu

Directorul Serviciului de Protecţie şi Pază,

Lucian-Silvan Pahonţu

Directorul Serviciului de Telecomunicaţii Speciale,

Marcel Opriş

Directorul Oficiului Registrului Naţional

al Informaţiilor Secrete de Stat,

Marius Petrescu

Bucureşti, 15 mai 2013.

Nr. 271.

ANEXA Nr. 1

STRATEGIA de securitate cibernetică a României

I. Introducere

1. Context

Dezvoltarea rapidă a tehnologiilor moderne de informaţii şi comunicaţii - condiţie sine qua non a edificării societăţii informaţionale - a avut un impact major asupra ansamblului social, marcând adevărate mutaţii în filozofia de funcţionare a economicului, politicului şi culturalului, dar şi asupra vieţii de zi cu zi a individului. Practic, în prezent, accesul facil la tehnologia informaţiei şi comunicaţiilor reprezintă una dintre premisele bunei funcţionări a societăţii moderne.

Spaţiul cibernetic se caracterizează prin lipsa frontierelor, dinamism şi anonimat, generând deopotrivă oportunităţi de dezvoltare a societăţii informaţionale bazate pe cunoaştere, dar şi riscuri la adresa funcţionării acesteia (la nivel individual, statal şi chiar cu manifestare transfrontalieră).

Alături de beneficiile incontestabile pe care informatizarea le induce la nivelul societăţii moderne, aceasta introduce şi vulnerabilităţi, astfel că asigurarea securităţii spaţiului cibernetic trebuie să constituie o preocupare majoră a tuturor actorilor implicaţi, mai ales la nivel instituţional, unde se concentrează responsabilitatea elaborării şi aplicării de politici coerente în domeniu.

România urmăreşte atât dezvoltarea unui mediu informaţional dinamic bazat pe interoperabilitate şi servicii specifice societăţii informaţionale, cât şi asigurarea respectării drepturilor şi libertăţilor fundamentale ale cetăţenilor şi a intereselor de securitate naţională, într-un cadru legal adecvat. Din această perspectivă se resimte necesitatea dezvoltării culturii de securitate cibernetică a utilizatorilor sistemelor informatice şi de comunicaţii, adesea insuficient informaţi în legătură cu potenţialele riscuri, dar şi cu soluţiile de contracarare a acestora. Cunoaşterea pe scară largă a riscurilor şi ameninţărilor derivate din activităţile desfăşurate în spaţiul cibernetic, precum şi a modului de prevenire şi contracarare a acestora necesită o comunicare şi cooperare eficiente între actorii specifici în acest domeniu.

Statul român îşi asumă rolul de coordonator al activităţilor desfăşurate la nivel naţional pentru asigurarea securităţii cibernetice, în concordanţă cu demersurile iniţiate la nivelul UE şi NATO. Problematica securităţii cibernetice a devenit prioritară pentru aceste organisme, care derulează demersuri reglementare necesare dezvoltării mecanismelor de apărare cibernetică.

Incidentele de securitate cibernetică şi atacurile cibernetice majore cu care s-au confruntat în ultimii ani unele state şi organizaţii internaţionale au determinat conştientizarea, la nivel internaţional, a necesităţii adoptării unor strategii şi politici în domeniul securităţii cibernetice. Astfel, există în prezent strategii naţionale de securitate cibernetică, precum cele ale Estoniei, Statelor Unite ale Americii, Marii Britanii, Germaniei şi Franţei, care fundamentează necesitatea demersurilor pentru dezvoltarea capabilităţilor proprii de contracarare a atacurilor cibernetice şi stabilesc cadrul de acţiune şi cooperare între diverse entităţi guvernamentale şi nonguvernamentale pentru limitarea consecinţelor. Conform acestor strategii, eforturile naţiunilor vizează implementarea unor măsuri de securitate care să conducă la creşterea nivelului de protecţie a infrastructurilor cibernetice, în special a celor care susţin infrastructurile critice naţionale.

Evoluţia rapidă a naturii ameninţărilor cibernetice a necesitat adoptarea, şi de către Organizaţia Nord-Atlantică, a unui nou concept şi a unei noi politici în domeniul apărării cibernetice. În acest sens, NATO şi-a redefinit rolul şi perimetrul de acţiune în domeniu şi a elaborat un plan de acţiune pentru dezvoltarea unor capabilităţi necesare protejării infrastructurilor cibernetice proprii, precum şi a unor mecanisme de consultare a statelor membre şi de asigurare a asistenţei în cazul unor atacuri cibernetice majore.

La nivelul UE sunt întreprinse demersuri în privinţa adoptării unei strategii europene pentru securitatea cibernetică, care să armonizeze eforturile statelor membre în abordarea provocărilor de securitate din spaţiul cibernetic şi protecţia infrastructurilor informatice critice.

Totodată, la nivelul UE, s-a conturat necesitatea adoptării unei politici privind lupta împotriva criminalităţii informatice. Iniţiativele subsecvente au pornit de la constatarea creşterii numărului de infracţiuni informatice, a tot mai amplei implicări a grupurilor de criminalitate organizată în criminalitatea informatică, precum şi a necesităţii unei coordonări a eforturilor europene în direcţia combaterii acestor acte. Având în vedere că atacurile cibernetice pe scară largă, bine coordonate şi direcţionate către infrastructurile cibernetice critice ale statelor membre, constituie o preocupare crescândă a UE, întreprinderea de acţiuni pentru combaterea tuturor formelor de criminalitate informatică, atât la nivel european, cât şi la nivel naţional, a devenit o necesitate stringentă.

Creşterea capacităţii de luptă împotriva criminalităţii informatice la nivel naţional, european şi internaţional implică, printre altele:

- creşterea gradului de cooperare şi coordonare între unităţile responsabile cu combaterea criminalităţii informatice, alte autorităţi şi experţi din cadrul Uniunii Europene;

- dezvoltarea unui cadru de reglementare coerent, la nivelul UE, privind lupta împotriva criminalităţii informatice, în coordonare cu statele membre, precum şi cu autorităţile europene şi internaţionale cu relevanţă în domeniu;

- creşterea nivelului de conştientizare a costurilor şi pericolelor pe care le implică criminalitatea informatică.

În acest context, România recunoaşte existenţa unor astfel de ameninţări şi susţine o abordare comună, integrată şi coordonată, atât la nivelul NATO, cât şi la nivelul UE, pentru a putea oferi un răspuns oportun la atacurile cibernetice.

2. Scop şi obiective

Scopul Strategiei de securitate cibernetică a României este de a defini şi de a menţine un mediu virtual sigur, cu un înalt grad de reziliență şi de încredere, bazat pe infrastructurile cibernetice naţionale, care să constituie un important suport pentru securitatea naţională şi buna guvernare, pentru maximizarea beneficiilor cetăţenilor, mediului de afaceri şi ale societăţii româneşti, în ansamblul ei.

Strategia de securitate cibernetică a României prezintă obiectivele, principiile şi direcţiile majore de acţiune pentru cunoaşterea, prevenirea şi contracararea ameninţărilor, vulnerabilităţilor şi riscurilor la adresa securităţii cibernetice a României şi pentru promovarea intereselor, valorilor şi obiectivelor naţionale în spaţiul cibernetic.

În scopul asigurării coerenţei şi eficienţei acţionale, Strategia de securitate cibernetică a României, denumită în continuare strategie, urmăreşte îndeplinirea obiectivului naţional de securitate privind "asigurarea securităţii cibernetice", cu respectarea principiilor şi caracteristicilor Strategiei naţionale de apărare şi Strategiei naţionale de protecţie a infrastructurilor critice.

Pentru asigurarea securităţii cibernetice a României, strategia stabileşte următoarele obiective:

a) adaptarea cadrului normativ şi instituţional la dinamica ameninţărilor specifice spaţiului cibernetic;

b) stabilirea şi aplicarea unor profile şi cerinţe minime de securitate pentru infrastructurile cibernetice naţionale, relevante din punct de vedere al funcţionării corecte a infrastructurilor critice;

c) asigurarea rezilienţei infrastructurilor cibernetice;

d) asigurarea stării de securitate prin cunoaşterea, prevenirea şi contracararea vulnerabilităţilor, riscurilor şi ameninţărilor la adresa securităţii cibernetice a României;

e) valorificarea oportunităţilor spaţiului cibernetic pentru promovarea intereselor, valorilor şi obiectivelor naţionale în spaţiul cibernetic;

f) promovarea şi dezvoltarea cooperării între sectorul public şi cel privat în plan naţional, precum şi a cooperării internaţionale în domeniul securităţii cibernetice;

g) dezvoltarea culturii de securitate a populaţiei prin conştientizarea faţă de vulnerabilităţile, riscurile şi ameninţările provenite din spaţiul cibernetic şi necesitatea asigurării protecţiei sistemelor informatice proprii;

h) participarea activă la iniţiativele organizaţiilor internaţionale din care România face parte în domeniul definirii şi stabilirii unui set de măsuri destinate creşterii încrederii la nivel internaţional privind utilizarea spaţiului cibernetic.

3. Concepte, definiţii şi termeni

În înţelesul prezentei strategii, termenii şi expresiile de mai jos au următoarea semnificaţie:

infrastructuri cibernetice - infrastructuri de tehnologia informaţiei şi comunicaţii, constând în sisteme informatice, aplicaţii aferente, reţele şi servicii de comunicaţii electronice;

spaţiul cibernetic - mediul virtual, generat de infrastructurile cibernetice, incluzând conţinutul informaţional procesat, stocat sau transmis, precum şi acţiunile derulate de utilizatori în acesta;

securitate cibernetică - starea de normalitate rezultată în urma aplicării unui ansamblu de măsuri proactive şi reactive prin care se asigură confidenţialitatea, integritatea, disponibilitatea, autenticitatea şi nonrepudierea informaţiilor în format electronic, a resurselor şi serviciilor publice sau private, din spaţiul cibernetic. Măsurile proactive şi reactive pot include politici, concepte, standarde şi ghiduri de securitate, managementul riscului, activităţi de instruire şi conştientizare, implementarea de soluţii tehnice de protejare a infrastructurilor cibernetice, managementul identităţii, managementul consecinţelor;

apărare cibernetică - acţiuni desfăşurate în spaţiul cibernetic în scopul protejării, monitorizării, analizării, detectării, contracarării agresiunilor şi asigurării răspunsului oportun împotriva ameninţărilor asupra infrastructurilor cibernetice specifice apărării naţionale;

operaţii în reţele de calculatoare - procesul complex de planificare, coordonare, sincronizare, armonizare şi desfăşurare a acţiunilor în spaţiul cibernetic pentru protecţia, controlul şi utilizarea reţelelor de calculatore în scopul obţinerii superiorităţii informaţionale, concomitent cu neutralizarea capabilităţilor adversarului;

ameninţare cibernetică - circumstanţă sau eveniment care constituie un pericol potenţial la adresa securităţii cibernetice;

atac cibernetic - acţiune ostilă desfăşurată în spaţiul cibernetic de natură să afecteze securitatea cibernetică;

incident cibernetic - eveniment survenit în spaţiul cibernetic ale cărui consecinţe afectează securitatea cibernetică;

terorism cibernetic - activităţile premeditate desfăşurate în spaţiul cibernetic de către persoane, grupări sau organizaţii motivate politic, ideologic ori religios ce pot determina distrugeri materiale sau victime, de natură să determine panică ori teroare;

spionaj cibernetic - acţiuni desfăşurate în spaţiul cibernetic, cu scopul de a obţine neautorizat informaţii confidenţiale în interesul unei entităţi statale sau nonstatale;

criminalitatea informatică - totalitatea faptelor prevăzute de legea penală sau de alte legi speciale care prezintă pericol social şi sunt săvârşite cu vinovăţie, prin intermediul ori asupra infrastructurilor cibernetice;

vulnerabilitatea în spaţiul cibernetic - slăbiciune în proiectarea şi implementarea infrastructurilor cibernetice sau a măsurilor de securitate aferente care poate fi exploatată de către o ameninţare;

riscul de securitate în spaţiul cibernetic - probabilitatea ca o ameninţare să se materializeze, exploatând o anumită vulnerabilitate specifică infrastructurilor cibernetice;

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

managementul identităţii - metode de validare a identităţii persoanelor când acestea accesează anumite infrastructuri cibernetice;

rezilienţa infrastructurilor cibernetice - capacitatea componentelor infrastructurilor cibernetice de a rezista unui incident sau atac cibernetic şi de a reveni la starea de normalitate;

entităţi de tip CERT - structuri specializate în înţelesul art. 2 lit. a) din Hotărârea Guvernului nr. 494/2011 privind înfiinţarea Centrului Naţional de Răspuns la Incidente de Securitate Cibernetică - CERT-RO.

4. Principii

Asigurarea securităţii cibernetice trebuie să constituie rezultatul unor abordări bazate pe evaluarea riscurilor, prioritizarea resurselor, implementarea şi monitorizarea eficienţei măsurilor de securitate identificate prin aplicarea managementului de risc şi respectarea următoarelor principii:

- coordonarea - activităţile se realizează într-o concepţie unitară, pe baza unor planuri de acţiune convergente destinate asigurării securităţii cibernetice, în conformitate cu atribuţiile şi responsabilităţile fiecărei entităţi;

- cooperarea - toate entităţile implicate (din mediul public sau privat) colaborează, la nivel naţional şi internaţional, pentru asigurarea unui răspuns adecvat la ameninţările din spaţiul cibernetic;

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

- prioritizarea - eforturile se vor concentra asupra securizării infrastructurilor cibernetice ce susţin infrastructurile critice naţionale şi europene;

- diseminarea - asigurarea transferului de informaţii, expertiză şi bune practici în scopul protejării infrastructurilor cibernetice;

- protejarea valorilor - politicile de securitate cibernetică vor asigura echilibrul între nevoia de creştere a securităţii în spaţiul cibernetic şi prezervarea dreptului la intimitate şi alte valori şi libertăţi fundamentale ale cetăţeanului;

- asumarea responsabilităţii - toţi deţinătorii şi utilizatorii de infrastructuri cibernetice trebuie să întreprindă măsurile necesare pentru securizarea infrastructurilor proprii şi să nu afecteze securitatea infrastructurilor celorlalţi deţinători sau utilizatori;

- separarea reţelelor - reducerea probabilităţii de manifestare a atacurilor cibernetice, specifice reţelei internet, asupra infrastructurilor cibernetice care asigură funcţiile vitale ale statului, prin utilizarea unor reţele dedicate, separate de internet.

II. Provocări şi oportunităţi

1. Ameninţări, vulnerabilităţi şi riscuri

Ameninţările specifice spaţiului cibernetic se caracterizează prin asimetrie şi dinamică accentuată şi caracter global, ceea ce le face dificil de identificat şi de contracarat prin măsuri proporţionale cu impactul materializării riscurilor.

România se confruntă, în prezent, cu ameninţări provenite din spaţiul cibernetic, la adresa infrastructurilor critice, având în vedere interdependenţa din ce în ce mai ridicată între infrastructuri cibernetice şi infrastructuri precum cele din sectoarele financiar-bancar, transport, energie şi apărare naţională. Globalitatea spaţiului cibernetic este de natură să amplifice riscurile la adresa acestora, afectând deopotrivă cetăţenii, mediul de afaceri şi cel guvernamental.

În general, infrastructurile cibernetice pot fi afectate de ameninţări de natură tehnică (de exemplu deficienţe sau defecţiuni tehnice), umană (de exemplu erori de operare, acţiuni voluntare) ori naturale (de exemplu fenomene meteo extreme, catastrofe naturale).

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

Ameninţările din spaţiul cibernetic se materializează - prin exploatarea vulnerabilităţilor de natură umană, tehnică şi procedurală - cel mai adesea în:

- atacurile cibernetice împotriva infrastructurilor care susţin funcţii de utilitate publică ori servicii ale societăţii informaţionale a căror întrerupere/afectare ar putea constitui un pericol la adresa securităţii naţionale;

- accesarea neautorizată a infrastructurilor cibernetice;

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

- spionajul cibernetic;

- cauzarea unui prejudiciu patrimonial, hărţuirea şi şantajul persoanelor fizice şi juridice, de drept public şi privat.

Principalii actori care generează ameninţări în spaţiul cibernetic sunt:

- persoane sau grupări de criminalitate organizată care exploatează vulnerabilităţile spaţiului cibernetic în scopul obţinerii de avantaje patrimoniale sau nepatrimoniale;

- terorişti sau extremişti care utilizează spaţiul cibernetic pentru desfăşurarea şi coordonarea unor atacuri teroriste, activităţi de comunicare, propagandă, recrutare şi instruire, colectare de fonduri etc., în scopuri teroriste;

- state sau actori nonstatali care iniţiază sau derulează operaţiuni în spaţiul cibernetic, în scopul culegerii de informaţii din domeniile guvernamental, militar, economic ori al materializării altor ameninţări la adresa securităţii naţionale.

2. Oportunităţi

În acelaşi timp, spaţiul cibernetic, devenit un nou domeniu de interacţiune în cadrul societăţii moderne, oferă o serie de oportunităţi generate de însăşi specificitatea acestuia. Astfel, au fost identificate următoarele oportunităţi pe care România le poate exploata prin intermediul spaţiului cibernetic:

- susţinerea politicilor şi promovarea intereselor naţionale;

- dezvoltarea şi susţinerea mediului de afaceri;

- creşterea calităţii vieţii prin dezvoltarea serviciilor oferite de societatea informaţională;

- îmbunătăţirea cunoaşterii şi susţinerea deciziilor strategice naţionale în era informaţională prin asigurarea capacităţilor şi instrumentelor cibernetice adecvate;

- creşterea nivelului de cunoaştere şi a capacităţii de predicţie în scopul avertizării timpurii privind riscurile şi ameninţările la adresa securităţii naţionale;

- creşterea capacităţilor tehnice şi a competenţelor resursei umane pentru realizarea obiectivelor de securitate naţională.

III. Direcţii de acţiune

România îşi propune asigurarea stării de normalitate în spaţiul cibernetic reducând riscurile şi valorificând oportunităţile, prin îmbunătăţirea cunoştinţelor, a capabilităţilor şi a mecanismelor de decizie. În acest sens, eforturile se vor focaliza pe următoarele direcţii de acţiune:

1. Stabilirea cadrului conceptual, organizatoric şi acţional necesar asigurării securităţii cibernetice

- constituirea şi operaţionalizarea unui sistem naţional de securitate cibernetică;

- completarea şi armonizarea cadrului legislativ naţional în domeniu, inclusiv stabilirea şi aplicarea unor cerinţe minimale de securitate pentru infrastructurile cibernetice naţionale;

- dezvoltarea cooperării între sectorul public şi cel privat, inclusiv prin stimularea schimbului reciproc de informaţii, privind ameninţări, vulnerabilităţi, riscuri, precum şi cele referitoare la incidente şi atacuri cibernetice.

2. Dezvoltarea capacităţilor naţionale de management al riscului în domeniul securităţii cibernetice şi de reacţie la incidente cibernetice în baza unui program naţional, vizând:

- consolidarea, la nivelul autorităţilor competente potrivit legii, a potenţialului de cunoaştere, prevenire şi contracarare a ameninţărilor şi minimizarea riscurilor asociate utilizării spaţiului cibernetic;

- asigurarea unor instrumente de dezvoltare a cooperării dintre sectorul public şi cel privat, în domeniul securităţii cibernetice, inclusiv pentru crearea unui mecanism eficient de avertizare şi alertă, respectiv de reacţie la incidentele cibernetice;

- stimularea capabilităţilor naţionale de cercetaredezvoltare şi inovare în domeniul securităţii cibernetice;

- creşterea nivelului de rezilienţă a infrastructurilor cibernetice;

- dezvoltarea entităţilor de tip CERT, atât în cadrul sectorului public, cât şi în sectorul privat.

3. Promovarea şi consolidarea culturii de securitate în domeniul cibernetic

- derularea unor programe de conştientizare a populaţiei, a administraţiei publice şi a sectorului privat, cu privire la ameninţările, vulnerabilităţile şi riscurile specifice utilizării spaţiului cibernetic;

- dezvoltarea de programe educaţionale, în cadrul formelor obligatorii de învăţământ, privind utilizarea sigură a internetului şi a echipamentelor de calcul;

- formarea profesională adecvată a persoanelor care îşi desfăşoară activitatea în domeniul securităţii cibernetice şi promovarea pe scară largă a certificărilor profesionale în domeniu;

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

4. Dezvoltarea cooperării internaţionale în domeniul securităţii cibernetice

- încheierea unor acorduri de cooperare la nivel internaţional pentru îmbunătăţirea capacităţii de răspuns în cazul unor atacuri cibernetice majore;

- participarea la programe internaţionale care vizează domeniul securităţii cibernetice;

- promovarea intereselor naţionale de securitate cibernetică în formatele de cooperare internaţională la care România este parte.

IV. Sistemul naţional de securitate cibernetică

Sistemul naţional de securitate cibernetică (SNSC) reprezintă cadrul general de cooperare care reuneşte autorităţi şi instituţii publice, cu responsabilităţi şi capabilităţi în domeniu, în vederea coordonării acţiunilor la nivel naţional pentru asigurarea securităţii spaţiului cibernetic, inclusiv prin cooperarea cu mediul academic şi cel de afaceri, asociaţiile profesionale şi organizaţiile neguvernamentale.

Misiunea SNSC constă în asigurarea elementelor de cunoaştere, prevenire şi contracarare a ameninţărilor, vulnerabilităţilor şi riscurilor specifice spaţiului cibernetic care pot afecta securitatea infrastructurilor cibernetice naţionale, inclusiv managementul consecinţelor.

Pentru îndeplinirea obiectivelor prezentei strategii, SNSC funcţionează ca un mecanism unitar şi eficient de relaţionare şi cooperare interinstituţională, în vederea adoptării şi aplicării cu celeritate a deciziilor.

SNSC acţionează pe următoarele componente:

Componenta de cunoaştere - furnizează suportul informaţional necesar elaborării măsurilor proactive şi reactive în vederea asigurării securităţii cibernetice.

Componenta de prevenire - este principalul mijloc de asigurare a securităţii cibernetice prin crearea şi dezvoltarea capabilităţilor necesare analizei şi prognozei evoluţiei stării acesteia.

Componenta de cooperare şi coordonare - asigură mecanismul unitar şi eficient de relaţionare în cadrul SNSC.

Componenta de contracarare - asigură reacţia eficientă la ameninţările sau atacurile cibernetice, prin identificarea şi blocarea manifestării acestora. Aceasta se realizează în scopul menţinerii sau restabilirii securităţii infrastructurilor cibernetice vizate, precum şi pentru identificarea şi sancţionarea autorilor, potrivit legii.

Funcţiile principale ale SNSC se realizează prin informare, monitorizare, diseminare, analizare, avertizare, coordonare, decizie, reacţie, refacere şi conştientizare, precum şi prin adoptarea de măsuri proactive şi reactive.

Măsurile proactive vizează:

- actualizarea şi armonizarea cadrului naţional de reglementare în domeniul securităţii cibernetice în concordanţă cu evoluţiile mediului de referinţă;

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

- colectarea de date şi informaţii referitoare la ameninţări, vulnerabilităţi şi riscuri identificate în spaţiul cibernetic;

- analiza, anticiparea şi prognoza evoluţiei stării de securitate cibernetică;

- realizarea şi eficientizarea cooperării între sectorul public şi cel privat între deţinătorii infrastructurilor cibernetice şi autorităţile statului abilitate să întreprindă măsuri de prevenire şi contracarare a ameninţărilor, precum şi de minimizare a efectelor unui atac cibernetic;

- ridicarea nivelului de instruire şi conştientizare a populaţiei asupra riscurilor derivate din utilizarea spaţiului cibernetic;

- interoperabilitatea cu alte sisteme naţionale şi internaţionale cu atribuţii în domeniul securităţii;

- protejarea infrastructurilor cibernetice naţionale şi a celor aparţinând NATO sau UE aflate în administrarea unor instituţii ori autorităţi publice;

- implementarea unui mecanism de management al riscului;

- asigurarea unui grad ridicat de autoadaptabilitate, în funcţie de evoluţiile spaţiului cibernetic;

- asigurarea confidenţialităţii, integrităţii, disponibilităţii, autenticităţii şi nonrepudierii informaţiilor din spaţiul cibernetic;

- asigurarea managementului identităţii în spaţiul cibernetic;

- operaţionalizarea capabilităţilor destinate managementului incidentelor de securitate cibernetică, inclusiv managementul consecinţelor;

- dezvoltarea mecanismelor pentru creşterea nivelului de cultură de securitate.

Măsurile reactive urmăresc:

- aplicarea planurilor de contingenţă în vederea minimizării efectelor unui atac cibernetic;

- aplicarea măsurilor cu privire la asigurarea continuităţii fluxurilor informaţionale şi decizionale;

- aplicarea unui plan de măsuri cu privire la asigurarea funcţionalităţii sistemelor în condiţii de securitate a serviciilor publice sau private;

- recuperarea şi restaurarea datelor;

- identificarea şi implementarea lecţiilor învăţate, rezultate în urma aplicării procedurilor de management al incidentelor, management al consecinţelor unui atac cibernetic, precum şi de continuitate a activităţilor.

Eficienţa activităţilor desfăşurate în SNSC depinde în mod esenţial de cooperarea, inclusiv între sectorul public şi cel privat, între deţinătorii infrastructurilor cibernetice şi autorităţile statului abilitate să întreprindă măsuri de prevenire şi contracarare a ameninţărilor, de investigare a atacurilor cibernetice, precum şi de minimizare a efectelor acestora.

Consiliul Suprem de Apărare a Ţării este autoritatea ce coordonează, la nivel strategic, activitatea SNSC. Consiliul Suprem de Apărare a Ţării avizează Strategia de securitate cibernetică a României şi aprobă Regulamentul de organizare şi funcţionare 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 permanenţi, reprezentanţi ai Ministerului Apărării Naţionale, Ministerului Afacerilor Interne, Ministerului Afacerilor Externe, Ministerului pentru Societatea Informaţională, Serviciului Român de Informaţii, Serviciului de Telecomunicaţii Speciale, Serviciului de Informaţii Externe, Serviciului

de Protecţie şi Pază, Oficiului Registrului Naţional pentru Informaţii Secrete de Stat, precum şi secretarul Consiliului Suprem de Apărare a Ţării. Conducerea COSC este asigurată de un preşedinte (consilierul prezidenţial pe probleme de securitate naţională) şi un vicepreşedinte (consilierul prim-ministrului pe probleme de securitate naţională). Coordonatorul tehnic al COSC este Serviciul Român de Informaţii, în condiţiile legii.

Guvernul României, prin Ministerul pentru Societatea Informaţională, asigură coordonarea celorlalte autorităţi publice care nu sunt reprezentate în COSC, în vederea realizării coerenţei politicilor şi implementarea strategiilor guvernamentale în domeniul comunicaţiilor electronice, tehnologiei informaţiei şi al serviciilor societăţii informaţionale şi societăţii bazate pe cunoaştere, iar prin Centrul Naţional de Răspuns la Incidente de Securitate Cibernetică - CERT-RO - asigură elaborarea şi diseminarea politicilor publice de prevenire şi contracarare a incidentelor din cadrul infrastructurilor cibernetice, potrivit ariei de competenţă.

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

Fiecare dintre instituţiile reprezentate în COSC cooperează cu organismele internaţionale ale UE, NATO, OSCE etc., fiecare pe domeniul său de competenţă.

V. Cooperarea între sectorul public şi cel privat

Dezvoltarea cooperării dintre mediul public şi cel privat, în scopul asigurării securităţii cibernetice, reprezintă o direcţie prioritară de acţiune la nivelul organismelor internaţionale sau alianţelor la care România este parte, având în vedere că spaţiul cibernetic reuneşte deopotrivă infrastructuri cibernetice deţinute şi administrate de stat, precum şi de entităţi private.

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

- cooperarea bazată pe încredere între stat şi mediul de afaceri, la toate nivelurile;

- creşterea nivelului de protecţie al infrastructurilor cibernetice prin corelarea măsurilor întreprinse cu resursele disponibile în sectorul public şi privat.

Responsabilitatea asigurării securităţii cibernetice revine tuturor actorilor implicaţi, ţinând cont de interesele complementare în acest domeniu pentru asigurarea legalităţii operaţiunilor desfăşurate, combaterea fenomenului criminalităţii informatice şi protecţia infrastructurilor critice interconectate cu spaţiul cibernetic şi se bazează pe sporirea încrederii reciproce.

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

- schimbul de informaţii privind ameninţări, vulnerabilităţi şi riscuri specifice;

- dezvoltarea capabilităţilor de avertizare timpurie şi de răspuns la incidente şi atacuri cibernetice;

- desfăşurarea de exerciţii comune privind securitatea spaţiului cibernetic;

- dezvoltarea de programe educaţionale şi de cercetare în domeniu;

- dezvoltarea culturii de securitate;

- reacţia comună în cazul unor atacuri cibernetice majore.

Realizarea obiectivelor menţionate presupune conlucrarea dintre sectorul public şi sectorul privat, inclusiv prin măsuri de prevenţie, conştientizare şi promovare a oportunităţilor în domeniul cibernetic.

VI. Concluzii

Asigurarea securităţii cibernetice se bazează pe cooperarea la nivel naţional şi internaţional pentru protejarea spaţiului cibernetic, prin coordonarea demersurilor naţionale cu orientările şi măsurile adoptate la nivel internaţional, în formatele de cooperare la care România este parte.

Având în vedere dinamismul evoluţiilor globale în spaţiul cibernetic, precum şi obiectivele României în procesul de dezvoltare a societăţii informaţionale şi implementare pe scară largă a serviciilor electronice este necesară elaborarea unui program naţional detaliat, care - pe baza reperelor oferite de prezenta strategie - să asigure elaborarea şi punerea în practică a unor proiecte concrete de securitate cibernetică.

Măsurile destinate operaţionalizării SNSC trebuie armonizate cu eforturile pe dimensiunea protecţiei infrastructurilor critice, respectiv cu evoluţia procesului de dezvoltare a capabilităţilor de tip CERT. În varianta optimă, SNSC trebuie să dispună de o structură flexibilă şi adaptivă care să înglobeze capabilităţi de identificare şi anticipare, resurse şi proceduri operaţionale de prevenire, reacţie şi contracarare, precum şi instrumente pentru documentare şi sancţionare a autorilor atacurilor cibernetice.

Este necesară implementarea, la nivel naţional, a unor standarde minimale procedurale şi de securitate pentru infrastructurile cibernetice, care să fundamenteze eficienţa demersurilor de protejare faţă de atacuri cibernetice şi să limiteze riscurile producerii unor incidente cu potenţial impact semnificativ.

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

de informaţii şi transferului de expertiză între autorităţile cu responsabilităţi în domeniu, dezvoltarea cooperării între sectorul public şi cel privat şi extinderea cooperării cu mediile neguvernamentale şi comunitatea academică.

SNSC va constitui platforma de cooperare şi armonizare a capabilităţilor de tip CERT existente la nivel naţional, valorificând instrumentele oferite de acestea, şi va acţiona pentru consolidarea expertizei în domeniul riscurilor cibernetice, prin stimularea sinergiilor între diferitele planuri de acţiune în domeniul securităţii cibernetice (militar-civil, public-privat, guvernamental-neguvernamental).

Dat fiind ritmul rapid de evoluţie a problematicii, prezenta strategie va fi testată şi revizuită permanent, inclusiv în contextul mai larg al Strategiei de apărare, în vederea adaptării continue la provocările şi oportunităţile 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 naţional destinat managementului riscului în domeniul securităţii cibernetice.