

HOTĂRÂRE nr. 718 din 13 iulie 2011

pentru aprobarea Strategiei naționale privind protecția infrastructurilor critice

EMITENT: GUVERNUL

PUBLICAT ÎN: MONITORUL OFICIAL nr. 555 din 4 august 2011

Data Intrării în vigoare: 04 August 2011

În temeiul art. 108 din Constituția României, republicată, și al art. 1 alin. (5) lit. a) 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 națională privind protecția infrastructurilor critice, prevăzută în anexa care face parte integrantă din prezenta hotărâre.

ART. 2

(1) În termen de 60 de zile de la data intrării în vigoare a prezentei hotărâri, Centrul de coordonare a protecției infrastructurilor critice constituit la nivelul Ministerului Administrației și Internelor potrivit art. 4 alin. (2) din Ordonanța de urgență a Guvernului nr. 98/2010 privind identificarea, desemnarea și protecția infrastructurilor critice, aprobată cu modificări prin Legea nr. 18/2011, va elabora planul de acțiune pentru implementarea, monitorizarea și evaluarea obiectivelor strategiei prevăzute la art. 1.

(2) După însușirea în cadrul Grupului de lucru interinstituțional pentru protecția infrastructurilor critice, constituit potrivit art. 5 din Ordonanța de urgență a Guvernului nr. 98/2010, aprobată cu modificări prin Legea nr. 18/2011, planul de acțiune prevăzut la alin. (1) se aprobă prin decizie a primului-ministru și se revizuieste anual sau ori de câte ori este necesar.

PRIM-MINISTRU
EMIL BOC

Contrasemnează:

Ministrul administrației și internelor,
Constantin-Traian Igaș

Ministrul transporturilor și infrastructurii,
Anca Daniela Boagiu

Ministrul economiei, comerțului
și mediului de afaceri,
Ion Ariton

Ministrul comunicațiilor
și societății informaționale,
Valerian Vreme

Ministrul mediului și pădurilor,
Laszlo Borbely

Ministrul apărării naționale,
Gabriel Oprea

Ministrul agriculturii și dezvoltării rurale,
Valeriu Tabără

Ministrul sănătății,
Cseke Attila

Ministrul educației, cercetării,
tineretului și sportului,
Daniel Petru Funeriu

Ministrul dezvoltării regionale
și turismului,
Elena Gabriela Udrea

Președintele Autorității Naționale
Sanitare Veterinare și pentru
Siguranța Alimentelor,
Radu Roatiș Chețan

Președintele Agenției Spațiale Române,
Marius-Ioan Piso

Directorul Serviciului Român de Informații,
George Cristian Maior

Directorul Serviciului de Informații Externe,
Mihai-Răzvan Ungureanu

Directorul Serviciului
de Telecomunicații Speciale,
Marcel Opriș

București, 13 iulie 2011.
Nr. 718.

ANEXĂ

STRATEGIA NAȚIONALĂ privind protecția infrastructurilor critice

1. Argument
2. Contextul general internațional
3. Situația actuală și cadrul normativ existent în România
4. Vulnerabilități, factori de risc și amenințări în domeniul protecției infrastructurilor critice
5. Scop și obiective strategice
6. Principiile realizării protecției infrastructurilor critice
7. Direcții de acțiune, modalități de realizare și rezultate așteptate pe termen scurt și mediu
8. Implicații financiare
9. Mecanisme de implementare, monitorizare și evaluare

1. Argument

Dezvoltarea economico-socială stimulată de progresul tehnologic accelerat și manifestarea fenomenului globalizării au consolidat interdependența puternică și interacțiunea sistemelor ce asigură securitatea și bunăstarea societății umane. Necesitatea interconexării sistemelor pe fondul tendinței de eliminare a barierelor administrative și de acces pe noile piețe emergente, concomitent cu integrarea rețelelor de infrastructuri, determină evoluții în planul securității și stabilității în plan global.

Prin adoptarea Ordonanței de urgență a Guvernului nr. 98/2010 privind identificarea, desemnarea și protecția infrastructurilor critice, aprobată cu modificări prin Legea nr. 18/2011, și a Hotărârii Guvernului nr. 1.110/2010 privind componența, atribuțiile și modul de organizare ale Grupului de lucru interinstituțional pentru protecția infrastructurilor critice s-a creat cadrul legal național pentru asigurarea protecției infrastructurilor critice, dar absența unui cadru strategic de dezvoltare a mecanismelor necesare protecției infrastructurilor critice poate genera paralelisme, ineficiență sau chiar situații conflictuale cu implicații asupra intereselor naționale și obiectivelor fixate în cadrul Directivei 2008/114/CE a Consiliului din 8 decembrie 2008 privind identificarea și desemnarea infrastructurilor critice europene și evaluarea necesității de îmbunătățire a protecției acestora.

În acest context se impune elaborarea Strategiei naționale privind protecția infrastructurilor critice - document-cadru destinat adoptării și implementării unor măsuri și acțiuni specifice în scopul reducerii efectelor negative induse de manifestarea factorilor de risc specifici asupra infrastructurilor critice, la nivel național și regional.

Strategia națională privind protecția infrastructurilor critice prezentată a fost elaborată în concordanță cu prevederile Strategiei naționale de apărare a României, ale Cartei albe a securității și apărării naționale și cu delimitările conceptuale instituționale în domeniu atât de la nivel național, cât și internațional, stabilind astfel politicile și direcțiile de acțiune din domeniu, necesare dezvoltării și completării cadrului normativ național.

2. Contextul general internațional

Evoluțiile rapide și, uneori, cu un grad ridicat de imprevizibilitate, dublate de dimensiunea și complexitatea vulnerabilităților și riscurilor, generează o provocare majoră pentru sistemele de protecție a infrastructurilor critice.

Interconexiunile transnaționale ale infrastructurilor și sfera de manifestare a riscurilor, ce au împrumutat elementele de reprezentare și evoluție configurate de procesul de globalizare,

prefigurează premise de perpetuare, prin "rezonanță", a riscurilor la adresa infrastructurilor critice și permit extinderea "în sistem cascadă", pe spațiul altor state, a efectelor agresiunii asupra unor sisteme sau procese.

Fenomenul globalizării, odată cu avantajele și transformările pozitive ce le aduce la nivel internațional, dă posibilitatea propagării rapide, la scară planetară, a amenințărilor directe la adresa securității tuturor. La tendințele de globalizare a insecurității trebuie să se răspundă prin măsuri ferme de blocare și eliminare a amenințărilor prezente și pericolelor viitoare, precum și instituirea unui sistem de globalizare a securității.

Riscurile și amenințările la adresa obiectivelor vitale pentru funcționarea societății și securitatea cetățenilor au căpătat noi valențe, cu dinamică ridicată și grad de intensitate crescut, fapt ce a condus la necesitatea unei abordări integrate a conceptului de "infrastructură critică". Pornind de la caracteristicile de bază ale infrastructurilor critice, elementul de criticitate al stabilității acestora, inclusiv în context transfrontalier, a căpătat noi conotații în planul strategiilor naționale/transnaționale.

Complexitatea protecției infrastructurilor critice și importanța acestora pentru stabilitatea socială, respectiv securitatea cetățeanului și a statului, a generat corelarea concretă a strategiilor inițiate la nivelul statelor și organizațiilor.

Conexiunile dintre funcționalitatea și viabilitatea infrastructurilor critice și elementele fundamentale ale vieții economico-sociale, politice și militare ale unui stat, alianțe etc. consolidează semnificativ liantul dintre elementul de securitate și rolul sistemelor de infrastructuri în exprimarea necesităților și promovarea intereselor naționale, indiferent de configurația contextuală.

În ultimii ani, producerea actelor teroriste, întreruperea deliberată a furnizării de materii energetice la nivelul unor state, producerea unor accidente tehnologice ca urmare a unor greșeli umane sau a unor dezastre/calamități naturale au scos în evidență vulnerabilitatea unor infrastructuri critice naționale, iar statele membre ale Uniunii Europene au întreprins acțiuni ferme în direcția stabilirii unui mod de acțiune comun în vederea protejării obiectivelor lor de valoare strategică.

În luna iunie a anului 2004, Consiliul Uniunii Europene a solicitat pregătirea unei strategii globale pentru protecția infrastructurilor critice, iar în 20 octombrie 2004, Comisia Europeană a adoptat Comunicarea privind protecția infrastructurilor critice în cadrul luptei împotriva terorismului, care prezintă propuneri privind modalitățile de îmbunătățire, la nivel european, a acțiunilor destinate prevenirii atacurilor teroriste asupra infrastructurilor critice, a pregătirii împotriva atacurilor respective și a reacției la acestea.

La 17 noiembrie 2005, Comisia Europeană a adoptat Carta verde privind programul european de protecție a infrastructurilor critice, care a expus o serie de opțiuni privind instituirea programului și a Rețelei de alertă privind infrastructurile critice. Reacțiile la acest document au evidențiat valoarea adăugată a unui cadru comunitar în materie de protecție a infrastructurilor critice. A fost recunoscută necesitatea de a spori capacitatea de protecție a infrastructurilor critice în Europa și de a ajuta la reducerea punctelor vulnerabile ale acestor infrastructuri și evidențiată importanța principiilor fundamentale de subsidiaritate, proporționalitate și complementaritate, precum și a dialogului cu părțile interesate.

În aprilie 2007, Consiliul Uniunii Europene a adoptat concluziile cu privire la Programul european privind protecția infrastructurilor critice, în care a reiterat faptul că statelor membre le revine responsabilitatea finală de a gestiona măsurile de protecție a infrastructurilor critice din interiorul frontierelor naționale.

În acest context, a fost adoptată Directiva 2008/114/CE, act normativ care a constituit un prim pas în cadrul unei abordări pas cu pas în direcția identificării și a desemnării infrastructurilor critice europene și a evaluării necesității de îmbunătățire a protecției acestora. Această directivă s-a concentrat asupra sectorului energetic și a sectorului transporturilor, dar urmează a fi reexaminată în vederea evaluării impactului acesteia și a necesității de a include alte sectoare în domeniul său de aplicare, cum ar fi sectorul tehnologiei informației și comunicațiilor ("TIC").

Comunitatea europeană acceptă faptul că sfera protecției infrastructurilor critice, în contextul globalizării, nu mai ține cont de granițele naționale și implică eforturi comune în sensul identificării și evaluării oricăror puncte vulnerabile ale acestora, ce pot constitui "ținte" ori noduri importante de reflexie a amenințărilor la adresa securității micro și macroregionale.

Climatul de stabilitate și securitate este condiționat de buna funcționare a rețelelor de infrastructuri critice, necesitatea protecției acestora fiind un element esențial pentru evitarea perturbării grave a societății.

3. Situația actuală și cadrul normativ existent în România

Evoluția amenințărilor la nivel global, corelată cu statutul politico-militar și economic actual al României în cadrul Alianței Nord-Atlantice și Uniunii Europene, a determinat translatarea potențialilor factori de risc și asupra infrastructurilor naționale asimilabile celor critice, mai ales, în contextul rolului jucat de țara noastră în asigurarea climatului de stabilitate și securitate regională, cu accent în zona bazinului Mării Negre.

Astfel, perspectiva manifestării unor potențiale amenințări a determinat abordări strategice, instituționale și funcționale într-un sistem integrat al problematicii protecției infrastructurilor critice naționale.

Având în vedere dependența mare față de serviciile oferite de infrastructurile critice, societatea a devenit foarte vulnerabilă. Această vulnerabilitate a crescut nu doar ca urmare a riscurilor și amenințărilor externe, ci și din cauza interdependențelor dintre diferitele infrastructuri din interiorul sistemelor relevante, context în care perturbările/întreruperile pot determina pagube imense pentru economia națională.

În materia protecției infrastructurilor critice, efortul statului și al societății trebuie direcționat, în principal, pe două mari categorii de amenințări: cea teroristă și cea generată de dezastre/calamități naturale, ce au un impact tot mai mare asupra infrastructurii considerate critică.

Primele etape în vederea configurării unui cadru legal normativ coerent destinat reglementării protecției infrastructurii critice în România au fost parcurse odată cu adoptarea Ordonanței de urgență a Guvernului nr. 98/2010, aprobată cu modificări prin Legea nr. 18/2011, și a Hotărârii Guvernului nr. 1.110/2010. În baza acestora a fost creat Grupul de lucru interinstituțional pentru protecția infrastructurilor critice, organism ce asigură cadrul de cooperare interinstituțională necesar elaborării proiectelor naționale indispensabile dezvoltării unei abordări integrate și fundamentate a protecției infrastructurilor critice.

4. Vulnerabilități, factori de risc și amenințări în domeniul protecției infrastructurilor critice

Mediul de securitate actual este caracterizat de mutații semnificative atât în privința relevanței actorilor regionali și globali și a caracteristicilor mediului de derulare a înfruntărilor, cât și a obiectivelor de gestionare optimă a problematicii. Astfel, motivațiile tradiționale, cum ar fi câștigarea de teritorii sau de resurse vitale, își schimbă sensul și sunt completate cu altele noi, cum ar fi cucerirea de piețe de desfacere sau protecția mediului. În acest context, au avut loc mutații și în strategiile de promovare a intereselor, care fixează ca obiective neutralizarea unor elemente ale infrastructurii critice ale competitorilor în locul disipării efortului pentru

neutralizarea în ansamblu a competitorului.

Pornind de la accepțiunile date - în Doctrina națională a informațiilor pentru securitate - conceptelor de "vulnerabilități", "factori de risc", "amenințări", "stări de pericol" și "agresiuni", acestea pot fi definite, din perspectiva infrastructurilor critice, astfel:

Vulnerabilitățile reprezintă stări de fapt, procese și fenomene ce diminuează capacitatea de reacție a infrastructurilor critice la riscurile existente ori potențiale sau care favorizează apariția și dezvoltarea lor, cu consecințe în planul funcționalității și utilității.

Necunoașterea sau gestionarea defectuoasă a vulnerabilităților poate genera factori de risc, amenințări ori stări de pericol la adresa obiectivelor, valorilor, intereselor și necesităților naționale subsumate infrastructurilor critice.

Factorii de risc desemnează situații, împrejurări, elemente, condiții sau conjuncturi interne și externe, uneori dublate și de acțiune, ce determină ori favorizează materializarea unei amenințări la adresa infrastructurilor critice, în funcție de o vulnerabilitate determinată, generând efecte de insecuritate.

Amenințările reprezintă capacități, strategii, intenții, planuri ce potențiază un pericol la adresa infrastructurilor critice, materializate prin atitudini, gesturi, acte, fapte ce creează stări de dezechilibru ori instabilitate și generează stări de pericol, cu impact asupra securității naționale.

Stările de pericol sunt situații, întâmplări care pot pune în primejdie sau pot amenința existența ori integritatea infrastructurilor critice.

Agresiunile sunt atacuri, inclusiv armate, care pun în primejdie existența, echilibrul sau integritatea infrastructurilor critice.

Infrastructura critică poate fi expusă diverselor tipuri de riscuri și amenințări, în funcție de modul de manifestare a acestora.

Spectrul general al riscurilor și amenințărilor include evenimente naturale, erori tehnice, tehnologice și umane, acțiuni sau atacuri săvârșite cu intenție, precum și alte forme de manifestare care prin natura ori amploarea lor pot afecta infrastructurile critice.

Aceste evenimente și incidente au diverse cauze și pot provoca pagube semnificative sau pot distruge elementele de infrastructură care sunt vitale societății și populației în general. Datorită nivelului mare de dependență față de serviciile de infrastructură, societatea a devenit foarte vulnerabilă atât din cauza dezastrelor și riscurilor, cât și în contextul unor importante interdependențe între diferite zone ale infrastructurii în cadrul sistemelor relevante.

După 11 septembrie 2001 principala amenințare asupra căreia se concentrează eforturile statelor pentru a-și dobândi și menține protecția și securitatea este reprezentată de terorismul internațional. Odată cu creșterea gradului de dependență a societății față de structurile sale de bază și a gradului de utilizare a tehnologiei moderne de către organizațiile teroriste a crescut și necesitatea asigurării protecției infrastructurii critice împotriva atacurilor teroriste. Nivelul acestei categorii de amenințare în România rămâne redus. În afara riscurilor rezultate în special din terorism, o atenție deosebită trebuie acordată pagubelor semnificative ce pot apărea în urma dezastrelor naturale.

Până în prezent, în România, infrastructura critică, în diferite sectoare, a fost afectată, în mod special, de fenomene meteorologice extreme. Este de așteptat ca, și în viitor, schimbările climaterice să adauge presiuni noi asupra infrastructurii critice chiar și în zonele cu climă temperată cum sunt cele din Europa Centrală.

O altă categorie de riscuri majore rezultă din afectarea echipamentelor din considerente de natură tehnică, pe fondul insuficienței/ineficienței operațiunilor de întreținere, reabilitare și modernizare, cât și în ceea ce privește dimensiunea cibernetică (hardware și software), cu

producerea de sincope în funcționarea sistemelor informatizate ale infrastructurilor critice, ca urmare a unor acte criminale, erori sau disfuncții tehnice/umane, dezastre naturale sau deficiențe manageriale.

În acest context, este necesară intensificarea demersurilor destinate protecției infrastructurilor critice, respectiv:

a) creșterea nivelului de comunicare și cooperare între autoritățile statului și cele din Uniunea Europeană, operatori economici și populație, luând în considerare și sensibilitatea anumitor categorii de informații;

b) optimizarea cooperării între responsabilii în domeniul prevenirii și managementului situațiilor de criză;

c) operaționalizarea parteneriatului public-privat în domeniul protecției infrastructurilor critice;

d) creșterea potențialului de autoprotecție, autogarantare a capacităților individuale sau instituționale afectate de disfuncții ori care pot compromite funcționarea infrastructurilor critice;

e) prioritizarea nivelului de risc acceptat în funcție de raportul cost-beneficiu determinat de probabilitatea de manifestare și impactul acestuia.

În ceea ce privește amenințările și evaluările asupra mediului actual de securitate s-au evidențiat principalele tipuri de astfel de evenimente care se pot manifesta pe teritoriul național:

a) criminalitatea organizată, în special cea transfrontalieră, a cărei escaladare poate fi potențată de creșterea rolului României în susținerea politicilor internaționale de contracarare a acestui fenomen;

b) hazarde naturale produse de fenomenele naturale;

c) defecțiuni tehnice, sincope în funcționarea sistemelor/echipamentelor, în special, ca urmare a vechimii mari în exploatare și insuficienței activităților de mentenanță;

d) erori/acțiuni umane, exploatarea deficitară/intruziunea neautorizată etc.

5. Scop și obiective strategice

Scopul strategiei este să asigure cadrul general pentru domeniul protecției infrastructurilor critice, în vederea promovării intereselor naționale și a realizării obiectivelor asumate în cadrul alianțelor la care România este parte.

Strategia vizează:

a) stabilirea reperelor pentru dezvoltarea continuă a capacităților naționale de protecție a infrastructurilor critice;

b) armonizarea cadrului normativ intern cu cel al Uniunii Europene și al Alianței Nord-Atlantice în domeniu;

c) implicarea tuturor autorităților naționale cu atribuții în domeniu, precum și a partenerilor din mediul privat, în formularea și implementarea ansamblului de măsuri structurale și procedurale care să asigure o acțiune coordonată, la nivel național, pentru identificarea, desemnarea și protecția infrastructurilor critice.

Obiectivele strategice:

1. Asigurarea caracterului unitar al procedurilor de identificare, desemnare și protecție a infrastructurilor critice naționale și europene;

2. Configurarea și operaționalizarea sistemului național de avertizare timpurie prin integrarea tuturor rețelelor și capacităților informațional-organizatorice existente;

3. Evaluarea corectă a nivelului de vulnerabilitate a infrastructurilor critice și identificarea măsurilor necesare pentru intervenția preventivă și diminuarea acestuia;

4. Dezvoltarea relațiilor de cooperare la nivel național, regional și internațional în domeniul

infrastructurilor critice.

6. Principiile realizării protecției infrastructurilor critice

Actuala strategie are la bază următoarele principii:

Principiul legalității - activitățile se desfășoară în baza legii și în conformitate cu aceasta;

Principiul subsidiarității - asigură luarea deciziilor cât mai aproape de cetățean, în paralel cu evaluarea permanentă a necesității unor acțiuni la nivel național, corelate cu posibilitățile existente în plan regional sau local;

Principiul complementarității - stabilirea unui cadru legislativ flexibil care să permită adoptarea de mijloace și metode racordate la specificul situației actuale, cu valorificarea și, după caz, adaptarea/dezvoltarea mecanismelor și măsurilor de asigurare a securității infrastructurii critice deja implementate;

Principiul confidențialității - diseminarea informațiilor referitoare la protecția infrastructurilor critice se va realiza într-un cadru care să asigure protejarea acelor informații specifice a căror divulgare ar putea genera vulnerabilități de securitate la nivelul respectivelor infrastructuri. Informațiile vor fi clasificate, iar accesul la acestea trebuie să se realizeze cu respectarea principiului "necesității de a cunoaște". Gestionarea și accesul la informații clasificate se realizează conform legii, de persoane care dețin certificat de securitate sau autorizație de acces, valabile pentru nivelul de secretizare al acestora;

Principiul proporționalității - măsurile de protecție vor fi proporționale cu nivelul de risc acceptat. Prin aplicarea unor tehnici de management al riscului adecvate, atenția va fi concentrată asupra domeniilor cu potențialul de risc cel mai mare, ținând seama de amenințări, criticitate, probabilitatea de producere a riscului identificat, raportul cost-beneficii, nivelul de securitate și protecție necesar și eficiența strategiilor disponibile. Vulnerabilitățile infrastructurilor critice vor fi clasificate, în funcție de proprietăți și efecte potențiale, în "acceptabile" - care impun măsuri de monitorizare asupra evoluției, respectiv "critice" - ce implică demersuri active de limitare/înlăturare;

Principiul cooperării între deținători - toți deținătorii de infrastructură critică, operatorii sau administratorii acestora, inclusiv asociațiile industriale ori de afaceri și organismele de standardizare, joacă un rol în protecția infrastructurilor critice. Toți deținătorii trebuie să coopereze și să contribuie la dezvoltarea și implementarea măsurilor de protecție a infrastructurilor critice în concordanță cu rolurile și responsabilitățile lor specifice. Autoritățile publice responsabile trebuie să asigure coordonarea procesului de dezvoltare și implementare a politicilor și măsurilor de protecție a infrastructurilor critice în domeniile din aria de competență. Proprietarii, operatorii și administratorii de infrastructuri critice vor fi angrenați atât la nivel național, cât și european;

Principiul securizării funcțiilor vitale - prioritatea în adoptarea și implementarea măsurilor de protecție o vor constitui acele servicii, facilități sau activități care sunt ori ar putea fi necesare pentru a menține funcțiile vitale ale societății, sănătății, siguranței, securității, bunăstării sociale sau economice a persoanelor și a căror perturbare ori distrugere ar avea un impact semnificativ la nivel național.

7. Direcții de acțiune, modalități de realizare și rezultate așteptate pe termen scurt și mediu

Pentru atingerea obiectivelor stabilite, factorii responsabili trebuie să aibă în vedere:

a) evidențierea tuturor riscurilor existente sau previzibile, în paralel cu identificarea elementelor și proceselor critice;

b) eliminarea disfuncțiilor ce pot afecta stabilitatea și funcționarea optimă a serviciilor esențiale având ca suport infrastructuri critice, prin aplicarea de măsuri proactive în cadrul unui

sistem eficient de management al riscurilor;

c) creșterea gradului de expertiză în domeniu și actualizarea permanentă a analizelor de risc, inclusiv prin evaluări comparative cu situații specifice manifestate pe teritoriul altor state, cu transpunerea acestor rezultate în standarde naționale;

d) respectarea normelor de confidențialitate a datelor și informațiilor a căror diseminare neautorizată poate afecta protecția sistemelor de infrastructură critică, conform legislației naționale în vigoare.

Obiectivul strategic nr. 1 - Asigurarea caracterului unitar al procedurilor de identificare, desemnare și protecție a infrastructurilor critice naționale și europene

Direcții de acțiune:

1.1. Stabilirea criteriilor sectoriale și a pragurilor aferente acestora ținând seama de caracteristicile sectoarelor individuale ale infrastructurilor critice

1.2. Determinarea pragurilor din cadrul criteriilor intersectoriale în funcție de gravitatea impactului perturbării sau al distrugerii unei anumite infrastructuri

1.3. Elaborarea unor metodologii comune pentru identificarea și clasificarea riscurilor, amenințărilor și punctelor vulnerabile legate de elementele de infrastructură

1.4. Identificarea și utilizarea de indicatori relevanți și racordați la necesități, cu grad sporit de aplicabilitate, în scopul decelării acelor categorii de infrastructuri care implică măsuri de protecție

1.5. Efectuarea de evaluări pe coordonatele legislativ-instituțional, organizatoric-funcțional și aplicativ, care să asigure un cadru stabil și dinamic, cu potențial de mobilitate ridicat, de identificare și protecție a infrastructurilor critice

1.6. Creșterea gradului și dinamicii de angrenare a responsabililor de pe diverse paliere în parcurgerea etapelor/operațiunilor procesului de implementare corespunzătoare cadrului normativ de identificare și protecție a infrastructurilor critice

1.7. Identificarea eficientă a riscurilor, a amenințărilor și a punctelor vulnerabile în sectoarele specifice pe baza concluziilor analizelor de risc și a fundamentelor racordate la realitățile din teren și a potențialului de sustenabilitate (implicații, efecte, resurse și capacitate de susținere), care să permită conturarea clară a pragurilor și criteriilor de selecție a infrastructurilor în vederea includerii în categoria celor critice

1.8. Crearea cadrului unitar de evaluare a riscurilor, stabilire a necesităților reale de protecție și, respectiv, a măsurilor de intervenție preventivă și/sau reacție ori de limitare a efectelor producerii unor stări de pericol în planul stabilității și securității.

Obiectivul strategic nr. 2 - Configurarea și operaționalizarea sistemului național de avertizare timpurie prin integrarea tuturor rețelelor și capacităților informațional-organizatorice existente

Direcții de acțiune:

2.1. Operaționalizarea punctelor de contact între proprietarii, operatorii și/sau administratorii de infrastructuri critice europene și autoritatea competentă a statului membru prin desemnarea ofițerilor de legătură pentru securitate

2.2. Realizarea unui flux informațional de expertiză/schimburi de bune practici, uniform și eficient, concomitent cu dezvoltarea capacității de adaptare a strategiilor de protecție a infrastructurilor critice, în raport cu evoluțiile formelor de manifestare a factorilor de risc de nivel național și macroregional

2.3. Punerea în aplicare la nivel național a unui mecanism de comunicare adecvat între autoritățile naționale responsabile și ofițerii de legătură pentru securitate sau echivalenții acestora, în scopul eficientizării schimbului de informații relevante privind riscurile și

amenințările identificate în legătură cu infrastructurile critice respective

2.4. Inițierea și coordonarea adecvată a unor activități de cercetare științifică în parteneriat public-privat, în vederea identificării unor metode de determinare și analiză a riscurilor, vulnerabilităților și măsurilor necesare realizării protecției infrastructurilor critice

2.5. Elaborarea unor aplicații informatice de modelare și simulare a funcționării și stabilire a interdependențelor infrastructurilor critice, în scopul realizării unui model de proces decizional, reducerii vulnerabilităților și creșterii capacității de reacție a populației, societății și/sau instituțiilor statului la nivel local, regional, național și internațional.

Obiectivul strategic nr. 3 - Evaluarea corectă a nivelului de vulnerabilitate a infrastructurilor critice și identificarea măsurilor necesare pentru intervenția preventivă și diminuarea acestuia

Direcții de acțiune:

3.1. Revizuirea standardelor de calitate, adaptarea mecanismelor de protecție, identificarea și contracararea pericolelor, ridicarea nivelurilor de redundanță, creșterea gradului de modularitate

3.2. Eficientizarea activităților și acțiunilor prin eliminarea birocrăției excesive, imixtiunilor în fluxul normal de informații și decizie, scurgerilor de informații, consumului nejustificat de resurse și a disipării răspunderii în cazul producerii unor incidente

3.3. Elaborarea planurilor de securitate ale operatorilor pentru fiecare infrastructură critică desemnată, identificarea elementelor de infrastructură critică și a soluțiilor de securitate existente sau puse în aplicare pentru protecția acestora și operaționalizarea unui sistem eficient de îndrumare și control

3.4. Realizarea unor "bănci de date" care să permită colectarea și prelucrarea datelor specifice domeniului infrastructurilor critice, precum și a studiilor de caz, manualelor de bune practici și lecțiilor învățate

3.5. Evaluarea necesităților de îmbunătățire a sistemelor de protecție a infrastructurilor critice, pentru a contribui la protecția persoanelor, bunurilor și mediului înconjurător.

Obiectivul strategic nr. 4 - Dezvoltarea relațiilor de cooperare la nivel național, regional și internațional în domeniul protecției infrastructurilor critice

Direcții de acțiune:

4.1. Dezvoltarea cooperării la nivel național și internațional în scopul realizării schimbului de date și informații cu privire la procesul de identificare și protecție a infrastructurilor critice europene

4.2. Crearea mecanismelor de cooperare interinstituțională pentru protecția infrastructurilor critice prin cooptarea reprezentanților desemnați de către autoritățile publice responsabile nominalizate în actul normativ ce transpune în legislația națională prevederile Directivei 2008/114/CE

4.3. Realizarea cooperării interinstituționale și constituirea unor grupuri de lucru la nivel de experți pentru identificarea soluțiilor optime de realizare a protecției elementelor de infrastructură și pentru stabilirea modalităților de intervenție

4.4. Asigurarea interoperabilității și îmbunătățirea comunicării interinstituționale și cu statele membre prin stabilirea unor calendare de întâlniri în formate bilaterale, pe domenii specifice sau în cadrul unor forumuri tematice

4.5. Implementarea măsurilor legislative și operaționale pe linia protecției infrastructurilor critice, ce decurg din calitatea României de membru al Uniunii Europene și al Alianței Nord-Atlantice, responsabilitate ce derivă inclusiv din perspectiva participării la asigurarea climatului de stabilitate și securitate regională

4.6. Consolidarea cooperării cu statele vecine, în vederea identificării acelor componente de

infrastructuri ce pot fi incluse în categoria infrastructurilor critice europene și inițierea demersurilor ce se impun pentru asigurarea capacității de protecție a acestora în raport cu cerințele de securitate naționale și internaționale

4.7. Îmbunătățirea și dezvoltarea dialogului între toate structurile cu atribuții și responsabilități în domeniu prin realizarea parteneriatului între proprietarii, administratorii și/sau operatorii infrastructurilor critice, Guvern și societate, în vederea managementului eficient al riscurilor și asigurării unui răspuns adecvat în cazul perturbării sau distrugerii infrastructurilor critice.

Transpunerea în realitate a acestor deziderate presupune intensificarea dialogului în format partenerial dintre sfera publică și cea privată, cu responsabilizarea tuturor participanților asupra necesității configurării unui climat de coeziune în privința măsurilor ce se impun a fi adoptate și capacității de răspuns/aplicabilitate în planul protecției infrastructurilor critice.

Pentru îndeplinirea direcțiilor de acțiune propuse, se va avea în vedere conjugarea efortului pe următoarele coordonate:

a) prevenire, diminuare și limitare a efectelor:

1. anticiparea vulnerabilităților și riscurilor;
2. pregătirea și planificarea continuă;
3. asigurarea controlului;
4. evaluarea, prin metode comprehensive și proactive, a factorilor de risc, cu adoptarea managementului de risc și strategiei de gestionare a crizelor;

b) răspuns/intervenție:

1. dezvoltarea unei capacități adecvate de răspuns la nivelul tuturor structurilor ce ar putea fi afectate, prin proiectarea unor măsuri de intervenție în situații de urgență (inclusiv de protecție fizică) și de management de criză;
2. exerciții și bune practici care să ofere un maximum de eficiență și flexibilitate față de orice provocare;

c) sustenabilitate:

1. analize de risc, indiferent de elementul de cauzalitate, care să confere suportul adaptării permanente la evoluțiile caracteristicilor de risc și standardelor de protecție a infrastructurilor critice;
2. corelarea resurselor cu necesitățile de identificare timpurie și prevenție/contracurare a riscurilor.

8. Implicații financiare

Activitatea de protecție a infrastructurilor critice presupune un efort conjugat și multidisciplinar în planul resurselor umane și materiale ce vor fi alocate conform competențelor în domeniu de către autoritățile publice responsabile și proprietarii, administratorii și/sau operatorii de infrastructuri critice.

Optimizarea sistemului de asigurare a resurselor pentru protecția infrastructurilor critice ar putea presupune o mărire a ponderii componentelor informaționale, generată atât de creșterea relevanței acestora în toate domeniile sociale, cât și ca urmare a diversificării amenințărilor care vizează acest domeniu.

9. Mecanisme de implementare, monitorizare și evaluare

În adoptarea procedurilor de implementare, monitorizare și evaluare, se vor avea în vedere următoarele coordonate:

a) legislative - actualizarea/completarea cadrului normativ specific în raport cu delimitările, atribuțiile și competențele ce revin instituțiilor angrenate ce acționează în domeniul protecției infrastructurilor critice;

b) instituționale - dezvoltarea capacității de a elabora, implementa, monitoriza și coordona aplicarea obiectivelor specifice;

c) umane - dezvoltarea și formarea profesională, prin:

1. profesionalizarea resurselor umane angrenate în procesul de identificare și protecție a infrastructurilor critice;

2. stabilirea "nișelor" formative în scopul creării oportunităților de specializare în plan european, ceea ce poate plasa România în poziția de furnizor de pregătire în domeniu;

d) de cooperare între sfera publică și cea privată - care să asigure armonizarea măsurilor la nivel național, schimbul de expertiză și dezvoltarea cercetării și inovației în domeniu.

În procesul de evaluare vor fi avute în vedere criteriile naționale, precum și tehnicile de evaluare stabilite la nivelul tuturor statelor membre ale Uniunii Europene.

Punerea în aplicare la nivel național a unui mecanism de comunicare adecvat între autoritățile naționale responsabile și ofițerii de legătură pentru securitate sau echivalenții acestora, în scopul realizării schimbului de informații relevante privind riscurile și amenințările identificate în legătură cu infrastructurile critice respective, este esențială pentru monitorizarea și coordonarea eficientă a activităților de protecție a infrastructurilor critice pe termen scurt și mediu.
