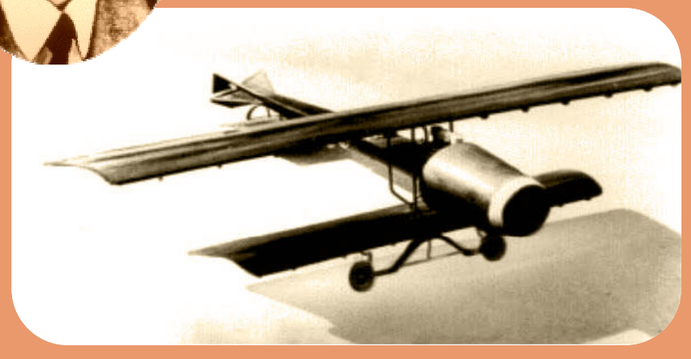
1910-2010

100 de ani

de la primul zbor al unui avion dotat cu motor cu reacție,
invenția inginerului român Henri Coandă



ISSN 1582-7410

REVISTA DE ŞTIINŢE MILITARE ANUL X, 2010 NR. 2 (19)

Revista de Ştiinţe Militare

Editată de Secţia de Ştiinţe Militare
a Academiei Oamenilor de Ştiinţă din România

Nr. 2 (19)
Anul X, 2010

Revista de Ştiinţe Militare

Editată de Secţia de Ştiinţe Militare
a Academiei Oamenilor de Ştiinţă din România

300 de ani
de la înscăunarea pe tronul Moldovei
a domnitorului Dimitrie Cantemir

Nr. 2 (19)
Anul X, 2010

Materialele publicate în acest număr al Revistei de Ştiinţe Militare au fost prezentate la simpozionul din 26 mai 2010 al Academiei Oamenilor de Ştiinţă din România, cu tema: ***"Protecţia infrastructurilor critice în corelaţie cu strategia de securitate naţională. Coordonarea cu acţiunile Alianţei Nord-Atlantice şi Uniunii Europene",*** ***ce s-a desfăşurat în sala de marmură a Cercului Militar Naţional din Bucureşti.***

Responsabilitatea integrală a asumării intelectuale a articolelor trimise redacţiei aparţine autorilor.

ISSN 1582-7410

C U P R I N S

CUVÂNT ÎNAINTE 5
General (r) prof. univ. dr. H.C. Vasile CÂNDEA

CONCEPTELE DE VALORI ŞI NIVELURI CRITICE 7
General (r) dr. Eugen BĂDĂLAN
General de brigadă (r) dr. Gheorghe ILIE

GUVERNAREA RISCULUI ÎN INFRASTRUCTURA CRITICĂ 18
General (r) prof. univ. dr. Gheorghe ILIE

O POSIBILĂ DINAMICĂ A INFRASTRUCTURII STRATEGICE 27
General de brigadă (r) dr. Gheorghe VĂDUVA

CONCEPTUL INTEGRONIC AL SECURITĂȚII INFRASTRUCTURII CRITICE (IC) 44
Colonel (r) prof. univ. dr. Eugen SITEANU
General de brigadă (r) prof. univ. dr. Gheorghe ILIE

PROTECȚIA INFRASTRUCTURII CRITICE – SARCINĂ PRIORITARĂ ÎN CADRUL STRATEGIEI DE SECURITATE A UNIUNII EUROPENE..... 56
General locotenent prof. univ. dr. Teodor FRUNZETI

INFRASTRUCTURA PENTRU APĂRARE – BENEFICIARĂ A PROGRAMELOR COMUNITARE 72
General (r) prof. univ. dr. Mircea MUREŞAN

PROTECȚIA INFRASTRUCTURILOR CRITICE. RISCURI LA ADRESA INFRASTRUCTURII CRITICE NAȚIONALE ŞI STRATEGII DE PROTECȚIE ŞI SECURITATE 89
Comandor (r) dr. Marian SANDU

SISTEME ŞI REŢELE DE COMUNICAŢII ŞI INFORMATICE MILITARE ŞI SPECIALE, CA PARTE VITALĂ A INFRASTRUCTURILOR CRITICE ALE ROMÂNIEI. ASIGURAREA PROTECŢIEI FIZICE ŞI INFORMAŢIONALE A ACESTORA 95
General maior (r) prof. cons. dr. Constantin MINCU

PROTECŢIA INFRASTRUCTURII CRITICE DE INFORMAŢIE 123
General locotenent (r) prof. univ. dr. Cristea DUMITRU

INFRASTRUCTURI CRITICE ÎN CEL DE-AL DOILEA RĂZBOI MONDIAL ŞI INFLUENŢA LOR ASUPRA ACŢIUNILOR MILITARE 142
General de brigadă (r) prof. univ. dr. Nicolae CIOBANU

PROTECTIA INFRASTRUCTURII INFORMAŢIONALE CRITICE 148
Colonel (r) prof. univ. dr Gruia TIMOFTE

COOPERAREA STRUCTURATĂ PERMANENTĂ ÎN DOMENIUL APĂRĂRII – PROVOCĂRI ŞI OPORTUNITĂŢI 158
Dragoş ILINCA

CUVÂNT ÎNAINTE

MESAJUL PREŞEDINTELUI ACADEMIEI OAMENILOR DE ŞTIINȚĂ DIN ROMÂNIA

Sunt onorat pentru prilejul de a adresa salutul meu lucrărilor Simpozionului ***"Protecția infrastructurilor critice în corelație cu strategia de securitate națională. Coordonarea cu acțiunile Alianței Nord-Atlantice şi Uniunii Europene"*** *organizat de Secția de Ştiințe Militare din Academia Oamenilor de Ştiință din România.*

Grupul de lucru INFRASTRUCTURA CRITICĂ din cadrul Academiei Oamenilor de Ştiință din România, din care fac parte şi câțiva membri din Secția de Ştiințe Militare, are aceleaşi preocupări în domeniul infrastructurii care devine din ce în ce mai mult unul dintre domeniile de maximă prioritate ale modului de viață al oamenilor.

Infrastructura redefineşte conceptele de geopolitică şi geostrategie, constituindu-se suporturi esențiale durabile ale unei dinamici de conexiune

şi de distorsiune care unifică şi separă, consolidează şi în acelaşi timp destabilizează societatea umană.

În cadrul acesteia fiecare stat îşi defineşte şi îşi identifică infrastructura critică de care depinde funcționarea tuturor sistemelor şi proceselor specifice tuturor organizațiilor.

Noi toți trăim pe un suport de infrastructură care trebuie în permanență consolidat, modernizat şi securizat. Depindem, deci, de aceste infrastructuri, încât nu mai putem trăi în afara lor. În consecință, eforturile noastre trebuie să se concentreze pe protecția acestor infrastructuri şi în mod deosebit pe cea a infrastructurii critice.

General (r) prof. univ. dr. H.C. Vasile CÂNDEA
Preşedintele Academiei Oamenilor de Ştiință din România

CONCEPTELE DE VALORI ŞI NIVELURI CRITICE

General (r) dr. Eugen BĂDĂLAN
General de brigadă (r) dr. Gheorghe ILIE

Conceptul de situaţie critică determină conceptul de infrastructură critică, securitatea cetăţenilor, în acelaşi raport pentru securitatea naţională. El se referă la situaţiile critice în raport cu securitatea naţională şi sunt analizate două probleme majore: valorile şi nivelurile critice. Valorile critice sunt valorile de stare critică cu valoarea maximă de 0,707 – valoare critică pentru supravieţuire. Nivelurile critice se referă la niveluri de risc care guvernează starea critică. Riscul asumat pentru criticitate procesuală este de 30%, în timp ce pentru cea de supravieţuire, riscul asumat este de 70% faţă de normalitatea procesului.

Raportul dintre cost şi nivelurile de risc care guvernează procesele critice asigură, în acelaşi timp, riscul operaţional, prin parametrul de calitate analitică.

Conceptul de risc

Nu există încă un consens în ceea ce priveşte definirea riscului, ci o multitudine de aprecieri despre risc, o varietate de sensuri atribuite conceptului de risc.

Iată câteva dintre aceste aprecieri:

– riscul e de natură analitică, neavând consistenţă fizică şi nici posibilităţi de concretizare;

– riscurile apar în cadrul tuturor activităţilor socio-economice;

– asocierea dintre risc şi hazardul particular nu e întotdeauna corectă;

– riscurile sunt acelea care conduc la mai multe variante de acţiune;

– riscul presupune determinarea probabilităţii producerii unui eveniment nedorit, a conjuncţiei de favorabilitate dintre ameninţări şi vulnerabilităţi, a

consecinţelor producerii acestuia şi a determinării elementelor ce îl caracterizează, dar şi a atitudinii faţă de acesta:

– gestiunea riscurilor necesită resurse serioase informaţionale, umane, materiale şi financiare, de aceea, gestiunea riscurilor, pentru a avea succes, trebuie considerată ca parte a top managementului, având un rol, cert, strategic;

– din punct de vedere al ingineriei securităţii, analiza de risc e singura modalitate de apreciere a nivelului de periculozitate a unui obiectiv de securitate şi trebuie efectuată şi luată în considerare atât la începutul proiectării sistemului de securitate, cât şi după implementarea acestuia.

De asemenea vom prezenta şi câteva definiţii ale riscului:

– riscul (R) reprezintă conjuncţia dintre ameninţări (A) şi vulnerabilităţi (V): $R=A\cap V$;

– riscul reprezintă un eveniment probabil, generator de pierderi;

– riscul este forma măsurabilă a incertitudinii;

– riscul este un indicator (o valoare) care defineşte probabilitatea şi ritmul de apariţie a unui eveniment sau acţiune care se produce;

– riscul reprezintă măsura incertitudinii;

– riscul reprezintă probabilitatea apariţiei unui eveniment şi a impactului acestuia;

– riscul reprezintă atât o valoare numerică (fie posibilitatea producerii, fie consecinţele unui eveniment nedorit), cât şi o atitudine de evaluare ştiinţifică, de prevenire a evenimentelor nedorite sau de atenuare a consecinţelor acestora.

Din punct de vedere al amplitudinii (magnitudinii), riscurile sunt:

– riscuri neglijabile, cuprinse între 0 şi 0,2;

– riscuri minore, între 0,2 şi 0,4;

– riscuri medii, între 0,4 şi 0,6;

– riscuri majore, între 0,6 şi 0,8;

– riscuri dezastruoase, între 80% şi 100%.

Din punct de vedere al apartenenţei la un proces, riscurile pot fi:

– riscuri de mediu;

– riscuri de proces;

– riscuri de infrastructură.

Riscul (R) reprezintă evoluţia probabilă (posibilă) a elementului X, din starea T_0 în starea T_r sub influenţa factorilor F_r care determină cu certitudine producerea evenimentului PE cu consecinţele CE:

$$R=p\cdot CE,$$

unde p este probabilitatea sau posibilitatea evoluţiei. Acest model e valabil şi dacă drept factori de risc se iau oportunităţile şi capabilităţile.

Categorisirea riscurilor e multicriterială şi cuprinde o multitudine de aspecte privind sensul dimensional, sursa, corelaţiile motivaţionale, atitudinea, magnitudinea, apartenenţa, locul şi cauzele, modul de manifestare, domeniul şi obiectivul caracterizat.

Probabilitatea producerii evenimentului nedorit se poate reprezenta printr-o scală cu şapte trepte:

CALITATIVĂ	CANTITATIVĂ
Sigură	1
Aproape sigură	0,93
Probabilă	0,75
Şanse aproape egale	0,5
Probabil NU	0,3
Aproape sigur NU	0,07
Imposibilă	0,00

Tabelul nr. 1

După cum rezultă din acest tabel, valoarea de 0,3 este critică în raport cu normalitatea procesului.

Conceptul de valoare critică

Simpla analiză a probabilităţii de producere a evenimentelor nedorite nu este suficient de edificatoare pentru stabilirea impactului acestora asupra unui obiectiv de securitate. Evenimentele care au frecvenţă mare de repetare trebuie tratate cu atenţie, dar tot aşa trebuie tratate şi evenimentele care sunt foarte puţin probabile, dar au consecinţe catastrofice. De exemplu, pentru o mare companie, cum ar fi, de exemplu CFR, furturile zilnice (cu frecvenţă foarte mare de repetare) sunt tratate foarte atent, dar la fel trebuie tratate şi evenimentele de tip cutremur, inundaţie sau incendiu, care, deşi au o frecvenţă mică de repetare, pot avea consecinţe catastrofice pentru acea companie.

La aceste aspecte se mai adaugă şi proprietatea unor evenimente nedorite de cumulare a efectelor şi care trebuie tratate, de asemenea, cu atenţie sporită. De pildă, cutremurele repetate, pe lângă pagubele aduse bunurilor, aduc cumulativ (efectul picăturii chinezeşti) pagube însemnate clădirilor, prin slăbirea în timp a rezistenţei lor constructive.

Din acest punct de vedere, s-a introdus un concept de evaluare a evenimentelor nedorite de **valori critice (cu stare critică)**.

Conceptul de stare critică vizează două aspecte majore determinate de **punerea în pericol a funcţionalităţii (procesualităţii),** pe de o parte, sau **existenţei unui obiectiv**, fiind însă strâns legat şi de sintagma şi semnificaţiile **infrastructurii critice**, pe de altă parte.

Din punctul de vedere al evaluării, starea critică înseamnă (*fig.1*):

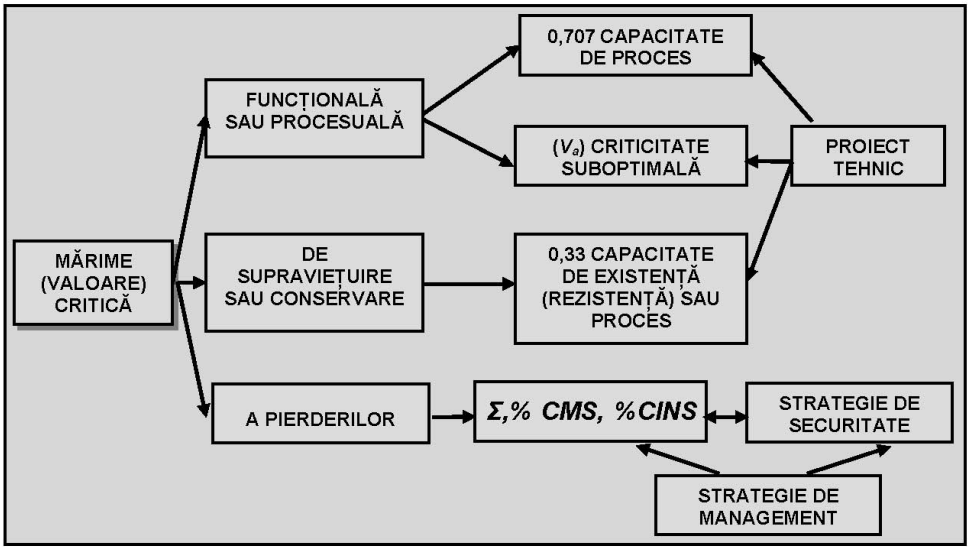


Fig.1 – Conceptul de mărime critică

- ***0,707*** din capacitatea de proces, infrastructură, asigurarea cu materii prime şi personal (**valoarea critică funcţională sau procesuală**) sau o altă valoare considerată suboptimală, dar admisibilă. Valoarea suboptimală poate fi mai mare sau mai mică decât ***0,707*** (**valoarea critică suboptimală**);
- ***0,33*** din capacitatea de existenţă (rezistenţă, proces) a obiectivului (**valoarea critică de supravieţuire** sau **de conservare**), cu menţinerea sau cu întreruperea funcţionalităţii procesului;
- o anumită sumă, un anumit procent din costurile măsurilor de securitate (***CMS***) sau un anumit procent din costurile de insecuritate (***CINS***) – (**mărimea critică a pierderilor**).

Dacă valorile din primele două cazuri critice se concretizează în proiectele obiectivelor, criticitatea pierderilor se stabileşte prin strategia de top management şi se concretizează în strategia de securitate. Deşi tehnic nu este cea mai edificatoare, mărimea critică a pierderilor (*atât pot să-mi permit să pierd*) este cel mai des folosită, fiind motivată de sensibilitatea investitorilor şi managerilor faţă de

valorile financiare. Mai nou, mărimea critică a pierderilor este înlocuită de **mărimea critică a costurilor** (*atât îmi permit să cheltuiesc*), nu ca soluţie tehnică diferită, ci doar ca element cu mai multă sensibilitate financiară – ***este greu să admit pierderi, dar îmi permit să cheltuiesc, ştiind pentru ce***.

Mărimea critică a costurilor aduce cu ea şi o oarecare certitudine pentru investitori şi manageri că nu cheltuiesc mai mult decât trebuie. În urma acestei consideraţii devine foarte importantă analiza costurilor care configurează mărimea critică a pierderilor (costurilor).

Costurile care se iau în considerare sunt **costurile reale** (***C_r***), care depind direct de (derivă din) acoperirea pagubelor cauzate de producerea evenimentelor nedorite şi reprezintă:

– **costurile** necesare **înlocuirii** - ***$C_î$*** - bunurilor distruse, dispărute sau devenite nefuncţionale în urma producerii evenimentelor nedorite;

– **costurile** necesare **substituirii** - ***C_s*** - (de completare) pentru o anumită perioadă de timp a bunurilor distruse, dispărute sau devenite nefuncţionale, parţial sau total, în urma producerii evenimentelor nedorit;

– **costurile** necesare **acoperirii** - ***C_a*** - veniturilor realizate ca urmare a blocării totale sau parţiale a proceselor de producţie din cauza bunurilor distruse, dispărute sau devenite nefuncţionale;

– **costurile adiacente** - ***C_p*** - (suplimentare, în plus) cauzate de acoperirea unor penalităţi sau ca urmare a încetinirii proceselor de producţie sau de muncă, ori a micşorării productivităţii acestora.

Costurile de înlocuire presupun acoperirea integrală a costurilor de achiziţie, montare - instalare şi punere în funcţiune. Aceste costuri pot fi egale cu cele iniţiale sau pot diferi, în funcţie de evoluţia pieţei de la achiziţia iniţială până la înlocuire.

Costurile de substituire reprezintă costurile necesare pentru bunul „împrumutat", precum şi cele de montare - instalare şi punere în funcţiune a acestuia. Substituirea reprezintă o înlocuire pe o anumită perioadă a bunului distrus, dispărut sau aflat în stare de nefuncţionare, cauzată de faptul că este necesară înlocuirea urgentă a acestuia (pentru deblocarea procesului), urmând ca apoi să se facă achiziţia unui bun nou, sau până când bunul parţial distrus este pus în funcţiune, ori bunul dispărut este recuperat şi returnat de poliţie.

Costurile de acoperire a veniturilor nerealizate din cauza unor bunuri distruse, dispărute sau aflate în stare de nefuncţionalitate ca urmare a producerii unui eveniment nedorit se referă la acele venituri care nu au putut fi realizate din cauza blocării proceselor de producţie sau de muncă.

Costurile adiacente trebuie analizate cu atenţie, deoarece acestea pot atinge valori deosebit de importante şi pe o perioadă apreciabilă de timp, existând

posibilitatea de a influenţa decisiv şi alte procese de producţie sau de muncă, în afara celor care au legătură directă cu utilizarea bunului distrus, dispărut sau aflat în stare de nefuncţionalitate, ca urmare a producerii evenimentului nedorit. De regulă, costurile reale cauzate de un eveniment nedorit reprezintă o sumă de costuri de înlocuire, substituire, acoperire şi adiacente, iar determinarea acestora reprezintă o aplicaţie financiară şi tehnică destul de complicată.

Pentru calcularea costurilor reale se poate folosi şi formalizarea:

$$C_r = (C_t + C_s + C_a + C_p) - V_a,$$

unde V_a este valoarea ce se poate obţine în urma compensării pierderilor prin asigurarea încheiată de organizaţie pe bunuri, procese şi /sau persoane.

La rândul lor, costurilor reale se mai împart în funcţie de modul de concretizare a acestora direct în valori sau în acţiuni de consecinţă. **Costurile directe** pot fi materializate în bani, valori negociabile, proprietăţi sau valori informaţionale. **Costurile indirecte** se materializează prin pierderea reputaţiei, micşorarea bunăvoinţei sau înţelegerii de parteneriat, pierderea angajaţilor şi/sau diminuarea moralului acestora.

Nivelurile critice

Similară repartizării riscurilor pe scalele de probabilitate, posibilitate sau frecvenţă, există şi repartizarea performanţelor, dar şi a costurilor, pe o scală asemănătoare (*fig. 2).* Poziţionarea nivelurilor critice pe scala performanţelor sau costurilor asigură o imagine sugestivă asupra stării procesului, dar şi a poziţionării celor două categorii de stări critice una faţă de cealaltă. În acelaşi timp, există şi o reprezentare a stării critice pe scala riscurilor, cu o poziţionare, evident, inversă faţă de pe scala performanţelor (*fig. 3).* Riscul asumat pentru criticitate procesuală (funcţională) este de ***30%***, în timp ce pentru cea de supravieţuire riscul asumat este de ***70%*** faţă de normalitatea procesului.

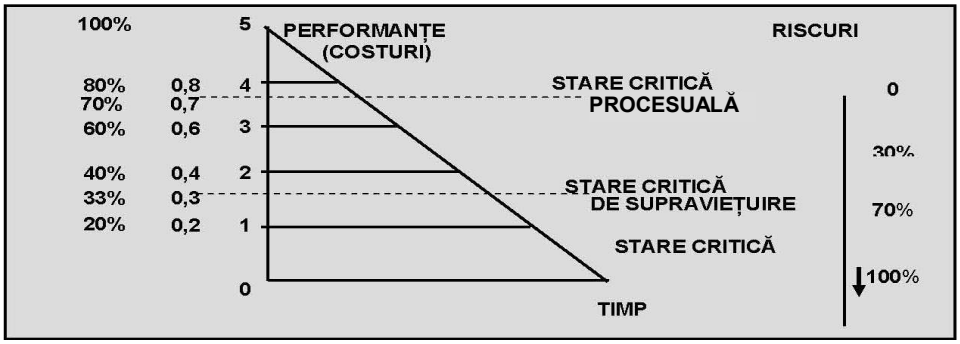


Fig. 2 **– Poziţia nivelurilor critice**

Deşi starea critică este considerată o problemă de prag (palier, limită), în realitate procesul stării critice nu este nici liniar şi nici static, manifestându–se, de regulă, ca un proces oscilant în jurul pragului stabilit. Acest lucru înseamnă că în jurul pragului critic au loc oscilaţii de performanţă ***(± ΔP***) care pot accentua starea critică (***Pc – ΔP***) sau pot să o amelioreze (***Pc + ΔP***).

Variaţia stării critice reprezintă o problemă deosebit de complexă, având în vedere faptul că este vorba de un proces la limită, cu sensibilitate ridicată şi unde mecanismele de reacţie sunt, de regulă, mai puţin eficace. Din această cauză, dar şi pentru a avea o imagine asupra dinamicii stării critice, pentru a-i putea guverna evoluţia, a fost adoptată clasificarea stării critice, partajarea acesteia pe niveluri critice similar partajării riscului.

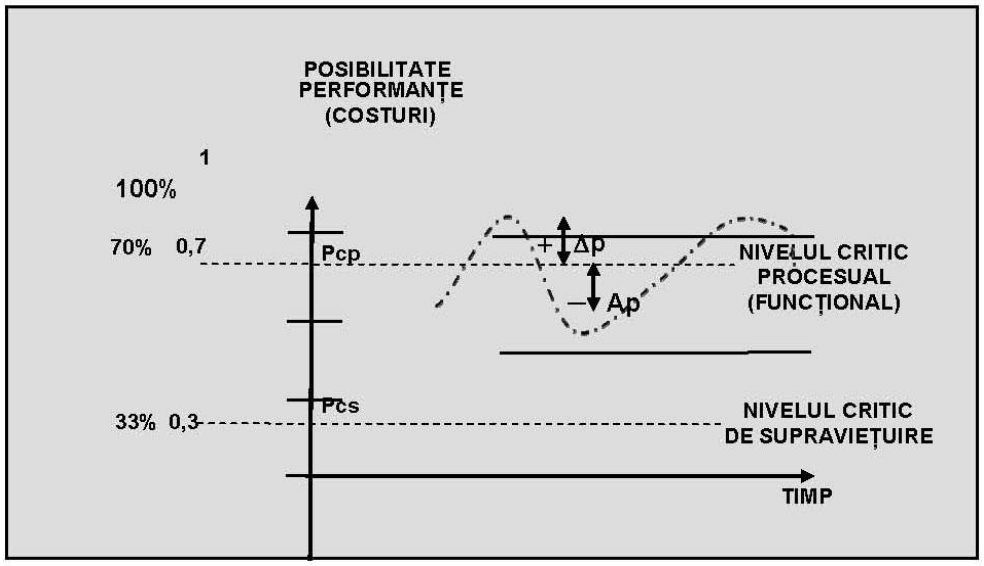


Fig. 3 **– Poziţionarea stării citice pe scala performanţelor (costurilor)**

Aspectul cel mai sensibil al acestei partajări este dat de faptul că nu sensul variaţiei stării critice este cel care stabileşte categoria, ci mărimea instabilităţii procesului aflat în situaţie critică. Cu cât variaţia procesului în jurul pragului critic este mai accentuată, cu atât procesul este mai expus unei destabilizări majore, fiind mai dificil de guvernat. Reciproca nu este însă totdeauna valabilă, deoarece mai trebuie luate în considerare şi viteza de variaţie, precum şi frecvenţa acesteia.

Ţinând seama de aceste aspecte, reducând problema doar la mărimea variaţiei, se poate reprezenta variaţia stării critice pe o scală similară variaţiei riscului (*fig. 4*). Această scală cuprinde tot cinci paliere, exprimate atât în valori absolute, cât şi în valori relative (diferenţa faţă de o valoare etalon sau stabilită pentru comparaţie).

Pe scala valorilor absolute sau relative, valoarea critică este partajată astfel:

– FATALĂ – atestă faptul că, în urma producerii evenimentului nedorit care a determinat variaţia, procesul este blocat funcţional, pentru o perioadă de timp ce poate scoate din funcţionare totală sistemul suport sau chiar să îl distrugă. Nivelul FATAL se consideră a fi cuprins între valorile ***5*** şi ***4,01***, adică până la GRAV; la fel se consideră şi celelalte paliere;

– GRAVĂ – deteriorările, respectiv pierderile cauzate de variaţia procesului, sunt foarte importante şi aduc prejudicii majore procesului, necesitând investiţii considerabile pentru restabilirea funcţională;

– MODERATĂ – deteriorările, respectiv pierderile cauzate de variaţii sunt apreciabile, dar nu afectează fundamental procesele de producţie sau de muncă; bunurile distruse, dispărute sau aflate în stare de nefuncţionalitate pot fi relativ înlocuite operativ; costurile pentru restabilirea normalităţii şi continuarea proceselor de producţie sau de muncă sunt acceptabile şi pot fi suportate;

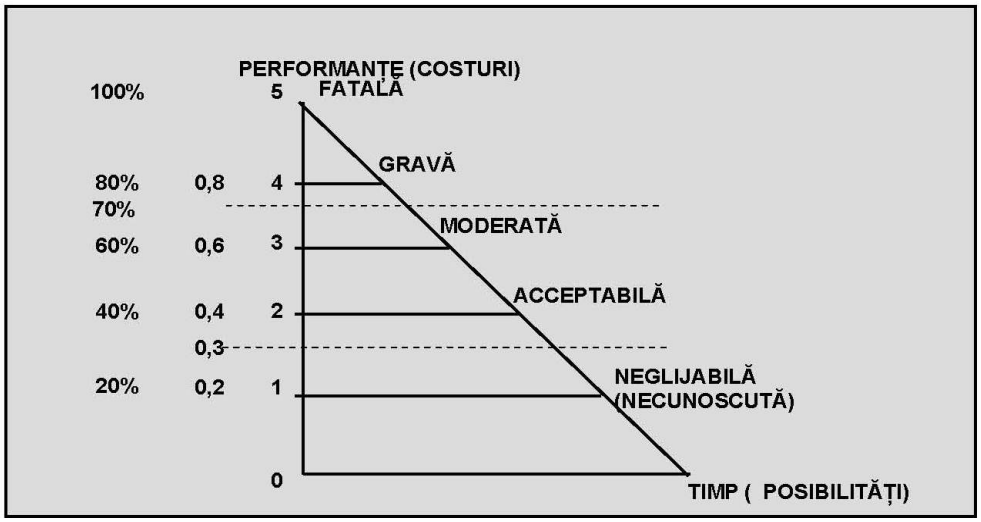


***Fig. 4* – Scala stării critice**

– ACCEPTABILĂ – pierderile cauzate de variaţiile datorate producerii evenimentului nedorit pot fi acoperite prin rezerve sau măsuri de redundanţă funcţională; mai apropiată de aprecierea de acceptabilă este situaţia în care procesul de producţie, de exemplu, a suferit pierderi sau distrugeri, fiind obligat să-şi diminueze randamentul (productivitatea), fără a se întrerupe însă;

– NEGLIJABILĂ (NECUNOSCUTĂ) – în această situaţie, pierderile cauzate de variaţii trebuie doar evidenţiate, acestea fiind suportate direct de proces, în cazul în care sunt evaluate; pierderile neevaluate se iau în evidenţă urmărindu–se influenţa lor asupra proceselor; dacă starea critică neglijabilă poate fi cu adevărat neglijată, stările critice necunoscute sunt obligatoriu monitorizate. Stările critice neglijabile se marchează cu *.

Costurile pentru securitate se compară cu cele rezultate în urma insecurităţii. Se remarcă faptul că valorile critice ale costurilor de securitate sunt mai mari atunci când depăşesc costurile de insecuritate (cheltuieşti mai mult decât pierzi) şi sunt optimale atunci când sunt egale cu acestea (*fig.5)* .

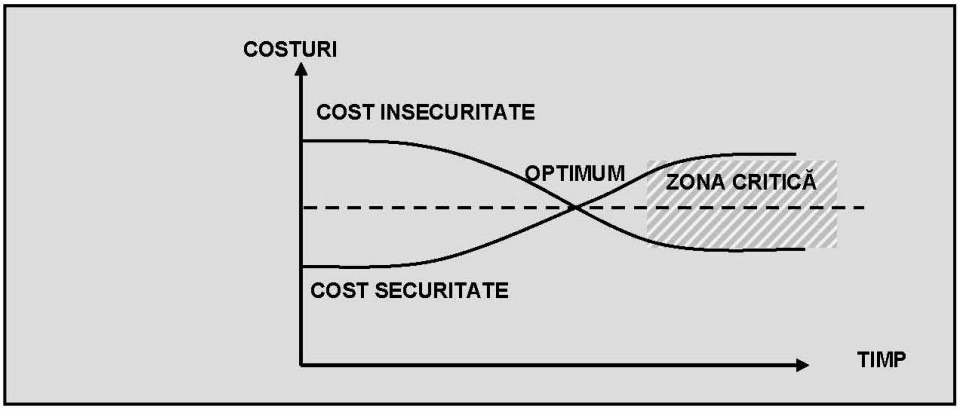


***Fig. 5* – Valorile costurilor de securitate**

Nu există posibilităţi de a recomanda diferite niveluri de costuri de securitate şi nici niveluri de diferenţe între acestea şi costurile de insecuritate; de aceea, fiecare organizaţie trebuie să-şi stabilească, în funcţie de strategia de securitate, costurile suportabile, precum şi nivelul critic al acestora.

O problemă deosebit de complexă a analizei de risc este legată de necesitatea de a evalua manifestarea critică a procesului în jurul pragului de referinţă, care poate fi şi critic.

Potrivit acestui concept, manifestarea unui proces caracterizat prin risc (să spunem MAJOR – ***M*** sau de tip ***B***) poate fi comparat cu un prag – tot de valoare majoră –, iar faţă de acesta poate fi considerat (în procente faţă de prag) ca fiind cu mărime critică NEGLIJABILĂ, ACCEPTABILĂ, ... sau FATALĂ. Asta înseamnă (*fig. 6*) că riscului dezastruos corespunzător simbolului ***B,*** ţinând seama de caracteristica mărimii sale critice, i se poate asocia şi unul din simbolurile ***F***, ***G***, ***M***, ***A*** sau ***N***, astfel:

-risc dezastruos cu stare critică fatală, ***DF*** sau ***BF***;
-risc dezastruos cu stare critică acceptabilă, ***DMA*** sau ***BA***.
-risc major cu criticitate neglijabilă (***MN***) sau necunoscută (***MN****).

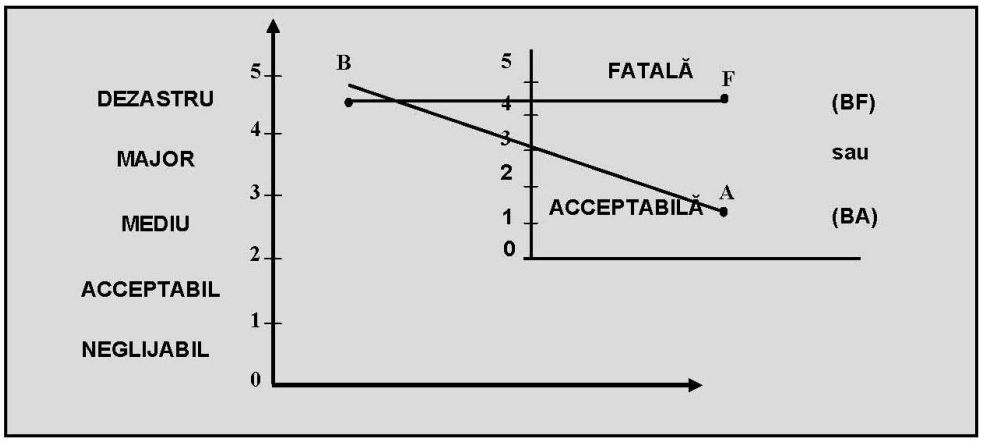


Fig. 6 **– Reprezentarea nuanţată a riscului**

Concluzii

1. Conceptul de stare critică vizează aspectele referitoare la punnerea în pericol a procesualităţii sau a existenţei procesului**.**
2. Între mărimea critică a pierderilor şi mărimea critică a costurilor există o relaţie de determinare, dar nu întotdeauna o relaţie de corespondenţă directă.
3. Diversitatea costurilor este remaracabilă şi se referă la costuri de înlocuire, substituire, acoperire şi adiacente.
4. Între valorile critice (***0,707*** şi ***0,33*** din performanţa maximă) şi nivelurile critice (***0,30*** şi ***0,70***) există o legătură invers proporţională.
5. Nuanţarea valorilor şi nivelurilor critice permite atât o analiză completă a stării de criticitate, cât şi o dublă guvernare în jurul performanţelor sau a riscului.

BIBLIOGRAFIE

BEDER, T. S., *The great risk bunt: Journal of Portofolio Management:* May issue, 1999.

CIOCOIU, N. C., *Managementul Riscului în afaceri şi proiecte*, Editura A.S.E., Bucureşti, 2006.

GREY, S., *Practical Risk Assessement for Project Management,* John Wilwy & Sons, 1995.

HOROBEŢ, A., *Managementul riscului în investiţiile internaţionale*, Editura All Beck, Bucureşti, 2005.

ILIE, GH., *Securitatea mediului de afaceri*, Editura UTI PRESS, Bucureşti, 2006.

ILIE, GH., *De la management la guvernare prin risc,* Editura UTI PRESS şi Editura DETECTIV, Bucureşti, 2009.

RITCHIE, B., MARSHALL, D., *Business Risk Management*, *Chapman & Hall*, London, 1993.

VASILESCU, I. P., *Psihologia riscului.,* Editura Militară, Bucureşti, 1986.

GUVERNAREA RISCULUI ÎN INFRASTRUCTURA CRITICĂ

General (r) prof. univ. dr. Gheorghe ILIE

În limbajul obişnuit, riscul este tratat ca pericol sau pierdere. În realitate, măsura riscului de incertitudine are conotaţii negative, dar şi pozitive (şansă, câştig, beneficiu). Conceptul de relevanţă de risc bazată pe risc, ca indicator de schimbări în performanţa analitică şi de consolidare este o parte a managementului sau un instrument de guvernare sistemică. Acceptanţa reprezintă necesitatea asumării raţionale a riscului şi implică cunoştinţe care reglementează asumarea riscurilor ca o măsură de credibilitate şi relaţionalitate între decident, problemă, sistem, mediu, evaluare şi expertiză managerială, comunicare şi managementul riscului, ca element principal al managementului de acţiune.

Consideraţii supra conceptului de risc

În limbaj natural, riscul este asimilat pericolului şi chiar hazardului, în realitate, însă, riscul nu reflectă numai pericolul sau hazardul, nu are numai conotaţie negativă, ci poate avea şi conotaţie pozitivă, fie în sensul unui câştig absolut direct în urma acţiunii în condiţii de risc asumat (profit), fie a unei pierderi mai mici decât cea anticipată sau calculată (câştig relativ). Pentru a înlătura această contradicţie de percepere este necesară definirea **conceptului de risc** (*fig.1*), care trebuie să impună necesitatea de a **analiza** şi a **accepta** riscul, de a-l **trata**, **percepându-l**, **evaluându-l** şi **determinându-l**, depăşind stadiul de a judeca riscul aşa cum este perceput în viaţa de zi cu zi.

În acelaşi timp, conceptul de risc nu trebuie să fie opus percepţiei şi experienţei de viaţă, ci trebuie să le explice, să le facă înţelese, să fundamenteze saltul de la a vorbi despre risc, la a-l exploata sau guverna, ceea ce înseamnă că pot

fi maximizate câştigurile şi minimizate pierderile. Totodată, conceptul de risc nu poate rămâne în sfera teoretică, având nevoie de a se ilustra prin situaţii specifice, prin cazuri reale, atât particulare, cât şi reprezentative în diverse domenii, inclusiv în domeniul infrastructurii critice.

Conceptul de risc trebuie să ţină seama (*fig.1*) de elementele cunoaşterii aperceptive şi să le orienteze spre concluzii, sinteze şi chiar abstractizări subscrise managementului, astfel:

– **cunoaşterea descriptivă** – faptele, întâmplările, consecinţele trebuie orientate spre înţelegere şi explicaţie;

– **cunoaşterea procedurală** – dezvoltarea socială sau procesuală trebuie orientată spre dezvăluirea cauzelor şi corelaţiilor, spre evaluarea impactului şi frecvenţelor de producere, realizându-se, astfel, baza prognozelor de evenimente viitoare;

– **acceptarea realităţii** trebuie orientată spre analiza evoluţiei, spre deducerea cauzelor şi spre înţelegerea în profunzime a fenomenelor;

– **experienţa personală**, **expertiza cunoştinţelor** şi **educaţia formală** trebuie să asigure orientarea, capacitatea de guvernare, exprimarea profesionalismului şi a personalităţii;

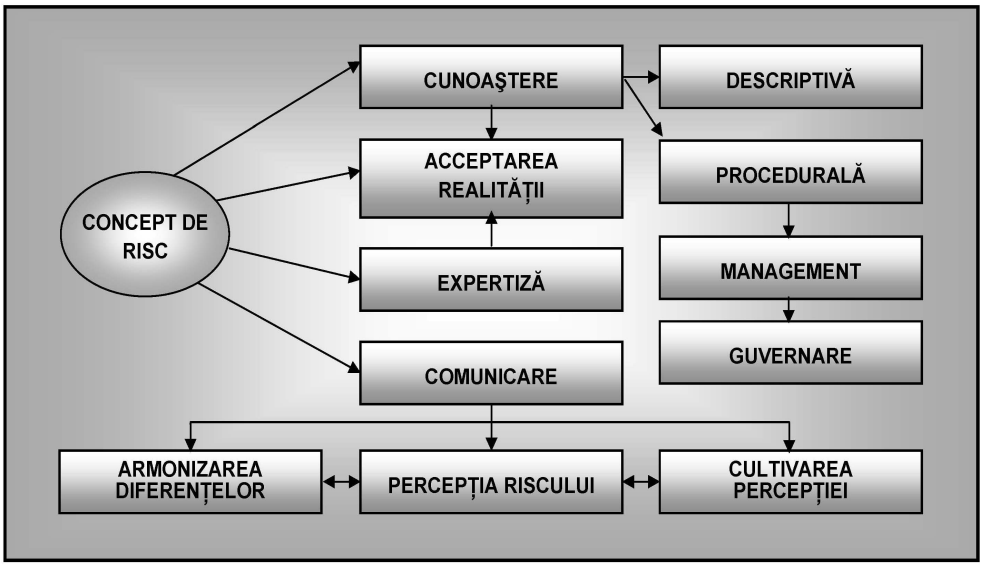


***Fig. 1*– Elementele conceptului de risc**

– **comunicarea** trebuie să asigure cadrul valorificării expertizei şi a sinergiei unităţii sau orientării spre acţiune;

– **armonizarea diferenţelor de gândire şi de îngrijorare** trebuie să fie susţinută de aprofundarea procesului cognitiv – baza înţelegerii, previziunii şi planificării;

– **percepţia despre risc** trebuie să fie orientată spre cunoaşterea realităţii, înţelegerea factorilor de risc, consecinţelor, necesităţii asumării şi a depărtării de interesele strict personale sau de poziţia individului faţă de locul producerii riscului;

– **cultivarea percepţiei despre risc** trebuie să urmeze un proces interactiv, construit spre fundamentarea şi adoptarea deciziilor, cultivându-se exprimarea expertizei şi responsabilităţii faţă de problematica supusă riscului, în interacţiunea socială.

Concluzionând asupra elementelor conceptului de risc, trebuie să subliniem uele aspecte.

- **Cunoaşterea** trebuie să stabilească o formalizare precisă a problemei, care se rezolvă prin decizie, şi să stăpânească relaţia sistemică a intrărilor, stărilor şi ieşirilor, a variaţiilor acestora, şi să anticipeze, cu o anumită probabilitate – în funcţie de riscul asumat – rezultatul deciziei. Cunoaşterea reprezintă un proces complex bazat pe conceptualitate, metodică şi proceduralitate, cu participare directă, intensă şi continuă. Cunoaşterea trebuie să mărească gradul de raţionalitate, să asigure completitudinea necesară variantelor de soluţii, probabilitatea şi consecinţele acestora. Cunoaşterea trebuie să asigure necesarul de cunoştinţe şi de construcţii pentru fundamentarea deciziilor care să permită reducerea semnificativă a incertitudinii şi apropierea de **incertitudinea reziduală** (considerată ireductibilă), dar care **poate fi dominată prin asumarea raţională a riscului**.

Optimalitatea cunoaşterii este un concept care trebuie privit nu numai din punct de vedere economic, ci şi din punctele de vedere al incertitudinii reziduale şi, mai ales, din cel al **confortului raţional al deciziei**.

- **Acceptanţa** reprezintă necesitatea asumării riscului atingerii obiectivelor propuse într-un mediu de incertitudine. Acceptanţa se mai asimilează şi cu **măsura credibilităţii**, constituiind, în acelaşi timp, un sistem multidimensional de relaţionalitate între decident, problemă, sistem, mediu şi consecinţe.

O definiţie larg răspândită[1] stabileşte că „*acceptanţa reprezintă capacitatea unui individ sau a unui competitor (decident) de a tolera (sau înţelege)*

[1] Richards, M.D. – *Managerial decision making: a review*, *in Contemporary Management: Issues and Viewpoints*, Editura J. W. McGuire, Prentince Hall, Englewood Cliffs, 1974.

abaterile de la o convenţie perfectată sau de la o performanţă previzionată, proiectată sau chiar garantată".

Nivelul toleranţei (acceptabilităţii) reprezintă o problemă de evaluare, de interes şi, deci, de decizie şi este strict determinat de domeniul la care se referă acceptabilitatea, iar adoptarea unuia dintre niveluri este o manifestare de putere în raport cu interesele proprii, dinamica variabilităţilor performanţelor, imprecizia (nivelul de definire) a relaţiilor şi a interfeţelor competitoare, precum şi a culturii şi a atitudinii celui care decide asupra nivelului de acceptanţă. Nivelul acceptabilităţii poate fi guvernat prin risc.

Motivaţia acceptabilităţii este intrinsecă, de interese, de atitudine şi de putere. Motivaţia este orientată şi guvernată de cultură şi expertiză, iar ca expresie a puterii, de responsabilitate.

Formele de acceptanţă sunt diverse şi se manifestă vizibil, angajat, sau mai puţin vizibil, relativ dezinteresat.

Reflectarea formelor de acceptanţă este diversă şi depinde evident de percepţie, ca o primă expresie, dar şi de reprezentativitatea problemei şi angajatului în proces, ca expresie a evaluării: **acceptanţa locului de muncă, acceptanţa pericolului la locul de muncă,** dar şi **neacceptanţa variantei unice,** ci a soluţiei „oarbe" bazată pe voinţă discreţionară.

- **Expertiza** reprezintă o caracteristică comportamentală a celor ce activează într-un anumit domeniu. Expertul* este de fapt un specialist care şi-a probat competenţa şi care este recunoscut şi apreciat ca atare.

În domeniul riscului, expertiza este o caracteristică colectivă a unei echipe care se ocupă de formalizarea problemelor şi proceselor guvernate prin risc, de evaluarea şi determinarea riscurilor, de realizarea planurilor de contingenţă pentru amendarea sau exploatarea riscurilor, de managementul sau guvernarea prin risc, precum şi de restabilirea proceselor după producerea unor evenimente nedorite sau neaşteptate.

- **Comunicarea despre risc** reprezintă atât o funcţie a comunicării unei organizaţii, cât şi o funcţie a managementului de risc. Ea presupune:

– **existenţa subiectului** care trebuie să fie un element de interes atât pentru comunicatori, cât şi pentru cei cărora li se transmite subiectul;

– **credibilitatea subiectului** se înscrie în tema potrivit căreia adevărul şi încrederea sunt elementele fundamentale ale comunicării;

– **voinţa de a comunica** trebuie să se manifeste în toate situaţiile, la toate nivelurile şi în toate sensurile;

* Mai multe detalii despre expert se găsesc în articolul "Strategia militară şi alte tipuri de strategii", publicat de Eugen Siteanu în Revista de Ştiinţe Militare nr.1., 2010, pp.79-80.

– **ştiinţa, atitudinea sau formaţia de a asculta** trebuie să fie prezentă atât la cei cărora li se adresează fluxul comunicării, cât şi la comunicatori;

– **posibilitatea anticipării** producerii evenimentelor eliminând surpriza şi incertitudinea, mărind raţionalitatea şi participarea în cunoştinţă de cauză;

– **relaţionalitatea schimbării,** atât ca efect al comunicării, cât şi ca element al participării la comunicare;

– **respectul identităţii** tuturor celor ce participă la comunicare, factor care asigură receptarea şi respectarea subiectului comunicării la adevărata sa valoare.

Când ne referim la comunicare, înţelegem precizia mesajelor de scop, claritatea mesajelor de colaborare, precum şi profesionalismul mesajelor de acţiune (procesare); de aceea, conform acestor elemente, managementul organizaţiei trebuie:

– să fie pregătit să îşi asume riscurile şi costurile;
– să posede ştiinţa comunicării;
– să transmită mesajele clar, corect, profesionist şi oportun;
– să recepţioneze reacţiile opoziţiei, să le analizeze constructiv şi să-şi corecteze excesele de putere.

Guvernarea riscului

Guvernarea riscului sau **guvernarea prin risc** reprezintă un element de interacţiune socială (*fig.2*) bazat pe expertiză şi percepţie colectivă, pe determinări şi corelaţii. Calitatea guvernării prin risc este direct determinată de individul (guvernantul), care îşi pune amprenta pe proces prin nivelul său cultural, opiniile şi interesele sale, în timp ce indivizii guvernaţi, deşi se află în centrul guvernării, suportă consecinţele şi reacţionează numai la efectele guvernării.

După identificarea ameninţărilor şi oportunităţilor, amendarea sau valorificarea acestora depinde direct de **implicarea decidentului** care îşi asumă guvernarea prin risc. În aprecierea implicării trebuie ţinută seama nu numai de expertiza decidentului, ci şi de atitudinea acestuia faţă de guvernarea riscului, care se poate manifesta sub formă de: aversiune, neutralitate, conservatorism, timiditate, încredere sau siguranţă.

Dacă analiştii şi managerii sunt afectaţi de acţiunea guvernată prin risc, fără a ignora prioritatea stabilită de ierarhie, asociază şi alte tipuri de criterii care se pot referi la:

– apropierea de locul observării sau implicării;
– nivelul atragerii intereselor directe;
– propagarea spre zona propie protejată;
– nivelul de perturbare a mediului propriu de existenţă;

– responsabilitatea implicării directe;
– atitudinea şi înţelegerea faţă de risc.

Analiştii şi managerii neafectaţi de acţiunea guvernată prin risc nu sunt dependenţi de magnitudinea variaţiilor consecinţelor şi, de aceea, recomandarea lor pentru tratarea riscurilor este adresată direct top managementului sau vârfului ierarhiei organizaţiei.

Eficienţa unei activităţi poate fi exprimată mai pragmatic în beneficiu.

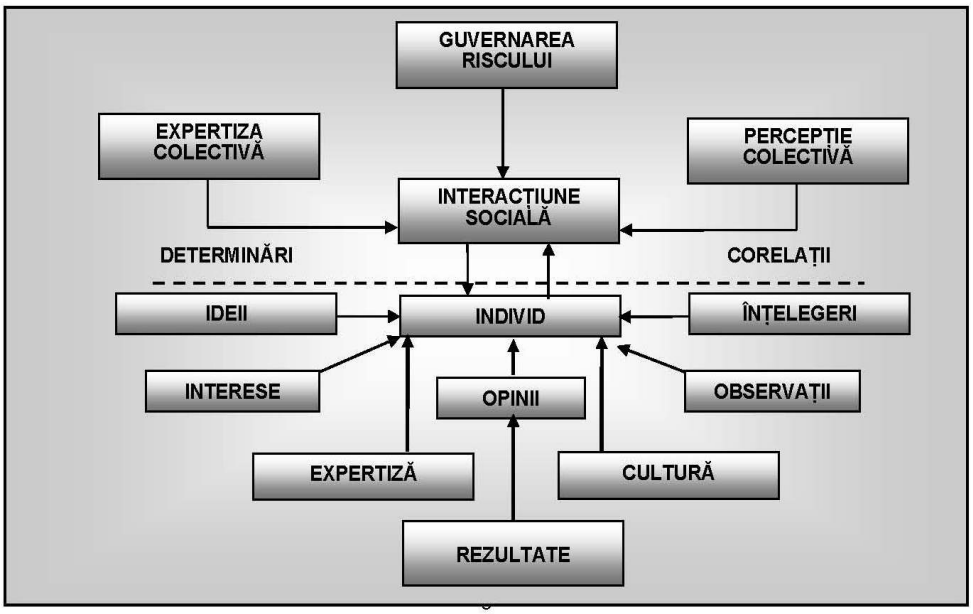


***Fig. 2* – Elementele guvernării prin risc**

Prin beneficiu se înţelege valoarea rămasă în urma activităţii după ce au fost scăzute toate costurile ce acoperă cheltuielile pregătirii, desfăşurării şi finalizării acţiunii, precum şi costul deciziei ca organizaţia să se oprească la acea acţiune (considerată singulară) sau să o repete la aceeaşi parametrii sau la parametrii modificaţi (superiori sau intensivi).

Dacă riscul a fost partajat între decidenţi şi executanţi (manageri şi lucrători), atunci şi beneficiul trebuie partajat în aceeaşi proporţie.

În raportul dintre manageri, planificatori şi utilizatori, privind adoptarea şi implementarea unor decizii (transformarea acestora în acţiuni), apar corelaţii complexe de loc, proces, responsabilitate, acţiune, atitudine şi participare (*fig.3*).

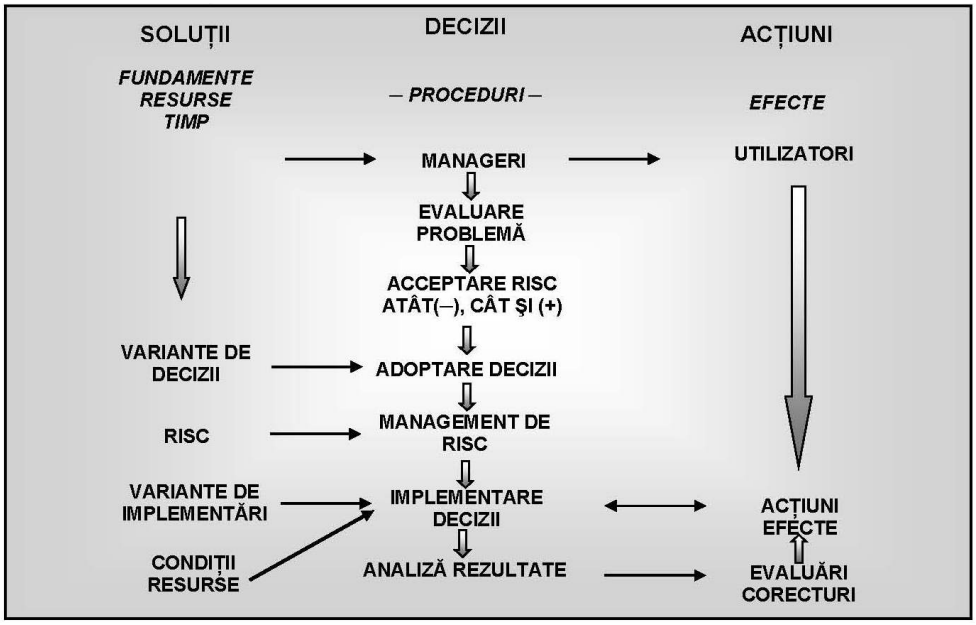


***Fig. 3* – Corelaţiile transformării deciziilor în acţiuni**

Nici organizaţia nu poate avea beneficiu dacă nu-şi asumă riscul costurilor asigurării muncii, după cum nici angajaţii nu pot avea beneficii dacă nu-şi asigură şi ei o parte a costurilor investiţiei pentru acţiune.

Acest lucru se datorează relaţiei dintre risc (**măsură a incertitudinii** acţiunii) şi eficienţă (exprimată prin **beneficiu**). În 1976, Lowrance[2] observă acest lucru, deşi în acea perioadă riscul luat în considerare avea numai cu conotaţie negativă.

Ţinând seama de dubla relevanţă a riscului, observaţia lui Lowrance trebuie completată cu precizarea că pentru o acţiune riscul asumat poate avea conotaţii pozitive (câştig) sau negative (pierderi) şi că acestea trebuie suportate în proporţia stabilită atât de decidenţi, ca şi de cei ce duc acţiunea la îndeplinire.

Fiind vorba de risc şi de mărimea proporţiilor de asumare, comunicarea nu trebuie să fie doar o simplă informare, ci un proces complex de înţelegere, hotărâri prin consens – decizii asumate, cu atât mai mult cu cât valenţele riscului asumat se

[2] Lowrance, W.W, *Of Acceptable Risk: Science and the Determination of Safety*, William Kaufmann, Los Altos, California, 1976.

schimbă de la etapă la etapă, chiar dacă, să presupunem, îşi păstrează aceleaşi valori determinate. De aceea, când se analizează valenţele riscului asumat, trebuie să se ţină seama şi de următoarele elemente dinamice:

– în funcţie de momentul de referinţă, **riscul asumat are valenţe diferite**; un risc de valoare mare este mai greu de guvernat la începutul acţiunii când variabilele au o dinamică mai mare şi, se apreciază că, poate fi guvernat cu mai puţin risc către sfârşitul acţiunii când apar chiar rezultate încurajatoare;

– pentru a aprecia cât mai bine valenţa riscului asumat pentru desfăşurarea acţiunii, valoarea acestuia trebuie comparată cu valoarea riscului asumat pentru situaţia neînceperii acţiunii; acest lucru este valabil şi pentru situaţia variantelor complementare, deci a alternativei;

– pentru a avea o imagine a dinamicii evoluţiei riscului asumat, valoarea curentă a acestuia, r_i, trebuie comparată în permanenţă cu media evoluţiei riscului, m_r, determinându-se astfel un grafic al distribuţiei evoluţiei, dr_i: $dr_i = m_r - r_i$;

– în ideea de a aprecia consistenţa riscului asumat (acesta fiind o sumă de riscuri ponderate), trebuie să se urmărească nu numai evoluţia riscului asumat,

ci şi a componentelor sale: $r_i = \sum_{j=1}^{n} p_j * r_j$, $\sum_{j=1}^{n} p_j = 1$, problema este cu atât mai complicată, cu cât în procesul desfăşurării acţiunii se pot schimba pe lângă valorile de risc şi ponderile acestora (se schimbă atât, r_j cât şi p_j).

În 1991, Haimes[3] aprecia că: „*între calitatea managerială şi eficienţa managementului de risc este o relaţie de corelaţie directă, în sensul că un management al riscului eficient determină o calitate managerială corespunzătoare*”. Mai mult chiar, completându-şi susţinerea, Haimes dezvoltă ideea că optimalitatea managementului de risc nu este o problemă determinată în principal de resurse, ci de înţelegerea procesului supus deciziei, de fundamentarea ştiinţifică a acesteia (determinarea riguroasă a riscului), de atitudinea decidenţilor faţă de risc şi de responsabilitatea organizatorică.

Termenul optimal este gândit în sensul Pareto al ierarhizării acţiunilor, obiectivelor, impactului temporal sau în perspectivă.

Optimalitatea este direct legată şi de natura multidimensională a riscului, multifactorial din punctul de vedere atât al structuralităţii, cât şi al percepţiei atitudinii faţă de risc. În afară de aceasta să reamintim faptul că riscul este măsura incertitudinii, iar incertitudinea ca stare este multidimensională şi dinamică,

[3] Haimes, Y. Y. – *Total risk management*. *Risk Analysis,* 1991.

modelul său de formalizare fiind multivariabil atât în intrare, cât şi ca stări şi în ieşire.

Concluzii

1. Riscul este un indicator analitic, diferit de pericol sau hazard, având atât conotaţii pozitive, cât şi negative.
2. Conceptul de risc nu trebuie opus percepţiei şi experienţei naturale, el trebuie însă să fundamenteze saltul de la a vorbi despre risc, la a-l exploata şi genera, să poată fi concretizat în aplicaţii şi să asigure dezvoltarea metodelor de management şi de guvernare prin risc.
3. Conceptul de risc se bazează pe cunoaştere, acceptanţă, expertiză şi comunicare.
4. Guvernarea riscului sau guvernarea prin risc reprezintă un element de interacţiune socială şi se bazează pe asumare, expertiză şi participare colectivă (de echipă).

BIBLIOGRAFIE

BEDER, T. S., *The great risk bunt: Journal of Portofolio Management:* May issue, 1999.

CIOCOIU, N. C., *Managementul Riscului în afaceri şi proiecte*, Editura A.S.E., Bucureşti, 2006.

GREY, S., *Practical Risk Assessement for Project Management,* John Wilwy & Sons, 1995.

HAIMES, Y. Y., *Total risk management*. *Risk Analysis,* 1991.

HOROBEŢ, A., *Managementul riscului în investiţiile internaţionale*, Editura All Beck, Bucureşti, 2005.

ILIE, GH., *Securitatea mediului de afaceri*, Editura UTI PRESS, Bucureşti, 2006.

ILIE, GH., *De la management la guvernare prin risc,* Editura UTI PRESS şi Editura DETECTIV, Bucureşti, 2009.

LOWRANCE, W.W., *Of Acceptable Risk: Science and the Determination of Safety*, William Kaufmann, Los Altos, California, 1976.

RITCHIE, *B*., *MARSHALL*, *D*., Business Risk Management, *Chapman & Hall*, London, *1993.*

RICHARDS, M.D., *Managerial decision making: a review*, *in Contemporary Management: Issues and Viewpoints*, Editura J. W. McGuire, Prentince Hall, Englewood Cliffs, 1974.

VASILESCU, I. P., Psihologia riscului., Editura Militară, Bucureşti, 1986.

O POSIBILĂ DINAMICĂ A INFRASTRUCTURII STRATEGICE

General de brigadă (r) dr. Gheorghe VĂDUVA

Infrastructura devine din ce în ce mai mult unul dintre domeniile de maximă prioritate ale modului de viață al oamenilor. Evident, ea a fost dintotdeauna importantă, dar, astăzi, mai mult ca ieri, şi mâine, poate, mult mai mult ca azi, infrastructura redefineşte conceptele de geopolitică şi geostrategie, constituindu-se în suporturi esențiale durabile şi foarte consistente ale unei dinamicii de conexiune, dar şi de distorsiune, care identifică şi certifică, unifică şi separă, reliefează şi estompează, consolidează şi modifică. În cadrul acesteia, fiecare stat, continentul european, fiecare entitate care contează în dinamica lumii îşi defineşte şi îşi identifică infrastructura critică sau esențială, de care depinde în mare măsură funcționarea tuturor sistemelor şi proceselor specifice societății omeneşti. Cândva, s-a vorbit de infrastructură şi suprastructură, de bază şi suprastructură etc. Nu contează însă prea mult cuvintele care se folosesc pentru a defini o realitate sau alta, ci realitatea care determină conceptul. Oamenii trăiesc pe un suport de infrastructură pe care încearcă în permanență să-l consolideze, să-l modernizeze şi să-l securizeze. Dependența de infrastructură este atât de mare, încât am putea spune că omul nu mai poate trăi în nici un fel în afara ei. De aceea, o foarte mare parte din efortul oamenilor se centrează şi se concentrează pe dinamica infrastructurii, îndeosebi pe cea a infrastructurii critice sau esențiale. Mai există însă o dimensiune a acestei infrastructuri, care, uneori, este pe nedrept confundată sau identificată sută la sută cu infrastructura critică. Este vorba de infrastructura strategică (IS) şi, în cadrul acesteia, de infrastructura critică strategică (ICS).

Criterii de identificare şi clasificare a IS şi ICS

DIRECTIVA 2008/114/CE A CONSILIULUI din 8 decembrie 2008 privind identificarea şi desemnarea infrastructurilor critice europene şi evaluarea necesității de îmbunătățire a protecției acestora[1] stabileşte, între altele, sfera de cuprindere şi conținutul noțiunii de *infrastructură critică* şi cere statelor membre ale Uniunii Europene să-şi identifice,

[1] *DIRECTIVA 2008/114/CE A CONSILIULUI din 8 decembrie 2008 privind identificarea şi desemnarea infrastructurilor critice europene şi evaluarea necesității de îmbunătățire a protecției acestora*, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:RO:PDF, accesat la 19.04.2010.

până în 2012, infrastructura critică națională (ICN), să contribuie la definirea şi identificarea infrastructurii critice europene (ICE) şi să elaboreze măsurile de protecție a acesteia, în sensul precizărilor acestui document.

Infrastructura critică nu este însă un produs al tuturor şi al nimănui, un dat, adesea un dat uitat, şi cam atât. Ea aparține statelor, unor proprietari publici sau privați şi se află în utilizarea sau în responsabilitatea unor operatori. Desigur, responsabilitatea principală şi finală pentru protecția ICN şi ICE, aşa cum se precizează în directivă, revine statelor şi, respectiv, proprietarilor/operatorilor de infrastructuri. Pentru aceasta, trebuie să fie elaborate şi puse în aplicare aşa-numitele „planuri de securitate pentru operatori (PSO) sau măsuri echivalente care să conțină o identificare a elementelor importante, o evaluare a riscurilor şi identificarea, selectarea şi stabilirea priorităților în ceea ce priveşte contramăsurile şi procedurile”[2].

Infrastructurile au, deci, o importanță colosală pentru viața oamenilor. Ele sunt însă extrem de vulnerabile atât la efectele fenomenelor naturale (cosmice, geofizice, climatice etc.), cât şi, mai ales, la acțiunile ostile şi distructive ale oamenilor. În războaiele din toate timpurile ale oamenilor împotriva oamenilor, primele care au fost vizate (create, construite, folosite sau distruse), în funcție de condițiile concrete ale confruntării, au fost infrastructurile. Oamenii şi-au construit, în timp de pace, case, localități, drumuri şi fortificații, iar în timp de război şi le-au distrus reciproc. Spre exemplu, în timpul războaielor din Iugoslavia, din ultimul deceniu al secolului al XX-lea, părțile şi-au distrus reciproc, în primul rând, casele. Cartierul de locuințe de lângă aeroportul din Sarajevo, ca şi turnul presei, o bijuterie arhitecturală, a fost în întregime ciuruit de gloanțe şi de proiectile. Vilele de pe valea Drinjacei, un afluent al Drinei, au fost aproape în întregime distruse de gloanțe sau de proiectile. Fosta cazarmă a vânătorilor de munte din Han Pijesak, transformată în depozite de alimente, a fost în întregime distrusă de bombardamentele NATO din 1995 asupra armatei lui Radko Mladic, fără să fie atinsă vreo altă clădire din această foarte frumoasă localitate. Şi bombardamentele NATO din 1999 asupra Iugoslaviei au vizat tot infrastructurile critice (clădiri importante, depozite, întreprinderi, rețele, comunicații, poduri etc.). Dintre toate armele cunoscute, doar bomba cu neutroni îşi propunea să nimicească oamenii şi să nu se atingă de infrastructuri. În rest, aproape toate armele create de om au vizat şi vizează distrugerea masivă sau precisă – „chirurgicală” se spune – a infrastructurilor critice şi îndeosebi a celor de importanță strategică.

---

[2] *Ibidem*, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:RO:PDF, accesat la 19.04.2010.

Infrastructurile constituie o condiţie esenţială a vieţii oamenilor. Fac parte din suportul material al civilizaţiei. Sunt mijloace materiale ale securităţii vieţii oamenilor, definesc modul de viaţă al omenirii, fac parte din natura umană, din realitatea umană. Din acest motiv, directiva europeană citată acordă o atenţie specială definirii, identificării şi securităţii acestora.

Directiva consideră că „Proprietarilor/operatorilor ICE ar trebui să li se permită accesul, în special prin intermediul autorităţilor competente din statele membre, la cele mai bune practici şi metodologii în materie de protecţie a infrastructurilor critice”[3]. Ea defineşte infrastructurile critice şi alte noţiuni (concepte) legate de acestea, astfel:

„(a) *infrastructură critică* înseamnă un element, un sistem sau o componentă a acestuia, aflat pe teritoriul statelor membre, care este esenţial pentru menţinerea funcţiilor societale vitale, a sănătăţii, siguranţei, securităţii, bunăstării sociale sau economice a persoanelor, şi a căror perturbare sau distrugere ar avea un impact semnificativ într-un stat membru ca urmare a incapacităţii de a menţine respectivele funcţii;

(b) *infrastructură critică europeană* sau *ICE* înseamnă o infrastructură critică localizată în statele membre, a cărei perturbare sau distrugere ar avea un impact semnificativ asupra a cel puţin două state membre. Importanţa impactului se evaluează din perspectiva criteriilor intersectoriale. Aceasta include efectele ce rezultă din relaţiile intersectoriale de dependenţă de alte tipuri de infrastructuri;

(c) *analiză de risc* înseamnă analizarea scenariilor de ameninţări semnificative, pentru a evalua vulnerabilitatea şi impactul potenţial al perturbării sau al distrugerii infrastructurii critice;

(d) *informaţii sensibile privind protecţia infrastructurilor critice* înseamnă informaţii cu privire la o infrastructură critică ce ar putea fi utilizate, în cazul divulgării, în vederea planificării şi realizării unor acţiuni care să determine perturbarea sau distrugerea instalaţiilor unor infrastructuri critice;

(e) *protecţie* înseamnă orice activitate care are drept scop asigurarea funcţionalităţii, a continuităţii şi a integrităţii infrastructurilor critice pentru a descuraja, diminua şi neutraliza o ameninţare, un risc sau un punct vulnerabil;

(f) *proprietari/operatori de ICE* înseamnă acele entităţi responsabile cu investiţiile într-un anumit element, sistem sau componentă a acestuia, desemnat ca ICE, prin prezenta directivă, şi/sau cu operarea curentă a acestora.

Criteriile intersectoriale pe care le are în vedere directiva sunt următoarele:

[3] *Ibidem*, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri= OJ:L:2008:345:0075:0082:RO:PDF, accesat la 19.04.2010.

(a) *criteriul privind victimele* (evaluat în funcţie de numărul posibil de decese sau vătămări);

(b) *criteriul privind efectele economice* (evaluat în funcţie de importanţa pierderilor economice şi/sau a degradării produselor sau serviciilor; inclusiv eventualele efecte asupra mediului);

(c) *criteriul privind efectul asupra publicului* (evaluat în funcţie de impactul asupra încrederii publicului, suferinţa fizică sau perturbarea vieţii cotidiene, inclusiv pierderea de servicii esenţiale).

În termen de un an de la desemnarea unei infrastructuri drept ICE, fiecare stat membru se asigură că există un PSO sau un echivalent al acestuia şi că acestea sunt revizuite periodic. Acest termen poate fi prelungit, în cazuri excepţionale, cu acordul autorităţii statului membru şi notificând Comisia"[4]. Acestea sunt, în linii generale, infrastructurile critice naţionale şi europene, potrivit viziunii acestui important document.

Ce sunt însă infrastructurile critice strategice (ICS)? Dar infrastructurile strategice (IS)? Are oare rost să vorbim de ICS şi de IS, când procesul de identificare a ICN şi ICE încă nu s-a încheiat? Este vorba de o identificare sau de o reidentificare?

S-ar părea că propunerea de a defini şi identifica IS şi ICS nu este încă de actualitate. În condiţiile în care Uniunea Europeană, statele membre şi, probabil, şi celelalte state, care nu sunt membre ale UE, îşi propun doar să definească, să redefinească şi să identifice ICN şi ICE – operaţiune foarte dificilă şi de durată –, centrarea efortului pe *dimensiunea strategică*, pe cea *operativă* (operaţională) şi pe cea *tactică* a infrastructurii reprezintă un salt peste o etapă sau, în orice caz, forţarea procesului. Noi considerăm că, dimpotrivă, definirea, redefinirea şi identificarea (reidentificarea, actualizarea) infrastructurii strategie şi îndeosebi a infrastructurii critice strategice reprezintă, în orice moment al existenţei societăţii omeneşti, o prioritate.

Printre *criteriile* importante care ar putea fi avute în vedere în definirea, identificarea, configurarea şi clasificarea *infrastructurii strategice* (IS) şi a *infrastructurii critice strategice* (ICS) s-ar situa, în opinia noastră, şi următoarele:

a) modul în care securitatea elementelor de infrastructură condiţionează funcţionarea sistemelor şi proceselor de generare a resurselor;

b) modul în care infrastructura şi securitate ei condiţionează acţiunile şi intervenţiile structurilor de forţă, acţiunile de interes vital, conexiunile de bază şi structura de rezistenţă a infrastructurii esenţiale, îndeosebi a celei critice;

---

[4] *Ibidem*, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:RO:PDF, accesat la 19.04.2010.

c) rolul şi locul pe care-l are infrastructura în gestionarea vulnerabilităţilor, în condiţii de risc extrem;

d) modul în care infrastructura permite conexarea, rutarea şi reconfigurarea fluxului informaţional;

e) modul în care infrastructura permite asamblarea şi buna funcţionare a suporţilor de reţea, a nodurilor de reţea şi reţelelor sistemelor C4I2SR, de care depind acţiunea rapidă, intervenţia promptă şi reacţia oportună;

f) modul în care condiţionează manevra strategică etc.

Există, desigur şi alte criterii, dar aceste considerăm că sunt cele esenţiale. Ele se cer conexate şi analizate împreună, întrucât infrastructura, chiar dacă este elementul cel mai puţin flexibil al mediului uman de viaţă, nu poate fi privită şi tratată cu rigiditate.

Configuraţia IS şi ICS

Infrastructura critică are cel puţin o triplă configuraţie:

- ca structură cu valoare materială, concentrată în „nuclee grele", care ancorează şi arondează sistemele şi procesele la o reţea de conexiuni intrinseci, în general, bine definită şi durabilă, cu funcţii de securitate şi stabilitate;
- ca element material al unui proces dinamic, cu efecte substanţiale de mişcare şi de transformare, ea însăţi fiind transformabilă;
- ca suport emergent al dezvoltării durabile.

Cea de a treia configuraţie are un semnificativ rol de suport generativ, iar procesul de generare urmează o linie complicată, stabilită de un decident, îndeosebi de un decident politic. Cu alte cuvinte, infrastructura strategică (IS), mai ales în componenta sa esenţială (critică), ICS, în anumite elemente şi structuri ale configuraţiei sale, cere un concept politic şi, ca atare, o decizie politică. Politicul intervine în configurarea şi dinamica IS (ICS) şi, de aici şi din această cauză, se conturează foarte multe relaţii şi determinări în paradox.

Dacă lucrurile stau aşa, rezultă o construcţie complicată, cu geometrie flexibilă, pe toate nivelurile de securitate şi apărare – politic, strategic, operativ şi tactic – în care IS şi îndeosebi ICS pot avea, pe de o parte, valori şi implicaţii speciale (politice, strategice, operative şi tactice) şi, pe de altă parte, evoluţii imprevizibile. Acestea pot fi denumite, infrastructuri strategice şi, respectiv, infrastructuri critice strategice (ICS). Acestea din urmă au şi valoare operativă (operaţională) (ICO) şi tactică (ICT).

Desigur, nu toată infrastructura strategică este şi critică. Nici toată infrastructura critică nu are valoare strategică, chiar dacă este destul de greu să operăm clasificări categorice. De exemplu, Transfăgărăşanul are importanţă strategică, face deci parte din IS, dar nu şi din infrastructura critică. Însă, în

anumite condiţii, Transfăgărăşanul poate deveni un element al infrastructurii critice naţionale (ICN), al infrastructurii critice europene (dacă peste Munţii Făgăraş va trece o conductă de transport energetic, spre exemplu) şi chiar al infrastructurii critice strategice (ICS).

Cele spuse mai sunt nu sunt nici jocuri de cuvinte, nici asocieri întâmplătoare, ci doar sugestii pentru o evaluare realistă şi serioasă, din perspective economice, politice, sociale, informaţionale, culturale şi militare, a tuturor componentelor infrastructurii, în funcţie de realitatea şi dinamica mediului de securitate naţional, regional, european şi internaţional.

Printre principalele IS şi ICS din care se identifică, se configurează, se gestionează şi se dezvoltă cele cu valori şi funcţii operaţionale şi tactice, se situează, în opinia noastră şi următoarele:

- reţelele de comunicaţii speciale sau anumite componente ale acestora;
- reţelele de comunicaţii strategice ale armatei;
- o anumită structură (cu elemente fixe şi variabile) din cadrul reţelei naţionale de telecomunicaţii;
- aerodromuri militare şi anumite aerodromuri civile;
- reţea de drumuri selectate din reţeaua naţională de drumuri, precum şi din cea europeană;
- reţea de căi ferate din cadrul reţelei naţionale CFR sau anumite tronsoane ale acesteia, în funcţie de situaţia concretă sau de evaluările care se fac pe această temă;
- anumite domenii de infrastructură din reţelele de telefonie mobilă;
- reţelele de calculatoare ale structurilor de acţiune, de intervenţie şi de reacţii rapide;
- reţelele energetice principale;
- reţelele energetice care asigură resursele necesare pentru intervenţia oportună şi reacţia rapidă;
- reţelele de infrastructuri ale instituţiilor de forţă etc.

Toată această enumerare nu spune mare lucru. La urma urmei, este normal ca toate acestea să facă parte din infrastructura strategică şi chiar din infrastructura critică, să fie, adică, infrastructuri critice, pe toate nivelurile de securitate şi apărare – politic, strategice, operativ şi tactic –, întrucât de calitatea şi funcţionalitatea lor depind securitatea (protecţia, siguranţa, apărarea) comunităţilor, a sistemelor şi, în ultimă instanţă, securitatea (protecţia, siguranţa, apărarea) vieţii oamenilor. Dincolo de acest adevăr cunoscut de toată lumea, intervin anumite principii şi caracteristici ale filosofiei şi fizionomiei IS şi IC şi îndeosebi a celei critice strategice m(ICS).

După opinia noastră, principiile care stau la baza configurării dinamice a IS şi ICS, dar şi a ICO şi ICT, sunt următoarele:

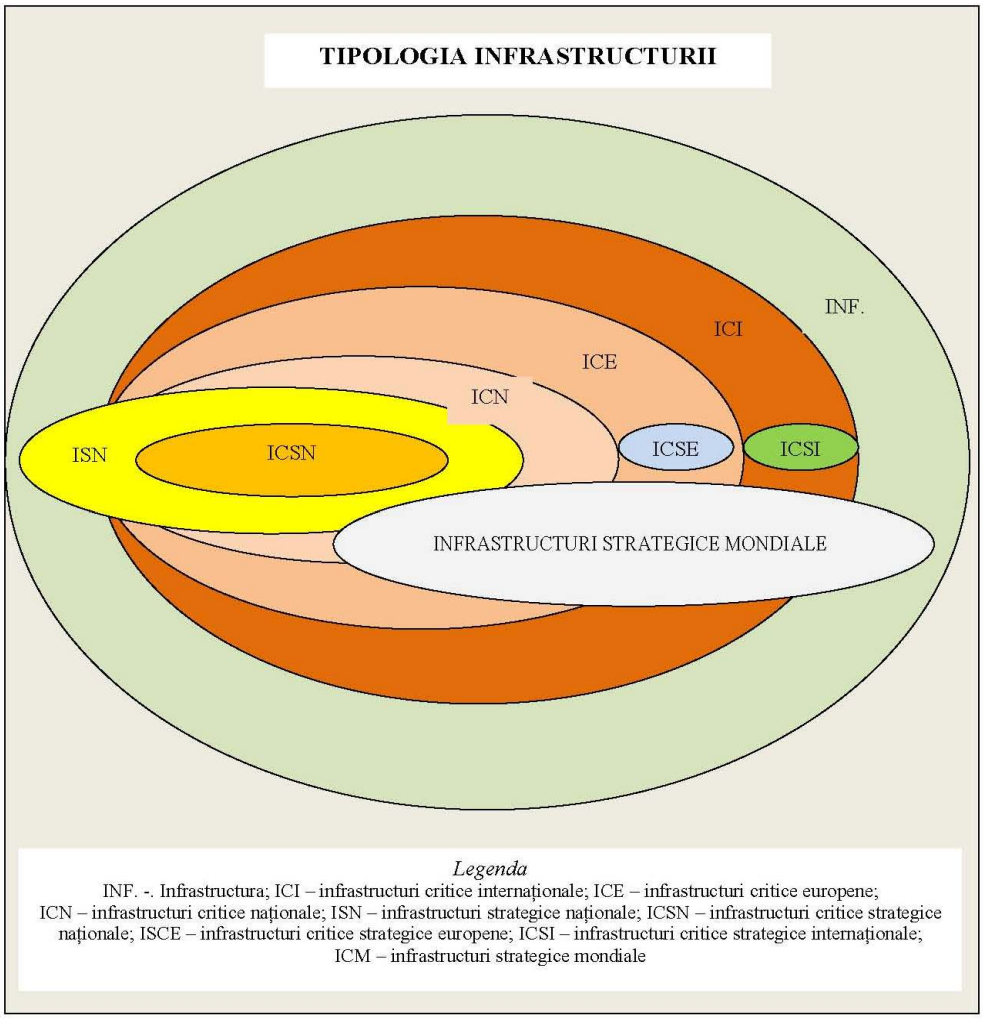
- selectivitatea;
- adaptabilitatea;
- rapiditatea
- complementaritatea;
- continuitatea;
- unicitatea;
- interoperabilitatea;
- integralitatea.

Ele se aplică atât de responsabilul (decidentul) politic (parlamente, guverne, preşedinţii), cât şi de responsabilul (decidentul) strategic, operativ şi tactic (structuri destinate să pună în operă decizia politică mai ales în ceea ce priveşte situaţiile-limită şi să-i asigure acesteia expertiza strategică, operativă şi tactică necesară), ţinându-se seama de o serie de caracteristici ale acesteia, inclusiv de caracteristici ale IS, ICS, ICO şi ICT. Celemai importante dintre aceste caracteristici considerăm că sunt următoarele:

- interdependenţa necesară şi reală;
- derivabilitatea;
- clasificarea;
- suport material pentru controlul riscului extrem;
- vulnerabilitatea indusă.

Există, desigur, şi alte caracteristici, întrucât, totdeauna, infrastructurile (strategice, critice şi critice strategice) – la toate nivelurile – au o dinamică specială, iar identificarea şi conexarea lor în sisteme de IS, de ICS sau chiar în sisteme de sisteme este complexă şi complicată, putând induce elemente de subiectivitate, omisiuni sau neînţelegeri ale interdeterminărilor. Acest lucru ar putea aduce prejudicii grave planului strategic, întrucât IS şi ICS nu pot fi reduse la o serie de străzi deteriorare, la nişte drumuri uitate sau la nişte linii telefonice pe stâlpi de lemn sau la interesele unor firme şi grupuri care exercită, de regulă, tot felul de presiuni asupra decidenţilor…

O posibilă schemă de definire, identificare şi corelare a dimensiunilor naţionale, europene şi strategice a infrastructurii se prezintă în schema de mai jos:



Aşadar, infrastructurile fac parte din ceea putem numi suportul material al unei civilizaţii. Ele sunt, deopotrivă, efecte ale unei activităţi omeneşti precise, menite să producă alte efecte, de ordinul doi sau chiar de ordinul trei, dar şi cauze-suport ale unor dezvoltări care se doresc a fi precise şi foarte consistente. Infrastructurile reprezintă natura umană materială a planetei şi, în acelaşi timp, sinteza sau interfaţa dintre om şi planetă, „ajustări” ale naturii, forma prin care

omul poate trăi pe planeta Pământ, adică forma şi formula infrastructurală care-l protejează şi îl propulsează. Protagoras spunea – exprimând prin aceasta esenţa gândirii înţelepte a sofiştilor – că *omul este măsura tuturor lucrurilor; a celor care sunt pentru că există şi a celor ce nu sunt pentru că nu există*. Omul este o fiinţă specială care îşi creează propriul mediu de viaţă, consonant cu cel natural sau disonant cu acesta, chiar conflictual cu natura naturii. Omul de azi, mai mult decât cel de ieri, are nevoie nu doar de o casă care să-l adăpostească, să-l protejeze şi să-l apere, ci şi de o autostradă pe care să circule cu maşina spre alte orizonturi, de o reţea de comunicaţii, prin care să comunice la distanţă cu un alt om, de alte case care, împreună cu casa lui, să formeze o localitate, de o reţea electrică prin care să aibă acces la energie şi la lumină şi de toate celelalte derivate infrastructurale din aceste infrastructuri primare. Casa asigură securitate omului, în măsura în care şi omul asigură securitate propriei sale case, dar şi caselor din jurul casei sale. Această relaţie de condiţionare simplă, în cerc, constituie, de fapt, suportul unei spirale care tinde spre infinit.

Infrastructurile nu sunt simple anexe ale vieţii omului, ci ele însele fac parte dintr-un *modus vivendi*. Sunt un *modus vivendi*. Ele reprezintă chiar forţa materială a acestui mod de a trăi. Securitatea lor înseamnă rezistenţă la factori distructivi – cutremure, inundaţii, alte fenomene geofizice, geoclimatice şi cosmice, degradare în timp etc. – şi la acţiunile distructive efectuate chiar de cel care le-a creat, adică de om.

Aceste acţiuni şi presiuni concentrate şi, în acelaşi timp, dispersate asupra infrastructurilor constituie, după părerea noastră, unul dintre marile paradoxuri ale civilizaţiei actuale, dar, aşa cum se ştie, şi paradoxurile fac parte din sistem.

Necesitatea securităţii şi securizării infrastructurilor critice rezultă din necesitatea de securitate a omului. Pentru că omul a fost, este şi, probabil, aşa va fi mereu, cea mai puternică (prin forţa şi calitatea de conexiune), cea mai dinamică (prin activitatea productivă şi creativă neîntreruptă) şi cea mai vulnerabilă fiinţă de pe pământ.

Provocări, sfidări, pericole şi ameninţări (PSPA) la adresa infrastructurilor critice strategice. Vulnerabilităţi. Riscuri. Risc extrem

Războaiele din spaţiul fostei Iugoslavii nu au fost numai lanţuri şi înlănţuiri de lupte între secesionişti şi federalişti sau între secesionişti şi secesionişti, ci şi războaie împotriva infrastructurilor. Locuitorii din zona Balcanilor, ca şi cei din zona Carpaţilor, au un cult al casei-familie, al casei complete, al casei durabile, al casei-adăpost, al casei-de-o-viaţă. Iar unul dinte obiectivele atacurilor a fost acela de a distruge case, cât mai multe case. Bombele atomice lansate în 1945 asupra oraşelor japoneze Hiroshima şi Nagasaki au distrus, deopotrivă infrastructuri şi

oameni – ca orice armă de nimicire în masă –, iar statele, organizaţiile internaţionale şi regionale şi oamenii nu s-au gândit prea mult la efecte, ci au continuat să-şi dezvolte, într-o continuă şi accelerată cursă a înarmărilor, mijloacele de distrugere a infrastructurilor şi de nimicire a oamenilor. Într-un târziu, s-a inventat bomba cu neutroni, menită să lase intacte infrastructurile, inclusiv mijloacele de luptă, şi să nimicească doar forţa vie. Războaiele ulterioare şi dezvoltările ulterioare care, în spaţiul conceptelor şi în cel al acţiunilor, au readus în prim plan problema distrugerii, într-o confruntare armată şi nu numai armată, a infrastructurii adversarului.

La ora actuală există, în opinia noastră, următoarele tipuri de provocări, sfidări, pericole şi ameninţări la adresa infrastructurilor de tot felul şi îndeosebi a infrastructurilor critice strategice: de natură cosmică; de natură geofizică şi climaterică; de natură umană.

Tip PSPA	Denumirea PSPA	Infrastructuri vizate	Probabilitate de producere	Posibile soluţii
Cosmice	Căderi de meteoriţi şi de alte corpuri cereşti	Localităţi, reţele de transport, reţele de comunicaţii, reţele energetice etc.	Foarte scăzută	Structuri de reţea care să permită rutarea
	Ciocniri cu corpuri cereşti	Toate infrastructurile	Foarte scăzută	Studierea acestei posibilităţi şi evaluarea impactului
	Radiaţie solară şi cosmică	Infrastructuri de comunicaţii; Infrastructuri IT; Infrastructuri de siguranţă şi securitate a ICS	Medie	Studierea comportamentului ionosferei; Sisteme de anihilare şi de neutralizare a radiaţiei solare şi cosmice
	Magnetism cosmic	Infrastructurile IT şi de comunicaţii; Alte infrastructuri sensibile la magnetismul cosmic	Medie	Crearea unor sisteme de protecţie a ICS împotriva efectelor nocive ale magnetismului cosmic
	Variaţii în ciclul solar	Localităţi, comunicaţii, reţele, reţele IT	Frecventă	Sisteme de protecţie împotriva radiaţiei solare

Tip PSPA	Denumirea PSPA	Infrastructuri vizate	Probabilitate de producere	Posibile soluţii
Geofizice	Cutremure	Localităţi, infrastructuri rutiere, feroviare, portuare, ale transportului aerian etc., reţele IT şi de comunicaţii etc.	Frecventă	Măsuri antiseismice, studierea fenomenului, sisteme de înştiinţare-alarmare performante etc.
	Erupţii vulcanice	Toate infrastructurile din zona	Foarte scăzută	Măsuri de protecţie la posibile erupţii vulcanice
	Efecte nocive ale magnetismului terestru	Infrastructurile IT	Frecventă	Măsuri de protecţie; formarea unei culturi
	Lunecări masive de teren	Locuinţe, reţele, comunicaţii, infrastructuri de producţie, de transport, de protecţie şi de securitate	Frecvente în zone cu activităţi miniere, în zone petrolifere etc.	Analiza factorilor de risc, lucrări de consolidare şi de protecţie a mediului
	Alte fenomene geofizice periculoase	Toate infrastructurile	Din ce în ce mai frecvente	Măsuri specifice
Climatice	Inundaţii, revărsări	Locuinţe, localităţi, infrastructuri feroviare şi rutiere, toate infrastructurile din aceste zone	Frecvente (de câteva ori pe an)	Analiză de risc extrem, îndiguiri, împăduriri, măsuri de echilibrare ecologică
	Furtuni, uragane	Locuinţe, localităţi, infrastructuri energetice, alte infrastructuri	Din ce în ce mai frecvente	
	Incendii produse de cicluri solare sau de încălzirea excesivă a planatei	Păduri şi infrastructurile legate de acestea sau din vecinătatea acestora, dar şi localităţi, reţele şi alte infrastructuri	Rare, dar posibile	Măsuri de protecţie a pădurilor şi de intervenţia rapidă pentru stingerea incendiilor de proporţii
Produse de oameni	Atacuri sau accidente cu arme, chimice, biologice, radiologice şi chiar nucleare	Toate infrastructurile din zonele respective, cu efect pe termen lung	Posibile, dar puţin probabile	Securizarea bazelor şi a infrastructurilor vizate
	Acţiuni teroriste	Infrastructurile de securitate, îndeosebi ICS, dar şi infrastructurile publice etc.	Diversificate şi frecvente	Măsuri de securitate a infrastructurilor, îndeosebi a ICS

Tip PSPA	Denumirea PSPA	Infrastructuri vizate	Probabilitate de producere	Posibile soluţii
Produse de oameni	Războaie frontaliere sau conflicte militare	Toate infrastructurile din zonă	Frecvente	Prevenirea războaielor
	Acţiuni împotriva unor infrastructuri, generate de efectele de falie	Toate infrastructurile din zona acestor efecte	Frecvente	Ameliorarea condiţiei umane
	Accidente tehnologice şi industriale	Toate infrastructurile, îndeosebi pe cele critice	Frecvente	Management cât mai corect
	Criminalitate violentă cu distrugeri de infrastructuri	Locuinţe, locuri publice	Frecvente	Securitate publică
	Trafic ilegal de arme, droguri şi persoane care afectează infrastructurile	Afectează infrastructurile în zonele în care sunt folosite	Frecvente	Securitate de reţea, transfrontalieră şi publică
	Atacul conductelor de petrol şi a altor instalaţii, cu efecte foarte mari etc.	Infrastructurile energetice	Frecvente	Securitatea reţelelor energetice

Strategii de protecţie, securitate şi apărare (SPSA) a infrastructurilor strategice (IS) şi infrastructurilor critice strategice (ICS)

Strategia sau strategiile de protecţie a infrastructurilor de tot felul şi îndeosebi a celor strategice (IS) şi a celor critice strategice (ICS) pot fi definite ca ansambluri coerente şi consistente, permanente şi interactive, de teorii, practici, experienţe, priceperi, abilităţi, resurse, capabilităţi manageriale, capacităţi logistice şi posibilităţi creative de a pune în aplicare decizii politice cu privire la clasificarea, asamblarea, protecţia, securitatea şi apărarea infrastructurilor critice strategice, de a genera doctrine, concepte şi acţiuni eficiente care să ducă la îndeplinirea acestui obiectiv de mare importanţă.

Protecţia, securitatea şi apărarea infrastructurilor strategice (IS) şi, îndeosebi, a infrastructurilor critice strategice (ICS) reprezintă un domeniu prioritar al tuturor statelor, organizaţiilor şi organismelor internaţionale. Evident, un astfel de obiectiv nu se poate realiza decât prin colaborare, cooperare şi parteneriat, prin interdisclinaritate şi acţiuni comune, de mare amploare, care, la rândul lor, permit elaborarea unor acţiuni tactice concrete, chiar punctuale.

O posibilă structură a politicilor, strategiilor, operaţiilor şi acţiunilor de protecţie, securitate şi apărare a infrastructurilor critice strategice, pe niveluri, ar putea fi următoarea:

NIVEL	STRUCTURI	COMPETENŢE	
		Formă	Conţinut
Politic	Preşedinte	Decizie, decretare	Executare, coordonare, mediere, asamblare
	Parlament	Decizie, validare	Legiferare, generare legislativă
	Guvern	Execuţie	Executare, iniţiere, generare
Juridic	Justiţie	Legalizare, legitimare	Supraveghere a aplicării legii
Politico-militar	CSAT	Politico-militară	Generare şi expertiză politici militare
Strategic	Statul Major General	Execuţie, generare	Strategii generative, expertiză
	Comandamentul strategic	Execuţie, aplicare	Strategii generative şi aplicative
	Statele Majore ale categoriilor de forţe	Execuţie, generare, aplicare	Doctrine generative
	ISU	Execuţie, generare, aplicare	Doctrine generative
	IGP	Execuţie, generare, aplicare	Doctrine generative
	CNJ	Execuţie, generare, aplicare	Doctrine generative
	IGPF	Execuţie, generare, aplicare	Doctrine generative
Operativ	Comandamentele operaţionale	Aplicative	Generare operaţii
	Structuri operative similare de la MAI	Aplicative	Generare operaţii şi operaţiuni
Tactic	Mari unităţi şi unităţi ale armatei	Aplicative	Acţiuni tactice
	Structuri şi formaţiuni ISU	Aplicative	Acţiuni tactice
	Pompieri	Aplicative	Acţiuni tactice
	Mari unităţi şi unităţi de jandarmi	Aplicative	Acţiuni tactice
	Structuri (formaţiuni) de poliţie	Aplicative	Acţiuni tactice
	Servicii de informaţii	Aplicative	Acţiuni tactice

În general, infrastructurile strategice şi infrastructurile critice strategice par uşor de definit şi de identificat. La urma urmei, ele sunt concepute, planificate şi realizate în funcţie de cerinţe şi de necesităţi. Fiecare stat îşi defineşte, îşi protejează, îşi securizează şi îşi apără infrastructurile strategice şi infrastructurile critice strategice, în funcţie de realităţile naţionale, regionale şi globale, de valorile şi de interesele sale. Aici, se pare că nu sunt prea multe de spus. Şi totuşi, există un dinamism şi în cazul infrastructurilor critice. Şi ele cresc şi descresc, în funcţie de o mulţime de factori interni sau externi, cu frecvenţă mare de manifestare sau aleatori, cu configuraţii şi intensităţi variabile. O cale ferată care nu este folosită şi întreţinută se deteriorează, autostrăzile prea intens circulate necesită, pe porţiuni mari, reparaţii frecvente etc. IS şi ICS sunt acele şi numai acele elemente de importanţă strategică ale infrastructurii şi, respectiv, acea infrastructură critică absolut necesară forţelor şi mijloacelor de acţiune, intervenţie sau reacţie de tip rapid. Ele se conexează cu ICO şi ICT şi, toate, împreună, asigură condiţii pentru acţiuni şi reacţii corespunzătoare, la toate nivelurile, în urgenţe şi, mai ales, în cele care impun riscul extrem. Spre exemplu, nu întreaga reţea de aprovizionare cu energie electrică alcătuieşte infrastructura critică strategică (ICS), ci doar acea parte care include acele componente (economice, informaţionale, militare etc.) care aprovizionează acele structuri ce au menirea să pună imediat în aplicare o decizie politică majoră cu privire la securitatea şi apărarea naţională.

Strategia care priveşte infrastructurile strategice (SIS) şi infrastructurile critice strategice (SICS) poate fi definită ca teorie, experienţă, practică, abilitate şi artă menită să pună în operă decizii politice cu privire la natura, structura, dinamica, dezvoltarea, transformarea, protecţia, securitatea şi apărarea infrastructurilor critice strategice, la identificarea, analizarea şi contracararea provocărilor, sfidărilor, pericolelor şi ameninţărilor la adresa acestora, la reducerea vulnerabilităţilor specifice, la definirea, asumarea şi gestionara riscului, inclusiv în dimensiunea sa majoră şi chiar extremă.

În general, infrastructurile strategice şi infrastructurile critice strategice sunt infrastructuri de risc extrem şi, de aceea, peste tot în lume, li se acordă o atenţie cu totul specială. Într-un anume sens, strategia IS şi strategia ICS fac parte din marea strategie, din strategia integrală sau din strategia totală, constituindu-se într-un fel de strategie de strategii sau de metastrategie. Dincolo de jocul de cuvinte sau de relaţionarea teoretică şi metodologică a modalităţilor de punere în operă a unei decizii politice cu privire la infrastructurile critice strategice, strategia infrastructurilor strategice şi infrastructurilor critice strategice ar putea avea următorul conţinut:

Strategii ale forţelor ICS

- Strategia forţelor generatoare de ICS – SFGICS;
- Strategia forţelor gestionare de ICS, ICO şi ICT – SFGsICS, SFGsICO, SFGsICT;
- Strategia forţelor care deservesc ICS – SFDICS;
- Strategia forţelor de acţiune, protecţie, securitate şi apărare a ICS (exogene, endogene) – SFPSAICS.

Strategii ale mijloacelor ICS

- Strategia mijloacelor fixe – SMFICS;
- Strategia mijloacelor mobile – SMMICS;
- Strategia mijloacelor conexe – SMCICS;
- Strategia mijloacelor de protecţie, de securitate şi de apărare – SMPSAICS.

Strategii ale resurselor ICS

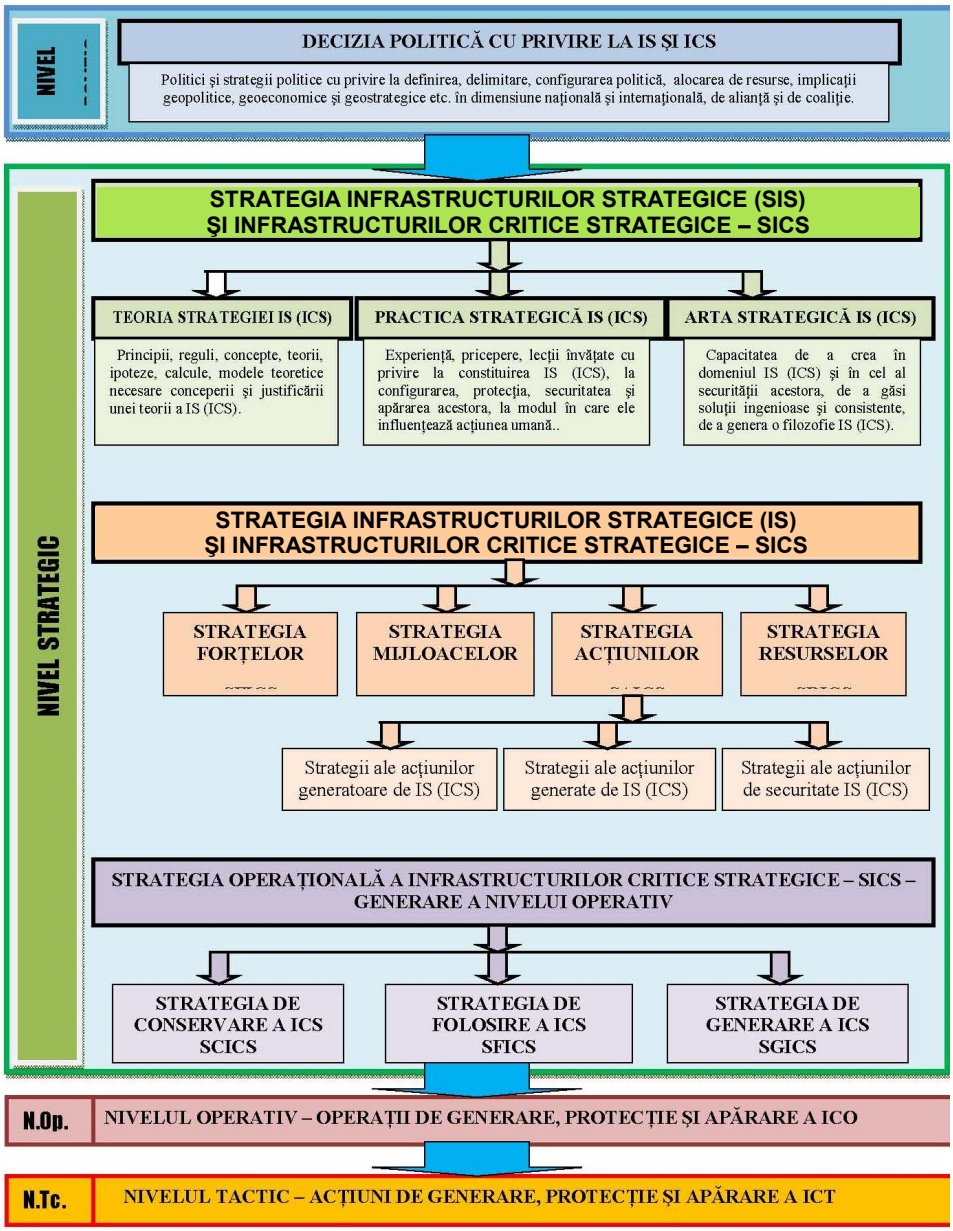
- Strategia resurselor generative – SRGICS;
- Strategii ale resurselor productive – SRPICS;
- Strategii ale resurselor de protecţie, securitate şi apărare – SRPSAICS.

Strategii ale acţiunilor (operaţiilor) ICS

- Strategia acţiunilor implicite;
- Strategii ale acţiunilor conexe;
- Strategii ale acţiunilor dinamice;
- Strategii ale acţiunilor indirecte.

Toate aceste tipuri de strategii trebuie să fie constituite în aşa fel încât să asigure corelarea principiilor cu realităţile, posibilităţile cu resursele.

Niveluri ale politicii, strategiei, artei operative şi tacticii domeniului infrastructurilor strategice (IS) şi infrastructurilor critice strategice (ICS)



Concluzii

1. Actualele preocupări ale Uniunii Europene şi ale altor state este să definească precis infrastructurile critice naţionale ICN şi europene ICE şi, în raport cu concluziile care se vor desprinde de aici, să elaboreze temeinice măsuri de securitate acestora. Este necesar să se procedeze astfel, întrucât ICN şi ICE au devenit deosebit de vulnerabile, iar securitatea şi apărarea lor reclamă imperios o dimensiune europeană. Faptul că IC sunt din ce în ce mai mult transfrontaliere creează nu numai dependenţe şi interdependenţe, ci şi un nou orizont de risc, de risc major şi, în anumite situaţii, chiar de risc extrem, care necesită o abordare specială, multidisciplinară şi complexă. De asemenea o astfel de realitate condiţionează substanţial şi redefinirea infrastructurii strategice.

2. Dar această abordare europeană – care se anunţă destul de consistentă, de necesară şi de urgentă – nu este, în opinia noastră şi suficientă. Foarte multe infrastructuri strategice devin interdependente, atât cele energetice, cele de transport rutier, maritim, fluvial şi aerian, cât şi cele care scapă percepţiei directe, dar nu sunt cu nimic mai prejos decât acestea (este vorba de infrastructurile critice din reţelele virtuale, dar nu numai). De fapt, cvasitotalitatea infrastructurilor naţionale şi europene sunt, într-o forma sau alta, interconectate şi, în mare măsură interdependente. Dar numai unele dintre acestea au valoare strategică. Identificarea, evaluarea şi configurarea lor, ca şi cunoaşterea şi înţelegerea modului de conexare şi de interdependenţă în plan strategic devin şi ele, la rândul lor, necesare, complexe, problematice şi greu soluţionabile.

3. Identificarea, configurarea şi securizarea (după principii şi criterii care se cer foarte bine elaborate) a infrastructurilor critice strategice devin puncte obligatorii de trecere spre dimensiunile operaţionale şi acţionale, care modelează atitudinea faţă de evoluţia anumitor componente ale mediului internaţional şi naţional de securitate spre asumarea unui risc major şi chiar a unui risc extrem.

BIBLIOGRAFIE

DIRECTIVA 2008/114/CE A CONSILIULUI din 8 decembrie 2008 privind identificarea şi desemnarea infrastructurilor critice europene şi evaluarea necesităţii de îmbunătăţire a protecţiei acestora, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:RO:PDF

Esperanza Lopez-Vasquez, *Perception du risque, stress et stratégies d'ajustement des sujets en situation de risque de catastrophe naturelle ou industrielle – Approche d'une psychologie sociale du risque,* Editeur ANRT, 2006.

Criza, conflictul, războiul, vol. I-IV, Editura Universităţii Naţionale de Apărare "Carol I", Bucureşti 2007.

Teodor Frunzeti, Mircea Mureşan, Gheorghe Văduva, *Război şi haos,* Editura CTEA, Bucureşti, 2009.

CONCEPTUL INTEGRONIC AL SECURITĂȚII INFRASTRUCTURII CRITICE (IC)

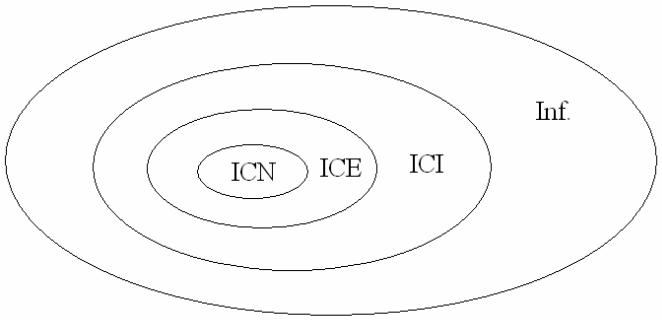
Colonel (r) prof. univ. dr. Eugen SITEANU
General de brigadă (r) prof. univ. dr. Gheorghe ILIE

În directiva 2008/114/CE a Consiliului UE din 8 decembrie 2008 se precizează că programul european privind protecția infrastructurilor critice (PEPIC) trebuie să se bazeze pe o abordare care să acopere toate riscurile, acordând prioritate amenințării teroriste[1]*. Directiva se referă la două sectoare ale infrastructurii critice (IC): energetic şi transporturi (rutiere, aeriene, maritime, fluviale şi căi ferate), dar, evident, acestea sunt în realitate mai multe: tehnologia informației şi comunicațiilor, radio, TV, internet etc. Din infrastructurile critice (IC) fac parte instalațiile infrastructurilor critice (IIC), sistemele, subsistemele etc.*

IC reprezintă unele elemente, unele sisteme (de exemplu instalații) sau componente ale lor, care sunt esențiale pentru menținerea funcțiilor societale vitale, a sănătății, siguranței, securității, bunăstării sociale sau economice a persoanelor şi a căror perturbare (defectare/deteriorare) sau distrugere ar avea un impact semnificativ într-un stat din cauza incapacității de a menține funcțiile respective. IC se pot clasifica în mai multe categorii: infrastructuri critice naționale (ICN), infrastructură critică europeană (ICE) şi infrastructura critică internațională (ICI) (figura 1).

[1] http://eur-lex.europa.ri/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:RO:PDF

Planul de securitate pentru operatori (PSO) identifică elemente de infrastructură critică (IC) şi soluţiile de securitate existente sau puse în aplicare pentru protecţia acestora.



Legenda
Inf. – Infrastructuri;
ICN – Infrastructuri critice naţionale;
ICE – Infrastructura critică europeană;
ICI - Infrastructura critică internaţională.

Figura 1. Tipuri de infrastructuri critice

Din analiza realizării infrastructurilor critice din orice ţară rezultă că acestea satisfac anumite cerinţe în condiţii specificate sau pot reprezenta totodată şi mijloace active pentru îndeplinirea unor obiective previzionate.

Dar, în procesul realizării obiectivului stabilit apare un decalaj între cerinţele impuse şi rezultatele obţinute în practică, care este cu atât mai mare cu cât trece mai mult timp între momentul stabilirii obiectivelor şi cel al obţinerii rezultatelor. Acest decalaj este o consecinţă de cognoscibilitate, tehnologie şi de timp şi determină comportări/funcţionări imprevizibile şi chiar periculoase ale infrastructurii critice atunci când apar factori perturbatori, care declanşează unele degajări/emanări energetice nedorite afectând siguranţa/securitatea nu numai a personalului de exploatare şi mentenanţă al infrastructurii respective, ci şi a altor persoane aflate în zona de risc.

În consecinţă, este necesară abordarea specială a securităţii infrastructurii critice nu numai pe baza tehnicilor de fiabilitate şi viabilitate, ci şi a unor metode corespunzătoare caracterului integronic al conceptului securităţii.

Securitatea IC (Sc) este atât o problemă socială, cât şi una funcţională. Această afirmaţie decurge din pagubele materiale produse de lipsa de securitate a IC şi din implicaţiile sustragerii, denaturării şi disimulării informaţiilor aferente acesteia. De aici rezultă că problema securităţii IC este esenţială pentru societate şi pentru instituţiile statului, oricare ar fi acesta, deoarece scopul realizării IC nu e obţinerea unei structuri în sine, ci acela de a proba în orice condiţii relaţional-poziţionale o capacitate operaţională ridicată de realizare a efectelor economico-sociale prestabilite (previzionate).

Capacitatea operaţională (Co) a IC reprezintă proprietatea acesteia de a-şi îndeplini scopul/obiectivul stabilit în anumite condiţii specificate[2]. Aşadar, IC nu poate fi desprinsă de mediul în care funcţionează şi nu poate fi apreciată în afara destinaţiei sale, ci numai în strânsă legătură cu parametrii funcţionali ai acesteia şi cu caracteristicile ei de fiabilitate, viabilitate şi securitate deoarece operativitatea IC a devenit o problemă vitală de securitate.

Ca urmare, IC trebuie să îndeplinească câteva cerinţe:

1. continuitatea conducerii (managementului) pentru a asigura raţionalitatea acţiunilor;
2. desfăşurarea în confidenţialitate a acţiunilor, pentru a-i preîntâmpina destabilizările sau acţiunile teroriste;
3. unitatea informaţională, pentru păstrarea caracterului unitar şi omogen al legăturilor şi fluxurilor informaţionale de conducere şi execuţie;
4. flexibilitatea funcţională de comportament şi a reglajelor, pentru a preîntâmpina discontinuităţi funcţionale şi a le asigura dinamica, autoreglajul, adaptabilitatea, viabilitatea, logica sistemică a IC şi componenţa necesară îndeplinirii misiunilor în securitate.

Aceste cerinţe impun cu stringenţă folosirea unor subsisteme şi sisteme de mare fiabilitate, care să funcţioneze şi în condiţii de excepţie, existenţa unor rezerve umane, informaţionale şi organizatorico-funcţionale pentru reconfigurare fizică şi parametrică, a unor mecanisme, tehnici şi măsuri speciale pentru a face faţă acţiunilor cu efecte periculoase (explozii, dezintegrări, degajări energetice, blocaje sau disfuncţiuni etc.), ceea ce determină pentru IC un comportament tolerant la acţiuni perturbatoare, nuanţat, în funcţie de un anumit risc raţional asumat (R) şi de preţul de cost posibil a fi suportat (C).

Fiabilitatea (F) este, în opinia unor autori[3], capacitatea unui sistem, în particular a IC, de a-şi îndeplini în mod corect funcţiunile, la un anumit moment sau într-o perioadă de timp dată, dacă este folosit în condiţiile pentru care a fost realizat şi este întreţinut şi reparat corespunzător.

Din această definiţie se înţelege că fiabilitatea (figura 2) are două componente: siguranţa în funcţionare (S) şi mentenanţa (M), care, la rândul lor, depind de proprietăţile tehnologico-constructive şi de elementele de rezervare funcţională, precum şi de măsurile tehnico-organizatorice pentru restabilirea disponibilităţii sistemului.

---

[2] SITEANU Eugen, BEDROS Naianu, ILIE Gheorghe, *Fiabilitatea produselor tehnice*, Editura AISTEDA, Bucureşti, 2009, p. 123.
[3] Ibidem, p. 125.

FIABILITATEA	
Siguranţa în funcţionare (S)	Mentenanţa (M)

Figura nr. 2. Componentele fiabilităţii (F) infrastructurii critice

Această dependenţă se poate exprima simbolic astfel: F=S+M (1)

Pe de altă parte, fiabilitatea infrastructurii critice reprezintă efectul unui complex întreg de factori a căror influenţă se regăseşte atât în cadrul sistemelor componente, cât şi în interdependenţa dintre acestea. La rândul său, fiabilitatea poate impune modificări structurale intime ale unor (sub)sisteme sau schimbarea condiţiilor de funcţionare pentru altele. De aceea, fiabilitatea trebuie abordată având în vedere toate aspectele, conexiunile, cauzele, factorii, efectele şi comportarea (sub)sistemelor, precum şi interacţiunile dintre acestea.

Din relaţia (1) şi din caracteristicile abordării sistemice a fiabilităţii, se poate scrie:

$$F = \sum_{i=1}^{k} p_i \cdot F_i + F', \qquad (2)$$

unde: F = fiabilitatea infrastructurii critice (IC);

k – numărul sistemelor (IIC) componente;

F_i – fiabilitatea sistemului (IIC)i;

P_i – ponderea funcţională a sistemului (IIC)i;

F' – componenta datorată organizării sistemice a IC.

În virtutea celor prezentate, fiabilitatea poate fi considerată drept o caracteristică de calitate a unui sistem, a unei IIC sau chiar a IC în ansamblul ei, determinată de influenţa tuturor sistemelor (subsistemelor) şi de sinergia infrastructurii critice (IC) (organizată sistemic), ceea ce ne conduce la câteva concluzii:

- nivelul fiabilităţii fiecărui sistem (IIC) influenţează nivelul fiabilităţii IC, cu o pondere egală cu ponderea sa funcţională;

- un defect al unui sistem (IIC) produce un defect al IC; local, efectele defectelor pot fi diferite, însă la nivelul IC ele produc fie o întrerupere, fie o eroare funcţională exprimată de relaţia:

$$eIC_j = \sum_{i=1}^{k} p \cdot e_i , \qquad (3)$$

unde: eIC_j – eroare funcţională j a IC; e_i – eroarea funcţională a sistemului i care o produce pe „eIC_j”; p_i – ponderea funcţională a sistemului $(IIC)_i$. Din cauza dependenţelor ei tehnologice şi organizatorice, putem conchide că nivelul fiabilităţii unei IC este determinat de costurile de realizare (Cr) şi de cele de exploatare (Ce). În consecinţă, se poate adopta o strategie de optimizare a dinamicii valorilor (costurilor) fiabilităţii IC, în funcţie de mărimea costurilor totale (Cr+Ce):

$$Min[X(F)]=Cr(Fo)+Ce(Fo), \quad (4)$$

în care X(F) este nivelul costurilor fiabilităţii IC; Fo este fiabilitatea optimă.

Pentru IC se impune condiţionarea valorii fiabilităţii fiecărui sistem (IIC) de un cost propriu şi a valorii fiabilităţii IC atât de costurile sistemelor (IIC), cât şi de un cost propriu suplimentar, ceea ce se poate exprima printr-o funcţie de forma:

$$X(F)=a_0x_0+a_1x_1+a_2x_2+ \ldots a_ix_i \ldots +a_kx_k, \quad (5)$$

unde: x_i, i=0,1,....,k, reprezintă costurile specifice infrastructurii critice (i=0) şi sistemelor componente: i=1, ... , k, iar a_i sunt ponderile funcţionale.

Rezultă că:

$$X(Fo)=\min(a_0x_0+a_1x_1+ \ldots +a_kx_k), \quad (6)$$

ceea ce nu implică minimul fiecărui x_i.

Între calitatea şi fiabilitatea IC există o legătură organică care e determinată de ideea că prima dintre ele reprezintă ansamblul proprietăţilor care asigură funcţionarea (utilizarea) IC conform destinaţiei acesteia, iar a doua este capacitatea IC de a-şi păstra calitatea pe toată perioada de utilizare, adică fiabilitatea IC este calitatea IC extinsă în timp (calitatea în funcţie de timp).

Ca urmare, prin similitudine cu variaţia calităţii în funcţie de costurile de realizare şi cele de exploatare (utilizare), pentru IC nivelul fiabilităţii poate fi reprezentat ca în figura 3.

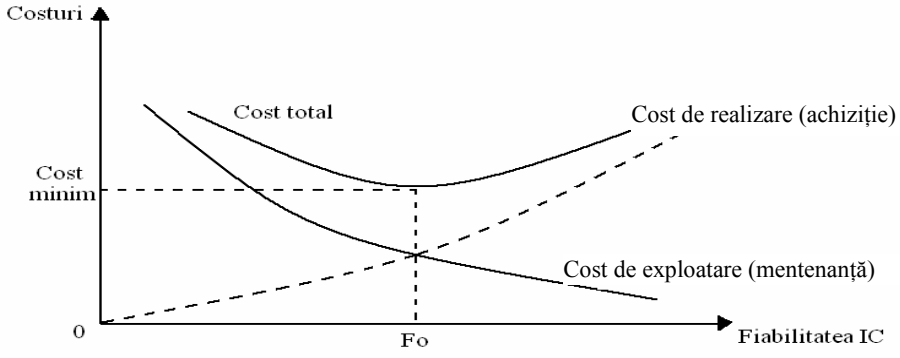


Figura 3. Dinamica fiabilităţii infrastructurii critice

Sursa: SITEANU Eugen, *Managementul logisticii de producţie,* Editura Academia Tehnică Militară, Bucureşti, 2009, p. 136.

Rezultă că valoarea optimă a fiabilităţii (Fo) este determinată de costurile minime, ceea ce implică o creştere a costurilor atât pentru IIC cu o fiabilitate mai mică decât fiabilitatea optimă (Fo), cât şi pentru cele cu o fiabilitate mai mare decât aceasta.

Viabilitatea IC, inclusiv a IIC, reprezintă capacitatea acesteia de a-şi conserva proprietăţile (caracteristicile) când mărimile sale de intrare (inputurile) şi perturbaţiile interne sau externe produc schimbări ale condiţiilor proiectate. Schimbările pot fi interpretate ca nişte cazuri de excepţie (erori sau întreruperi de funcţionare). Rezultă că viabilitatea IC este proprie acelei IC care se poate adapta fie prin readaptare (reconfigurare), fie prin intermediul unei rezerve de funcţionare (figura 4).

VIABILITATEA IC	
Readaptare (reconfigurare) (Ra)	rezervă de funcţionare (M')

Figura 4. Componentele viabilităţii IC

Aşadar, viabilitatea V se poate exprima prin relaţia:

$$V=Ra+M', \text{ sau } V=\sum_{i=1}^{k} q_i \cdot V_i + V', \quad (7)$$

unde: k reprezintă numărul sistemelor (IIC) componente; q_i este ponderea sistemului i; V_i – viabilitatea sistemului i; V' este o componentă datorată organizării sistemice a IC.

Viabilitatea IC este o manifestare a calităţii IC; similar fiabilităţii, ea e dependentă de costuri.

Asemănător cu definiţia fiabilităţii, securitatea IC este capacitatea acesteia de a-şi conserva caracteristicile funcţionale sub acţiunea factorilor distructivi sau care-i produc mutaţii periculoase pentru mediul înconjurător sau pentru oamenii din zona de risc.

SECURITATEA IC		
Conservare (remodelare) (Cv)	Readaptare funcţională (Ra)	Siguranţă în funcţionare (S)

Figura 5. Componentele securităţii IC

Securitatea (Sc) se poate exprima prin relaţia:

$$Sc=Cv+Ra+S, \quad (8)$$

conform componentelor din figura 5 sau:

$$Sc = \sum_{i=1}^{k-n} m_i \cdot S_i + S_c' ; \; n \leq k, \quad (9)$$

unde: (k-n) este numărul sistemelor (IIC) care contribuie la securitatea IC; S_i este securitatea sistemelor (IIC)i; m_i este ponderea sistemului i; S_c' este componenta datorită caracteristicilor de sistem ale IC.

S-a constatat că unele sisteme nu participă la realizarea efectivă a securităţii IC şi de aceea, dacă există n sisteme din acestea rezultă că securitatea fiecărui sistem, din cele (k-n) participante la securitatea IC, influenţează securitatea IC cu o pondere anumită, iar o infracţiune/excepţie sau o eroare a unui sistem ar putea determina o infracţiune pentru IC provocându-i o eroare funcţională. De aceea e necesară tratarea securităţii IC ca dependentă de infracţiuni, de erori funcţionale.

În mod similar fiabilităţii şi viabilităţii, securitatea IC depinde de costuri, faţă de care se poate stabili o valoare optimă (So), însă criteriul este de această dată mai complex şi reprezintă o corelaţie, un raport între cost şi risc.

Pe baza teoremei lui Bayes pentru calcularea parametrilor securităţii prin desfăşurarea arborelui probabilistic al evenimentelor în sens invers şi simplificând problema[4] se poate reduce analiza calitativă a securităţii IC prin rezolvarea funcţionalei de câştig (ESc) de forma:

$$ESc=max[0, (A-C(p)-p.w)],$$

unde: A este valoarea de optim economic; p este probabilitatea de fatalitate de producere a infracţiunii (excepţiei sau erorii) care destabilizează IC; C(p) este costul sistemului de securitate; w sunt pierderile suferite de IC în urma destabilizării.

Pornind de la această relaţie şi făcând câteva transformări[5] se ajunge la relaţia:

$$\frac{d(CSo)}{dSo} = W ,$$

[4] SITEANU Eugen, BEDROS Naianu, ILIE Gheorghe, *Fiabilitatea produselor tehnice*, Editura AISTEDA, Bucureşti, 2009, p. 132.
[5] Ibidem.

unde: So este valoarea optimă a securității IC; CSo este costul sistemului optim de securitate.

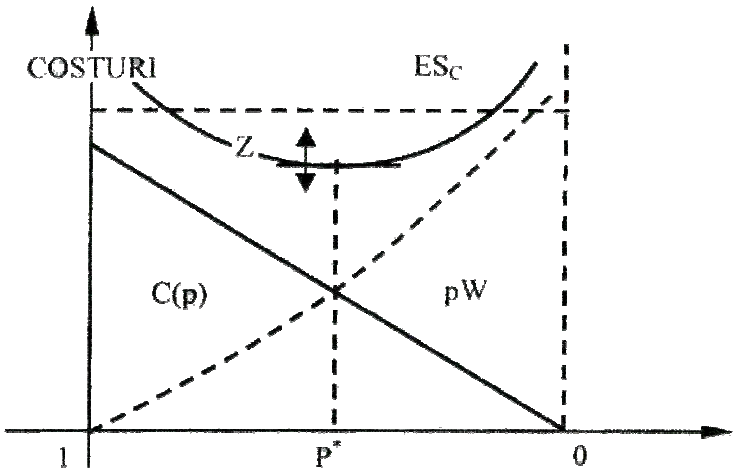


Figura 6. Dinamica funcționalei ESc

Funcționala ESc se poate reprezenta grafic (figura 6). Din acest grafic se vede că funcția z depinde de A şi de p, adică de riscul asumat prin proiectare (R):

$$z=A-[C(p)+p\cdot w].$$

După simplificări se obține riscul: R=1-A

Ca urmare, jocul corelațiilor dintre cost şi risc ar putea fi pus în evidență prin dinamica securității IC (figura 7).

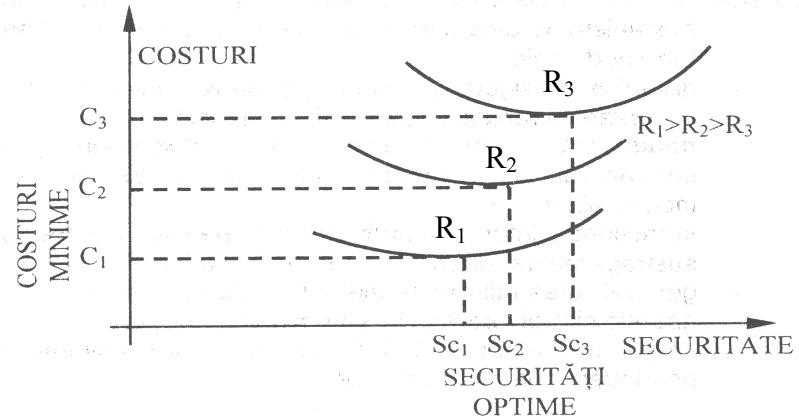


Figura 7. Dinamica securității infrastructurii critice

În analiza şi asigurarea securităţii IC o mare importanţă o reprezintă perisabilitatea măsurilor şi mecanismelor specifice. Ele sunt supuse la uzură şi îmbătrânire tehnologică şi morală, dar şi la presiuni cognitive de către teroriştii. Prin urmare, mecanismele de securitate "înghețate" sunt compromise, iar "spargerea" acestora este doar o problemă de studiu, timp şi bani din partea adversarilor sau teroriştilor.

Din analiza celor trei concepte (de fiabilitate, viabilitate şi securitate) se desprinde proprietatea securităţii de a integra în sfera sa fiabilitatea şi viabilitatea. Caracterul integronic al securităţii se bazează pe următoarele aspecte:

- asocierea conceptului de securitate a infrastructurii critice (IC) celui de calitate;
- caracteristica integratoare a IC privind funcţionarea, raportul energetico-informaţional şi capacitatea instructiv-educativă;
- pentru IC, ierarhizarea obiectivelor începe, obligatoriu, cu funcţionarea în securitate şi continuă, de la caz la caz, cu reziliența (capacitatea operaţională ca rezultantă a viabilităţii) sau disponibilitatea IC (ca rezultantă a siguranţei în funcţionare, a mentenabilităţii);
- generalizarea noţiunii de eroare ca efect al defectării, excepţiilor şi infracţiunilor;
- funcţionalitatea în securitate presupune şi impune IC fiabilitate şi viabilitate deosebite;
- existența în cadrul IC a unei interdependențe între funcţionare, raportul energetico-informaţional şi capacitatea instructiv-adaptivă ale acestora;
- inexistența unor metode practice de tratare separată a aspectelor complexe de securitate;
- rezultatele practice obţinute prin tratarea securităţii cu metodele şi tehnicile specifice fiabilităţii;
- generalizarea tehnicilor diferenţiale de realizare a securităţii între prevenire, tolerare, respingere sau transparență;
- apariţia şi dezvoltarea rapidă a metodei toleranţei la erori, aparent transparentă la cauze, datorită mutării analizei şi deciziei de la intrarea IC la ieşirea lor;
- dezvoltarea tehnicilor de proiectare şi de realizare a calculatoarelor.

Prin asocierea conceptelor securitate-calitate şi a modelului cibernetic al optimului securităţii se asigură un caracter unitar şi universal tratării securităţii IC, pe baza primordialităţii sale ca parametru de calitate. Astfel, întreaga problematică se transferă în zona manifestărilor de ieşire ale infrastructurii critice datorită erorilor, dar fără diminuarea eficienței studiului dependenței cauzale.

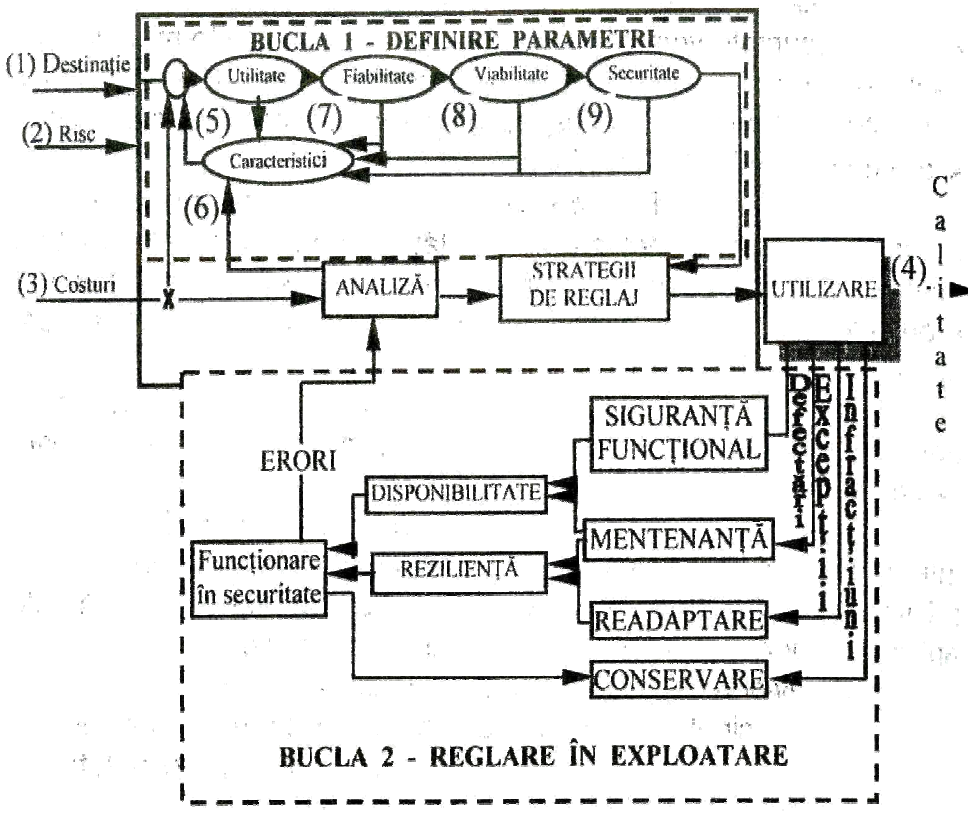


Figura 8. Modelul cibernetic al optimului securităţii infrastructurii critice

Plecând de la asocierea calitate-securitate, s-a determinat modelul cibernetic al optimului securităţii IC, ţinând seama de structura acesteia şi de fluxul transformărilor defecte-excepţii şi infracţiuni în erori. Modelul impune cicluri de reglaje şi elemente cu eficacitate sporită (fig. 8).

Intrările în sistemul de optimalitate a securităţii sunt destinaţia, nivelul de risc asumat şi costurile, iar ieşirea este calitatea (nivelul erorilor).

În structura modelului infrastructurii critice pot fi reţinute două cicluri: primul, intern – de determinare a valorilor de reglaj, care se aplică la execuţie (utilizare), şi un al doilea, extern – după ce se cunosc rezultatele aplicării – valori cu care începe procesul de optimizare.

În figură se observă următoarele bucle de reglaj:

- principală: de definire a caracteristicilor (parametrilor), cu alte trei bucle (pentru fiabilitate, viabilitate şi securitate);
- secundară: de reglare în exploatare;
- complementară: pentru strategia de reglaj;
- operaţională: pentru analiza erorilor.

Avantajele unei asemenea abordări sunt următoarele:

- se evidenţiază legătura dintre fiabilitate, viabilitate şi securitate;
- se stabilesc traseele şi posibilităţile de reglaj;
- se poate controla raportul dintre nivelul de risc şi securitatea IC, dintre tratarea erorilor, stabilirea strategiei de reglaj şi costul activităţii, dintre elementele tehnologice şi cele organizatorice;
- oferă posibilitatea pătrunderii în esenţa conceptului de securitate şi demonstrează viabilitatea aplicării strategiei de toleranţă la erori.

Modelul din figură are un caracter de generalitate, domeniul de aplicare depăşeşte cadrul protecţiei informaţiilor.

Pornind de la relaţiile de aditivitate (1), (7) şi (8) şi ţinând cont de faptul că cele trei concepte (fiabilitate, viabilitate şi securitate) se comportă optimal în funcţie de risc şi cost, pe baza asocierii conceptului de securitate a IC, se poate trage conchide că integrarea realizată de securitate depăşeşte stadiul actual de cunoaştere a activităţilor de securitate şi cadrul protecţiei informaţiilor. Integrarea fiabilităţii şi viabilităţii în securitate se exprimă prin dependenţa specifică a sistemelor (IIC) şi conceptelor de organizarea superioară a IC pe o bază genetică întrucât toate cele trei concepte depind unul de celălalt atât existenţial, cât şi evolutiv.

Baza genetică este eroarea, iar teoria, metodologia şi practica fiabilităţii au tendinţe de generalizare sau generează elemente comune în definire şi dezvoltare (funcţia de încredere, regimurile critice, structurile de cauzalitate, metodele cibernetice şi analitice de fiabilitate, viabilitate şi securitate, strategiile de mentenanţă şi rezilienţă, previziunea şi estimarea comportării sistemice etc).

Caracterul tolerant la erori şi reglajul probează o organizare asemănătoare şi un anumit tip de aport informaţional şi energetic.

Cele trei concepte îşi păstrează însă principalele manifestări de independenţă, formând în IC (cu deosebire în cele tehnice şi economice) un adevărat lanţ calitativ-fiabil, viabil şi în securitate.

Integrarea acestor niveluri calitative reprezintă un proces de supervizare, în sensul că mai multe caracteristici de fiabilitate conferă sistemului (IC) şi viabilitate, iar mai multe caracteristici de viabilitate oferă acestuia securitate.

Problema nu este însă exhaustivă, existând o mulţime de exemple când legătura fiabilitate – securitate este directă (cu preponderenţă la sistemele informatice).

Informatizarea proceselor, inteligenţa artificială şi manifestările acesteia de tip expert sau neural conferă valenţe şi niveluri superioare de integrare – strict dedicate unor sisteme (IC), deci şi efecte de comportament particular.

În concluzie, gradul de integrare al fiabilităţii şi viabilităţii în securitate este de tip aditiv, dar se conturează deja posibilităţile ca cercetările viitoare ale conceptului de securitate – desprins recent de dimensionarea sa minimală de efect al fiabilităţii – să stabilească forţe de legătură interioare tot mai puternice, cu efecte benefice asupra comportamentului adaptiv.

Drept forţă integratoare se recomandă toleranţa la erori, ca manifestare de calitate, demers necesar, în special, în cazul IC, cu efect în timp real.

Prin urmare, o IC nu poate fi caracterizată ca SIGURĂ decât dacă este FIABILĂ şi VIABILĂ în acelaşi timp, datorită faptului că ea este compusă din elemente tehnice, informatice şi este de tip mixt (om-maşină).

În consecinţă, considerăm că tratarea separată a IC (tehnică sau organizatorică) nu mai este posibilă. De asemenea, problema rezervelor trebuie extinsă de la rezerva de mijloace, materiale şi resurse umane la rezerva informatică, constând din strategii şi variante de management previzionar în funcţie de timp, situaţie, cost şi risc asumat, la variante organizatorice adaptate la situaţie (câştiguri şi pierderi) şi la resurse, precum şi la variante de realizare a viabilităţii IC pentru o anumită funcţionare în securitate acceptată.

BIBLIOGRAFIE

SITEANU Eugen, BEDROS Naianu, ILIE Gheorghe, *Fiabilitatea produselor tehnice*, Editura AISTEDA, Bucureşti, 2009.

SITEANU Eugen, *Managementul logisticii de producţie,* Editura Academia Tehnică Militară, Bucureşti, 2009.

PROTECȚIA INFRASTRUCTURII CRITICE – SARCINĂ PRIORITARĂ ÎN CADRUL STRATEGIEI DE SECURITATE A UNIUNII EUROPENE

General locotenent prof. univ. dr. Teodor FRUNZETI

Astăzi, omenirea se confruntă constant cu o multitudine de pericole, riscuri şi ameninţări în materie de securitate. În prezent, provocări de securitate, cu impact semnificativ asupra infrastructurii critice, vin şi din spaţiul virtual ***via*** *Internet. Datorită vulnerabilităţii lor, infrastructurile critice europene şi naţionale sunt o „ţintă" predilectă a riscurilor şi ameninţărilor de securitate. De aici, necesitatea de a realiza protecţia lor eficace atât la nivel european, cât şi naţional.*

Ce este o infrastructură?

Termenul generic de infrastructură acoperă persoane, organizaţii, procese, produse, prestaţii, flux de informaţii chiar construcţiile şi echipamentele tehnice şi fizice care izolează sau unesc, permit funcţionarea societăţii, a economiei şi a statului, asigurând aprovizionarea lor cu bunuri şi servicii esenţiale. De fapt, infrastructurile fac parte din structura de rezistenţă a unui ansamblu coerent de componente, sunt relaţionale şi funcţionale şi constituie în totalitate suportul necesar pentru ca sistemul să se identifice, să se individualizeze, să intre în relaţii cu alte sisteme, să se stabilizeze şi să funcţioneze optim.

Din definiţia dată termenului de infrastructură se constată următoarele aspecte esenţiale:

- compoziţie foarte diversificată – de la fiinţa umană la sisteme de comandă;
- elementele componente sunt în relaţii de interdependenţă şi interacţionează continuu;
- se comportă asemenea unui sistem deschis;
- relaţia de tip feed-back între infrastructură, ca întreg sau componentele sale separat, cu mediul în care există şi îşi îndeplineşte funcţiile specifice;
- roluri bine definite în funcţionarea societăţii umane ca entitate;
- se comportă asemenea unui centru de gravitate[1], e aceea, atingerea sa, prin orice mijloace, conduce la apariţia şi manifestarea sensibilităţii şi slăbiciunii sale în îndeplinirea rolurilor trasate sau asumate.

Infrastructura se întâlneşte la trei niveluri[2]:

- sectoare (de exemplu, energie, finanţe, sănătate publică);
- sub-sectoare (de exemplu, aprovizionare cu electricitate, cu petrol, cu gaz natural);
- obiecte specifice/elemente (de exemplu, staţii de exploatare a reţelelor, sisteme de comandă, linii de înaltă tensiune, baraje, conducte).

Tipuri de infrastructuri

Există mai multe tipuri de infrastructuri, clasificate în diferite categorii în consens cu criteriile alese. Infrastructurile se pot împărţi, ***în funcţie de locul, rolul şi importanţa lor pentru stabilitatea şi funcţionalitatea sistemelor, precum şi pentru siguranţa şi securitatea sistemelor şi proceselor,*** în trei mari categorii:

- infrastructuri obişnuite;
- infrastructuri speciale;
- infrastructuri critice.

[1] Vezi: CSII col (r) dr. Petre Duţu, Metode şi procedee de identificare a centrelor de gravitate pe timpul conflictelor armate, Bucureşti, UNAp, 2005, pp. 7-14.

[2] Vezi: Stratégie générale du Conseil fédéral pour la protection des infrastructures critiques. Bases de la stratégie nationale pour la protection des infrastructures critiques, http://www.bevoelkerungsschutz.admin.ch/internet/bs/fr/home/themen/ski.parsysrelated1.76002.downloadList.58248.DownloadFile.tmp/grundstrategieski20090518f.pdf

Infrastructurile obişnuite reprezintă o structură, un cadru, care asigură construcţia şi funcţionarea sistemului. Aceste infrastructuri nu prezintă calităţi deosebite, în afara celor care le justifică existenţa şi prezenţa în cadrul sistemelor şi proceselor. O ţară, spre exemplu, va avea întotdeauna drumuri, căi ferate, localităţi, şcoli, spitale, biblioteci. Pe parcurs, unele dintre acestea pot deveni speciale sau chiar critice, în funcţie de noul rol pe care îl pot avea, de dinamica importanţei şi de alte criterii. Spre exemplu, localităţile care au aerodromuri, puternice centre de comunicaţii, centrale nucleare, noduri de cale ferată sau alte obiective de importanţă strategică pot face parte din infrastructurile speciale şi, în anumite condiţii, chiar din infrastructurile critice.

Infrastructurile speciale au un rol deosebit în funcţionarea sistemelor şi proceselor, asigurându-le acestora o eficienţă sporită, calitate, confort, performanţă. De regulă, infrastructurile speciale sunt infrastructuri de performanţă. Unele dintre acestea, mai ales cele care pot avea prin extensie sau prin transformare un rol important în stabilitatea şi securitatea sistemelor pot dobândi şi statutul de infrastructură critică.

Infrastructurile critice (IC) sunt, de regulă, acele infrastructuri de care depind stabilitatea, siguranţa şi securitatea sistemelor şi proceselor. Ele pot face parte din categoria infrastructurilor speciale. Nu este însă obligatoriu ca toate infrastructurile care sunt sau pot deveni, la un moment dat, critice să facă parte din aceasta categorie de infrastructuri. Este foarte posibil ca, în funcţie de situaţie, chiar şi unele dintre infrastructurile obişnuite cum ar fi, spre exemplu, drumurile de ţară sau canalele magistrale din sistemele de irigaţii, să devină infrastructuri critice. De aceea, în definirea infrastructurilor critice, pot să intervină şi alte elemente, ceea ce conduce la concluzia că în identificarea şi evaluarea unor astfel de structuri există un criteriu de flexibilitate.

Din alt punct de vedere se afirmă că prin infrastructură critică se înţelege un punct, sistem sau parte a acestuia care este indispensabilă în menţinerea funcţiilor vitale din societate, sănătate, securitate şi a bunăstării economice sau sociale ale cetăţenilor, şi a cărei oprire sau distrugere ar avea un impact semnificativ într-un stat membru datorită slăbiciunii acestor funcţii[3]. De fapt, infrastructurile critice sunt instalaţiile fizice şi tehnologice de informaţii, reţelele, serviciile şi activele care, în caz de oprire sau distrugere, pot să aibă grave incidenţe asupra sănătăţii, securităţii sau bunăstării economice a cetăţenilor. Infrastructurile critice se găsesc în numeroase sectoare ale economiei, inclusiv în sectoarele bancar şi financiar, în transporturi (rutiere, feroviare, navale, aeriene), în sistemul energic, în servicii, în

[3] *Protection des infrastructures critiques,* http://www.libertysecurity.org/article2101.html

sănătatea şi aprovizionarea cu produse alimentare şi comunicaţii, ca şi unele servicii administrative de bază.

Totuşi, pare iluzoriu să se poată stabili o diferenţă, printre infrastructurile critice a căror scoatere din uz ar avea impacturi grave dincolo de statul membru asupra căruia ele sunt implantate, între cele care nu ar atinge decât un stat membru legat, probabil mediat, şi cele care ar atinge mai multe state membre. De aici, clasificarea infrastructurilor critice din UE în două categorii: 1) infrastructuri critice ce privesc doar un singur stat membru, care poartă numele de *infrastructuri critice naţionale* (ICN) şi semnifică faptul că scoaterea lor din uz nu are repercusiuni grave în afara teritoriului naţional de implementare; 2) infrastructuri critice ce privesc mai multe state membre (adică două sau mai multe). Ele se numesc *infrastructuri critice europene* (ICE) şi sunt cele a căror scoatere din funcţiune are consecinţe grave pentru două sau mai multe state membre ale UE[4].

Elementul determinant al definirii ca infrastructură critică (IC) a UE ar fi existenţa sau nu a unui efect transfrontalier, potrivit unui incident ce ar putea avea sau nu un impact grav dincolo de frontierele statului membru unde instalaţia este situată. Celălalt element de luat în consideraţie în materie de protecţie a infrastructurilor critice (PIC) ţine de faptul că sistemele bilaterale ale cooperării între statele membre în materie de PIC constituie un instrument verificat şi eficace al gestionării IC atunci când acestea sunt situate într-o zonă frontalieră între două state membre[5].

Infrastructurile critice europene (ICE) ar putea cuprinde resursele fizice, serviciile, tehnologiile informaţiei, reţelele şi activele a căror oprire sau distrugere ar avea grave incidenţe asupra sănătăţii, securităţii, siguranţei sau bunăstării economice sau sociale a cetăţenilor UE. În acest context, se impune recensământul progresiv al tuturor ICE având în vedere interdependenţele ce există între acestea în cadrul UE. Studiile de interdependenţă contribuie la analiza impactului potenţial al ameninţărilor împotriva anumitor IC şi permit mai ales să se ştie care state membre ar fi atinse în caz de incident major ce afectează IC. Interdependenţele între întreprinderi, sectoarele industriale, competenţele teritoriale şi autorităţile statelor membre, ca şi interdependenţele în sânul aceloraşi sectoare sau entităţi, în particular atunci când sunt create prin tehnologiile informaţiilor şi comunicaţiilor, ar trebui luate în consideraţie. Comisia Europeană, statele membre şi proprietarii/utilizatorii infrastructurilor critice colaborează pentru a recenza aceste

[4] Livre vert sur un programme européen de protecţion des infrastructures critiques, http://eur-lex.europa.eu/LexUriServ/site/fr/com/2005/com2005_0576fr01.pdf, p.4.

[5] Livre vert sur un programme européen de protecţion des infrastructures critiques, http://eur-lex.europa.eu/LexUriServ/site/fr/com/2005/com2005_0576fr01.pdf, p.7.

interdependenţe şi de a aplica, dacă este posibil, strategii adecvate de limitare a riscurilor.

Anumite infrastructuri naţionale au un caracter vital, astfel încât dereglarea sau distrugerea lor ar avea un impact devastator sau destabilizator asupra securităţii economice naţionale. De asemenea, o atenţie deosebită trebuie acordată identificării legăturilor infrastructurilor şi sectoarelor ce au ca scop:

- continuitatea funcţiilor statului;
- sistemele de comunicaţii şi transport informatizate;
- serviciile de sănătate publică (inclusiv prevenire, supraveghere, servicii de laborator);
- serviciile de sănătate individuale.

Stabilirea acestor legături este necesară pentru a se putea asigura capabilităţile de protejare a infrastructurilor, împotriva atacurilor intenţionate care ar diminua semnificativ abilităţile:

- guvernului, în ceea ce priveşte desfăşurarea de misiuni fundamentale de securitate economică naţională şi asigurarea sănătăţii şi a siguranţei publice generale;
- organelor administrative centrale şi locale, în ceea ce priveşte menţinerea ordinii şi asigurarea unui minimum de servicii publice de bază;
- sectorului privat, în ceea ce priveşte funcţionarea armonioasă a economiei şi furnizarea serviciilor de telecomunicaţii, a serviciilor energetice, financiare şi de transport de bază.

Este bine cunoscut că infrastructuri critice se întâlnesc în toate sectoarele de activitate umană. Astfel, se vorbeşte de: *infrastructuri critice din transporturi* (rutiere, feroviare, navale, aeriene); *infrastructuri critice din comerţ*; *infrastructuri critice industriale; infrastructuri critice din sistemul energetic; infrastructuri critice din agricultură; infrastructuri critice din comunicaţii şi informaţii; infrastructuri critice din sănătate* etc.

Indiferent, însă, despre ce tipuri de infrastructuri critice este vorba, se cuvin subliniate trei aspecte esenţiale ale acestora: *ele pot să aparţină fie sectorului public, fie sectorului privat*. Uneori ele pot fi proprietatea puterilor publice, dar să fie administrate de către un operator privat; oricare ar fi proprietarul, *întărirea măsurilor ce vizează să asigure securitatea acestor instalaţii trebuie să aparţină puterilor publice*; *dimensiunea transnaţională* constituie o realitate şi trebuie avută în vedere în analiza acestui tip de infrastructură în contextul în care este vorba de statele membre ale UE.

Vulnerabilităţi, pericole şi ameninţări pentru infrastructurile critice

Infrastructura critică se referă la acele sisteme, fizice sau virtuale, lanţuri de aprovizionare, reţele tehnologice informatice şi de comunicare a căror distrugere, degradare sau indisponibilitate ar afecta în mod semnificativ sectorul social sau economic al naţiunii sau ar afecta abilitatea ţării de a-şi asigura şi garanta securitatea naţională. De aceea, infrastructurile critice au reprezentat întotdeauna domeniul cel mai sensibil, cel mai vulnerabil al oricărui sistem şi proces. Sensibilitatea derivă din rolul lor deosebit în structura, stabilitatea şi funcţionarea unui sistem, indiferent de sistem sau proces. Vulnerabilitatea defineşte imposibilitatea asigurării, prin proiect şi/sau realizarea efectivă a protecţiei corespunzătoare, dar şi prin creşterea presiunilor programate, direct sau indirect, intenţionate sau aleatorii asupra lor. În acest caz, vulnerabilitatea este direct proporţională cu rolul pe care îl joacă infrastructurile respective. De aici, rezultă că, oricât de bine ar fi protejate, infrastructurile critice vor avea întotdeauna un grad de vulnerabilitate ridicat, întrucât, de regulă, sunt primele vizate atunci când se urmăreşte destabilizarea şi chiar distrugerea unui sistem sau unui proces.

Identificarea, optimizarea şi securizarea infrastructurilor critice reprezintă o prioritate indiscutabilă, atât pentru gestionarii de sisteme şi procese, cât şi pentru adversarii acestora, adică pentru cei care urmăresc să atace, să destabilizeze şi să distrugă sistemele şi procesele vizate. Infrastructurile critice nu sunt şi nu devin critice, doar la atacuri sau din cauza atacurilor, ci şi din alte cauze, unele dintre ele greu de depistat şi de analizat. De regulă, mai ales după atacurile teroriste de la 11 septembrie 2001 asupra complexului World Trade Center şi asupra Pentagonului, se consideră că infrastructurile sunt sau pot deveni critice în raport cu atacurile teroriste sau cu alte ameninţări, îndeosebi asimetrice. Acesta este doar un aspect sau un criteriu de identificare a infrastructurilor critice. Mai sunt însă şi altele care ţin, deopotrivă, atât de stabilitatea şi funcţionalitatea sistemelor şi proceselor, cât şi de raporturile acestora cu mediul exterior. În acelaşi timp, infrastructurile devin critice prin posibilele daune aduse unui sector de activitate sau mai multora de diferite fenomene naturale (cutremure, inundaţii, alunecări de teren, furtuni, cicloane, ploi torenţiale, căderi masive de zăpadă) şi/sau unele acţiuni umane voluntare/intenţionate[6].

Infrastructurile rutiere critice sunt vulnerabile atât la fenomene naturale (de exemplu, căderi masive de zăpadă, ploi torenţiale, alunecări de teren, cutremur devastator), cât şi la acţiunile distructive umane (de exemplu, accidente de

[6] Vezi: Protection des infrastructures critiques, http://www.bevoelkerungsschutz.admin.ch/internet/bs/fr/home/themen/ski.parsysrelated1.76002.downloadList.22047.DownloadFile.tmp/2berichtski20090518f.pdf, pp.2-3.

circulaţie, atentate teroriste de tip maşini capcană şi/sau oameni „bombă”). În acelaşi timp, domeniul transporturilor rutiere este deosebit de vulnerabil, cel puţin în România, şi datorită drumurilor judeţene, naţionale şi europene. Aici, avem în vedere calitatea, lăţimea şi dotarea lor cu utilităţi pentru conducători auto, în special, şi pentru cei care le folosesc în mod curent, în general,. În opinia noastră, nu numai starea drumurilor din ţara noastră le face să intre rapid în „rolul” de infrastructuri critice, ci şi capacitatea lor de a asigura deplasarea fluentă a autovehiculelor. Practic, cele mai multe drumuri naţionale şi europene de la noi sunt prevăzute doar cu o bandă de circulaţie pe sens, ceea ce îngreunează deplasarea optimă a autovehiculelor, pe de o parte, şi nu permite „absorbţia” tuturor autovehiculelor care există în ţară, pe de altă parte.

De asemenea, în caz de intemperii nu sunt asigurate oportun serviciile de eliminare a „obstacolelor” de pe calea de rulare, ceea ce sporeşte vulnerabilitatea infrastructurilor din transporturi.

Comerţul este un alt domeniu care este destul de vulnerabil faţă de fenomenele naturale – de exemplu, inundaţii, cutremur, alunecări de teren, căderi masive de zăpadă – şi de acţiunile umane răuvoitoare intenţionate (de pildă, atacuri teroriste, accidente datorate incompetenţei sau neglijenţei în serviciu). De aceea, şi în acest sector de activitate se adoptă măsuri de protecţie a infrastructurilor specifice. Este vorba de depozitele de mărfuri, transportul produselor, îndeosebi a celor perisabile, serviciile vitale pe care le oferă – de la transportul de mărfuri şi persoane la cele din domeniul sănătăţii.

Nevoia de protecţie a infrastructurilor critice europene şi naţionale

Nevoia de protecţie a infrastructurilor critice este un deziderat important pentru toate statele lumii, inclusiv pentru ţările europene, indiferent de nivelul lor de dezvoltare, de mărime, de numărul de locuitori sau putere militară. Aceasta dintr-o serie de motive, printre care, în opinia noastră, semnificative par a fi următoarele:

1) *multitudinea de pericole, riscuri şi ameninţări de securitate cu care se confruntă toate statele lumii, inclusiv cele europene.* Astăzi, statele lumii se confruntă cu pericole, riscuri şi ameninţări de securitate, de o mare diversitate ca natură – atentate teroriste (de exemplu, New –York 2001, Madrid 2004, Londra 2005), catastrofe naturale (de exemplu, cutremurele din 2010, din ianuarie în Haiti şi din februarie în Chile, inundaţiile din 2002 din Europa), accidente de muncă, neglijenţă în serviciu, rea-voinţă. Toate acestea afectează şi infrastructurile critice, din toate sectoarele de activitate. De la această realitate nu fac excepţie nici statele membre ale Uniunii Europene;

2) *riscurile, pericolele şi ameninţările de securitate sunt într-o continuă creştere, iar ca manifestare sunt globale şi multiforme*. Printre acestea, un loc aparte îl ocupă: terorismul internaţional; atacurile informatice; compromiterea informaţiilor strategice; riscurile de pandemie (vezi cazul gripei aviare şi a celei denumite AN1H1); catastrofele naturale (cutremure, inundaţii, alunecări de teren, tsunami, cicloane, furtuni);

3) *existenţa unei interdependenţe economice, sociale, politice şi nu numai* între statele membre ale UE. Acest fapt conduce la amplificarea vulnerabilităţii infrastructurilor critice din ţările membre şi din Uniunea Europeană, ca entitate socială, politică, economică. De aici, nevoia de a renova şi armoniza la nivel european procesul de protecţie a infrastructurilor critice;

4) *infrastructurile critice devin din ce în ce mai mult interdependente* pe măsură ce procesele economice, tehnologice şi sociale legate de globalizare se intensifică. Orice atingere adusă unei infrastructuri critice într-un stat membru al Uniunii Europene antrenează obligatoriu un prejudiciu pentru numeroase state membre şi pentru întreaga economie europeană şi nu numai.

5) *complexitatea mediului de securitate internaţional, regional şi naţional*[7]. În prezent, mediul de securitate cunoaşte o evoluţie alertă atât datorită efectelor multiple ale globalizării şi integrării regionale, cât şi diversificării provocărilor de securitate. Această fluiditate a mediului de securitate are un impact puternic şi asupra infrastructurilor critice europene şi naţionale afectând semnificativ funcţionarea lor normală. În final, această disfuncţionalitate se răsfrânge negativ asupra societăţii în ansamblul său aducând atingere vieţii şi activităţii tuturor oamenilor.

Toate aceste motive subliniază necesitatea absolută ca factorii responsabili să adopte şi să pună în practică programe de măsuri, pe termen scurt, mediu şi mai ales lung, pentru a asigura protecţia infrastructurilor critice. Prin urmare se impune existenţa şi funcţionarea optimă a unei strategii de securizare a infrastructurilor critice din Uniunea Europeană. Această strategie ar trebui să fie ***globală şi integrată***.

Protecţia infrastructurilor critice

Obiectivele protecţiei infrastructurilor critice definesc nivelul de securitate atins cu mijloacele financiare disponibile şi determină măsurile ce rezultă din aceasta. Orice obiectiv de protecţie nu este absolut şi depinde de situaţia în materie de securitate. Totuşi, trebuie avut în vedere că există atât obiective generale de

[7] Vezi: Petre Duţu, *Mediul de securitate în contextul globalizării şi integrării regionale*, Bucureşti, UNAp, 2007

protecţie, cât şi obiective specifice. Acestea din urmă trebuie definite pentru fiecare sector de infrastructură (de exemplu, aprovizionarea minimală cu electricitate în sectorul energetic). Ele depind de tipul şi de caracterul critic al infrastructurii analizate. Acesta din urmă descrie importanţa sa relativă în raport cu consecinţele pe care o perturbare, o slăbiciune sau o distrugere ar avea-o pentru populaţie sau bazele sale de existenţă.

Protecţia infrastructurilor critice europene (ICE) şi a infrastructurilor critice naţionale (ICN) se întemeiază pe principii cum sunt[8]:

➢*Gestiunea integrală a riscurilor*. ICE şi ICN trebuie să facă faţă multor riscuri şi ameninţări. Acestea se impune a fi tratate ca şi cum ar fi un sistem coerent. O asemenea abordare ar permite definirea măsurilor ce pot elimina sau limita efectele nedorite produse de trecerea riscurilor din starea latentă în cea de manifestare activă. În acest sens, se pot aminti următoarele domenii:

- prevenirea (de exemplu, măsuri de amenajare a teritoriului);
- pregătirea (de exemplu, planuri de urgenţă sau de continuitatea a activităţilor);
- intervenţia (de exemplu, sistemele de alarmă, protecţie fizică asigurată prin forţele de securitate, comunicarea de criză unită);
- repunerea în starea de funcţionare (de exemplu, repararea provizorie a infrastructurilor);
- reconstrucţie (de exemplu, a infrastructurilor afectate de materializarea unor ameninţări).

Gestiunea integrală a riscurilor trebuie considerată ca un proces. Prin urmare, niciun domeniu de activitate umană ce conţine infrastructuri critice nu trebuie socotit prioritar în sine, ci în funcţie de utilitate sa socială atât la nivel naţional, cât şi la nivel european.

➢*Evantaiul de pericole*. Analiza pericolelor şi a riscurilor ia în seamă întreaga paletă a acestora, de la hazard la atingere intenţionată a infrastructurii vizate. Astfel, se are în vedere ansamblul pericolelor pertinente (pericole naturale, tehnice şi sociale, violenţa) fără a le ierarhiza.

➢*Rezilienţa*. Aceasta este un aspect foarte important în măsura în care este imposibil de protejat toate infrastructurile în permanenţă şi de o manieră exhaustivă. Într-o modalitate generală, se va asigura întoarcerea la starea „normală” în cel mai scurt timp. Capacitatea de rezilienţă a unei infrastructuri este definită de cinci elemente: 1) soliditatea sistemului în ansamblul său (societate, sector, element de infrastructură); 2) existenţa redundanţei; 3) capacitatea în a pune în practică

[8] LEGE privind protecţia infrastructurilor critice şi înfiinţarea Autorităţii Naţionale pentru Protecţia Infrastructurilor Critice, http://webapp.senat.ro/pdf/09L125FG.pdf.

măsurile auxiliare; 4) rapiditatea acestora; 5) capacitatea societăţii de a face faţă la situaţiile de criză.

➢*Proporţionalitate*. Măsurile reţinute trebuie să rămână într-un raport de justă proporţie între evaluarea riscurilor şi obiectivele de protecţie vizate. Echilibrul între costuri, protecţie şi securitate trebuie să fie menţinut fără a împiedeca inutil libertăţile publice nici să contravină dreptului. De asemenea, se va urmări să se evite orice distorsiune superfluă a pieţei atât la nivel naţional, cât şi la nivel european.

➢*Subsidiaritate*. Măsurile incumbă atât exploatarea infrastructurilor critice cât şi în sectorul public. Sectorul privat, căruia aparţin multe infrastructuri critice, poartă o responsabilitate specială în materie ca şi în termeni de investiţie. În ceea ce priveşte puterile publice, ele sunt chemate înainte de toate să protejeze propriile infrastructuri critice şi să susţină ajutorul pentru exploatarea lor. Totodată, se cuvine avut în vedere întotdeauna statutul României de membru al Uniunii Europene.

În adoptarea măsurilor de protecţie a infrastructurilor critice se are în vedere parcurgerea succesivă a următorilor paşi:

✓*Definirea priorităţilor*. Pentru o utilizare optimă a resurselor, se cuvine stabilirea unei ordini de priorităţi a infrastructurilor critice.

✓*Concepţia privind protecţia infrastructurilor critice.* Integralitatea măsurilor de protecţie a infrastructurilor critice este concepţia esenţială în acest domeniu. Conceperea măsurilor de protecţie are în vedere un larg evantai de riscuri şi ţine seama de un ciclu complet de gestionare a acestora din urmă. Conceptele de protecţie se referă la sectoarele critice şi la elementele specifice de importanţă naţională. Ele completează conceptele puse în practică în diferite subsectoare. De fapt, întreaga protecţie se face potrivit legii în vigoare[9].

✓*Elaborarea documentelor de bază.* Acestea se fac potrivit prevederilor legale în materie, naţionale şi ale Uniunii Europene.

✓*Comunicarea riscurilor.* Adesea oamenii nu sunt conştienţi de importanţa infrastructurilor critice şi de consecinţele posibile ale slăbiciunilor lor. De aceea trebuie ca cei responsabili – utilizatori, actori din economie, administratori şi populaţia – să fie sensibilizaţi asupra riscurilor şi pericolelor şi toţi să fie informaţi de comportamentul pe care trebuie să-l adopte în caz de eveniment, precum şi asupra posibilităţilor de protecţie. Aici, intervine Autoritatea Naţională pentru Protecţia Infrastructurii Critice care are obligaţia să elaboreze Planul Naţional de Protecţie a Infrastructurii Critice şi realizează Sistemul naţional informatic de

[9] LEGE privind protecţia infrastructurilor critice şi înfiinţarea Autorităţii Naţionale pentru Protecţia Infrastructurilor Critice, http://webapp.senat.ro/pdf/09L125FG.pdf

protecţie al infrastructurii critice. Prin aceasta se urmăreşte implementarea planurilor specifice de protecţie a infrastructurilor critice şi actualizarea băncii de date din sistemul naţional informatic.

Atitudinea activă a UE faţă de protecţia infrastructurilor critice

Uniunea Europeană a adoptat o atitudine activă în ceea ce priveşte protecţia infrastructurilor critice de pe teritoriul său. Această atitudine se fondează înainte de toate pe Strategia de securitate a UE, document ce defineşte principalele ameninţări, obiectivele de urmărit şi rolul major de actor mondial al Uniunii[10]. În acelaşi timp, pornind de la prevederile acestui document, ce vizează construirea unei Europe mai sigure într-o lume mai bună, UE şi-a elaborat programe diverse de acţiune concertată şi sistematică pentru a limita atât cât este posibil efectele riscurilor şi ameninţărilor de securitate asupra sa, a statelor membre şi a cetăţenilor europeni. În acest context, o atenţie sporită a fost acordată infrastructurilor critice europene şi naţionale ale statelor membre.

În acest sens, Comisia Europeană a adoptat o serie de documente, cu valoare de programe de acţiune pentru protecţia flexibilă, eficace şi creatoare a tuturor infrastructurilor critice europene şi naţionale. Printre acestea se află şi Programul european de protecţie a infrastructurilor critice (PEPIC)[11] şi Directiva Consiliului European din decembrie 2008 privind recensământul şi desemnarea infrastructurilor critice europene, ca şi evaluarea necesităţii ameliorării protecţiei lor[12].

În esenţă, Programul european de protecţie a infrastructurilor critice vizează prezervarea vieţii şi bunurilor persoanelor expuse, în UE, la riscuri generate de actele teroriste, catastrofele naturale şi de accidente. Practic, se urmăreşte ca orice întrerupere sau manipulare a infrastructurilor critice să fie, pe cât este posibil, scurtă, excepţională, relativ facil de administrat, geografic izolată şi să nu aducă atingere decât într-o măsură foarte limitată bunăstării statelor membre, cetăţenilor lor şi Uniunii Europene. Unei asemenea cerinţe i se răspunde concret atât la nivel naţional, cât şi al UE prin adoptarea de măsuri precise în vederea întăririi prevenirii, pregătirii şi răspunsul eficace faţă de orice ameninţare la adresa infrastructurilor critice. Orice daună pe care ar putea să o sufere o infrastructură într-un stat membru sau orice pierdere a unei astfel de infrastructuri ar putea

[10] La stratégie européenne de sécurité, http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_terrorism/r00004_fr.htm

[11] Livre vert sur un programme européen de protecţion des infrastructures critiques, http://eur-lex.europa.eu/LexUriServ/site/fr/com/2005/com2005_0576fr01.pdf,

[12] Council Directive 2008/114/EC of 8 December 2008, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32008L0114:EN:HTML:NOT

antrena un prejudiciu pentru numeroase state membre şi pentru economia europeană în ansamblul său. Probabilitatea unui asemenea prejudiciu este în creştere deoarece, cu noile tehnologii (de exemplu, Internetul) şi liberalizarea pieţelor (de exemplu, cea a gazului şi a electricităţii), un mare număr de infrastructuri fac parte dintr-o reţea mai largă. În aceste condiţii, măsurile comune de protecţie a infrastructurilor critice, europene şi naţionale, trebuie să se definească prin flexibilitate, eficacitate şi creativitate, într-un context global şi integrat. O asemenea protecţie trece prin comunicare, coordonare şi cooperare atât la nivel naţional, cât şi nivelul UE, între toţi cei interesaţi.

Programul european de protecţie a infrastructurilor critice conţine, în principal, următoarele elemente fundamentale: definirea infrastructurilor critice europene şi a infrastructurilor critice naţionale; stabilirea principiilor ce stau la baza conlucrării şi cooperării europene în materie de protecţie a infrastructurilor critice (de exemplu, principiul subsidiarităţii, principiul confidenţialităţii, principiul proporţionalităţii) şi a cadrului comun de acţiune; metodologia de punere în operă a măsurilor stabilite la nivel european; stabilirea surselor de finanţare.

În opinia noastră, o atenţie sporită se impune a fi acordată cadrului comun realizat prin punerea în practică a PEPIC, deoarece el conţine principalele elemente ale cooperării, conlucrării şi comunicării între cei interesaţi, pe de o parte, şi rolurilor majore pe care acest cadru comun îl joacă, pe de altă parte. Printre componentele acestui cadru comun, se află[13]:

- ✓ principii comune în materie de protecţie a infrastructurilor critice;
- ✓ coduri/norme stabilite în comun;
- ✓ definiţii comune asupra bazei în care definiţiile sectoriale ar putea fi stabilite;
- ✓ o listă comună de sectoare de infrastructuri critice;
- ✓ domenii de acţiune prioritară în materie de infrastructuri critice; o descriere a responsabilităţilor actorilor vizaţi;
- ✓ puncte de referinţă convenite; metode de comparare a diferitelor sectoare de infrastructuri şi de stabilire între ele a unei ordini de prioritate.

De fapt, cadrul comun, la nivelul UE, pentru protecţia infrastructurilor critice în Europa o dată pus în operă ar asigura ca toate statele membre să ofere niveluri de protecţie suficiente şi uniforme ale infrastructurilor lor critice şi că, în fapt, concurenţa pe piaţa internă nu este falsificată. Prin urmare, este indispensabil să existe un limbaj comun între statele membre ale UE asupra subiectului în măsura în care noţiunea de caracter european al unei infrastructuri critice se bazează pe

[13] Livre vert sur un programme européen de protecţion des infrastructures critiques, http://eur-lex.europa.eu/LexUriServ/site/fr/com/2005/com2005_0576fr01.pdf,p.7.

realitatea interdependenţei între state sau a consecinţelor grave pe care le-ar avea asupra unuia sau a mai multor state membre scoaterea din uz sau distrugerea unei infrastructuri critice situate la unul dintre ele. Acest cadru comun serveşte la ierarhizarea infrastructurilor critice într-un clasament intersectoare şi interstate membre. De asemenea, cadrul comun permite definirea şi clarificarea responsabilităţilor între statele membre şi întreprinderile ce fac parte din infrastructurile critice.

Directiva **2008/114/CE** a Consiliului European din 8 decembrie 2008, document ce are o strânsă legătură cu PEPIC, priveşte recensământul şi desemnarea infrastructurilor critice europene ca şi evaluarea necesităţii de a le ameliora protecţia[14]. Practic, această directivă instaurează o procedură de recensământ şi de desemnare a infrastructurilor critice europene (ICE). În acelaşi timp, ea defineşte o abordare comună pentru a evalua aceste infrastructuri cu obiectivul declarat de a le ameliora protecţia în vederea garantării şi asigurării mai bune a nevoilor cetăţenilor europeni.

Statele membre, potrivit acestei directive, trebuie să procedeze la recensământul ICE potenţiale cu ajutorul Comisiei Europene la nevoie. Ele trebuie să utilizeze o serie de criterii pentru a inventaria aceste ICE potenţiale. Criteriile intersectoriale ţin seama de eventualele victime, de efectele economice şi de incidenţele asupra populaţiei, în timp ce criteriile sectoriale au în vedere particularităţile fiecărui sector al ICE. Se impune făcută precizarea că această directivă nu se referă la toate ICE, ci doar la sectoarele de energie şi de transporturi şi unele subsectoare legate de acestea.

Fiecare stat membru trebuie să inventarieze într-o manieră cooperativă ICE potenţiale situate pe teritoriul său. Acest proces implică discuţii cu celelalte state membre susceptibile de a fi afectate semnificativ în cazul întreruperii serviciilor oferite de această infrastructură. De asemenea, directiva face precizarea că pentru ca o infrastructură critică naţională să fie recunoscută oficial desemnată ca ICE, statul membru pe teritoriul căruia ea este situată trebuie să-şi dea acordul.

Potrivit acestei directive, recensământul şi desemnarea ICE de statele membre trebuie să se facă cel mai târziu până în ianuarie 2011. Pe de altă parte, statele membre pe teritoriul cărora se află ICE trebuie să notifice în fiecare an Comisiei Europene numărul de ICE potenţiale şi ICE desemnate pentru fiecare sector. În acest scop, statele membre trebuie să vegheze la aceasta ca la un plan de securitate operator (PSO) sau o măsură echivalentă să fie pusă în practică pentru fiecare ICE desemnat ca atare. Obiectivul procesului de elaborare a PSO este de a

[14] Infrastructures critiques européennes, http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_terrorism/jl0013_fr.htm

inventaria diferitele puncte de ICE, ca şi măsurile de securitate aplicate pentru protecţia lor. De asemenea, fiecare stat trebuie să stabilească care sunt ameninţările posibile pentru fiecare ICE de pe teritoriul său şi să le comunice Comisiei Europene. Această măsură permite evaluarea corectă a riscurilor şi ameninţărilor de securitate pentru ICE şi stabilirea măsurilor adecvate de protecţie a lor atât prin forţe proprii, cât şi cu sprijinul UE.

În opinia noastră, punerea în practică a prevederilor PEPIC şi a directivei analizate succint mai sus va spori eficacitatea protecţiei ce se asigură atât la nivel naţional, cât şi european a infrastructurilor critice europene.

Concluzii

Uniunea Europeană şi statele membre, pentru a exista şi funcţiona optim, în beneficiul cetăţenilor lor, au nevoie de infrastructuri fiabile.

Se înţelege prin infrastructuri critice cele care sunt deosebit de importante pentru funcţionarea sistemului în ansamblul său ori pentru funcţionarea altor infrastructuri. Altfel spus, infrastructurile critice sunt acele infrastructuri a căror perturbare, slăbiciune sau distrugere au consecinţe grave asupra sănătăţii, vieţii publice, mediului ambiant, politicii, securităţii şi bunei stări economice sau sociale atât la nivelul UE, cât şi la nivel naţional.

Ele sunt reunite în cadrul sectoarelor energetic, transporturi şi comunicaţii, sănătate, aprovizionare a populaţiei şi nu numai. Punerea în practică a măsurilor de protecţie a infrastructurilor critice este diferită de la o ţară membră a UE la alta, de la un sector de activitate la altul, dar mai avansate pentru elemente specifice cum sunt centralele nucleare sau barajele.

Protecţia infrastructurilor critice europene şi naţionale are ca scop să reducă probabilitatea şi amploarea daunelor unei perturbări, a unei slăbiciuni sau a unei distrugeri a acestora şi, în caz că inevitabilul se produce, să se reducă la maximum durata de indisponibilitate. Ea este astfel chemată să contribuie în mod eficace la protecţia populaţiei şi a bazelor sale de existenţă. De aceea, toate măsurile de protecţie a infrastructurilor critice europene şi naţionale se impun a fi concrete şi puse în practică, într-o manieră concertată, de către cei responsabili cu aceasta.

BIBLIOGRAFIE

Adrian V. Gheorghe, Analiza de risc şi de vulnerabilitate pentru infrastructurile critice ale societăţii informatice-societatea cunoaşterii, http://www.acad.ro/pro_pri/doc/st_b02.doc

Council Directive 2008/114/EC of 8 December 2008, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32008L0114:EN:HTML

Critical Foundations. Protecting America's Infrastructures. The Report of the President's Commission on Critical Infrastructure Protection, Washington DC, October 1997

Critical Infrastructure Protection, http://www.ag.gov.au/www/agd/agd.nsf/Page/Nationalsecurity_CriticalInfrastructureProtection

Critical Infrastructure Protection, http://www.usfa.dhs.gov/fireservice/subjects/emr-isac/index.shtm

CSII dr. Petre Duţu, *Metode şi procedee de identificare a centrelor de gravitate pe timpul conflictelor armate,* Bucureşti, UNAp, 2005

Petre Duţu, *Mediul de securitate în contextual globalizării şi integrării regionale*, Bucureşti, UNAp, 2007

Infrastructures critiques, http://www.euractiv.com/fr/securite/infrastructures-critiques/article-140627

Infrastructures critiques européennes, http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_terrorism/jl0013_fr.htm

LEGE privind protecţia infrastructurilor critice şi înfiinţarea Autorităţii Naţionale pentru Protecţia Infrastructurilor Critice, http://webapp.senat.ro/pdf/09L125FG.pdf

Livre vert sur un programme européen de protection des infrastructures critiques, http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexplus!prod!DocNumber&lg=fr&type_doc=COMfinal&an_doc=2005&nu_doc=576,

Protection des infrastructures critiques, http://www.libertysecurity.org/article2101.html

Protection des infrastructures critiques, http://www.bevoelkerungsschutz.admin.ch/internet/bs/fr/home/themen/ski.parsysrelated1.76002.downloadList.22047DownloadFile.tmp/2berichtski20090518f.pdf

Promovarea conceptului de Protecţie a Infrastructurilor Critice în România, http://www.eurisc.org/component/docman/doc_download/13-septimiu-caceu-promovarea-conceptului.html

Proposition de directive du Conseil concernant le recensement et le classement des infrastructures critiques européennes ainsi que l'évaluation de la nécessité d'améliorer leur protection, http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexplus!prod!DocNumber&lg=fr&type_doc=COMfinal&an_doc=2006&nu_doc=787

Stratégie générale du Conseil fédéral pour la protection des infrastructures critiques. Bases de la stratégie nationale pour la protection des infrastructures critiques, http://www.bevoelkerungsschutz.admin.ch/internet/bs/fr/home/themen/ski.parsysrelated1.76002.downloadList.58248DownloadFile.tmp/grundstrategieski20090518f.pdf

INFRASTRUCTURA PENTRU APĂRARE - BENEFICIARĂ A PROGRAMELOR COMUNITARE

General (r) prof. univ. dr. Mircea MUREŞAN

Infrastructura pentru apărare constituie una dintre cele mai complexe şi mai sensibile probleme ale unei naţiuni, luând în considerare procesele actuale de integrare europeană şi internaţională ale unei organizaţii. Menţinerea securităţii actuale atât la nivel global, cât şi la nivel naţional este influenţată de transformările generate de integrarea economică la nivel mondial precum şi de dezvoltarea economiei la nivel naţional; de exemplu, migraţia forţei de muncă constituie un factor generator de noi riscuri şi ameninţări. Ca atare, conceptul tradiţional de securitate trebuie redefinit pentru a lua în calcul şi riscurile nonconvenţionale. În acest context, devine tot mai evident faptul că interesele şi obiectivele de securitate ale statelor pot fi realizate doar prin cooperare internaţională, în special cooperarea cu statele care au o fragilă stabilitate internă, pentru a diminua internalizarea riscului.

Procesele de aderare la NATO şi de integrare în Uniunea Europeană au determinat adaptări substanţiale ale strategiei de securitate a României. Calitatea de membru implică, în mod obligatoriu, configurarea treptată a unui rol specific şi activ al ţării noastre în cadrul celor două organizaţii şi asigurarea resurselor necesare pentru îndeplinirea acestui rol. Un element important al acestei strategii îl constituie infrastructura pentru apărare, incluzând şi elementele vitale care vizează pregătirea teritoriului, economiei şi a societăţii pentru a face faţă riscurilor şi ameninţărilor la adresa securităţii naţionale.

Existenţa unui sistem de infrastructură teritorială modern şi eficient, compatibil cu cel din cadrul acestor două organizaţii, reprezintă o piesă foarte

importantă în evoluţia României atât ca membru al NATO, cât şi ca stat membru al Uniunii Europene. De asemenea, încheierea aşa-numitului acord de acces dintre România şi Statele Unite ale Americii privind amplasarea facilităţilor militare americane pe teritoriul ţării noastre semnat la Bucureşti la 6 decembrie 2005, facilităţi care în perspectivă vor fi folosite şi de către NATO, demonstrează că potenţialele avantaje ale României, inclusiv cele ale infrastructurii teritoriale, sunt analizate cu atenţie şi vor fi incluse în viitoarele procese de planificare. Mai mult, organizarea la Bucureşti a Summitului NATO 2008 confirmă faptul că România poate să răspundă aşteptărilor aliaţilor săi şi că România rămâne un generator de securitate important.

Domeniile teoretice şi pragmatice pe care le implică cercetarea influenţei programelor comunitare cu finanţare externă asupra infrastructurii de apărare sunt numeroase. Cercetarea presupune analiza consistentă a situaţiei economiei româneşti, a economiei de piaţă, a stucturii de apărare, de sănătate şi de educaţie şi a efectelor acestora asupra securităţii interne, europene şi internaţionale. Vom încerca să analizam în ce măsură finanţarea dobândită de la Uniunea Europeană, sub forma programelor comunitare a contribuit şi contribuie la creşterea capacităţii infrastructurii româneşti de a răspunde nevoilor de apărare naţională şi europeană, şi cum pot fi aceste programe utilizate în cel mai eficient mod posibil.

Securitatea energetică şi alimentară, securitatea transporturilor şi a infrastructurii, securitatea sanitară, culturală şi ecologică, securitatea financiară şi informaţională constituie elemente cheie ale sistemului naţional de apărare. Infrastructura teritorială încorporează ansamblul construcţiilor, lucrărilor, obiectivelor, amenajărilor care, prin natura lor, deţin permanent sau pot obţine prin convertire/adaptare o utilizare în război sau în situaţii de criză, în sensul, pe de o parte, de a amplifica avantajele şi proprietăţile oferite de factorul natural geografic şi, pe de altă parte, de a contribui la valorificarea la cote maxime a capacităţii de apărare a tuturor forţelor precum şi la menţinerea viabilităţii Sistemului Naţional de Apărare. Infrastructurile de transport sunt obiective de interes naţional, atât cele civile cât şi cele militare, prin care se satisfac cererile de servicii publice, de transport călători şi mărfuri, şi se asigură necesităţile strategice ale ţării. Ele contribuie direct atât la asigurarea legăturii între toate localităţile ţării, cât şi la depăşirea frontierelor administrative şi la integrarea ţării în spaţiul economic, social şi cultural internaţional, european şi mondial. Pentru asigurarea funcţionalităţii infrastructurii de transport este necesară oprirea deteriorării tehnice şi operaţionale a sistemului de transport; restabilirea infrastructurii transporturilor şi alinierea la cerinţele actuale (viteză, elasticitate, confort, siguranţa circulaţiei şi protecţia mediului); racordarea economică la sistemul european de transport în contextul integrării sistemului naţional de transport în cel european; dezvoltarea

infrastructurii specifice transporturilor multimodale; modernizarea liniilor de cale ferată care să permită viteze de circulaţie de 140-160 km/h, precum şi a parcului de vagoane; reabilitarea sectoarelor prioritare din reţeaua de drumuri naţionale şi locale precum şi continuarea construirii de autostrăzi; continuarea modernizării porturilor, a trecerilor permanente peste cursurile de apă; modernizarea etapizată a infrastructurii aeroportuare pentru toate aeroporturile; extinderea lucrărilor de construcţii, montaj şi punere în exploatare a noi tronsoane de metrou.

În ceea ce priveşte asigurarea funcţionalităţii infrastructurii de telecomunicaţii, se impune realizarea reţelei naţionale de bază pe cablurile de fibră optică şi tehnologie S.D.H. (Ierarhia Digitală Sincronă), cu trei inele naţionale; realizarea inelelor regionale pe structura de bază în tehnologia SDH, ce vor face posibilă asigurarea legăturilor de rezervă între oricare localitate urbană de pe teritoriul ţării; conectarea centrelor mici cu cele regionale; realizarea sau dezvoltarea unor centre de comunicaţie de tip protejat inclusiv la comutaţie internaţională în scopul asigurării unui sistem de rezervare garantată; asigurarea posibilităţilor, prin lucrările de tip permanent, pentru conectarea directă a centrelor de transmisiuni la reţeaua naţională de fibră optică.

Dezvoltarea şi modernizarea infrastructurii reprezintă condiţia esenţială pentru progresul şi prosperitatea unei ţări, infrastructura reprezentând, pentru orice stat, coloana vertebrală a economiei. Ritmul de dezvoltare a României depinde astfel în mod esenţial de crearea unei infrastructuri moderne care să permită atragerea atât a investitorilor străini, cât şi a celor autohtoni.

România are de recuperat un decalaj foarte mare în domeniul infrastructurii, faţă de restul ţărilor membre ale Uniunii Europene. Mai multe studii internaţionale arată că starea proastă a drumurilor şi lipsa investiţiilor în acest segment reprezintă un impediment major în calea dezvoltării economice; aşadar două treimi din suprafaţa totală a infrastructurii din România trebuie refăcută. În aceste condiţii, modernizarea infrastructurii la standarde europene este una dintre priorităţile naţionale pentru perioada 2007-2013, aceasta din urmă fiind principala beneficiară a fondurilor de coeziune ale Uniunii Europene.

În România, dezvoltarea regională a început să se contureze o dată cu funcţionarea programului PHARE, în 1996. Realizarea unei dezvoltări regionale şi de reducere a disparităţilor economice şi sociale existente între diversele regiuni implică toate domeniile, de la cele strict economice (înfiinţare de IMM-uri, infrastructură, mediu, dezvoltarea agriculturii) la cele social-culturale (şomaj, resurse umane, educaţie). Dezvoltarea regională este un concept care urmăreşte impulsionarea şi diversificarea activităţilor economice, stimularea investiţiilor în sectorul privat, contribuţia la reducerea şomajului şi, nu în cele din urmă, să conducă la o îmbunătăţire a nivelului de trai. Infrastructura teritorială constituie, în

general, unul dintre cele mai deficitare domenii ale amenajării teritoriului din România.

Infrastructura teritorială a României este caracterizată prin sectoarele critice de căi rutiere şi feroviare nemodernizate, în stare necorespunzătoare de viabilitate şi cu o capacitate redusă de preluare a fluxurilor mari, prin puncte critice precum pasajele la nivel, traversările de localităţi, poduri, care prezintă disfuncţionalităţi majore. De asemenea, numeroase zone/localităţi sunt lipsite de legături telefonice, nu sunt racordate la sistemul energetic, nu sunt valorificate resursele de energie neconvenţională de care dispun, traseele intens solicitate sunt deficitare în asigurarea transportului în comun între localităţi, gările şi aeroporturile sunt nemodernizate.

Regiunile din România sunt sub nivelul mediu de dezvoltare economică al regiunilor din ţările membre ale Uniunii Europene, dar suferă şi de discrepanţe interne. Această situaţie face necesară adoptarea unui ansamblu de măsuri precum sprijinirea creşterii economice şi îmbunătăţirea condiţiilor de viaţă prin valorificarea eficientă a potenţialului regional şi local, stimularea iniţiativelor, stimularea cooperării interregionale interne, măsuri care au ca scop diminuarea dezechilibrelor regionale şi prevenirea altor dezechilibre internaţionale. Pentru a putea fi aplicată politica de dezvoltare regională s-au înfiinţat opt regiuni de dezvoltare, care cuprind tot teritoriul României. Fiecare regiune de dezvoltare cuprinde mai multe judeţe. Regiunile de dezvoltare nu sunt unităţi administrativ-teritoriale, nu au personalitate juridică, fiind rezultatul unui acord liber între consiliile judeţene şi cele locale.

Denumirea şi componenţa regiunilor de dezvoltare în România este următoarea:

⇨Regiunea de Dezvoltare **Nord-Est** - care grupează judeţele Bacău, Botoşani, Iaşi, Neamţ, Suceava şi Vaslui;

⇨Regiunea de Dezvoltare **Sud-Est** - care grupează judeţele Brăila, Buzău, Constanţa, Galaţi, Vrancea şi Tulcea;

⇨Regiunea de Dezvoltare **Sud-Muntenia** - care grupează judeţele Argeş, Călăraşi, Dâmboviţa, Giurgiu, Ialomiţa, Prahova şi Teleorman;

⇨Regiunea de Dezvoltare **Sud-Vest Oltenia** - care grupează judeţele Dolj, Gorj, Mehedinţi, Olt şi Vâlcea;

⇨Regiunea de Dezvoltare **Vest** - care grupează judeţele Arad, Caraş-Severin, Hunedoara şi Timiş;

⇨Regiunea de Dezvoltare **Nord-Vest** - care grupează judeţele Bihor, Bistriţa-Năsăud, Cluj, Sălaj, Satu Mare şi Maramureş;

⇨Regiunea de Dezvoltare **Centru** - care grupează judeţele Alba, Braşov, Covasna, Harghita, Mureş şi Sibiu;

⇨Regiunea de Dezvoltare **Bucureşti-Ilfov** - care grupează municipiul Bucureşti şi judetul Ilfov.

România a primit din momentul aderării la Uniunea Europeană asistenţă financiară pentru dezvoltare. Fondurile sunt alocate statelor membre potrivit politicilor Uniunii Europene. *Politica de coeziune economică şi socială (PCES)* reprezintă politica fundamentală a UE, fiindu-i alocat 1/3 din bugetul său, şi urmăreşte reducerea disparităţilor de dezvoltare economică şi socială între statele membre/regiunile UE, îmbunătăţirea funcţionării Pieţei unice şi promovarea dezvoltării stabile şi durabile a UE. Politicile complementare de dezvoltare sunt *Politica agricolă comună a Uniunii Europene* (PAC) şi *Politica comună de pescuit* (PCP).

Mijloacele financiare prin care se implementează PCES se numesc instrumente structurale şi cuprind fondurile structurale (Fondul European de Dezvoltare Regională şi Fondul Social European), şi Fondul de Coeziune. Aceste 3 fonduri sunt cunoscute sub denumirea generică de Fonduri Structurale şi de Coeziune (FSC).

Fondul European de Dezvoltare Regională (FEDR) susţine dezvoltarea economică durabilă la nivel regional şi local prin mobilizarea capacităţilor locale şi diversificarea structurilor economice în domenii precum cercetare şi dezvoltare tehnologică, inovare şi antreprenoriat, societatea informaţională, IMM-uri, protecţia mediului, turism, energie.

Fondul Social European (FSE) contribuie la sporirea adaptabilităţii forţei de muncă şi a întreprinderilor, creşterea accesului pe piaţa forţei de muncă, prevenirea şomajului, prelungirea vieţii active şi creşterea gradului de participare pe piaţa muncii a femeilor şi a migranţilor, sprijinirea incluziunii sociale a persoanelor dezavantajate şi combaterea discriminării.

Fondul de Coeziune (FC) finanţează proiecte în domeniul protecţiei mediului şi reţelelor de transport transeuropene, proiecte în domeniul dezvoltării durabile precum şi proiecte care vizează îmbunătăţirea managementului traficului aerian şi rutier, modernizarea transportului urban, dezvoltarea şi modernizarea transportului multimodal.

Documentele de programare care stau la baza implementării Fondurilor Structurale şi de Coeziune la nivel naţional sunt: Planul Naţional de Dezvoltare 2007-2013 (PND), Cadrul Strategic Naţional de Referinţă 2007-2013 (CSNR) şi Programele Operationale (PO). Fiecare PO este detaliat printr-un Program Complement (PC).

Pentru accesul la Fondurile Structurale şi de Coeziune (FSC) ale Uniunii Europene, România a elaborat Planul Naţional de Dezvoltare 2007-2013, pe baza strategiilor sectoriale de dezvoltare şi a strategiei naţionale de dezvoltare regională,

realizându-se astfel o programare a dezvoltării economice şi sociale a ţării, similară celei realizate de statele membre ale UE. Strategia stabileşte patru priorităţi tematice:

- ⇨ dezvoltarea infrastructurii la standarde europene;
- ⇨ îmbunătăţirea competitivităţii pe termen lung a economiei româneşti;
- ⇨ dezvoltarea şi utilizarea mai eficientă a capitalului uman;
- ⇨ construirea unei capacităţi administrative eficiente.

De asemenea, s-a stabilit o prioritate teritorială „Promovarea dezvoltării teritoriale echilibrate".

Implementarea strategiei Cadrului Strategic Naţional de Referinţă 2007-2013 se realizează prin programele operaţionale. Programele Operaţionale sunt elaborate de către Autorităţile de Management şi stabilesc domeniile majore de intervenţie ale Fondurilor Structurale şi de Coeziune, conform prevederilor regulamentelor europene. Elaborarea lor se realizează în coordonarea metodologică a Ministerului Finanţelor Publice. Finanţarea acţiunilor indicative din Programele Operaţionale se realizează din fonduri europene şi naţionale (buget de stat, bugete locale, alte surse publice, surse private).

Cadrul Strategic Naţional de Referinţă descrie strategia care sprijină Programele Operaţionale, care vor fi cofinanţate de Fondul European pentru Dezvoltare Regională, Fondul European Social şi Fondul de Coeziune.

Obiectivul global al *Programul Operaţional Sectorial de Transport* (finanţat din FEDR si FC) este de a promova un sistem de transport în România, care să faciliteze circulaţia rapidă şi eficientă, în condiţii de siguranţă şi la standarde europene, a persoanelor şi bunurilor, la nivel naţional şi internaţional. Pentru realizarea obiectivului POST, se propune ca fondurile de la UE şi de la buget să se concentreze pe modernizarea şi dezvoltarea infrastructurii TEN-T (Reţele Transeuropene de Transport) şi naţionale, pe toate modurile de transport. Reţeaua feroviară are un rol important în infrastructura de transport din România, iar dezvoltarea sa implică nu numai investiţii în infrastructură, ci şi îmbunătăţirea calităţii serviciilor. În cadrul acestui proces de modernizare, o atenţie deosebită va fi acordată dezvoltării durabile a sectorului transport.

→ *Axa prioritară 1*: Modernizarea şi dezvoltarea axelor prioritare TEN-T are scopul de a întări coeziunea teritorială dintre România şi statele membre UE, prin reducerea semnificativă a duratelor călătoriilor, în condiţii de siguranţă şi servicii de calitate sporite, către destinaţiile principale, în România şi în Europa, atât pentru pasageri, cât şi pentru mărfuri, de-a lungul axelor prioritare TEN-T 7, 18 şi 22. Aceasta se va realiza prin construirea de autostrăzi şi modernizarea celor existente, modernizarea infrastructurii feroviare şi navale, cu scopul de a creşte calitatea, eficienţa şi viteza de furnizare a serviciilor de transport şi creşterea

volumului traficului de pasageri şi marfă. Această axă prioritară se va concentra asupra dezvoltării reţelei de autostrăzi (prioritatea TEN-T nr.7) şi modernizării infrastructurii feroviare din punct de vedere al interoperabilităţii (prioritatea TEN-T nr.22). Se va acorda o atenţie specială transportului naval pe căile navigabile interioare (prioritatea TEN-T nr.18).

→ *Axa prioritară 2*: Modernizarea şi dezvoltarea infrastructurii naţionale de transport în afara axelor prioritare TEN-T urmăreşte modernizarea şi dezvoltarea infrastructurii rutiere, feroviare, navale şi aeriene din reţeaua naţională care se află în afara axelor prioritare TEN-T. Va creşte volumul şi viteza traficului de pasageri şi marfă, în condiţii de siguranţă şi calitate a serviciilor sporite, inclusiv în ceea ce priveşte interoperabilitatea feroviară. Pentru atingerea acestui obiectiv, POST va lua în considerare şi celelalte programe operaţionale şi va evita suprapunerile cu operaţiunile din cadrul acestora.

→ *Axa prioritară 3*: Modernizarea materialului rulant feroviar de pasageri din reţelele feroviare naţionale şi TEN-T urmăreşte promovarea echilibrului dintre modurile de transport. Urmăreşte furnizarea de servicii mai rapide, mai sigure şi de o calitate mai bună, la standarde europene de interoperabilitate, pentru transportul feroviar naţional şi internaţional de persoane, prin modernizarea materialului rulant de cale ferată, astfel încât transportul feroviar să poată concura cu transportul rutier, din ce în ce mai utilizat. Acest obiectiv se înscrie în efortul general de revitalizare a căilor ferate, pentru echilibrarea modurilor de transport, obiectivul Cartei Albe a CE: Politica europeană în transport până în 2010.

→ *Axa prioritară 4*: Dezvoltarea durabilă a sectorului de transport urmăreşte implementarea principiilor de dezvoltare durabilă a sectorului transport în România, conform concluziilor Consiliului European de la Cardiff (1998) şi Strategiei europene de dezvoltare durabilă (Gothenburg 2001). Va promova nivele crescute de siguranţă, va minimiza efectele adverse asupra mediului şi va promova transportul intermodal şi combinat.

Obiectivul global al *Programului Operaţional Sectorial de Mediu* (finanţat din FEDR şi FC) este de a îmbunătăţi standardele de viaţă şi calitatea mediului, punându-se accent în special pe respectarea acquis-ului privind mediul. Programul sectorial operaţional pentru mediu urmăreşte reducerea decalajului dintre Uniunea Europeană şi România, în ceea ce priveşte respectarea standardelor de mediu, luând în considerare următoarele scopuri pe termen lung: asigurarea accesului general la utilităţile publice de bază, îmbunătăţirea calităţii mediului şi consolidarea capacităţii instituţionale şi a guvernării. Obiectivele specifice ale axelor prioritare sunt formulate pe baza acquis-ului European de mediu şi a angajamentelor asumate în procesul de negociere la Capitolul 22 “Mediu”.

→ *Axa prioritară 1* - Extinderea şi modernizarea infrastructurii de apă şi apă uzată are ca obiective: asigurarea serviciilor de apă şi canalizare, la tarife accesibile, furnizarea de apă potabilă de calitate corespunzătoare în toate aglomerările urbane; îmbunătăţirea calităţii cursurilor de apă; creşterea calităţii managementului nămolurilor provenite din staţiile de epurare a apelor uzate.

→ *Axa prioritară 2* - Dezvoltarea sistemelor de management integrat al deşeurilor şi reabilitarea siturilor contaminate are ca obiective: creşterea ratei de conectare la servicii publice de salubritate, la un nivel calitativ adecvat şi la tarife accesibile; reducerea cantităţii de deşeuri depozitate; creşterea cantităţii de deşeuri reciclate şi refolosite; reducerea numărului de situri contaminate.

→ *Axa prioritară 3* - Îmbunătăţirea sistemelor municipale de termoficare în zonele prioritare selectate are ca obiective: reducerea emisiilor de poluanţi provenite de la centralele publice de termoficare; ameliorarea nivelului minim de concentraţie al poluanţilor în localităţile vizate; îmbunătăţirea stării de sănătate a populaţiei din localităţile vizate.

→ *Axa prioritară 4* - Implementarea sistemelor adecvate de management pentru protejarea naturii urmăreşte conservarea diversităţii biologice, a habitatelor naturale, a speciilor sălbatice de floră şi faună; asigurarea managementului durabil al zonelor protejate.

→ *Axa prioritară 5* - Implementarea unei infrastructuri adecvate pentru prevenirea riscurilor naturale în zonele cele mai vulnerabile are ca scop un management durabil al inundaţiilor în zonele cele mai expuse la risc; asigurarea protecţiei şi reabilitării litoralului Mării Negre.

Obiectivul general al *Programul Operaţional Sectorial Creşterea Competitivităţii Economice* (finanţat din FEDR) este de a contribui la creşterea productivităţii întreprinderilor româneşti, în primul rând prin modernizarea celor existente şi crearea unora noi, în special IMM-uri în sectoarele productive şi de servicii pentru afaceri. Dezvoltarea antreprenoriatului prin îmbunătăţirea accesului la finanţare şi la infrastructura de afaceri poate avea un rol important în conturarea unui mediu economic sănătos, cu reale posibilităţi de dezvoltare. Dezvoltarea infrastructurii de cercetare, dezvoltare şi inovare (CDI), creşterea calităţii şi diversificarea ofertei de servicii inovative destinate sectorului productiv, valorificarea potenţialului TIC (tehnologia informaţiilor şi comunicaţiilor) în procesele administrative ca şi în viaţa cotidiană, va avea rezultate aplicabile direct în economie şi va oferi pieţei o nouă generaţie de produse şi servicii cu valoare adăugată semnificativă.

Reducerea intensităţii energetice, producerea de energie din surse regenerabile, ca şi implementarea de tehnologii moderne pentru reducerea emisiilor datorate marilor instalaţii energetice va avea un impact direct asupra

competitivităţii economice, dar şi asupra protecţiei mediului. Nu în ultimul rând, promovarea României şi a potenţialului ei turistic poate impulsiona mediul economic în general şi competitivitatea prin sporirea încrederii investitorilor străini şi creşterea atractivităţii spaţiului românesc în străinătate.

→ *Axa prioritară 1*: un sistem inovativ de producţie are ca obiective: îmbunătăţirea/valorificarea echipamentului de producţie, prin extinderea şi modernizarea sa, inovarea proceselor productive şi sprijin pentru adoptarea standardelor internaţionale, promovarea creşterii gamei de produse; îmbunătăţirea serviciilor de consultanţă specializate şi sprijin pentru internaţionalizare în scopul dezvoltării segmentului de piaţă; asigurarea unui cadru favorabil dezvoltării antreprenoriatului prin reducerea constrângerilor existente în domeniile de eşec ale pieţei - acces la finanţare, instrumente financiare inovatoare, accesabilitatea infrastructurii şi a serviciilor de afaceri.

→ *Axa prioritară 2*: cercetare şi dezvoltare pentru asigurarea competitivităţii urmăreşte sprijinirea modernizării şi dezvoltării capacităţilor şi infrastructurii CDI, pentru a îmbunătăţi gama de servicii inovatoare şi calitatea acestora şi a stimula cererea de inovare din sectorul productiv.

→ *Axa prioritară 3*: TIC pentru sectoarele public şi privat are ca scopuri extinderea infrastructurii TIC, în special în zonele de eşec ale pieţei; promovarea introducerii inovării în sectorul productiv, în procesele administrative şi sociale; dezvoltarea unei pieţe pentru o nouă generaţie de conexiuni pentru produse şi servicii, sprijin pentru crearea de portaluri, dezvoltarea de sisteme informaţionale integrate pentru creşterea interoperabilităţii bazate pe sisteme GIS (geographic information systems) şi dezvoltarea de aplicaţii e-business.

→ *Axa prioritară 4*: creşterea eficienţei energetice şi dezvoltarea durabilă a sistemului energetic, a cărei obiective sunt: creşterea eficienţei energetice; intensificarea folosirii de surse energetice regenerabile; reducerea impactului sectorului energetic asupra mediului.

→ *Axa prioritară 5*: România – destinaţie atractivă pentru turism şi afaceri are ca scop îmbunătăţirea imaginii României ca şi destinaţie turistică, în scopul creşterii atractivităţii nu doar în scop turistic, ci şi pentru afaceri, precum şi crearea unui sistem integrat de oferte turistice.

Scopul *Programul Operaţional Regional* (finanţat din FEDR) este de a accelera creşterea economică a regiunilor rămase în urmă. Obiectivul poate fi atins doar printr-o coordonare strânsă cu acţiunile prevăzute pentru celelalte programe operaţionale. POR va acorda prioritate regiunilor rămase în urmă, folosind resurse regionale şi locale. Principalul mijloc de sprijinire a regiunilor este finanţarea diferenţiată, astfel încât regiunile rămase în urmă să primească proporţional mai multe fonduri decât cele dezvoltate.

→ *Axa prioritară 1*: îmbunătăţirea infrastructurii publice regionale şi locale prevede îmbunătăţirea infrastructurii de bază în transport, educaţie şi a infrastructurii sociale, cu scopul de a creşte atractivitatea şi accesibilitatea regiunilor şi de a stimula dezvoltarea lor socio-economică. Se va acorda o atenţie specială regiunilor mai puţin dezvoltate şi, de asemenea, zonelor din regiunile mai prospere care trec printr-o perioadă de declin. Domeniile principale de intervenţie identificate în infrastructura de transport şi socială sunt: reabilitarea/ modernizarea reţelelor judeţene şi locale de transport rutier; reabilitarea/ modernizarea/ dezvoltarea serviciilor de sănătate şi a infrastructurii sociale şi de siguranţă publică; reabilitarea/ modernizarea/ dezvoltarea infrastructurii educaţionale.

→ *Axa prioritară 2*: întărirea mediului de afaceri regional şi local urmăreşte creşterea contribuţiei economiilor locale şi regionale la crearea produsului intern brut, prin sprijinirea acelor economii care au devenit mai puţin competitive în economia de piaţă şi crearea de structuri economice funcţionale, pentru susţinerea utilizării eficiente a potenţialului endogen al regiunilor – resurse naturale, materii prime, resurse umane – şi pentru stimularea economiilor regionale. Domeniile principale de intervenţie sunt: dezvoltarea structurilor de sprijin pentru afaceri specifice fiecărei regiuni şi sprijinirea iniţiativelor antreprenoriale locale.

→ *Axa prioritară 3*: dezvoltarea turismului regional şi local urmăreşte crearea de surse suplimentare de venit la nivel regional/local şi crearea de noi locuri de muncă, prin dezvoltarea patrimoniului istoric, natural şi cultural al tuturor regiunilor (şi în interiorul regiunilor, în zonele izolate, cu potenţial turistic, care pot contribui la dezvoltarea lor economică şi la reducerea gradului de izolare). Domeniile principale de intervenţie sunt: restaurarea şi dezvoltarea patrimoniului cultural şi istoric; dezvoltarea resurselor turistice naturale în contextul dezvoltării durabile; creşterea calităţii serviciilor turistice din punct de vedere al condiţiilor de cazare şi recreere.

→ *Axa prioritară 4*: dezvoltarea urbană durabilă urmăreşte creşterea rolului centrelor urbane în dezvoltarea economică locală şi regională prin regenerarea/revitalizarea oraşelor mici şi mijlocii, precum şi a unor părţi ale oraşelor mari, cu scopul reducerii disparităţilor existente. Domeniile principale de intervenţie vor fi legate de sprijinirea regenerării urbane prin finanţarea de proiecte integrate de regenerare urbană pentru zonele urbane defavorizate („zone urbane de acţiune”), delimitate clar, din punct de vedere spaţial, în interiorul zonelor urbane. Aceste proiecte vor viza: reabilitarea mediului construit, dezvoltarea centrelor urbane şi a spaţiilor publice pentru a creşte calitatea vieţii şi a încuraja activităţile economice; stimularea antreprenoriatului, crearea de oportunităţi de ocupare, furnizarea de servicii de consiliere; sprijinirea incluziunii sociale, care va asigura

şanse egale pentru bărbaţi şi femei, precum şi condiţii pentru o mai bună integrare în viaţa socială şi piaţa muncii.

Obiectivele strategice ale *Programul Operaţional Sectorial Dezvoltarea Resurselor Umane* (finanţat din FSE) POS DRU sprijină îndeplinirea obiectivelor comune la nivel European, în ceea ce priveşte participarea sporită pe piaţa muncii a unei forţe de muncă înalt calificate şi adaptabile, îmbunătăţirea sistemului educaţional şi creşterea adaptabilităţii acestuia la cererea pieţei muncii, promovarea educaţiei pe tot parcursul vieţii, creşterea adaptabilităţii angajaţilor şi a întreprinderilor, asigurarea calificărilor şi cunoştinţelor necesare integrării şi mobilităţii pe piaţa muncii şi facilitarea dezvoltării economice. PO urmăreşte promovarea şi dezvoltarea tuturor formelor de economie socială ca şi modalitate de asigurare a incluziunii sociale a personalelor care aparţin grupurilor vulnerabile, minorităţilor etnice sau populaţiei rromă.

→ *Axa prioritară 1* – educaţia şi formarea profesională în sprijinul creşterii economice şi dezvoltării societăţii bazate pe cunoaştere are ca obiective asigurarea premiselor pentru dezvoltarea unui capital uman competitiv prin dezvoltarea rutelor flexibile de învăţare pe tot parcursul vieţii, furnizarea de servicii educaţionale şi de formare profesională continuă moderne şi de calitate pentru toţi, care să răspundă cerinţelor specifice ale pieţei muncii şi societăţii bazate pe cunoaştere; modernizarea sistemului de educaţie şi formare profesională astfel încât să satisfacă nevoile pieţei muncii şi asumarea unei abordări comune a învăţării şi instruirii; sprijinirea asigurării calităţii, elaborarea curriculelor şcolare în sprijinul competitivităţii, asigurarea relevanţei ofertelor educaţionale.

→ *Axa prioritară 2* – conectarea învăţării pe tot parcursul vieţii cu piaţa muncii urmăreşte crearea premiselor pentru îmbunătăţirea nivelului de educaţie, dezvoltarea de programe de învăţare bazate pe acţiune şi creşterea capacităţii de angajare a resurselor umane pe tot parcursul vieţii, în contextul societăţii bazate pe cunoaştere; asigurarea educaţiei pe tot parcursul vieţii şi a însuşirii competenţelor şi aptitudinilor cerute pe piaţa muncii.

→ *Axa prioritară 3* – creşterea adaptabilităţii forţei de muncă şi a întreprinderilor se referă, în principal, la specializarea şi adaptarea forţei de muncă.

→ *Axa prioritară 4* – modernizarea Serviciului Public de Ocupare are ca scopuri modernizarea SPO, diversificarea şi actualizarea serviciilor în sprijinul unei bune funcţionări a pieţei muncii.

→ *Axa prioritară 5* – promovarea măsurilor active de ocupare şi *Axa prioritară 6* - Promovarea incluziunii sociale urmăresc, în special, ocuparea forţei de muncă şi reducerea şomajului.

Obiectivul general al *Programul Operaţional pentru Dezvoltarea Capacităţii Administrative* (finanţat din FSE) PO DCA este acela de a contribui la

realizarea obiectivelor naţionale şi ale Uniuni Europene de a obţine progresul în dezvoltarea socio-economică potrivit obiectivelor de coeziune şi convergenţă. Realizarea obiectivului general se va reflecta în creşterea activităţilor economice din România, creşterea gradului de ocupare a forţei de muncă şi în îmbunătăţirea măsurabilă a furnizării de servicii publice la nivelul administraţiei publice centrale şi locale. Aceste realizări vor fi legate în mod direct de implementarea cu succes a unui pachet de reforme ale administraţiei publice care vizează întărirea capacităţii de management.

→ *Axa prioritară 1*: întărirea intervenţiilor de politici publice în administraţia centrală are ca obiective: să contribuie la dezvoltarea capacităţii administrative a administraţiei centrale din România; să modernizeze şi să integreze procesele de formulare a propunerilor de politici publice (PPP-uri) şi relaţionarea lor cu planurile instituţionale strategice (PIS-uri); finalizarea reformelor funcţiei publice care vizează raţionalizarea structurilor administraţiei centrale, implementarea managementului performanţei şi consolidarea reformelor prin intervenţii durabile de instruire; introducerea unei culturi de monitorizare şi evaluare a rezultatelor.

→ *Axa prioritară 2*: dezvoltarea capacităţii de îmbunătăţire a performanţei serviciilor în administraţia locală urmăreşte să contribuie la reforma administraţiei publice la nivel judeţean şi subjudeţean prin implementarea unui pachet de management al reformei care se adresează unor elemente cheie ale ciclului de management strategic; să modernizeze şi să integreze procesele privind planificarea strategică şi a activităţilor, managementul resurselor umane (managementul performanţei) şi rezultatul activităţilor de monitorizare şi evaluare; să ofere sprijin pentru implementare organizaţiilor judeţene şi subjudeţene (municipalităţi şi comune), pentru creşterea eficienţei şi calităţii furnizării de servicii publice.

Obiectivul *Programului Operaţional pentru Asistenţă Tehnică* (finanţat din FEDR) la nivel naţional este de a asigura sprijin pentru coordonarea şi implementarea instrumentelor structurale în România.

→ *Axa prioritară 1*: sprijin pentru implementarea instrumentelor structurale şi pentru coordonarea programelor are ca obiectiv: atingerea unei capacităţi administrative suficiente pentru o implementare şi absorbţie eficientă şi efectivă a instrumentelor structurale în perioada 2007-2013 şi pregătirea intervenţiilor viitoare ale instrumentelor structurale.

→ *Axa prioritară 2*: dezvoltarea şi sprijinirea în continuare a funcţionării Sistemului Informatic Unic de Management (SMIS) va asigura funcţionarea SMIS, dezvoltarea organizaţională şi funcţională şi extinderea continuă a sistemului, astfel încât să permită accesul prompt la date din toate instituţiile implicate în procesul

instrumentelor structurale şi instituirea unui management eficient al programelor europene, în conformitate cu reglementările naţionale şi europene.

→ *Axa prioritară 3*: diseminarea de informaţii şi promovarea instrumentelor structurale urmăreşte informarea potenţialilor candidaţi cu privire la oportunităţile existente şi promovarea cunoaşterii publice a obiectivelor şi realizărilor instrumentelor structurale şi ale Planului Naţional de Dezvoltare, precum şi asigurarea recunoaşterii rolului instrumentelor structurale ale UE.

Planul Naţional de Dezvoltare (PND) este un concept specific politicii europene de coeziune economică şi socială (Cohesion Policy), menit să ofere o concepţie coerentă şi stabilă privind dezvoltarea statelor membre ale Uniunii Europene, transpusă în priorităţi de dezvoltare, programe, proiecte, în concordanţă cu principiul programării fondurilor structurale. PND are rolul major de a alinia politica naţională de dezvoltare la priorităţile comunitare de dezvoltare, prin promovarea măsurilor considerate stimuli de dezvoltare socio-economică durabilă la nivel european.

În condiţiile decalajelor importante de competitivitate pe care România le prezintă în raport cu statele membre UE, creşterea competitivităţii economice şi dezvoltarea economiei bazate pe cunoaştere reprezintă creşterea productivităţii întreprinderilor româneşti pentru reducerea decalajelor faţă de productivitatea medie la nivelul Uniunii. Se urmăreşte generarea până în anul 2015 a unei creşteri medii a productivităţii de cca. 5,5% anual, permiţând României să atingă un nivel de aproximativ 55% din media UE. Se urmăreşte susţinerea investiţiilor productive (utilaje şi tehnologii noi), susţinerea certificării întreprinderilor şi a produselor, crearea unui mediu favorabil finanţării afacerilor, dezvoltarea infrastructurii de afaceri (incubatoare, centre de afaceri, clustere emergente), sprijinirea eforturilor de internaţionalizare a întreprinderilor, precum şi prin promovarea potenţialului turistic românesc.

Obiectivul general al strategiei în domeniul transporturilor îl reprezintă asigurarea unei infrastructuri de transport extinse, moderne şi durabile, precum şi a tuturor celorlalte condiţii privind dezvoltarea sustenabilă a economiei şi îmbunătăţirea calităţii vieţii, astfel încât volumul activităţii de transport în PIB să crească de la 3,6 miliarde euro (în prezent) la minimum 7,0 miliarde euro până în 2015. Pentru atingerea acestui obiectiv, strategia dezvoltării şi modernizării infrastructurii de transport se va realiza prin intermediul modernizării şi dezvoltării infrastructurii de transport transeuropene şi a reţelelor de legătură, prin modernizarea şi construcţia de infrastructuri rutiere, feroviare, navale şi aeroportuare transeuropene şi modernizarea şi construcţia reţelelor de legătură la TEN-T, prin modernizarea şi dezvoltarea infrastructurii de transport de interes naţional şi îmbunătăţirea serviciilor aferente, prin modernizarea şi construcţia de

infrastructuri rutiere, feroviare (inclusiv serviciile aferente) şi navale. Dezvoltarea durabilă a sectorului transporturi se va realiza, de asemenea, prin promovarea intermodalităţii, îmbunătăţirea siguranţei traficului pe toate modurile de transport, reducerea impactului lucrărilor şi activităţilor de transport asupra mediului înconjurător şi punerea în siguranţă a infrastructurii de transport.

În ceea ce priveşte protecţia mediului, se urmăreşte îmbunătăţirea standardelor de viaţă prin asigurarea serviciilor de utilităţi publice la standardele de calitate şi cantitate cerute, în sectoarele de apă şi deşeuri, prin dezvoltarea sistemelor de infrastructură de apă şi apă uzată în localităţile vizate şi crearea/consolidarea companiilor regionale de profil, şi prin dezvoltarea sistemelor integrate de management al deşeurilor (colectare, transport, tratare/eliminare a deşeurilor în localităţile vizate; închiderea depozitelor neconforme). De asemenea, se doreşte îmbunătăţirea sistemelor sectoriale de management de mediu, cu accent pe: dezvoltarea sistemelor specifice de management al apei şi deşeurilor, a celor de management al resurselor naturale (conservarea diversităţii biologice, reconstrucţia ecologică a sistemelor deteriorate, prevenirea şi intervenţia în cazul riscurilor naturale – în special inundaţii), precum şi pe îmbunătăţirea infrastructurii de protecţie a aerului.

Dezvoltarea economiei rurale şi creşterea productivităţii în sectorul agricol vizează dezvoltarea unei agriculturi competitive bazată pe cunoaştere şi iniţiativă privată, precum şi protejarea patrimoniului natural cultural şi istoric al zonelor rurale din România. Se doreşte creşterea competitivităţii economiei agro-alimentare şi silvice prin adaptarea ofertei la cerinţele pieţei, în cadrul căreia va fi acordat sprijin financiar cu precădere pentru modernizarea fermelor şi îmbunătăţirea capitalului uman din agricultură (măsuri de consultanţă şi sprijinire a tinerilor fermieri, măsuri de încurajare a asocierii producătorilor), precum şi pentru îmbunătăţirea calităţii produselor; creşterea standardelor de viaţă în zonele rurale prin diversificarea activităţilor rurale: stimularea activităţilor nonagricole, promovarea agroturismului precum şi dezvoltarea de microîntreprinderi în amontele şi avalul producţiei agricole, toate acestea în contextul unor servicii de bază de bună calitate. Dezvoltarea economică durabilă a fermelor şi a exploataţiilor forestiere, vizează implementarea unor acţiuni ce privesc utilizarea durabilă a terenului agricol şi forestier, materializate în acordarea de plăţi pentru agromediu si bunăstarea animalelor, plăţi compensatorii pentru terenurile cu handicap natural, precum şi prime de împădurire, dar şi în realizarea unor acţiuni de prevenire a calamităţilor naturale.

Diminuarea disparităţilor de dezvoltare între regiunile ţării presupune creşterea economică mai accelerată a regiunilor slab dezvoltate, în vederea diminuării disparităţilor de dezvoltare interregionale şi intraregionale.

Operaţionalizarea priorităţii PND privind dezvoltarea echilibrată a tuturor regiunilor ţării se va realiza printr-o abordare integrată, bazată pe o combinare a investiţiilor publice în infrastructura locală, politici active de stimulare a activităţilor de afaceri şi sprijinirea valorificării resurselor locale. Se urmăreşte îmbunătăţirea infrastructurii publice regionale şi locale: creşterea competitivităţii regiunilor ca locaţii pentru afaceri prin îmbunătăţirea infrastructurii de transport, a infrastructurii de sănătate, servicii sociale şi educaţie, precum şi a infrastructurii de siguranţă publică pentru situaţii de urgenţă, dezastre naturale şi tehnologice; consolidarea mediului de afaceri regional şi local: dezvoltarea infrastructurii de afaceri şi sprijinirea activităţilor locale de afaceri cu caracter inovativ, favorizând şi crearea unor necesare conexiuni între activităţile productive şi cele de cercetare-dezvoltare-inovare; dezvoltarea turismului regional şi local: creşterea gradului de atractivitate turistică a regiunilor prin crearea unei infrastructuri adecvate şi îmbunătăţirea serviciilor specifice, dezvoltarea de forme alternative de turism, protecţia şi promovarea patrimoniului natural şi cultural la nivel local şi regional; dezvoltare urbană durabilă: regenerarea zonelor urbane afectate de restructurarea industrială sau care se confruntă cu grave probleme socio-economice, precum şi consolidarea reţelei de centre urbane cu potenţial de dezvoltare, pentru a le permite să acţioneze ca motoare ale creşterii economice regionale); cooperarea teritorială europeană. Această subprioritate se încadrează în noul Obiectiv de intervenţie din cadrul Politicii de Coeziune pentru perioada 2007-2013, „Cooperare teritorială europeană", dedicat integrării armonioase şi echilibrate a întregului teritoriu al UE, prin sprijinirea cooperării între diferitele sale entităţi teritoriale la nivel transfrontalier, transnaţional şi interregional, în probleme de importanţă comunitară. Subprioritatea va fi realizată prin promovarea de acţiuni în domeniul cooperării transfrontaliere, transnaţionale şi interregionale, în vederea integrării socio-economice a zonelor de graniţă şi creşterii atractivităţii şi accesibilităţii regiunilor României în cadrul teritoriului european.

Pentru România este necesară declanşarea unui amplu proces de dezvoltare, modernizare şi asigurare a protecţiei infrastructurii critice, a elementalor vitale ce vizează pregătirea instituţiilor, societăţii, economiei şi teritoriului naţional pentru a face faţă riscurilor şi ameninţărilor la adresa securităţii. Este necesară reconfigurarea instituţiilor şi procedurilor naţionale în concordanţă cu dinamica procesului unional şi pentru adaptarea legislaţiei, a doctrinelor şi strategiilor la exigenţele impuse de noile riscuri şi ameninţări, la provocările generate de schimbările meteo-climatice, precum şi la cerinţele determinate de nevoile de cooperare în cadrul NATO, Uniunii Europene şi parteneriatelor strategice.

Opţiunile strategice ale României au în vedere dezvoltarea rapidă a unor reţele de infrastructură specializate, eficiente şi rezistente la diferite încercări. Acestea trebuie să fie compatibile cu reţelele europene şi euroatlantice, capabile să potenţeze atât dezvoltarea susţinută şi modernizarea accelerată a economiei, cât şi securitatea naţională. În acest scop, vor fi lansate programe ample de investiţii naţionale, în cooperare şi în parteneriat. Domeniile de interes major privesc în mod deosebit: infrastructura de transport, construcţia de autostrăzi şi modernizarea rapidă a infrastructurii feroviare – şi reţeaua de management a traficului; infrastructura energetică; infrastructura de comunicaţii; managementul potenţialului hidrografic şi protecţia împotriva inundaţiilor; restructurarea sistemului bazelor militare.

Principalele direcţii de acţiune pentru adaptarea şi modernizarea infrastructurii vor fi: reabiltarea, modernizarea şi dezvoltarea infrastructurii de transport în vederea îmbunătăţirii calităţii serviciilor, eficientizării transportului de călători şi marfă şi alinierea la standardele sistemului european de transport; dezvoltarea, securizarea şi realizarea – pe rute alternative – a unor noi reţele de aprovizionare cu energie, în consens cu proiectele strategice ale Uniunii Europene şi cu interesele României în regiunea Mării Negre; promovarea noilor tehnologii şi dezvoltarea sistemului informatic din domeniul securităţii, în conformitate cu standardele europene; adaptarea programului naţional de securitate aeronautică şi portuară la noile tipuri de ameninţări; modernizarea infrastructurii militare specifice, precum şi pregătirea şi modernizarea capacităţilor oferite în cadrul NATO, Uniunii Europene şi parteneriatelor strategice; identificarea domeniilor de risc, elaborarea hărţilor cuprinzând riscuri probabile şi dezvoltarea într-o concepţie nouă a infrastructurii, pentru apărarea populaţiei de pericolele unor calamităţi naturale, dezastre şi accidente ecologice; reducerea riscului de declanşare a unor incidente sau accidente nucleare şi asigurarea securităţii instalaţiilor nucleare.

Un rol important revine elaborării unei strategii unitare de fiabilizare, protecţie, pază şi apărare a infrastructurii critice, capabilă să asigure continuitate, coerenţă, unitate metodologică şi procedurală, precum şi o reală eficienţă antiteroristă. Securitatea infrastructurii critice va viza atât contracararea riscurilor generate de acţiuni ostile, cât şi a celor produse de accidente sau forţe ale naturii. Ea trebuie să prevadă atât măsurile de suport şi rezistenţă, cât şi cele de reabilitare rapidă a funcţionării activităţilor în cazul distrugerii sau avarierii elementelor de infrastructură.

Aflată într-o etapă nouă, cea a apartenenţei reale la comunitatea europeană şi euroatlantică, România îşi afirmă, prin strategia sa de securitate naţională, vocaţia de contributor activ, substanţial şi predictibil la securitatea internaţională şi regională, de ţară cu un profil strategic distinct în cadrul NATO şi al Uniunii

Europene. Printr-o abordare integratoare a direcţiilor strategice de acţiune şi a eforturilor consacrate înfăptuirii obiectivelor propuse, acest proiect naţional poate deveni o realitate, având ca rezultat o ţară modernă, mai sigură şi prosperă, componentă activă şi demnă a comunităţii europene şi euroatlantice. Viziunea ce animă această strategie şi direcţiile de acţiune stabilite vor constitui baza conceptuală pentru elaborarea celorlalte documente vizând funcţionarea instituţiilor ce compun sectorul securităţii naţionale, precum şi elementele de bază în fundamentarea programelor de alocare a resurselor.

Principala resursă pentru îndeplinirea acestui program o reprezintă voinţa politică a forţelor cărora poporul le-a încredinţat responsabilitatea guvernării şi legătura acestora cu poporul, cu oamenii care şi-au pus speranţele în acest program. Responsabilitatea politică faţă de oameni şi pentru securitatea lor este, în acelaşi timp, o imensă responsabilitate morală.

Realizarea obiectivelor strategiei securităţii naţionale implică un efort major de conştientizare a acestei răspunderi şi a nevoii de consolidare a bazei politice şi civice a guvernării, precum şi cerinţa apelului la judecata poporului şi la angajarea sa conştientă în realizarea programului. Experienţa de aproape două decenii în dinamizarea eforturilor vizând construcţia democraţiei şi a prosperităţii dă măsura maturităţii societăţii româneşti, iar apartenenţa ţării noastre la comunitatea euroatlantică reprezintă principala garanţie de securitate.

BIBLIOGRAFIE

*** Strategia de Securitate Naţională a României, Bucureşti, 2007
*** Cadrul Strategic Naţional de Referinţă 2007-2013
*** Planul Naţional de Dezvoltare a României 2007-2013
Cernăianu, Adrian, *Infrastructura teritorială şi acţiunile militare*, Editura Universităţii Naţionale de Apărare „Carol I", Bucureşti, 2003
www.fondurile-europene.ro
www.guv.ro

PROTECȚIA INFRASTRUCTURILOR CRITICE. RISCURI LA ADRESA INFRASTRUCTURII CRITICE NAȚIONALE ŞI STRATEGII DE PROTECȚIE ŞI SECURITATE

Comandor (r) dr. Marian SANDU

Infrastructurile critice pot fi deteriorate, distruse sau perturbate de acte teroriste deliberate, catastrofe naturale, neglijență, accidente sau piraterie informatică, activități criminale şi comportament rău intenționat. Pentru a salva viața şi bunurile oamenilor ce locuiesc in comunitatea UE, expusi riscului provocat de terorism, dezastre naturale şi accidente, orice disfuncționalitate sau manipulări de infrastructuri critice ar trebui, în măsura posibilului, să fie scurtate, gestionate, izolate geografic şi minimalizate în detrimentul bunăstării statelor membre, cetățenilor lor şi Uniunii Europene. Recentele atentate teroriste de la Madrid şi Londra, au subliniat riscul de atacuri teroriste împotriva infrastructurii europene. Răspunsul UE trebuie să fie rapid, prin urmare, coordonat şi mai eficient.

Situația politico-economică a României şi impactul acesteia asupra infrastructurii critice

În timp ce amenințările la care este expusă țara noastră evoluează şi interesele noastre în materie de securitate persistă, este posibilă apariția unui fenomen de degradare a capacității de răspuns a statului român la diversele provocări, riscuri şi amenințări la adresa securității naționale.

Societatea românească este marcată de trei mari procese centrifuge: managementul defectuos al procesului tranziției economice şi sociale (*cu accente pe fenomenul corupției, inerției birocratice şi politizării instituțiilor statului)*

standardele mult prea ridicate impuse de instituţiile europene (*care nu pot fi de prea multe ori îndeplinite, dar care impun mari restricţii multor proiecte de investiţii majore)* efectele nefaste ale crizei financiare mondiale (*care se reflectă în mod direct asupra capacităţii statului de a asigura cofinanţările necesare pentru demararea marilor proiecte de infrastructură).*

Toate acestea au dus, în mod gradual, dar dramatic, la două efecte pe termen mediu şi lung:

- diminuarea eficienţei instituţiilor statului în modernizarea infrastructurii pe toate cele trei paliere (aerian, terestru şi naval);

- degradarea continuă a infrastructurii existente, ceea ce semnifică, de fapt, lipsa resurselor (de toate tipurile) pentru conservarea, păstrarea infrastructurii critice deja existente.

În schimb, trebuie recunoscut faptul că în spaţiul electromagnetic evoluţia infrastructurii a avut o caracteristică exponenţială datorită investiţiilor majore ale companiilor multinaţionale în dezvoltarea comunicaţiilor prin satelit, telefoniei mobile şi comunicării prin INTERNET. Totuşi, dispunerea acestor infrastructuri pe teritoriul României nu înseamnă, în mod necesar, că acestea şi aparţin României, acesta fiind şi primul exemplu de infrastructură critică la nivel european care trebuie protejată împotriva diverselor tipuri de riscuri. Şi nu neapărat împotriva riscurilor naturale, ci împotriva atacurilor teroriste.

Referindu-ne la România şi la infrastructura „clasică", de fapt, principalele riscuri la adresa securităţii naţionale, în care evident că includem, ca o parte vitală, şi „cantitatea şi calitatea" infrastructurii critice, este indecizia politică, lipsa unei viziuni clare de securitate, factorul economic şi interesele specifice. În plus, la acestea se adaugă şi incoerenţa sau, mai bine spus, lipsa de coeziune a decidenţilor de la Bruxelles în identificarea axelor principale de interes în domeniul infrastructurii critice europene la care România este conectată.

Dinamica riscurilor la adresa infrastructurii critice

Poate fi considerată infrastructura critică, mai bine spus calitatea ei, un indicator de rangul întâi al gradului de asigurare a securităţii naţionale? Mai mult decât celelalte dimensiuni ale securităţii, infrastructura declanşează mereu un discurs dramatic în favoarea securizării, atât din partea guvernelor, cât mai ales din partea societăţii civile, însă rezultatele nu sunt întotdeauna încununate cu succes, chiar şi atunci când măsurile luate sunt de mare amploare.

Priorităţile celor două agende nu sunt întotdeauna clare şi, oricum, chiar dacă acestea pot converge la un moment dat, ele nu vor evidenţia, mai niciodată, importanţa infrastructurii ca generator de securitate, ci mai mult ca generator de bunăstare. Ceea ce ar fi suficient, totuşi.

Există dezbateri aprinse asupra tipului de probleme ce pot fi politizate şi cele care necesită intervenţie imediată. Evident, dezastre concrete, precum Cernobâlul sau inundaţiile masive (vezi cazul Asiei de Sud-Est devastată de tsunami şi cel al României), dictează acţiuni imediate care să prevină repetarea lor.

Totuşi, în general, locaţia geografică şi nivelul de bunăstare al ţării respective joacă un rol decisiv în interesul acordat combaterii efectelor dezastrului. De exemplu, guvernele ţărilor sărace tind să perceapă politicile industriale de mediu drept ceva pe care nu şi-l pot permite.

Studiile de specialitate[1] au arătat că, în principal, există trei categorii de ameninţări la adresa securităţii infrastructurii.

1. Ameninţările din partea mediului natural la adresa civilizaţiei umane, ce nu sunt rezultatul acţiunilor umane:

- cosmice: căderi de meteoriţi, asteroizi, radiaţii cosmice, solare, magnetism cosmic sau solar, schimbarea ciclului solar;
- geofizice: cutremure, erupţii vulcanice, magnetism terestru, alunecări de teren, tsunami etc.
- climatice: inundaţii, furtuni, uragane, incendii, încălzirea globală;
- ciclul natural de întoarcere la o epocă glaciară.

2. Ameninţările cauzate de acţiunile umane asupra sistemelor naturale sau structurilor planetei, atunci când schimbările făcute par a constitui ameninţări existenţiale la adresa unei părţi sau a întregii civilizaţii. Un exemplu evident este poluarea, ce are printre efecte distrugerea stratului de ozon, deşi dezbaterile sunt foarte aprinse asupra ritmului şi gradului în care poluarea într-adevăr afectează climatul!

3. Ameninţările cauzate de acţiunile umane asupra sistemelor naturale sau structurilor planetei, atunci când schimbările făcute nu par a constitui ameninţări existenţiale la adresa unei părţi sau a întregii civilizaţii, însă, pe termen lung, există efecte perverse (de exemplu, exploatarea resurselor minerale).

4. Ameninţările cauzate de utilizarea diverselor forme şi metode ale luptei armate neconvenţionale: atacuri chimice, biologice, radiologice şi nucleare, acţiuni teroriste, acţiuni tehnologice. Oricum, însă, orice formă de război, fie ea şi convenţional, aduce mari prejudicii mediului prin violenţa acţiunilor de luptă şi prin distrugerile provocate.

Pentru România însă, un alt tip de ameninţare îl poate reprezenta indecizia politică în gestionarea infrastructurii. De exemplu, dacă între 1967 si 1989

[1] Buzan, Barry, Ole Waever şi Jaap de Wilde, *Security: A New Framework for Analysis*, Lynne Rienner Publishers Inc., USA, Colorado, 1998.

România şi-a mărit capacitatea de transport rutier de la 4.000 de kilometri de drumuri naţionale la 15.000 de kilometri prin modernizarea mai multor drumuri judeţene, între 1990 şi 2009, situaţia practic a stagnat, doar câteva sute de kilometri de drum naţional fiind modernizate, fiind construite doar aproximativ 200 de km de autostradă. Această indecizie duce, pe de o parte, la lipsa infrastructurii necesare preluării fluxului extraordinar de bunuri şi servicii ceea ce poate duce, implicit, la o ameninţare la adresa dezvoltării economice a ţării. Pe de altă parte, lipsa de preocupare pentru întreţinerea infrastructurii existente poate duce la o degradare continuă a acesteia. De exemplu, din cauza lipsei de investiţii în acest domeniu au avut loc mai multe incidente, cum ar fi prăbuşirea podului feroviar de la Grădiştea, de pe ruta Bucureşti - Giurgiu, în 2005. Acesta nu a mai fost refăcut, prelungindu-se drumul cu 70 de kilometri faţă de distanţa iniţială.

Strategii** *de protecţie şi securitate

Nu se poate spune că există o strategie bună şi o strategie mai puţin bună atunci când vorbim despre protecţia infrastructurii, ci doar despre capacitatea de transformare a acestora în proiecte şi despre capacitatea de aplicare a lor. Şi România a încercat să pună la punct diverse strategii comune pentru gestionarea infrastructurii critice.

Există, însă, câteva elemente care, din start, viciază eficienţa acestora:

- lipsa reală a unui element central, unic coordonator în acest domeniu – cum există, de exemplu, în Statele Unite Agenţia FEMA (Federal Emergency Management Act);
- absenţa unui buget clar, dedicat, specific infrastructurii, dar şi existenţa unei alocări separate, sectoriale a fondurilor;
- incoerenţa politicilor guvernamentale şi punerea accentului pe problematici diferite, în funcţie de interesele de moment ale agenţiilor guvernamentale respective;
- nu în ultimul rând, falimentul politicilor comune europene, în domeniul energiei, securităţii, agriculturii etc.

Europa şi infrastructura

Atât timp cât infrastructura critică era legată doar de teritoriul naţional, această temă nu a prezentat o preocupare majoră a Europei. Însă, odată cu procesul de integrare graduală a tuturor statelor la construcţia europeană, s-a ajuns la concluzia, evidentă de altfel, că infrastructura nu mai deserveşte un stat anume, ci

* O definiţie a strategiei este dată de Eugen Siteanu în articolul "Strategia militară şi alte tipuri de strategii", în Revista de Ştiinţe Militare nr.1., 2010, pp.79-80.

este o componentă a marii infrastructuri europene. De aceea, nimeni nu mai poate spune că viabilitatea drumurilor, reţelelor de transport energetic, conductelor de gaze[2], transportului maritim[3] şi fluvial sunt apanajul exclusiv al statelor naţionale. Globalizarea accelerată a impus concluzia unei anumite pierderi a suveranităţii statelor în acest domeniu, o pierdere a suveranităţii, de astă dată, în sens pozitiv. Deoarece este evident că, pentru a-şi asigura securitatea propriei infrastructuri, trebuie să se bazeze pe o cooperare, pe o strategie de protecţie comună, în cadrul instituţiilor şi structurilor europene comune, şi totuşi, de prea multe ori, se spune că Europa sau Uniunea Europeană, din punct de vedere al omogenităţii infrastructurii, se termină la graniţa Ungariei cu România.

Europa este interesată să aibă o infrastructură solidă, de încredere şi care să fie în aşa fel proiectată şi întreţinută încât să poată prelua necesităţile curente şi să poată fi de încredere pentru viitoarele dezvoltări ale economiei europene din următoarele decenii. Şi totuşi, orice politică comună este, nu în ultimul rând, un produs al mentalităţilor politice specifice fiecăruia din statele membre.

„O protecţie eficientă a infrastructurii critice necesită comunicare, coordonare şi cooperare la nivel interstatal, dar şi la nivelul instituţiilor europene, acolo unde se manifestă principalii actori internaţionali din Europa. O structură de protecţie la nivel european trebuie să fie stabilită pentru a putea fi siguri că fiecare stat membru asigură acelaşi nivel de protecţie şi oferă un nivel optim de informaţii referitoare la infrastructura critică”[4].

Organismul european specializat, EPCIP - European Programme for Critical Infrastructure Protection, încearcă de ceva timp să coaguleze anumite strategii de protecţie a infrastructurii paneuropene tocmai datorită faptului că europenii au realizat fragilitatea acestui sistem în faţa riscurilor de toate tipurile. Două sunt însă cele mai dificile sarcini. În primul rând, identificarea interdependenţelor dintre structurile naţionale pentru a putea avea o mai bună evaluare a punctelor slabe, a ameninţărilor şi riscurilor. În al doilea rând, cel mai delicat aspect este convingerea statelor membre de a împărtăşi informaţii şi de a accepta conlucrarea europeană, cunoscut fiind faptul că fiecare stat membru va încerca mereu să reţină o anumită cantitate de suveranitate în ceea ce acesta va

[2] Şi aici exemplul este cu atât mai elocvent, cu cât, de un deceniu încoace, Europa se confruntă cu ameninţări periodice la adresa securităţii sale energetice datorită constantelor şantaje la care este supusă de către Ucraina în privinţa aprovizionării cu gaz rusesc.

[3] Operaţiunile navale NATO din Marea Mediterană sunt un exemplu în acest sens; dar şi fenomenul pirateriei din largul coastelor Africii de Vest ar putea constitui un semnal de alarmă pentru libertatea liniilor de comunicaţii strategice în Oceanul Atlantic.

[4] Green Paper on a European Programme for Critical Infrastructure Protection, , EU Comission, Brussels, 17.11.2005.

considera că este doar interesul lui național de securitate. De altfel nu acesta nu ar fi primul domeniu în care europenii nu se pot pune de acord cu politicile comune: politica comună agricolă, energetică, externă, fiscală sau de imigrație, toate suferă de pe urma lipsei de viziuni comune a statelor membre. Şi în cazul infrastructurii critice europene există mari dezbateri, în principal datorită definițiilor vagi şi a delimitărilor neclare referitoare la ce este național (infrastructură națională) şi ce este comun, european.

BIBLIOGRAFIE

Abraham-Frois, Gilbert, *Economia politică,* Editura Humanitas, Bucureşti, 1994

Blaug, Mark, *Economic Theory In Retrospect*, Cambridge University Press: New York, 1996

Smith, Adam, *Avuția națiunilor, Cercetare asupra naturii şi cauzelor ei*, Chişinău Universitas, 1992

Articole

Bachtler, John, "Reflections on the Reform of the Structural Funds", *RSA International*

Conference:Evaluation and EU Regional Policy, Aix en Provence: 1 June 2002

KOK, Wim, Enlarging the European Union: Achievements and Challenges?", *Robert Schuman*

Center for Advanced Studies, European University Institute: Florence, 2003

SISTEME ŞI REŢELE DE COMUNICAŢII ŞI INFORMATICE MILITARE ŞI SPECIALE, CA PARTE VITALĂ A INFRASTRUCTURILOR CRITICE ALE ROMÂNIEI. ASIGURAREA PROTECŢIEI FIZICE ŞI INFORMAŢIONALE A ACESTORA

General maior (r) prof. cons. dr. Constantin MINCU

Articolul prezintă argumente privind necesitatea de a studia infrastructura critică din România, incluzând diverse sisteme (reţele), precum şi comunicaţiile militare speciale. Totodată, subliniază rolul şi locul unor astfel de sisteme şi reţele pentru apărarea şi securitatea naţională şi scoate în evidenţă riscurile şi vulnerabilităţile cu care se confruntă aceste infrastructuri, precum şi unele măsuri necesare a fi luate pentru protecţia fizică şi informaţională, în cazul acţiunilor militare ostile, dezastre naturale sau alte fenomene negative.

În final, sunt formulate câteva concluzii şi propuneri.

Argumente pentru abordarea temei

Infrastructurile critice – resurse vitale pentru buna funcţionare a societăţii (asigurarea siguranţei vieţii cetăţenilor, a bunurilor materiale de bază, a serviciilor publice cele mai importante) sunt de câţiva ani buni în atenţia responsabililor politici, economici şi militari din mai multe ţări ale lumii şi face obiectul studiilor, planurilor şi acţiunilor unor organizaţii internaţionale (ONU, NATO, UE).

Conceptul **„infrastructură critică”** a fost folosit, în mod oficial, în iulie 1996, în Statele Unite, în preambulul unui act normativ elaborat de Casa Albă, intitulat: Ordinul Executiv pentru Protecţia Infrastructurilor Critice (Executive Order Critical Infrastructure Protection).

Apreciindu-se că securitatea, economia şi chiar supravieţuirea lumii industrializate ar fi esenţial dependente de trei elemente strâns interrelaţionate[1]: **energia, comunicaţiile şi computerele** – actul normativ explica şi definea atunci infrastructura critică[2] ca fiind „parte din infrastructura naţională care este atât de vitală încât distrugerea sau punerea ei în incapacitate de funcţionare poate să diminueze grav apărarea sau economia SUA[3]”.

Ulterior, sfera de cuprindere a acestui concept se va extinde, iar tema se va dezvolta. Îndeosebi după „momentul 9/11” – prima dovadă că nicio ţară, oricât de puternică ar fi ea, chiar şi Statele Unite, nu-şi va mai apăra eficient şi de una singură centrii ei vitali (**telecomunicaţiile,** sistemele de aprovizionare cu electricitate şi apă, depozitele de gaze şi de petrol, finanţele şi băncile, **centrele de comandă şi infrastructurile militare,** serviciile de urgenţă etc.).

În Startegia Naţională de Securitate a Spaţiului Cibernetic (The National Startegy to Secure Cyberspace) sunt nominalizate **la infrastructuri critice:** „instituţii publice şi private din sectoarele agriculturii, alimentaţiei, aprovizionării cu apă, sănătăţii publice, serviciilor de urgenţă, guvernării, **industriei de apărare, informaţiilor şi telecomunicaţiilor,** energiei, transporturilor, sistemelor bancare şi financiare, chimice şi a materialelor periculoase, precum şi cele poştale şi de navigaţie”[4].

Şi la nivelul **NATO** şi al **Uniunii Europene** sunt preocupări concrete pentru a defini infrastructurile critice şi pentru a propune soluţii concrete de protecţie a acestora în faţa unor atacuri ostile sau a unor calamităţi naturale de amploare.

Problematica infrastructurilor critice a fost şi este dezbătută în continuare de numeroşi specialişti civili şi militari, din multe ţări ale lumii industriaizate, rămânând o problemă deschisă, atât pentru analiză şi fundamentare teoretică, cât şi pentru acţiune practică, în actele de bună guvernare.

Trebuie să remarc că şi numeroşi specialişti români s-au aplecat cu convingere, cu bune rezultate în plan ştiinţific şi acţional, pentru a defini concepte, pentru a inventaria cu acurateţe infrastructurile critice ale României şi pentru a

[1] http://en.wikipedia.org/wiki/critical_infrastructure_protection
[2] http://www.whitehousegov/news/releases/2001/10/20011016-12.html
[3] Executive Order Critical Infrastructure Protection; http://www.fas.org/irp/offdocs/eo1301.htm
[4] The National Strategy to Secure Cyberspace, february, 2003

propune decidenţilor politici şi celor din administraţie elaborarea unui cadru normativ (legi, hotărâri de Guvern etc.), urmat de punerea, cât mai urgent în practică a măsurilor principale, în mod deosebit pentru reţelele vitale (energie, apă, sisteme informaţionale, sisteme de transport, sisteme financiar-bancare) [5].

Atât specialiştii străini, cât şi cei români, civili şi militari, care au analizat domeniul infrastructurilor critice, au acordat o mare atenţie rolului şi locului sistemelor informaţionale complexe (globale, zonale, naţionale, militare, speciale, comerciale, private etc.) în asigurarea vieţii normale a populaţiei, în funcţionarea economiilor, a sistemelor financiar-bancare, a securităţii şi apărării naţionale şi a conducerii politice şi administrative a unui stat, alianţe sau uniuni politico-economice.

Trebuie să arăt că acest gen de sisteme şi reţele de comunicaţii şi informatice sunt tratate de mulţi autori ca **subiect al războiului informaţional**[6], la pace, criză sau război, cu efecte grave asupra funcţionării lor în siguranţă, fapt care induce în mod direct dereglarea sau compromiterea totală a altor sisteme (subsisteme) servite: conducerea politică şi administrativă, apărarea naţională, siguranţa ţării şi a populaţiei, sistemele economice, financiar-bancare şi cele care privesc utilităţile vitale (energie, apă, alimente etc.).

Locul şi rolul sistemelor de comunicaţii şi informatice militare şi speciale în cadrul infrastructurii critice

a. Sistemele de comunicaţii şi informatice militare au constituit şi continuă să constituie elemente vitale în exercitarea comenzii şi controlului la toate

---

[5] Autori şi lucrări:
Dr. Grigore Alexandrescu, Dr. Gheroghe Văduva, *Infrastructuri critice, pericole, ameninţări la adresa acestora, sisteme de protecţie,* Editura U.N.Ap. Carol I, Bucureşti, 2006;
George Dediu, Alexandru Manafu, *Protecţia infrastructurilor critice – o nouă provocare,* Editura U.N.Ap. Carol I, Bucureşti, 2006;
Dr. Constantin-Gheorghe Balaban, *Infrastructurile critice, un domeniu care se cere investigat,* Revista Geopolitică, Anul VI – nr. 27, pp. 49-55.

[6] Autori şi lucrări:
Radu Dan Septimiu Popa, *Războiul informaţional şi securitatea naţională,* Ed. Militară, Bucureşti, 2009;
Teodor Frunzeti, *Securitatea naţională şi războiul modern,* Ed. Militară, Bucureşti, 1999;
M. Mureşan, Gh. Văduva, *Războiul viitorului, viitorul războiului*, Editura U.N.Ap. Carol I, Bucureşti, 2006;
Robert H. Anderson, *Physical Vulnerabilities of Critical US Information Systems* (internet, Iaver May 03.pdf);
Adrian V. Gheorghe, *Analiza de risc şi de vulenrabilitate pentru infrastructurile critice ale societăţii informatice – societatea cunoaşterii.*

eşaloanele armatei, începând cu nivelul strategic şi până la cel luptător. Numeroşi autori, în principal militari, au elaborat cărţi, studii, analize, proiecte, manuale şi articole în care au demonstrat locul şi rolul sistemelor complexe de tipul C4I (+ variante) într-un război modern, demonstrând totodată, pe lângă calităţile lor tehnice şi operaţionale şi vulnerabilităţi reale ce decurg din metodele şi procedeele războiului informaţional modern, dar şi cele care sunt create de calamităţi naturale majore, accidente grave, erori de proiectare şi realizare sau erori umane.

Pentru a înţelege mai bine care este „averea" disponibilă în acest moment în armata noastră care trebuie protejată fizic şi informaţional faţă de multiple vulnerabilităţi şi ameninţări, se cuvine să reamintim câteva aspecte, să le spunem teoretice şi metodologice.

- **Sistem C4I (+variante)** nu este privit ca un singur sistem, ci mai mult ca un **sistem de sisteme** în care fiecare sistem produce şi/sau consumă servicii. C4ISR reprezintă integrarea doctrinelor, procedurilor, structurilor organizaţionale, personalului, echipamentelor tehnice şi produselor software, facilităţilor, comunicaţiilor şi cercetării pentru a sprijini abilitatea comandantului de a realiza comanda şi controlul de-a lungul întregii game de operaţii militare. C4ISR asigură comandanţii cu date oportune şi precise şi sisteme pentru planificare, monitorizare, conducere, control şi raportarea desfăşurării operaţiilor.
- **Subsistemul de de comandă şi control** constă din facilităţile, echipamentele, procedurile şi personalul esenţiale pentru un comandant în planificarea, comanda şi controlul forţelor subordonate şi primite în sprijin pentru îndeplinirea misiunii.
- **Subsistemul de comunicaţii** reprezintă un ansamblu de echipamente, metode, proceduri şi personal (dacă e necesar), organizat pentru a îndeplini funcţiile de transfer a informaţiilor. Cuprinde sisteme de transmisie, de comutaţie şi de utilizator. Poate îndeplini şi funcţii de stocare şi prelucrare în sprijinul transferului de informaţii.
- **Subsistemul informatic (de calculatoare)** constituie un ansamblu de echipamente, metode, proceduri şi personal (dacă e necesar), organizat pentru a îndeplini funcţiile de prelucrare a informaţiilor. Poate transfera informaţii în sprijinul funcţiilor de prelucrare (de exemplu: în cadrul reţelelor locale de calculatoare).
- **Sistemul de informaţii (cercetare)** – echipamente, metode, proceduri şi personal pentru realizarea produselor informative prin colectarea, prelucrarea, integrarea, evaluarea, analiza şi interpretarea informaţiilor la dispoziţie privind forţele ostile sau potenţial ostile, zonele actuale sau potenţiale de acţiune.

- **ISR** – sistem care colectează şi prelucrează informaţii pentru realizarea produselor informative despre ameninţări şi mediu pe timpul operaţiilor, precum şi informaţii pentru identificarea, urmărirea şi angajarea ţintelor.
- **Arhitectura sistemelor C4ISR** trebuie să fie abordată din trei puncte de vedere (operaţional, sistemic şi tehnic) concomitent cu relaţiile dintre ele. **Din punct de vedere operaţional**, arhitectura se referă la centrele reţelei, misiunilor şi sarcinile realizate, informaţiile care trebuie vehiculate pentru îndeplinirea misiunii (tipul, frecvenţa, misiunile şi activităţile sprijinite, natura acestora). **Din punct de vedere sistemic** sunt analizate: sistemul în ansamblu, serviciile şi funcţionalitatea interconectării asigurate pentru sprijinul activităţilor operaţionale prin schimbul de informaţii între centrele reţelei. **Din punct de vedere tehnic** este analizat setul minim de reguli care guvernează organizarea, interacţiunile şi interdependenţele dintre părţile (elementele) sistemului în scopul satisfacerii cerinţelor operaţionale. Aceasta cuprinde o serie de standarde tehnice, rutine de implementare, selecţia standardelor, regulilor şi criteriilor care pot fi organizate, în ce gestionează sistemul sau serviciile elementelor pentru o arhitectură dată.
- **Sistemele menţionate**, cu funcţiile lor prezentate pe scurt, sunt reprezentate pe teren de o serie de reţele şi facilităţi tehnice şi operaţionale realizate în perioada 1990-2010, atât cât s-a putut în condiţii politice şi economice dificile.

b. Sistemele de comunicaţii şi informatice speciale

Telecomunicaţiile speciale reprezintă un segment a ceea ce se numesc telecomunicaţiile de stat (anexa nr. 1) destinate asigurării unor comunicaţii securizate de voce şi date pentru autorităţile publice ale statului român:

- Parlamentul României;
- Preşedenţia României;
- Guvernul României;
- instituţiile care desfăşoară activităţi în domeniul apărării, siguranţei naţionale şi ordinii publice;
- administraţia publică centrală şi locală;
- autoritatea judecătorească:
  - Curtea Supremă de Justiţie;
  - Ministerul Public;
  - Consiliul Superior al Magistraturii;
- Curtea de Conturi;
- Curtea Constituţională;
- organele de conducere din cadrul organismelor guvernamentale şi al unor organisme neguvernementale de interes naţional.

Aceste sisteme şi reţele speciale se caracterizează prin acoperire naţională, un înat grad de protecţie şi confidenţialitate şi prin măsuri fizice şi informaţionale de protecţie faţă de diferite riscuri şi situaţii potenţial periculoase.

Denumirea de „telecomunicaţii speciale" a fost adoptată în 1993 din considerentul delimitării lor de sfera telecomunicaţiilor publice ori private, precum şi al particularizării acestora în cadrul telecomunicaţiilor de stat.

Specificitatea reţelelor de telecomunicaţii speciale este dată atât de modul de organizare a infrastructurii, cât şi de organizarea serviciilor.

Sistemul telecomunicaţiilor guvernamentale dispune de reţele performante proprii, separate, pe cât posibil, de alte reţele, cu un grad **sporit de rezervare şi reconfigurare,** care au posibilitatea de a efectua un număr mare de servicii prin recurgerea la tehnologii superioare celor din majoritatea reţelelor publice şi private.

Rezultă destul de clar ca sistemele şi reţelele STS (Legea nr. 92/1996) au un rol vital pentru conducerea politică, administrativă, militară şi, în unele cazuri – economică a ţării şi instituţiilor principale şi, sub acest aspect, se califică pe deplin ca infrastructură critică ce trebuie protejată în faţa unui set întreg de riscuri şi ameninţări.

Prezentarea, pe scurt, a unor sisteme şi reţele de comunicaţii şi informatice militare şi speciale, cu rol vital în asigurarea securităţii şi apărării ţării

Infrastructura IT&C a M.Ap.N

În perioada 1991 – 2010 în armata României a fost proiectată, realizată şi dezvoltată Reţeaua de Transmisiuni Permanentă (R.T.P) care reprezintă o reţea distribuită, încorporând, din punct de vedere operaţional şi tehnic, 253 de centre de comunicaţii cu diferite dezvoltări, de la cele nodale principale, până la modulele desfăşurabile în teatrele de operaţii şi extensiile externe pentru comunicaţiile cu NATO şi UE. Această reţea, parte principală a Sistemului de Transmisiuni al Armatei României (STAR), asigură infrastructura de bază (staţionară) pentru comunicaţii multicanal (voce, date, videoconferinţă) pentru conducerea operaţională şi administrativă a tuturor structurilor armatei la pace, criză şi război. Are o dezvoltare geografică naţională, fiind extinsă în aproape toate oraşele reşedinţă de judeţ şi în alte numeroase locaţii unde sunt unităţi şi interese de ordin militar.

Rolul de **infrastructură critică** a acestei reţele derivă din funcţiile ei în folosul conducerii strategice, operative şi tactice şi din resursele puse la dispoziţie pentru cooperarea intercategorii şi interforţe, precum şi cele necesare unor proiecte cu mare valoare militară pentru apărare (de exemplu pentru SCCAN şi SCOMAR).

Pe lângă aceste calităţi operaţionale şi tehnice reţeaua are şi unele vulnerabilităţi în ceea ce priveşte asigurarea funcţionării sigure şi neîntrerupte în condiţiile în care ar putea fi supusă unor acţiuni ostile prin atacuri fizice sau radioelectronice, prin mijloacele cunoscute ale războiului informaţional (cu toate formele sale active şi pasive).

Se pot face analize de risc de ordin general şi punctual şi propune măsuri concrete de protecţie.

- **Reţeaua de Comunicaţii de Sprijin de Campanie (R.C.S.C)** asigură infrastructura mobilă pentru comunicaţii multicanal, fiind destinată pentru refacerea unor tronsoane RTP distruse sau scoase din funcţiune temporar sau/şi pentru extinderea RTP în zone încă neacoperite pentru puncte de comandă.
- **Reţeaua Radio cu Servicii Integrate (R.R.S.I)** asigură echipamentele şi procedurile pentru comunicaţii monocanal utilizând staţii radio HF şi VHF cu salt de frecvenţă, cu dispozitive de criptare pentru voce şi date.
- **Sistemul Criptat de Videoconferinţă (V.T.C)** asigură servicii de videoconferinţă criptate utilizând ca suport de comunicaţii RTP/RMNC. Beneficiarii sunt structurile principale de conducere ale M.Ap.N şi S.M.G.
- **Sistemul de comunicaţii prin satelit (S.C.S)** asigură suportul de comunicaţii în locaţii greu accesibile, izolate sau îndepărtate (în teatrele de operaţii din străinătate – Irak, Afganistan etc.).
- **Sistemul de comunicaţii şi informatică desfăşurabil (S.C.I.D)** asigură servicii de voce şi date pentru forţele dislocabile în teatrele de operaţii, precum şi pentru conectarea acestora la Sistemul NATO General de Comunicaţii (N.G.C.S).
- **Sisteme de comunicaţii mobile Tetra Dimetra** destinate să asigure unele comunicaţii mobile pentru structurile centrale ale M.Ap.N şi S.M.G, categoriile de forţe ale armatei şi comandamentele operaţionale şi de armă precum şi cooperarea cu structuri din sistemul naţional de apărare, îndeosebi în situaţii de urgenţă în baza prevederilor Legii nr. 363/2004.

Toate sistemele şi reţelele menţionate fac parte din infrastructura critică a M.Ap.N şi, în consecinţă, trebuiesc luate măsuri de protecţie fizică şi informaţională, potrivit standardelor actuale valabile în NATO şi UE.

Infrastructura de comunicaţii speciale de conducere şi cooperare din administrarea S.T.S

- **Infrastructura de telecomunicaţii integrate de capacitate mare, redundantă, cu puncte de prezenţă în capitală şi în reşedinţele de judeţ.** Aceasta se bazează pe echipamente profesionale în tehnologii moderne, care utilizează pentru transport reţelele de fibră optică şi radiorelee.

Capacităţile de transport sunt suficiente pentru asigurarea comunicaţiilor între reşedinţele de judeţ şi Bucureşti în perspectiva următorilor ani pentru toate nevoile exprimate de către autorităţi. Această infrastructură de telecomunicaţii integrate asigură servicii de comunicaţii pentru reţele de voce, date şi video.

Într-un termen scurt infrastructura radioreleu proprie va fi extinsă până la nivelul municipiilor, oraşelor şi localităţilor în care există entităţi ale autorităţilor publice.

- **Infrastructura de radiocomunicaţii mobile** constă în reţelele locale convenţionale şi în sistemele profesionale în tehnologiile TETRAPOL şi TETRA-DIMETRA şi furnizează servicii în regim de mobilitate pentru autorităţile publice cu atribuţii în domeniul siguranţei cetăţeanului şi securităţii naţionale.

În prezent, utilizatorii serviciilor platformei comune TETRA-DIMETRA sunt: Ministerul Administraţiei şi Internelor (Poliţia Română, Poliţia de Frontieră, Inspectoratul General pentru Situaţii de Urgenţă, Jandarmeria Română, Instituţia Prefectului), Serviciul Român de Informaţii, Ministerul Sănătăţii – serviciile medicale de urgenţă (serviciul de ambulanţă, SMURD), Ministerul Finanţelor Publice (Autoritatea Naţională a Vămilor), primăriile (Poliţia Comunitară), Ministerul Apărării Naţionale şi Serviciul de Protecţie şi Pază.

- **Infrastructura pentru servicii de comunicaţii de date**

Infrastructura reţelei integrate de mare capacitate permite realizarea unor reţele naţionale securizate de arie extinsă pentru autorităţi. Beneficiari mai importanţi: Ministerul Finanţelor Publice, Ministerul Justiţiei şi Libertăţilor Cetăţeneşti, Ministerul Administraţiei şi Internelor, Ministerul Apărării Naţionale, Ministerul Agriculturii, Pădurilor şi Dezvoltării Rurale, Ministerul Mediului, Ministerul Afacerilor Externe şi Ministerul Muncii, Familiei şi Protecţiei Sociale. Reţeaua este securizată şi criptată conform standardelor NATO.

- **Infrastructura pentru servicii Internet**

Dezvoltată în urma nevoilor exprese ale instituţiilor publice şi componentelor SNAOPSN (Sistemul Naţional de Apărare, Ordine Publică şi Siguranţă Naţională) în condiţiile în care serviciile de Internet au devenit o componentă principală a funcţionării oricărei instituţii a statului.

- **Infrastructura pentru servicii satelitare**

A fost dezvoltată ca alternativă la serviciile oferite de infrastructura terestră şi pentru asigurarea serviciilor de comunicaţii în cazul misiunilor temporare, în locurile unde infrastructura terestră nu oferă servicii. Prin intermediul acestei infrastructuri sunt asigurate în mod operativ serviciile de telecomunicaţii pentru gestionarea situaţiilor de urgenţe oriunde situaţia impune prezenţa autorităţilor şi forţelor de intervenţie, iar serviciile reţelelor terestre nu sunt disponibile.

Prin infrastructura satelitară se asigură continuitatea conducerii statului în situaţii de calamităţi sau dezastre, în situaţiile în care reţele terestre nu mai sunt funcţionale, precum şi pe durata activităţilor oficiale în străinătate ale conducerii statului. Infrastructura este disponibilă pentru utilizarea de către componentele de urgenţă ale autorităţilor publice.

- **Infrastructura pentru servicii telefonice** include comutatoarele telfonice şi reţeaua de cabluri telefonice proprii, prin care sunt oferite serviciile telefonice speciale „S" şi „TO", precum şi serviciile de cooperare IC.

Aspectele care necesită acordarea unei atenţii deosebite care privesc această infrastructură sunt cele generate de schimbarea tehnologiilor în reţelele de acces ale operatorilor care furnizează servicii conexe, de asigurare a protecţiei comunicaţiilor în acest mediu public, precum şi de costurile ridicate ale acestui tip de suport.

- **Infrastructura de servicii video** funcţionează pe infrastructura de comunicaţii integrate şi asigură serviciile de videoconferinţă securizată pentru Guvernul României şi Instituţia Prefectului.

- **Infrastructura TESTA** a fost dezvoltată în baza Deciziei nr. 387/2004 a Comisiei Europene, sub forma unei reţele destinate susţinerii proiectelor de interes comun şi pentru oferirea unei platforme de comunicaţii protejate şi fiabile destinată schimbului de date între administraţiile publice la nivel european.

- **Infrastructura de chei publice (PKI)** realizată de S.T.S se adresează instituţiilor componente ale SNAOPSN şi autorităţilor publice.

- **Infrastructura de protecţie a telecomunicaţiilor speciale** asigură serviciile de securitate a telecomunicaţiilor speciale şi de cooperare prin:
  - descoperirea, identificarea, localizarea şi înlăturarea surselor de perturbaţii accidentale (analiza problemelor de interferenţă) sau intenţionate (emisii neautorizate) şi asigurarea disponibilităţii frecvenţelor radio din gestiunea S.T.S.;

- executarea de controale tehnice a reţelelor de telecomunicaţii speciale în vederea asigurării confidenţialităţii comunicaţiilor speciale;
- zonarea locaţiilor pentru prevenirea scurgerii de informaţii clasificate secrete de stat prin intermediul radiaţiilor electromagnetice compromiţătoare emise de echipamentele S.T.S.

- Sistemul naţional unic pentru situaţii de urgenţă – 112 extins până la nivelul tuturor municipiilor şi oraşelor din România.

Toate sistemele şi reţelele menţionate necesită un proces amănunţit de analiză a vulnerabilităţilor de ordin fizic şi informaţional în vederea identificării unor măsuri eficiente de protecţie.

Protecţia fizică şi informaţională a sistemelor şi reţelelor militare şi speciale în condiţiile manifestării unor acţiuni de război informaţional, producerii unor dezastre naturale şi a altor fenomene negative

Vulnerabilităţi şi ameninţări informaţionale pentru securitatea naţională:

Ca în orice domeniu de activitate, şi în cel privind informaţiile şi sistemele informaţionale pentru securitatea naţională există anumite vulnerabilităţi, adică părţi mai puţin studiate şi slăbiciuni ale sistemului, infrastructurii, mediului de control sau proiectării reţelelor, care nu sunt generate de acţiunile adversarilor, ci de soluţiile proprii adoptate, ce pot fi atacate relativ uşor şi exploatate pentru a deteriora integritatea acelui stat.

Vulnerabilităţile informaţionale constituie o componentă a **vulnerabilităţii de securitate**[7], generată de stări de fapt, procese sau fenomene din viaţa internă a comunităţii naţionale, care diminuează capacitatea de reacţie a societăţii la riscurile existente ori potenţiale de orice natură, inclusiv informaţionale sau care favorizează apariţia şi dezvoltarea acestora, cu consecinţe privind realizarea securităţii naţionale.

În general, vulnerabilităţile informaţionale sunt cu atât mai mari, cu cât reţelele informaţionale şi structura informaţiilor sunt de complexitate mai mare, fiind greu de optimizat, administrat şi protejat. De asemenea, vulnerabilităţile sporesc direct proporţional cu nivelul tehnologic implementat în construcţia şi funcţionarea echipamentelor (mai ales digitale) sistemelor informaţionale.

Rezultă că obiectivul principal al conflictelor militare contemporane nu trebuie să fie acela de distrugere totală a tehnicii, armamentului sau forţei vii a

[7] *Doctrina naţională a informaţiilor pentru securitate,* Editura SRI, Bucureşti, 2004.

adversarului, ci, mai ales, de neutralizare şi dezintegrare a sistemelor complexe ale acestuia, în principal a sistemelor informaţionale. În acest context, s-a impus tot mai mult conceptul de **infrastructuri critice ale ţării** de care depind[18] stabilitatea, siguranţa şi securitatea sistemelor şi proceselor. Nu este însă obligatoriu ca toate infrastructurile care sunt sau pot deveni, la un moment dat, critice să facă parte din această categorie de infrastructuri. Infrastructurile critice sunt acele infrastructuri cu rol important în asigurarea securităţii, în funcţionarea sistemelor şi în derularea proceselor economice, sociale, politice, informaţionale şi militare. Caracterul critic al unor infrastructuri, în principal informaţionale, este determinat, mai ales, de condiţia de unicat a unui sistem sau proces, de rolul său în funcţionarea stabilă a infrastructurii şi de vulnerabilităţile acesteia.

Siguranţa naţională, apărarea ţării şi ordinea publică constituie domenii importante ale infrastructurilor critice, în care se mai regăsesc structurile aferente tehnologiei informaţiei şi comunicaţiilor, reţelele administraţiei de stat, diplomatice, energetice, de transport, de alimentare cu apă, sistemul financiar şi medical.

Principalele vulnerabilităţi ale infrastructurii informaţionale privind securitatea naţională, apreciem că ar putea fi următoarele:

- posibilităţile de interceptare a informaţiilor din reţelele de comunicaţii şi calculatoare atât de către utilizatori, cât şi de adversar;
- volumul foarte mare de informaţii produse, vehiculate şi prelucrate în sistemele informaţionale, care pot fi supuse cercetării şi atacului adversarilor potenţiali, distruse, falsificate sau sustrase;
- afectarea infrastructurii informaţionale, ceea ce determină dificultăţi în managementul acesteia, imposibilitatea detectării accesului fraudulos la informaţii şi favorizarea atacurilor cibernetice;
- folosirea aceloraşi benzi de frecvenţă, modulaţii şi regimuri de lucru la echipamentele bazate pe propagarea undelor electromagnetice, atât în reţelele de comunicaţii proprii, cât şi în cele ale adversarilor potenţiali;
- utilizarea de echipamente tehnice, componente software şi baze de date cu structuri şi exploatare standardizate (comerciale) în toate reţelele de calculatoare din organizaţiile implicate în securitatea naţională, eventual şi în reţelele de comunicaţii ale acestora, ceea ce favorizează acţiunile teroriste şi criminalitatea organizată împotriva ţării noastre;

[8] Gr. Alexandrescu, Gh. Văduva, *Infrastructuri critice. Pericole, ameninţări la adresa acestora. Sisteme de protecţie,* Editura UNAp, Bucureşti, 2006

- dependenţa infrastructurii sistemelor informaţionale pentru securitatea naţională de infrastructura informaţională comercială a ţării, ceea ce creează condiţii pentru acces fraudulos şi dezinformare;

- posibilitatea încorporării (ascunderii) din timp, în echipamentele de calcul şi de comunicaţii, de către firmele furnizoare de aparatură, a unor module software maliţioase, care pot fi activate de către adversari la momente hotărâte de aceştia, creând dezordine şi haos în reţelele informaţionale şi cele decizionale;

- prin conectarea la Internet, Intranet sau Extranet, organizaţiile de care depinde securitatea naţională devin vulnerabile la pătrunderi neautorizate (cu rea intenţie sau din neatenţie);

- existenţa unor reţele informaţionale cu număr mare de noduri şi cu o largă interconectivitate, greu de sincronizat şi gestionat, ceea ce permite penetrarea acestora, accesul neautorizat, capturarea fizică a unor echipamente sau a unor noduri (centre) de comunicaţii în totalitate, interceptarea sau întreruperea unor fluxuri de informaţii importante şi/sau introducerea de informaţii false care să afecteze procesele decizionale;

- digitalizarea exhaustivă a structurii informaţionale a securităţii naţionale are un impact contradictoriu: pe de o parte, omogenizează, sincronizează şi sporeşte gradul de compatibilitate şi interoperabilitate a reţelelor informaţionale pentru sistemul securităţii naţionale, iar, pe de altă parte, determină stăpânirea cu greutate a complexităţii şi a nivelului deosebit de ridicat de tehnicitate al acestora, oferind condiţii pentru atacul cibernetic de la distanţă sau din interiorul lor;

- nerespectarea integrală a cerinţelor şi standardelor Uniunii Europene şi NATO privind compatibilitatea şi interoperabilitatea sistemelor informaţionale, mai ales în ce priveşte schimbul de informaţii (formatul mesajelor), accesul la bazele de date, criptarea automată a comunicărilor şi caracteristicile canalelor pentru legătură;

- posibilitatea folosirii de către adversari potenţiali a războiului electronic împotriva mijloacelor radioelectronice din principalele sisteme informatice şi de comunicaţii, cu precădere asupra canalelor care asigură legătura surselor de informaţii cu organele centrale de fuziune şi prelucrare a datelor;

- interceptarea de către adversar (forţele ostile) a comunicărilor transmise prin radio, decriptarea acestora în timp oportun în cazul folosirii unor sisteme criptografice neperformante şi folosirea în scopuri proprii a acestor informaţii pentru obţinerea superiorităţii informaţionale asupra statului român;

- mijloacele tehnice actuale ale sistemelor informaţionale nu au asigurată protecţia deplină împotriva atacului fizic, electromagnetic şi cibernetic, acestea putând fi distruse, deteriorate sau extrasă informaţia stocată;

- dispunerea în locuri necorespunzătoare, din punct de vedere funcţional şi al securităţii fizice şi electromagnetice a echipamentelor tehnice ale sistemelor informaţionale, în principal a mijloacelor de comunicaţii şi de calcul, ceea ce sporeşte vulnerabilitatea de interceptare a informaţiilor şi de atac fizic;

- utilizarea pentru exploatarea sistemelor informaţionale privind securitatea naţională a unor persoane insuficient verificate şi neloiale, predispuse a fi racolate de către adversarii potenţiali şi determinate să efectueze acţiuni de sabotaj sau să furnizeze acestora informaţii obţinute fraudulos;

- neutralizarea legăturii radio pe unde scurte, mai ales la distanţe mari, bazată pe propagarea undelor electromagnetice prin ionosferă, prin schimbarea caracteristicilor electrice ale acesteia, ceea ce determină atenuarea, modificarea aleatoare a direcţiei de propagare şi reflectarea numai parţială a undelor electromagnetice;

- existenţa, la adversarii potenţiali, a armelor electronice cu radiaţii infraacustice, bazate pe propagarea în spaţiu a undelor subsonice, care acţionează asupra personalului, determinând inactivarea acestuia anumite perioade de timp şi, implicit, întreruperea funcţionării sistemelor informaţionale;

- instalarea antenelor mijloacelor de comunicaţii în câmp deschis sau în spaţii fără proprietăţi naturale de protecţie, ceea ce permite scoaterea lor uşoară din funcţiune şi întreruperea legăturii, mai ales a celei cu staţii radio şi radioreleu de putere mare;

- suprimarea accesului la Internet al sistemelor informaţionale privind securitatea naţională, pentru izolarea acestora, în vederea împiedicării folosirii de către adversari şi persoanele neautorizate a unor surse de documentare proprii, cuprinzând informaţii neclasificate;

- utilizarea Internetului pentru acţiuni teroriste[9] de dezinformare şi atac cibernetic asupra infrastructurii informaţionale critice a securităţii naţionale;

- proiectarea necorespunzătoare a infrastructurii, cu redundanţă informaţională redusă, centralizată excesiv şi cu posibilităţi scăzute de replicare a informaţiilor existente în bazele de date;

- preocuparea insuficientă pentru ascunderea şi mascarea elementelor infrastructurii informaţionale, măsuri neadecvate de pază şi apărare a acestora;

Din prezentarea efectuată rezultă că există numeroase vulnerabilităţi, dar dintre acestea, esenţiale sunt cele care împiedică: organizarea optimă a sistemelor informaţionale, alegerea echipamentelor tehnice utilizate şi a produselor software

[9] Vasile Marin, *Elemente de analiză geopolitică a ordinii internaţionale contemporane*, Bucureşti, 2003. (Terorismul contemporan are deja caracter mondial. El se anexează pe extremismul religios violent, pe extremismul politic şi pe efectele dezrădăcinării.).

comerciale cu înalte performanţe funcţionale, realizarea calitativă a programelor (software) de aplicaţii şi a bazelor date de către specialiştii organizaţiilor privind securitatea naţională, precum şi a software-ului pentru criptarea automată, sigură, a informaţiilor în sistemele informaţionale, măsurile de securitate adoptate.

Organizarea optimă a sistemelor informaţionale constituie condiţia fundamentală pentru funcţionarea eficientă a acestora pe timpul războiului informaţional, iar reconfigurarea în timp real, mobilitatea şi adaptabilitatea lor la mediul de informaţii în continuă dezvoltare şi la situaţiile şi standardele ce trebuie avute în vedere, ca ţară membră a Uniunii Europene şi NATO, se impun a fi respectate în totalitate şi aplicate cu fermitate pentru a se îndeplini condiţiile de compatibilitate şi interoperabilitate.

Formatul standard al documentelor purtătoare de informaţii trebuie să fie unificat cu Uniunea Europeană şi NATO, iar completarea acestora să se poată efectua atât în limba română, cât şi în limbile engleză sau franceză.

Adaptarea sistemelor la mediul de informaţii, mai ales în situaţii de criză şi conflict militar, impune echiparea acestora cu mijloace tehnice capabile să suporte fluxuri informaţionale de 2-3 ori mai mari decât în condiţii normale de funcţionare pe timp de pace.

Fiabilitatea sistemelor informaţionale trebuie să fie proiectată astfel încât probabilitatea de funcţionare fără defecţiuni a structurilor tehnice şi informaţionale să fie mai mare de 0.95, asigurându-se totodată o probabilitate redusă de detectare şi interceptare a comunicărilor.

O atenţie deosebită se va acorda organizării şi exploatării optime a bazelor de date ale reţelelor de calculatoare.

Ameninţări informaţionale interne

Analiza efectuată evidenţiază următorii factori interni, care pot constitui ameninţări asupra sistemelor informaţionale privind securitatea naţională:

- lipsa de preocupare pentru dobândirea superiorităţii informaţionale asupra statelor şi forţelor potenţial ostile;
- neconcordanţa între cerinţele de informaţii pentru luarea deciziilor şi conducerea acţiunilor privind securitatea naţională şi posibilităţile reale de dobândire a acestora;
- proiectarea, organizarea sau funcţionarea necorespunzătoare a sistemelor informaţionale;
- dotarea sistemelor informaţionale cu mijloace de culegere a datelor, comunicaţii şi calculatoare neperformante, greu de exploatat şi de asigurat protecţia, utilizarea necorespunzătoare a acestora;

- influenţa mediului de securitate intern şi internaţional asupra proceselor informaţionale ale structurilor de informaţii specializate ale statului şi a cooperării acestora cu organe similare ale celorlalte ţări membre ale Uniunii Europene şi NATO;

- organizarea necorespunzătoare a bazelor de date, existenţa unor produse software neperformante sau cu erori intenţionate pentru gestiunea, prelucrarea şi afişarea informaţiilor, lipsa de preocupare pentru utilizarea inteligenţei artificiale, pentru realizarea activităţilor informaţionale şi a celor de management;

- slaba pregătire profesională şi experienţa redusă a personalului, implicat în organizarea, exploatarea şi asigurarea funcţionării sistemelor informaţionale;

- clasificarea necorespunzătoare a categoriilor de informaţii şi date privind securitatea naţională şi certificarea eronată a dreptului de acces la acestea a personalului;

- neloialitatea unor persoane care exploatează echipamentele tehnice ale sistemelor informaţionale;

- securitatea redusă a datelor şi informaţiilor pe timpul transmiterii, memorării, prelucrării şi afişării acestora, accesul neutorizat al unor persoane străine.

Răspunderea pentru asigurarea superiorităţii informaţionale asupra adversarilor potenţiali şi a altor forţe ostile revine şefilor structurilor de informaţii specializate, aceasta trebuind să fie urmărită cu consecvenţă atât pe timp de pace, cât şi în situaţii de criză sau de conflict militar.

Fragilitatea superiorităţii informaţionale este dată de calitatea informaţiei de a fi obţinută în timp real, cu forţele şi mijloacele structurilor de informaţii specializate, precum şi din surse deschise sau primite de la organele cu care cooperează. Caracterul nonlinear al acesteia determină ca mici intrări de informaţie să poată produce efecte disproporţionate atât pe timp de pace sau criză, dar mai ales pe timpul conflictului militar.

Un rol important îl are stabilirea din timp de pace, prin legi şi instrucţiuni, a cerinţelor de informaţii privind securitatea naţională, diferenţiat pe domenii de activitate şi eşaloane ierarhice de conducere, a modalităţilor şi răspunderilor pentru obţinerea acestora, precum şi a conţinutului lor informaţional, forma de prezentare şi operaţiile de prelucrare la care sunt supuse.

În acest sens, trebuie avut în vedere că implementarea tehnologiei moderne a informaţiei şi comunicaţiilor, precum şi a metodelor de management moderne constituie o componentă esenţială a definirii forţei.

Experienţa dobândită privind asigurarea securităţii naţionale a dovedit că organizarea necorespunzătoare a sistemelor informaţionale, lipsa de preocupare pentru funcţionarea acestora şi înlăturarea defecţiunilor ce pot apărea, constituie cauza principală a lipsei de informaţii relevante şi a imposibilităţii dobândirii superiorităţii informaţionale. Trebuie să se aibă în vedere că informatica şi comunicaţiile moderne, deşi au un rol hotărâtor, prezintă şi numeroase vulnerabilităţi tehnologice care trebuie diminuate sau înlăturate prin măsuri organizatorice şi tehnice adecvate.

Chiar dacă nu sunt supuse atacului informaţional al adversarilor potenţiali, bazele de date şi software-urile pot crea neajunsuri serioase în cazul când nu sunt organizate, realizate şi exploatate corespunzător. Principala răspundere pentru funcţionarea lor eficientă revine personalului de specialitate din sistemul informaţional, mai ales inginerilor, analiştilor şi programatorilor, precum şi operatorilor de la mijloacele de comunicaţii. Corelat cu aceasta, un impact major asupra informaţiilor îl are realizarea unei securităţi reduse a informaţiilor în toate verigile sistemelor informaţionale, care creează posibilitatea de acces neautorizat şi de transmitere la adversar a unor date, din cauza lipsei de loialitate a unor persoane care sunt implicate în vehicularea fluxurilor de informaţii.

Totodată, există şi cauze tehnice care pot constitui ameninţări informaţionale interne, rezultate mai ales din dotarea necorespunzătoare cu echipamente moderne de culegere, transmitere şi prelucrare a informaţiei, precum şi a unor loturi de rezervă pentru acestea.

Se impune, aşadar, efectuarea unor cheltuieli importante pentru dotarea sistemelor informaţionale cu tehnică modernă, pentru că succesul în realizarea securităţii naţionale se obţine cu un preţ ridicat.

Ameninţări informaţionale externe

Ameninţările informaţionale externe cuprind ansamblul acţiunilor specifice, executate de adversarii potenţiali şi forţele ostile ţării noastre pentru interzicerea sau îngreuierea executării funcţiilor decizionale şi operaţionale privind securitatea naţională. Acestea urmăresc limitarea sau excluderea activităţilor proprii privind culegerea de informaţii, deteriorarea sau distrugerea senzorilor şi a altor surse de date şi interzicerea funcţiilor informaţionale privind securitatea naţională.

Conform concluziilor formulate în literatura de specialitate[10], principalele ameninţări informaţionale externe asupra structurilor decizionale şi acţionale privind securitatea naţională sunt următoarele:

- atacul fizic împotriva surselor de date şi a mijloacelor de transmitere, prelucrare şi afişare a informaţiilor;
- atacul electronic asupra mijloacelor de culegere, transmitere şi prelucrare a informaţiilor;
- atacul cibernetic împotriva sistemelor informaţionale ale structurilor de informaţii pentru securitatea naţională şi cele ale organizaţiilor economice, financiare, diplomatice etc.;
- pirateria software;
- atacul fizic şi electronic asupra organelor decizionale ale statului nostru (preşedinţie, parlament, guvern etc.) privind securitatea naţională;
- atacul psihologic asupra tuturor structurilor decizionale şi acţionale ale ţării noastre (politice, economice, sociale, de apărare etc.)

Aceste ameninţări nu sunt noi, ele fiind generate de însăşi dezvoltarea societăţii informaţionale, dar trebuie cunoscute, studiate cu atenţie şi stabilite cu precizie măsurile corespunzătoare pentru combaterea lor.

Este cunoscut că obiectul culegerii de informaţii pentru securitatea naţională constă în asigurarea cunoaşterii exacte a situaţiei internaţionale, mai ales în zona de interes a României, Uniunii Europene şi NATO, precum şi a situaţiei interne din ţara noastră şi din ţările vecine, realizându-se astfel anticiparea acţiunilor agresive ale adversarilor potenţiali sau ale unor grupuri ostile şi prevenirea surprinderii.

În prezent[11] securitatea se identifică cu protecţia a tot ceea ce afectează bazele înseşi ale statului şi organizaţiilor internaţionale la care am aderat şi cu care executăm acţiuni în comun.

Această evoluţie a modificat şi obiectivele serviciilor de informaţii, care nu se mai concentrează atât de mult pe informaţii despre parametrii militari şi strategici ai unor terţe ţări, cât mai ales pe aspecte şi fenomene economice, sociale şi politice a căror logică de acţiune răspunde unor modele şi condiţii diferite şi, în special, cu mult mai imprevizibile decât în trecut.

Se dovedeşte că existenţa unor informaţii sigure, complete şi oportune constituie suportul principal al conducerii şi coerenţei proceselor decizionale privind securitatea naţională. De aceea, atacul fizic al adversarilor potenţiali şi

[10] J. S. Gansler, H. Binnendjic, *Information Assurance, Trend in Vulnerabilities, Threat and Technologies.*

[11] Doctrina *naţională a informaţiilor pentru securitate,* Editura SRI, Bucureşti, 2004.

grupurilor ostile împotriva surselor şi mijloacelor pentru obţinerea informaţiilor constituie, probabil, principala vulnerabilitate pentru sistemele informaţionale de orice natură, din ţara noastră.

Atacul electronic asupra mijloacelor de culegere, transmitere şi prelucrare a informaţiilor se bazează pe utilizarea de energii electromagnetice înalte (lasere, arme cu frecvenţe radio, arme cu microunde etc.) pentru neutralizarea sau distrugerea mijloacelor electronice (radare, senzori, staţii radio, radiorelee, calculatoare etc.) utilizate în sistemele informaţionale şi afectarea biofizică a personalului.

Apreciem că acest atac constituie ameninţarea fizică principală asupra mijloacelor tehnice ale sistemelor informaţionale existente la structurile de informaţii privind securitatea naţională.

Protecţia împotriva acestor arme, care atacă echipamentele tehnice şi personalul sistemelor informaţionale, are un rol hotărâtor pentru funcţionarea neîntreruptă a mijloacelor electronice utilizate pentru culegerea, transmiterea, prelucrarea şi diseminarea informaţiilor.

Atacul cibernetic asupra structurii informaţionale a securităţii naţionale reprezintă o ameninţare deosebit de importantă, care are în vedere „spaţiul virtual" ce vizează mai ales produsele software şi firmware, protocoalele şi bazele de date ale sistemelor informatice utilizate în reţelele de calculatoare şi de comunicaţii. Acţiunile externe specifice atacului cibernetic au în vedere reducerea însemnată a posibilităţilor de efectuare corectă a serviciilor în cadrul sistemului informaţional, deteriorarea software-ului de aplicaţie ce are, de regulă, caracter confidenţial sau secret, pentru a genera informaţii greşite din datele prelucrate.

Aceste ameninţări externe sunt favorizate de neaplicarea unor reguli sigure de protecţie şi securizare a informaţiilor pe timpul transmiterii şi prelucrării datelor culese de către surse. Ele fructifică lacune şi/sau slăbiciuni existente în structura sistemului de securitate a reţelelor proprii de comunicaţii şi calculatoare.

Atacul cibernetic are legătură cu pirateria software[12], care poate fi desfăşurată de agresori locali sau plasaţi în orice puncte din spaţiul interconectat al informaţiei şi urmăresc, după caz, paralizarea completă a sistemelor informatice sau defectarea (căderea) lor intermitentă, la momente de timp dinainte stabilite.

Atacul cibernetic urmăreşte şi deteriorarea programelor (sistemelor expert) folosite în procesele decizionale şi acţionale privind securitatea naţională, ceea ce depăşeşte cu mult sfera informaţională propriu-zisă şi poate genera decizii greşite care, într-o formă sau alta, să avantajeze adversarii potenţiali.

[12] J. S. Gansler, H. Binnendjic, *Information Assurance, Trend in Vulnerabilities, Threat and Technologies.*

Atacul împotriva capacităţii de conducere a organelor centrale şi locale ale ţării urmăreşte neutralizarea sistemelor decizionale, personalului şi tehnicii, precum şi a comenzii structurilor operaţionale subordonate acestora, pentru paralizarea activităţilor privind securitatea naţională (siguranţa cetăţenilor, ordine publică, apărare, situaţii de urgenţă etc.) a celor economice, financiare, sociale etc. Este îndreptat asupra capacităţilor fizice şi intelectuale ale conducătorilor, funcţionarilor din administraţia de stat şi locală, personalului de ordine publică, apărare şi intervenţie în situaţii de urgenţă.

Ca metodă de acţiune, adversarii potenţiali sau grupurile ostile pot folosi capturarea unora dintre persoanele de conducere, parlamentari, miniştri, diplomaţi, ofiţeri superiori etc. pentru dezorganizarea diferitelor domenii de activitate şi/sau atacul pentru influenţarea stării biofizice a întregului personal pentru scoaterea lui definitivă sau temporară din activităţile desfăşurate.

La această ameninţare contribuie practic şi atacul psihologic, care se bazează pe folosirea informaţiilor împotriva minţii umane, pentru a modifica sau anula percepţii, atitudini sau comportamente ale oamenilor. Ca urmare, pot apărea erori umane în procesele decizionale şi de comandă-control, care vor diminua capacitatea de conducere a statului şi a diferitelor domenii de activitate.

Pentru legătura organelor centrale ale statului cu cele ale Uniunii Europene, NATO şi ale altor organisme internaţionale, precum şi pentru legăturile diplomatice etc. un rol important îl au reţelele radio pe unde scurte care pot fi neutralizate prin schimbarea caracteristicilor electrice ale ionosferei.

Existenţa în sistemele de asigurare a informaţiilor şi de comunicaţii ale sistemelor informaţionale privind securitatea naţională a unor radare, staţii radio şi radio-relee, care funcţionează cu frecvenţe radio de înaltă energie şi folosesc antene cu câştig foarte mare, poate constitui un risc important pentru personalul de exploatare şi unele categorii de aparatură electronică, în principal, calculatoare, din compunerea acestora. Rezultă că sistemele informaţionale ale structurilor de stat privind securitatea naţională pot avea unele vulnerabilităţi ce pot fi exploatate de către adversari sau grupuri ostile, dar şi de persoane din interiorul acestora, rău intenţionate.

Cunoaşterea vulnerabilităţilor şi ameninţărilor informaţionale permite luarea de măsuri severe, organizatorice şi tehnice, pentru diminuarea sau înlăturarea completă a acestora.

Măsuri de protecţie a sistemelor şi reţelelor militare şi speciale

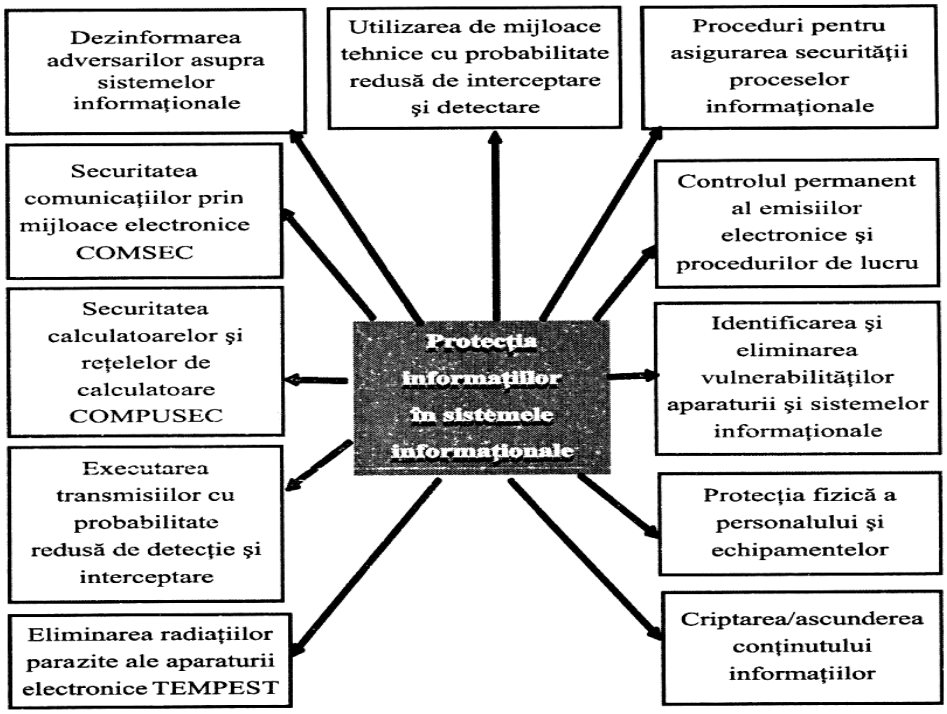
Protecţia sistemelor informaţionale se referă la luarea unor măsuri speciale de apărare a datelor vehiculate prin acestea, prin intermediul

echipamentelor de prelucrare automată a datelor, software de sistem şi de aplicaţie, precum şi al comunicaţiilor.

Cinci valori patrimoniale ale sistemelor informaţionale (echipamente, software, materiale, date, servicii) pot constitui ţinta următoarelor ameninţări: pierdere, respingere (nerecunoaştere), compromitere şi corupere.

Securitatea sistemului informaţional pentru securitatea naţională depinde de dinamica sa, iar ameninţările asupra acestuia sunt îndreptate împotriva structurilor organizatorice, echipamentelor, programelor de aplicaţie şi sistemului de operare, materialelor utilizate în reţelele de calculatoare, informaţiilor memorate pe diverse suporturi magnetice, hârtiilor de valoare aflate în sistem sau a serviciilor prestate de componentele acestuia.

Enumerarea principalelor măsuri de protecţie a informaţiilor[13] în sistemele informaţionale se prezintă în figura următoare:



[13] Information Protection Capabilities, Joint Doctrine Encyclopedia, US Army, 1997.

În general[14], ameninţările privind securitatea sistemelor informaţionale şi a informaţiilor vehiculate prin acestea pot fi grupate astfel:

- pierderea unor echipamente sau componente fizice;
- respingerea serviciilor;
- folosirea neautorizată a echipamentelor;
- accesarea informaţiilor clasificate;
- modificarea neautorizată a informaţiilor;
- pierderea informaţiilor;
- folosirea neautorizată a informaţiilor;
- aflarea neautorizată a secretelor privind produsele software utilizate;
- modificarea neautorizată a programelor utilizatorilor;
- pierderea sau folosirea neautorizată a produselor software.

Perimetrul sistemelor informaţionale, în care sunt păstrate şi vehiculate informaţiile clasificate, trebuie să fie zonat, în principiu, existând trei zone de securitate, anume: clasa I, clasa a II-a şi zona administrativă.

Se va organiza o evidenţă strictă asupra documentelor clasificate şi a persoanelor autorizate care au avut acces la acestea, pentru a se evita compromiterea accidentală sau intenţionată a informaţiilor, organizându-se, în acest scop, monitorizarea lor continuă şi neîntreruptă.

Preocupările pentru protecţia informaţiilor clasificate în sistemele informaţionale s-au amplificat considerabil odată cu trecerea la prelucrarea automată a datelor, întrucât:

- densitatea informaţiei este mult mai mare decât în sistemele clasice bazate pe hârtie, iar suporturile magnetice actuale (mai ales memory stick) cu capacităţi de ordinul zecilor de gigabaiţi pot memora cantităţi foarte mari de informaţie, ce poate fi sustrasă cu relativă uşurinţă;
- dispare transparenţa documentelor;
- accesarea datelor în sistemele de calcul moderne se poate efectua cu mai mare uşurinţă prin accesul neautorizat al unor persoane externe sau din cadrul organizaţiei privind securitatea naţională;
- eventualele atacuri cibernetice asupra sistemelor de calcul pe care sunt stocate informaţiile sunt greu de depistat;
- remanenţa suporturilor magnetice, după ce au fost şterse, poate constitui o cale sigură de a reface informaţiile înregistrate anterior;
- existenţa în memoriile calculatoarelor a informaţiilor de sinteză (agregate) cu valoare decizională ridicată permite obţinerea prin activităţi criminale a unor date utilizabile direct de către adversari;

[14] D. Oprea, *op. cit.,* p. 38.

- comunicaţiile şi reţelele de calculatoare au devenit tot mai performante, dar prezintă şi vulnerabilităţi însemnate, ceea ce permite ca atacurile informaţionale asupra acestora să se poată efectua în principal prin acţiuni cibernetice din orice loc de pe globul pământesc;

- standardele de securitate a informaţiilor în sistemele informaţionale existente nu permit o protecţie sigură a acestora şi necesită cheltuieli foarte mari şi specialişti cu înaltă calificare, măsuri care sunt greu de realizat.

Mecanismele de protecţie utilizate în sistemele informaţionale trebuie să fie cât mai simple, uşor de întrebuinţat, să ofere un număr cât mai mic de erori sau alarme false şi să demonstreze completitudine, caracterizată printr-o funcţionare normală la orice şi corectitudine, prin oferirea răspunsurilor anticloate la înregistrarea unor intenţii frauduloase. Mecanismul de protecţie trebuie să aibă o perioadă cât mai mare de supravieţuire şi să asigure permanent un nivel determinat al protecţiei. De asemenea, trebuie să ofere soluţii de funcţionare normală a echipamentelor sistemului informaţional în situaţia întreruperii alimentării cu energie electrica a acestora, defectării sistemului de comunicaţii şi variaţiilor bruşte ale temperaturii.

Apreciem că protecţia componentelor sistemelor informaţionale privind securitatea naţională împotriva atacurilor informaţionale, cu precădere împotriva celor electronice şi cibernetice, trebuia să constituie preocuparea principala a tuturor specialiştilor din domeniile informaţiilor, comunicaţiilor şi informaticii, întrucât globalizarea ameninţărilor la adresa acestora poate produce efecte de-zastruoase, ce afectează grav securitatea naţională.

De aceea, proiecţia sistemelor informaţionale privind securitatea naţională trebuie să aibă în vedere ansamblul mijloacelor tehnice a celor trei componente principale ale acestora, anume:

- subsistemul de asigurare a informaţiilor;
- subsistemul de comunicaţii;
- subsistemul reţelelor de calculatoare (informatic).

Subsistemul de asigurare (culegere) a informaţiilor este cel care dă semnificaţia şi importanţa sistemelor informaţionale, întrucât el furnizează materia primă (date şi informaţii) care priveşte securitatea naţională.

Mijloacele tehnice moderne utilizate pentru culegerea informaţiilor sunt numeroase şi se bazează pe utilizarea celei mai înalte tehnologii rezultată din simbioza electronicii, comunicaţiilor moderne şi informaticii. Ca urmare, ele prezintă anumite vulnerabilităţi care pot fi exploatate în cadrul războiului informaţional al adversarilor potenţiali (reali), prin atacarea lor fizică, electromagnetică sau cibernetică.

Scoaterea din funcţiune a unora dintre acestea poate cauza întreruperea unor fluxuri informaţionale, din cauza împiedicării funcţionării surselor de informaţii, respectiv senzori, mijloace de ascultare şi supraveghere, aparatură de goniometrare şi de obţinere a imaginilor etc. Principalul mijloc de protecţie a acestora constă în paza şi apărarea lor neîntreruptă, precum şi dispunerea echipamentelor în locuri (spaţii) protejate faţă de impulsurile electromagnetice şi energiile de mare putere.

Protecţia împotriva interceptării radiaţiilor parazite

Radiaţiile (emisiunile) compromiţătoare sunt constituite din semnale neintenţionate care, dacă sunt interceptate şi analizate, asigură dezvăluirea conţinutului informaţiei transmise, recepţionate, supuse prelucrării sau altor operaţiuni în echipamentele sistemelor de comunicaţii şi de calcul. Studiul efectuat asupra domeniului menţionat este cunoscut sub denumirea de TEMPEST (Transient Electro Magnetic Pulse Emanation Standardizing), care defineşte ansamblul investigaţiilor, studiilor şi controlului asupra radiaţiilor compromiţătoare ale echipamentelor electronice.

Protecţia[15] împotriva interceptării şi analizei radiaţiilor parazite pe timpul funcţionării acestora se realizează prin:

- diminuarea nivelului radiaţiilor parazite până la valorile prevăzute prin standarde şi norme de specialitate;
- limitarea accesului personalului neautorizat în raioanele de instalare a echipamentelor de comunicaţii şi de calcul şi eliminarea din aceste raioane a oricăror aparate capabile să înregistreze şi să retransmită radiaţiile parazite la distante convenabile adversarilor;
- măsurarea continuă a nivelului radiaţiilor parazite în gamele de lucru ale echipamentelor de comunicaţii şi adoptarea unor măsuri organizatorice şi tehnice severe pentru eliminarea sau reducerea posibilităţilor de interceptare a acestora;
- pregătirea temeinică a personalului de exploatare asupra măsurilor de protecţie a echipamentelor de comunicaţii şi de calcul.

Protecţia fizică a personalului şi echipamentelor tehnice

Protecţia fizică reprezintă o componentă importantă a managementului sistemului informaţional, care se realizează prin monitorizarea umană şi/sau electronică a zonei protejate, folosirea de bariere şi proceduri standardizate, chei de

[15] AR 381-14(S), *Technical Surveillance Countermeasures and TEMPEST*, SUA, 1998.

control, documente de acces specializate, iluminări şi alte soluţii care interzic accesul neautorizat.

În general, protecţia fizică trebuie să asigure:

- securitatea personalului şi compartimentarea strictă a accesului la echipamentele de comunicaţii şi de calcul;
- protecţia împotriva acţiunilor de spionaj, sabotaj, defectare şi furt;
- reducerea expunerii la ameninţări care pot cauza refuzul serviciilor sau alterarea neautorizată a informaţiilor;
- controlul şi supravegherea continuă a echipamentelor şi a locurilor de lucru ale personalului (monitorizarea video);
- reinscripţionarea cheilor de criptare după fiecare oprire a echipamentelor criptografice;
- asigurarea pazei neîntrerupte şi apărării punctelor cheie ale sistemelor de comunicaţii şi reţelelor de calculatoare.

Securitatea, din punctul de vedere al personalului, trebuie să aibă în vedere următoarele activităţi:

- selecţia;
- verificarea prin prisma securităţii;
- supravegherea continuă;
- instruirea şi conştientizarea.

Rezultă că protecţia informaţiilor şi a sistemelor informaţionale privind securitatea naţională împotriva operaţiilor informaţionale ofensive ale adversarilor potenţiali este o măsură defensivă absolut necesară în toate situaţiile.

Concluzii şi propuneri

Din tratarea teoretică a problematicii privind importanţa doctrinară şi acţională a războiului informaţional în viziunea Alianţei Nord-Atlantice şi, implicit, în concepţia de transformare a Armatei României, precum şi a celei referitoare la asigurarea informaţională a securităţii naţionale rezultă, evident, unele concluzii, esenţializarea acestora permiţându-ne să apreciem că:

- informaţia este, fără îndoială, un element esenţial al factorului de putere, oricare ar fi domeniul de manifestare, dar nu este suficientă deţinerea ca atare a acesteia, utilizarea ei oportună confirmând, de fapt, eficacitatea şi puterea utilizatorului informaţional;
- în contextul extrem de alert al noii revoluţii informaţionale, revoluţie care, practic, determină libertatea neîngrădită a cunoaşterii în geopolitica globalizării, războiul informaţional reprezintă componenta sau, după caz, dominanta oricărei confruntări, indiferent de domeniul în care se manifestă: social, militar, economic, fizic etc.;

- în actualul context informaţional global, dar şi al unei acerbe competiţii desfăşurate la nivelul tuturor subsistemelor sistemului social global, inclusiv, evident, a celui militar, războiul informaţional este, deopotrivă, omniprezent, inevitabil şi continuu;

- scopul organic al războiului informaţional, în oricare dintre formele sub care se poate desfăşura operaţional-ofensiv sau defensiv, constă în dobândirea superiorităţii informaţionale, cu consecinţe în afirmarea superiorităţii/victoriei în domeniul căruia îi este subsumat, în cazul nostru, cel privind securitatea naţională;

- imposibilitatea practică de a-l limita în vreun fel, ca arie de desfăşurare, spaţialitate şi obiectivele urmărite, indiferent de domeniul în care se manifestă şi în care este utilizat, conferă războiului informaţional atributele spaţiale ale globalizării, putând considera, pe drept cuvânt, că este, deopotrivă, vector şi consecinţă a acesteia;

- în ceea ce priveşte armele şi tehnicile utilizate în războiul informaţional, acestea nu au nicidecum un caracter imuabil, dincolo de cele deja consacrate, fiind posibilă, în circumstanţe imprevizibile, apariţia unor „arme", instrumente şi tehnici necunoscute încă de ducere a războiului informaţional, inclusiv prin utilizarea unor noi principii ale fizicii;

- din perspectiva împlinirilor tehnologiei postmoderne, războiul informaţional pune în evidenţă atât virtuţile incontestabile ale revoluţiei informaţionale, cât şi limitele acesteia în contextul înfruntărilor care o exprimă deopotrivă;

- războiul informaţional şi informaţia, în sensul cognoscibil al practicii umane, sunt unii dintre vectorii cei mai determinanţi ai noii revoluţii în afacerile militare;

- în asigurarea informaţională a securităţii naţionale, resursele informaţionale au un rol decisiv, calitatea şi oportunitatea acestora relevând capacitatea structurilor de informaţii ale statului, precum şi nivelul de racordare instituţională la rigorile aplicate ale revoluţiei informaţionale;

- conţinutul informaţiilor care alimentează afirmarea complexă a securităţii naţionale este extrem de eterogen, practic nedefinit şi neprincipializat doctrinar, motiv pentru care, în perspectiva coagulării sistemice a acestei problematici, apreciem că este util să se procedeze la sistematizarea criterială coerentă a acestora;

- eficienţa asigurării informaţionale a securităţii naţionale depinde, decisiv, de capabilităţile decizionale ale structurilor instituţionale împuternicite cu asemenea responsabilităţi;

- explozia informaţională, fără precedent, ca amploare şi anvergură, în istoria umanităţii, îngreuiază obţinerea conţinutului util al informaţiilor prin care

asigurăm securitatea naţională, realitate care impune utilizatorilor avizaţi ai informaţiilor dobândite, un discernământ profesional desăvârşit;

Pe baza concluziilor formulate în urma studiului multilateral al literaturii de specialitate considerăm că putem formula următoarele **propuneri:**

- detalierea conceptului de război informaţional, în accepţiunea utilizării sale pentru asigurarea securităţii naţionale, în funcţie de cele trei situaţii majore în care poate fi utilizat: la pace, în situaţii de criză şi în caz de război;
- studiul sistematic al conţinutului asigurării informaţionale a securităţii naţionale, cu luarea în consideraţie a tuturor domeniilor care contribuie la aceasta şi a necesităţilor lor de informare, comandă şi control, precum şi a măsurilor de protecţie a reţelelor de comunicaţii şi de calculatoare aferente;
- includerea securităţii informaţiilor printre priorităţile naţionale;
- problematica războiului informaţional să devină disciplină obligatorie de studiu în toate structurile de învăţământ ale instituţiilor care răspund pentru securitatea naţională;
- în cadrul măsurilor privind pregătirea ţării pentru apărare (exerciţii, aplicaţii etc.) să fie incluse şi acţiunile de descoperire şi contracarare a ameninţărilor informaţionale privind securitatea naţională;
- studiul temeinic al normelor şi instrucţiunilor NATO privind războiul informaţional, de către toate structurile privind securitatea naţională, în părţile ce le privesc;
- pregătirea personalului de informatică care exploatează reţelele de calculatoare ale structurilor din sistemul securităţii naţionale pentru prevenirea şi lichidarea atacurilor cibernetice;
- corelarea doctrinară şi operaţională a războiului informaţional, ca formă a luptei armate, cu principalele forme de luptă utilizate în prezent, dar şi cu legile şi principiile luptei armate, avându-se însă în vedere şi posibilităţile de utilizare independentă a acestuia;
- protecţia împotriva ameninţărilor informaţionale să constituie o preocupare continuă a tuturor structurilor care răspund de securitatea naţională, dar şi a celorlalte organizaţii atât pe timp de pace, dar mai ales în situaţii de criză şi conflict militar;
- procurarea şi dotarea cu mijloace moderne de război informaţional defensive, dar şi ofensive a principalelor structuri ale statului care răspund de securitatea naţională.

BIBLIOGRAFIE

*** Constituţia României, Monitorul Oficial al României, nr. 233/1999;

*** Doctrina naţională a informaţiilor pentru securitate, Editura SRI, Bucureşti, 2004

*** Doctrina pentru informaţii, contrainformaţii şi securitate a armatei, Bucureşti, 2005

*** Legea privind protecţia informaţiilor clasificate, nr. 182/2002, publicată în M.Of. nr. 248/2002

*** Legea privind securitatea naţională a României nr. 51/1991, publicată în M. Of. Nr. 163/1991

*** Securitatea informaţiilor, Centrul de Expertiză în Domeniul Securităţii, Bucureşti, 2008

*** Sisteme informaţionale – Sesiunea anuală de comunicări ştiinţifice cu participare internaţională, Editura UNAp. "Carol I", Bucureşti, 2007

*** Strategia de securitate naţională a României, Bucureşti, 2007

Alexandrescu C. şi alţii, *Supremaţia electromagnetică*, Editura UNAp, Bucureşti, 1999

Alexandrescu C., *Ameninţări informaţionale asupra sistemelor de comandă şi control în acţiunile militare moderne "SI-2007"*

Alexandrescu C., Teodorescu C., *Războiul electronic contemporan,* Editura Sylvi, 1999

Alexandrescu Gr., Văduva Gh., *Infrastructuri critice: Pericole, ameninţări la adresa acestora: Sisteme de protecţie,* Editura UNAp. "Carol I", Bucureşti, 2006

Bădălan Eugen, *Securitatea României, actualitate şi perspective*, Editura Militară, Bucureşti, 2001

Constantin Alexandrescu, Decebal Ilina, Constantin Mincu, *Bazele matematice ale organizării sistemelor de transmisiuni*, Editura Militară, Bucureşti, 1994

Dr. Constantin Mincu, Dr. Gruia Timofte, *Compatibilitatea Sistemelor Radioelectronice,* Editura Olimp, Bucureşti, 1999

Dr. Constantin Mincu, dr. Victor Greu, Ing. Costel Rotariu, *Salt de frecvenţă şi contrasalt de frecvenţă,* Editura Militară, Bucureşti, 1998

ENSA Risk Management/Risk Assesment (European Network and Information Security Agency)

EUROCOM D/1 Tactical Communications Systems. Basic Parametersm 1986

FM 3-13 Information Operations: Doctrine, Tactics, Techniques and Procedures, US Army, 2003
FM 34-1 Intelligence and Electronic Warfare Operations, Headquarters Department of the Army, Washington DC
Frunzeti Teodor, *Securitatea naţională şi războiul modern,* Editura Militară, Bucureşti, 1999
Hlihor C., *Geopolitica şi geostrategia în analiza relaţiilor internaţionale contemporane,* Editura UNAp, Bucureşti, 2005
Ilie Gh., Stoian I., Ciobanu V., *Securitatea informaţiilor,* Editura Militară, Bucureşti, 1996
ISO/IEC 27001 Information Technology. Security Technique. Information Security Management Systems – Requirements
Mureşan M., Văduva Gh., *Războiul viitorului*, viitorul războiului, Editura UNAp, Bucureşti, 2005
Robert H. Anderson, *Physical Vulnerabilities of Critical US Information Systems* (internet, Iaver May 03.pdf)
Toffler Alvin şi Heidi, *Război şi anti-război,* Editura Antet, Bucureşti, 1995
Toffler Alvin, *Powershift, puterea în mişcare*, Editura Antet, Bucureşti, 1995

Reviste de specialitate:

1. Gândirea Militară Românească, anii 2001-2010;
2. Buletinul Universităţii Naţionale de Apărare "Carol I", 2008-2010;
3. Revista Forţelor Terestre, anii 2005-2010;
4. Impact Strategic, anii 2006-2010;
5. Revista de ştiinţe militare, anii 2006 – 2009;
6. Romanian Military Thinking Journal, anii 2005 – 2010.

PROTECȚIA INFRASTRUCTURII CRITICE DE INFORMAȚIE

General locotenent (r) prof. univ. dr. Cristea DUMITRU

Tehnologiile informației şi comunicațiilor (TIC) sunt din ce în ce mai prezente în activitățile de zi cu zi. Parte din aceste sisteme TIC, servicii, rețele şi infrastructuri reprezintă o componentă esențială a economiei şi a societății moderne, furnizarea de bunuri şi servicii sau platformă de sprijin pentru un număr de alte infrastructuri critice. Infrastructurile TIC sunt considerate infrastructuri critice de informații, deoarece întreruperea sau degradarea lor ar putea avea un impact grav asupra unor funcții societale vitale. Acest studiu se concentrează pe prevenirea atacurilor cibernetice, pe îmbunătățirea securității şi rezilienței infrastructurii de informații critice.

Introducere

Tehnologia informației şi comunicațiilor (TIC) evoluează continuu datorită progresului tehnologic, mediului de afaceri şi presiunilor exercitate de competitivitatea din toate sectoarele economiei. În pofida naturii sale dinamice, apreciem că domeniul TIC asigură comunicații şi procese sigure şi de încredere, în acord cu nevoile guvernelor, mediului de afaceri şi populației secolului XXI. Infrastructura TIC a traversat o transformare dramatică în ultimul deceniu. Creşterea explozivă a utilizării rețelelor pentru a conecta diversitatea sistemelor informatice a determinat, cu relativă uşurință, obținerea informațiilor, comunicarea şi controlul acestor sisteme de la mare distanță. Datorită creşterilor de productivitate obținute şi a noilor capabilități furnizate de aceste sisteme conectate în rețea, acestea au fost încorporate într-un număr foarte mare de aplicații civile, incluzând domeniile educației, comerțului, ştiințific şi ingineriei, divertismentului etc. Aceste sisteme informatice conectate în rețea au pătruns, de asemenea, în practic fiecare sector al infrastructurilor critice – comunicațiile, utilitățile publice,

finanţele, transporturile, siguranţă şi ordine publică, apărare. Pe bună dreptate, considerăm că toate aceste sectoare depind, în prezent, de infrastructura TIC.

Majoritatea oamenilor utilizează componentele infrastructurii TIC – în special, calculatoare de birou conectate la Internet şi telefoane mobile – care pemit mesageria electronică, mesageria instant, schimbul şi descărcarea de sunete şi imagini, comerţ online, căutare de informaţii, jocuri interactive, precum şi servicii de telefonie. Oamenii lucrează, de asemenea, cu tehnologii informatice care conduc procesele zilnice din industrie şi administraţie, pe care se bazează entităţile economice pentru realizarea unei game largi de funcţiuni, precum proiectarea, producţia, inventarierea, efectuarea vânzărilor şi plăţilor, stocarea şi identificarea informaţiilor, educaţia şi instruirea, cercetarea şi dezvoltarea.

Mai puţin vizibil şi, cu siguranţă, mai puţin înţeles este faptul că aceste tehnologii – calculatoare, dispozitive de stocare în masă a informaţiilor, componente de reţea şi ale reţelelor de mare viteză, cum ar fi: ruterele şi comutatoarele, sistemele şi aplicaţiile software, dispozitivele integrate şi cele fără fir, precum şi Internetul în sine – sunt, în prezent, esenţiale pentru toate infrastructurile critice. Sistemele de calcul controlează managementul centralelor electrice, barajelor, sistemului energetic naţional, sistemelor de control ale traficului aerian, sistemelor de distribuţie a utilităţilor publice, sistemului financiar, pentru a numi numai câteva din elementele constituente ale infrastructurilor critice. Sprijinul acestor instalaţii fizice sensibile pe infrastructura TIC determină faptul că infrastructura TIC este, la rândul ei, o infrastructură critică, a cărei protecţie apreciem că este de interes naţional.

Evoluţia conceptului de protecţie a infrastructurii critice

Apariţia conceptului de protecţie a infrastructurii critice este rezultatul a doi factori relaţionaţi şi, uneori, intercondiţionaţi. Expansiunea spectrului de ameninţări, după încheierea Războiului Rece, în special, în termeni de actori ostili şi capabilităţile acestora pe de o parte, şi noul tip de vulnerabilităţi determinate de dependenţa societăţii moderne de sisteme informatice conceptual nesigure, pe de cealaltă parte. Pe timpul Războiului Rece, ameninţările erau percepute, în principal, ca fiind derivate din intenţiile agresive ale statelor pentru a obţine dominaţia asupra altor state. Printre altele, opinăm că sfârşitul Războiului Rece a condus şi la dispariţia ameninţărilor lipsite de echivoc. Urmare a dezintegrării Uniunii Sovietice, o varietate de noi ameninţări a apărut pe agenda de securitate a majorităţii statelor. Principala calitate distinctivă a acestor „noi” provocări o reprezintă elementul de nesiguranţă, care se referă la identitatea şi obiectivul potenţialilor adversari, perioada în care pot apărea anumite ameninţări, constrângerile ce pot fi impuse statului de către alte state, capabilităţile împotriva

cărora trebuie să fii pregătit să acţionezi, precum şi incertitudinea asupra tipului de provocare pentru care trebuie să te pregăteşti. În mod clar, noţiunea de „ameninţare", ce presupune o acţiune iminentă, directă şi sigură, nu mai descrie cu acurateţe provocările secolului XXI. Aceste provocări pot fi apreciate, mai degrabă, ca fiind „riscuri" care, prin definiţie, sunt indirecte, neintenţionate, nesigure şi estimat a se produce în viitor, întrucât acestea se materializează doar atunci când se produc în realitate.

Ca rezultat al acestor riscuri difuze şi datorită dificultăţilor în localizarea şi identificarea inamicilor, o parte a politicilor de securitate şi-a schimbat centrul de greutate de la acţiuni, capabilităţi şi motivaţii, către vulnerabilităţile generale ale societăţilor. Lozinca acestei dezbateri a devenit „asimetria", iar forţele armate americane au devenit promotorul acestui tip de percepere a ameninţărilor încă de la începutul anilor 90. Statele Unite au rămas singura superputere militară pe arena internaţională şi par predestinate a fi ţinta conflictelor asimetrice. În mod particular, acei adversari care foarte probabil ar fi fost înfrânţi în cazul unui conflict armat cu Statele Unite au putut plănui să îngenucheze Statele Unite lovindu-le în punctele vitale, care în mod fundamental nu sunt exclusiv ţinte militare, dar esenţiale pentru funcţionarea societăţilor industrializate. Aceste puncte vitale sunt definite, în mod general, ca fiind infrastructuri critice. Acestea sunt predestinate să fie critice datorită faptului că incapacitarea sau distrugerea lor poate avea un impact semnificativ asupra securităţii naţionale şi bunăstării economice şi sociale a unei naţiuni.

Teama că acţiunile asimetrice pot fi îndreptate asupra unor ţinte ce nu sunt militare a fost agravată de cel de-al doilea factor, aşa numita revoluţie informatică. Majoritatea infrastructurilor critice îşi datorează buna funcţionare sistemelor de control bazate pe o gamă largă de aplicaţii software. În multe situaţii, TIC a devenit omniprezentă, conectând alte sisteme de infrastructură critică determinând interrelaţionarea şi interdependenţa acestora. Aceste tehnologii sunt considerate, în general, ca fiind nesigure. Securitatea nu a fost vreodată elementul determinant al unui proiect de sistem, iar presiunea ca un anumit produs să ajungă mai repede pe piaţă este foarte mare, ceea ce ne conduce la concluzia că şi în continuare ne putem aştepta la o explozie de vulnerabilităţi ale sistemelor şi reţelelor de calculatoare, având drept efect infrastructuri cu instabilităţi, puncte critice de avarie şi interdependenţe extinse. În acelaşi timp, TIC a fost şi este considerată ca fiind mult mai uşor de atacat asimetric, nefiind necesare sisteme de armament specializat sau forţe armate. Dacă în lumea reală graniţele sunt deja, în multe privinţe, permeabile, în spaţiul cibernetic acestea pur şi simplu nu există.

Confruntate cu această percepţie a ameninţării, Statele Unite au fost primul stat care a destinat o atenţie concentrată şi amplă noii vulnerabilităţi a

infrastructurilor critice. În 1997, preşedintele Comisiei de protecţie a infrastructurilor critice a identificat noile riscuri apărute în sectoarele de activitate precum informatica şi comunicaţiile, sistemul bancar şi de finanţe, energia, distribuţia fizică a utilităţilor, precum şi serviciile de urgenţă. Aceste riscuri au fost considerate ca fiind de importanţă naţională pentru Statele Unite, deoarece dacă aceste elemente de infrastructură devin indisponibile pentru o perioadă semnificativă de timp vor apărea consecinţe serioase la nivelul întregului stat[1].

În concordanţă cu această abordare, infrastructurile critice trebuie să includă mijloacele TIC, reţelele, serviciile şi instalaţiile, care odată distruse sau avariate ar putea avea un impact serios asupra stării de sănătate, securităţii sau bunăstării economice ale cetăţenilor, precum şi asupra capacităţii de funcţionare eficientă a guvernului ţării. Aceste infrastructuri critice pot fi deteriorate de ameninţări structurale sau de către atacuri intenţionate ale unor agresori. Prima categorie de risc ar putea include, de exemplu, catastrofe naturale, catastrofe cauzate de erori umane (cum ar fi, distrugerea unui baraj, accident la un reactor nuclear etc.), personal insuficient de exploatare datorat unor epidemii sau greve, deficienţe organizaţionale determinate de cauze umane sau tehnice, grave erori umane, avarii tehnice, precum şi întreruperi majore ale alimentării cu energie electrică. În cea de-a doua categorie, spectrul posibililor atacatori este foarte larg, de la adolescenţi plictisiţi, angajaţi disponibilizaţi sau nedreptăţiţi, crimă organizată, fanatici şi celule teroriste, până la state ostile.

Opţiunile de atac pot varia în limite largi, de la atacurile hackerilor şi până la distrugerea fizică a instalaţiilor civile sau militare. Principala ţintă a eforturilor iniţiale de protecţie a infrastructurilor critice a fost reprezentată de riscurile provenite din spaţiul cibernetic. Infrastructura de informaţii globală pare să faciliteze atacurile anonime declanşate de oriunde de pe glob, servind în acelaşi timp ca sursă de instrumente de atac pentru oricine. Pe baza acestei percepţii a ameninţării, pe timpul mandatului preşedintelui american Bill Clinton, a fost cristalizată o politică de protecţie a infrastructurilor critice, ce a fost în mare măsură dedicată securităţii informaţiei. În multe privinţe şi alte state au urmat această cale, cu o concentrare similară asupra aspectului informaţiei. Cu toate acestea, după atacurile teroriste de la 11 septembrie 2001, s-a putut remarca un oarecare recul în domeniul protecţiei infrastructurii critice de informaţie în favoarea dezbaterii protecţiei infrastructurilor critice în ansamblu. Cel puţin din punctul de vedere al Statelor Unite, se poate remarca o concentrare a eforturilor

[1] President's Information Technology Committee, *Cyber Security: A Crisis of Prioritization*, National Coordination Office for Information Technology Research and Development, February 2005, Virginia, U.S.A., p.5.

pentru micşorarea sau eliminarea riscurilor structurale în cadrul unei politici contrateroriste tot mai viguroase. În Statele Unite, protecţia infrastructurilor critice a devenit o componentă cheie a securităţii naţionale şi este discutată, în prezent, predominant în contextul dezvoltării strategiilor antiteroriste. Aspectele fizice ale protecţiei infrastructurilor critice au câştigat o mai mare importanţă, în timp ce prioritatea protecţiei infrastructurii critice de informaţie s-a diminuat uşor. În acelaşi timp, această orientare a protecţiei infrastructurilor critice către contraterorism a devenit o marotă şi pentru dezbaterile recente din Uniunea Europeană, care au început să dezvolte o politică a protecţiei infrastructurilor critice care constă, în principal, pe coordonarea măsurilor adoptate de către statele membre.

În pofida fluctuaţiilor asupra modului în care este considerată protecţia infrastructurilor critice, realităţile ultimilor ani obligă la acordarea unei atenţii sporite protecţiei infrastructurii critice de informaţie. În unele publicaţii oficiale, sintagma de protecţie a infrastructurilor critice este folosită preponderent, chiar dacă documentele se referă numai la aspectele de informaţie ale problemei. Motivul acestei situaţii constă în faptul că protecţia infrastructurilor critice nu poate şi nu trebuie să fie discutată separat de protecţia infrastructurii critice de informaţie. În opinia noastră, protecţia infrastructurilor critice înseamnă mai mult decât protecţia infrastructurii critice de informaţie, dar protecţia infrastructurii critice de informaţie este o parte esenţială a protecţiei infrastructurilor critice. O abordare exclusivă a ameninţărilor din spaţiul cibernetic ce ignoră importanţa ameninţărilor tradiţionale din mediul fizic este tot atât de periculoasă ca şi neglijarea dimensiunii virtuale, fiind necesară tratarea conjugată a celor două concepte interelaţionate. Cu toate acestea, există cel puţin o caracteristică care face distincţie între cele două concepte. Dacă protecţia infrastructurilor critice cuprinde sectoarele critice ale infrastructurii unui stat, protecţia infrastructurii critice de informaţie este doar un subset al unui efort amplu de protecţie, întrucât aceasta se referă doar la măsurile de realizare a protecţiei infrastructurii critice de informaţie. Încercând să explicăm sintagma de infrastructură critică de informaţie, vom observa că infrastructura critică de informaţie este o parte a infrastructurii naţionale sau globale de informaţie care este, în mod esenţial, necesară pentru funcţionarea continuă a serviciilor infrastructurilor critice ale statului. Infrastructura critică de informaţie poate fi redusă, într-o mare măsură, la sectorul TIC, fără a fi însă pe deplin congruentă cu acesta, incluzând componente cum ar fi: telecomunicaţiile, calculatoarele / aplicaţiile software, internetul, sateliţii, reţelele de fibră optică etc. Termenul este folosit, de asemenea, pentru a defini totalitatea calculatoarelor şi reţelelor interconectate şi a fluxurilor lor de informaţii critice.

Datorită rolului pe care îl joacă infrastructurile de informaţii în interconectarea altor infrastructuri critice, precum şi a furnizării unor noi modalităţi prin care acestea din urmă pot fi atacate, infrastructura critică de informaţie deţine un rol foarte special în ansamblul efortului de realizare a protecţiei infrastructurilor critice. Considerăm că infrastructura critică de informaţie reprezintă o coloană vertebrală a infrastructurilor critice, dat fiind faptul că fluxul de date neîntrerupt este esenţial pentru funcţionarea infrastructurilor, în general, şi a serviciilor pe care acestea le asigură. Sistemele SCADA (Supervisory, Control, and Data Acquisition – achiziţia de date, control şi supraveghere) centralizate sunt larg utilizate pentru monitorizarea şi controlul de la distanţă al infrastructurilor. Dar sistemele bazate pe SCADA nu sunt securizate, atât timp cât sistemele şi reţelele folosesc produse comerciale, echipamentele de reţea sunt bazate pe IP, iar interconectarea necesită serviciul de internet, care finalmente deschide uşa potenţialilor agresori.

Politica Uniunii Europene în domeniul protecţiei infrastructurii critice de informaţie

Uniunea Europeană este unul dintre actorii principali pe plan internaţional în privinţa asigurării informaţionale. Protecţia infrastructurii critice de informaţie, Societatea Informaţională şi securitatea informaţiei sunt considerate a fi probleme de cea mai mare importanţă. Drept urmare, Uniunea Europeană a lansat iniţiative şi programe de cercetare pentru a studia diversele aspecte ale revoluţiei informaţionale şi impactul acesteia asupra educaţiei, mediului de afaceri, sănătăţii cetăţenilor şi comunicaţiilor.

Atacurile teroriste de la Madrid, în 2004, şi Londra, în 2005, au evidenţiat riscul atacurilor teroriste îndreptate, într-un sens mai larg, împotriva infrastructurilor europene. Deteriorarea sau pierderea unei infrastructuri într-unul dintre statele membre poate avea efecte negative asupra multor altora şi a economiei europene ca întreg.

Comunicatul Comisiei Uniunii Europene, din 20 octombrie 2004, referitor la protecţia infrastructurilor critice în cadrul luptei împotriva terorismului oferă o definiţie a infrastructurilor critice, enumerează sectoarele critice identificate şi discută criteriile pentru determinarea potenţialelor infrastructuri critice. În comunicat, infrastructurile critice sunt definite după cum urmează: „Infrastructurile critice constau în acele tehnologii fizice şi de informaţii, reţele, servicii şi bunuri care, în cazul deteriorării sau distrugerii, ar putea avea un impact serios asupra sănătăţii, siguranţei şi securităţii sau bunăstării economice ale cetăţenilor, ori asupra funcţionării eficiente a guvernelor din statele membre. Infrastructurile

critice cuprind multe sectoare ale economieişi servicii guvernamentale importante”[2].

În documentul emis ulterior de Comisia Uniunii Europene, Cartea verde a Programului european de protecţie a infrastructurilor critice, protecţia infrastructurii critice de informaţie este definită ca fiind „Ansamblul activităţilor şi programelor desfăşurate de către proprietarii, operatorii, fabricanţii, utilizatorii şi autorităţile mandatate care sunt destinate menţinerii performanţelor infrastructurii critice de informaţie dincolo de un nivel minim predefinit de servicii, în situaţiile apariţiei defecţiunilor, atacurilor sau accidentelor şi are drept obiectiv minimizării efectelor şi procesului de recuperare. În consecinţă, protecţia infrastructurii critice de informaţie trebuie considerată ca fiind mai degrabă un fenomen intersectorial şi mai puţin unul limitat la anumite sectoare. Protecţia infrastructurii critice de informaţie trebuie coordonată strâns în relaţie cu protecţia infrastructurilor critice, dintr-o perspectivă holistică”[3].

În aprilie 2005, Uniunea Europeană a înfiinţat un grup de lucru destinat să exploreze măsurile adoptate de către statele membre pentru a combate ameninţările (inclusiv cele din spaţiul cibernetic) îndreptate împotriva infrastructurilor critice. Ca parte a proiectului Coordonarea cercetării în domeniul protecţiei infrastructurii critice de informaţie (Critical Information Infrastructure Research Coordination – CI2RCO), grupul de lucru trebuia să identifice grupurile de cercetare şi programele care vizau securitatea tehnologiei informaţiilor în infrastructurile critice, cum ar fi reţelele de telecomunicaţii şi reţelele de alimentare cu energie electrică. Proiectul CI2RCO a fost o acţiune co-finanţată prin FP7, Programul cadru nr.7, pentru Prioritatea tehnologiilor Societăţii Informaţionale. Principalele obiective ale proiectului CI2RCO sunt:

- încurajarea unei abordări coordonate, în toată Europa, a cercetării şi dezvoltării protecţiei infrastructurii critice de informaţie;
- stabilirea unui domeniu de cercetare european pentru protecţia infrastructurii critice de informaţie, ca parte unui obiectiv strategic mai amplu pentru Societatea Informaţională, care să vizeze integrarea şi consolidarea domeniului în termeni de securitate şi fiabilitate;
- desfăşurarea de activităţi şi acţiuni din domeniul protecţiei infrastructurii critice de informaţie în statele membre şi candidate.

[2] Cf. Commission of the European Communities, *Critical Infrastructure Protection in the Fight Against Terrorism*, COM(2004) 702 final, Brussels, 20.10.2004, p.3.
[3] Cf. Commission of the European Communities, *Green Paper on a European Programme for Critical Infrastructure Protection*, COM(2005) 576 final, Brussels, 17.11.2005, p.19.

Aceste obiective sunt îndeplinite prin următorul set de activităţi de coordonare:

- înfiinţarea unei reţele de protecţie a infrastructurii critice de informaţie;
- identificarea programelor şi proiectelor de cercetare şi dezvoltare în domeniul protecţiei infrastructurii critice de informaţie finalizate, aflate în desfăşurare sau planificate la nivelul naţional şi al Uniunii Europene;
- analizarea domeniului de cercetare a protecţiei infrastructurii critice de informaţie din Europa, în concordanţă cu criterii corespunzătoare de evaluare;
- calibrarea activităţilor de protecţie a infrastructurii critice de informaţie, împreună cu proprietarii infrastructurilor critice de informaţie, într-un feedback continuu, pentru a identifica lipsurile existente în activităţile şi acţiunile de protecţie a infrastructurilor critice de informaţie curente şi planificate;
- organizarea unor conferinţe sau ateliere pentru a iniţia şi a dezvolta reţele pentru evaluarea, finalizarea şi diseminarea rezultatelor;
- furnizarea unei platforme pe internet pentru a oferi un sprijin de informare şi cooperare susţinut a reţelei de protecţie a infrastructurii critice de informaţie[4].

Activitatea proiectului CI2RCO s-a încheiat la sfârşitul lunii februarie 2007.

Pe data de 14 martie 2004, Uniunea Europeană a înfiinţat Agenţia europeană de securitate a reţelelor şi a informaţiei (ENISA – European Network and Information Security Agency), în scopul întăririi eforturilor europene de coordonare a securităţii informaţiei. ENISA este destinată să asigure un nivel înalt de securitate a reţelelor şi a informaţiei în cadrul comunităţii statelor membre ale Uniunii Europene. Prin aceasta, agenţia contribuie la dezvoltarea securităţii reţelelor şi a informaţiei în beneficiul cetăţenilor, consumatorilor, întreprinderilor şi organizaţiilor din sectorul public din Uniunea Europeană.

Agenţia asistă Comisia Uniunii Europene, statele membre şi, în consecinţă, comunitatea de afaceri în respectarea cerinţelor de securitate a reţelelor şi a informaţiei, incluse în legislaţia Uniunii Europene, prezente şi viitoare, din domeniu. Până la urmă, ENISA serveşte drept centru de expertiză atât pentru statele membre cât şi pentru instituţiile Uniunii Europene, pentru a oferi asistenţa necesară pentru problemele legate de securitatea reţelelor şi a informaţiei[5].

---

[4] Cf. Elgin M. Brunner and Manuel Suter, *International CIIP Handbook 2008/2009*, Center for Security Studies, ETH Zurich, 2008, pp.477-478.

[5] European Network and Information Security Agency (ENISA). Work Programme 2008, *Build on Synergies – Achieve Impact*. http://www.enisa.europa.eu/ doc/pdf/ management_board/decisions/enisa_wp_2008.pdf.

În 2008, mandatul ENISA a fost extins fără modificări până în martie 2012. În acelaşi timp, Consiliul şi Parlamentul European au făcut un apel pentru continuarea discuţiilor referitoare la viitorul ENISA şi pentru orientarea generală a eforturilor europene către o securitate sporită a reţelelor şi a informaţiei.

Pentru protecţia infrastructurilor critice de informaţie, Comisia Europeană a lansat o iniţiativă politică la sfârşitul lunii martie 2009 şi a emis un comunicat către Parlamentul European, Consiliu, Comitetul Economic şi Social European şi Comitetul Regiunilor privind protecţia infrastructurilor critice de informaţie, intitulat „Protejarea Europei de atacuri cibernetice şi perturbaţii de amploare, ameliorarea gradului de pregătire, a securităţii şi a rezilienţei". Activităţile prevăzute în acest comunicat se derulează în cadrul Programului european pentru protecţia infrastructurii critice. În motivaţia acestui comunicat, se arată că reţelele şi serviciile de comunicaţii electronice furnizează fundamentul economiei europene, acestea fiind vitale cetăţenilor, mediului de afaceri şi guvernelor. Acestea sunt denumite, în mod generic, ca fiind infrastructura critică de informaţie. Infrastructurile de informaţie alcătuite din linii telefonice, cabluri de fibră optică şi reţele de calculatoare ne conduc vieţile şi trebuie să fie sigure. Mari părţi ale economiei europene se bazează pe infrastructura critică de informaţie. Totodată, multe servicii şi activităţi devin din ce în ce mai dependente de funcţionarea reţelelor TIC. Deoarece aceste reţele tind să fie descentralizate, cu un mare grad de interconectare şi interdependenţă, defectarea acestor infrastructuri poate genera un fenomen în cascadă, cu efecte dincolo de graniţele naţionale. Practic, infrastructurile TIC sunt considerate infrastructuri critice de informaţie, întrucât distrugerea sau perturbarea acestora poate avea un impact grav asupra unor funcţii societale vitale.

Comunicatul conţine prevederi noi privind securitatea şi integritatea reţelelor şi informaţiei, în special în vederea accentuării obligaţiilor operatorilor de a depune toate eforturile pentru luarea măsurilor corespunzătoare care să conducă la limitarea riscurilor, la garantarea continuităţii furnizării serviciilor şi la notificarea breşelor de securitate. Aceste procese converg înspre obiectivul general de ameliorare a securităţii şi a rezilienţei infrastructurilor critice de informaţie.

Această iniţiativă politică ia în considerare activităţile NATO privind politica comună în domeniul apărării împotriva criminalităţii cibernetice, respectiv ale Autorităţii de Management pentru Apărare împotriva Criminalităţii Cibernetice şi Centrul de Excelenţă pentru Apărare împotriva Criminalităţii Cibernetice. Nu în ultimul rând, iniţiativa ţine seama şi de evoluţiile internaţionale în domeniu, în special de principiile G8 cu privire la protecţia infrastructurilor critice de informaţie, Rezoluţia 58/199 a Adunării Generale a ONU privind crearea unei culturi mondiale a securităţii cibernetice şi protecţia infrastructurilor critice de

informaţie şi recenta recomandare a OECD privind protecţia infrastructurilor critice de informaţie[6].

Datorită dimensiunii comunitare şi internaţionale a problemei, opinăm că este necesară o abordare integrată la nivelul Uniunii Europene pentru sporirea securităţii şi rezilienţei infrastructurilor crititice de informaţie, care să completeze şi să aducă valoare adăugată programelor naţionale existente şi schemelor de cooperare bilaterală şi multilaterală dintre statele membre. Discuţiile legate de politicile publice iniţiate în urma evenimentelor din Estonia sugerează că efectele unor atacuri similare pot fi limitate prin măsuri preventive şi prin acţiuni coordonate desfăşurate în momentul crizei. Schimburile mai structurate de informaţii, precum şi de bune practici la nivelul Uniunii Europene pot facilita în mod considerabil combaterea ameninţărilor transfrontaliere din spaţiul cibernetic.

În accepţiune europeană, infrastructurile critice de informaţie cuprind tehnologiile informaţiei şi comunicaţiilor (TIC), care asigură platformele fundamentale de informaţie şi comunicare pe baza cărora sunt furnizate bunuri şi servicii fundamentale, inclusiv funcţii societale vitale, cum ar fi: aprovizionarea cu electricitate şi apă, serviciile de transport, bancare, de sănătate şi de urgenţă. Infrastructurile critice de informaţii sunt caracterizate de un nivel înalt de integrare a unor sisteme complexe, de interdependenţa în raport cu alte infrastructuri critice, precum şi de interconectarea transfrontalieră. Aceste infrastructuri critice sunt astfel expuse unui mare număr de riscuri, care poate da naştere unor deficienţe ale sistemelor cu consecinţe catastrofale, afectând simultan serviciile societale vitale în numeroase state membre. Riscurile ar putea proveni din erori umane, deficienţe tehnice, atacuri provocate de factorul uman (inclusiv de natură criminală sau din motive politice) şi catastrofe naturale.

Guvernele şi ansamblul furnizorilor de servicii vitale nu fac cunoscute publicului deficienţele de securitate şi rezilienţă decât dacă sunt obligaţi să o facă. Chiar şi în aceste condiţii, se cunosc numeroase exemple de ameninţări la adresa infrastructurilor critice cauzate de deficienţele de securitate şi de rezilienţă de la nivelul infrastructurilor critice de informaţie:

- în 2007 şi 2008, au avut loc atacuri cibernetice de amploare în Estonia, Lituania şi Georgia;
- în 2008, întreruperea cablurilor submarine intercontinentale din Mediterana şi din Golful Persic a afectat traficul internet în numeroase ţări;

[6] Cf. Comisia Comunităţilor Europene, *Protejarea Europei de atacuri cibernetice şi perturbaţii de amploare: ameliorarea gradului de pregătire, a securităţii şi a rezilienţei*, COM(2009) 149 final, Brussels, 30.03.2009, p.4.

- în aprilie 2009, responsabilii federali cu securitatea din SUA au avertizat cu privire la pătrunderea în reţeaua electrică a SUA a unor „spioni cibernetici", în urma cărora au rămas în reţea programe informatice care ar putea fi folosite pentru a perturba sistemul;
- în luna iulie, SUA şi Coreea de Sud au fost nevoite să facă faţă unor întreruperi manifeste ale serviciilor (implicând preluarea controlului asupra unui număr de 100.000-200.000 de calculatoare, devenite „zombi"), ceea ce a afectat funcţionarea a numeroase site-uri guvernamentale.

În scopul unei mai bunei înţelegeri a mediului de lucru şi a constrângerilor impuse de acesta, trebuie luată în considerare natura distribuită a internetului, care permite utilizarea nodurilor de reţea drept vectori de atac, cum ar fi botneturile. Totuşi, natura distribuită reprezintă o componentă cheie a stabilităţii şi rezilienţei şi poate contribui la o redresare mai rapidă decât în cazul procedurilor supraformalizate, de sus în jos. Acest lucru impune o analiză precaută, de la caz la caz, a politicilor publice şi a procedurilor operaţionale instituite.

Pentru abordarea acestor provocări, comunicatul propune cinci piloni:

- pregătire şi prevenire: garantarea unui ridicat nivel de pregătire la toate nivelurile;
- depistare şi reacţie: furnizarea de mecanisme adecvate de alertă rapidă;
- redresarea după incidente şi atenuarea efectelor acestora: întărirea mecanismelor Uniunii Europene de apărare a infrastructurilor critice de informaţie;
- cooperare internaţională: promovarea pe plan internaţional a priorităţilor Uniunii Europene în domeniu;
- criterii pentru sectorul TIC: sprijinirea implementării directivei privind identificarea şi clasificarea infrastructurilor critice europene[7].

Politica NATO în domeniul apărării spaţiului cibernetic

NATO şi-a iniţiat programul de apărare cibernetică în 2002, după incidentele petrecute în timpul operaţiunilor din Balcani, de la sfârşitul anilor '90. După începerea operaţiunilor militare ale NATO împotriva Serbiei, numeroase grupuri de hackeri pro-sârbe au atacat infrastructura de internet a NATO cu obiectivul declarat de a afecta capabilităţile de ducere a luptei ale NATO. Website-ul de relaţii publice pentru războiul din Kosovo, pe care Alianţa dorea să posteze poziţia sa în conflict prin briefinguri şi buletine de informaţii, a fost practic inoperabil timp de mai multe zile din cauza atacurilor de tip DDoS (DDos – Distributed Denial-of-Service). Ca urmare a acestei experienţe, liderii NATO au

[7] Cf. Comisia Comunităţilor Europene, *Protejarea Europei de atacuri cibernetice şi perturbaţii de amploare: ameliorarea gradului de pregătire, a securităţii şi a rezilienţei*, COM(2009) 149 final, Brussels, 30.03.2009, p.8.

decis, la Summitul de la Praga din 2002, implementarea unui Program tehnic de apărare cibernetică al NATO, precum şi înfiinţarea unei capabilităţi NATO de răspuns la incidentele pe calculator (NCIRC - NATO Computer Incident Response Capability). Din acel moment, NATO se echipase cu o organizaţie capabilă să furnizeze mai multe acţiuni de importanţă critică, de la detecţia şi prevenirea viruşilor de calculator şi intruziunii neautorizate în reţelele NATO şi până la managementul dispozitivelor criptografice pentru internet. În plus, experţii NATO asigură suportul tehnic pentru incidentele de securitate ale calculatoarelor, precum şi politicile din domeniu.

NATO a perceput atacurile din spaţiul cibernetic asupra Estoniei ca fiind o problemă serioasă de securitate operaţională. Până la producerea acestor atacuri, NATO viza, în principal, protecţia propriilor sisteme informatice şi mai puţin asistarea aliaţilor pentru protejarea propriilor lor sisteme. Atacurile au demonstrat necesitatea unei politici de apărare cibernetică a Alianţei, care să abordeze şi nevoia cooperării pentru protecţia sistemelor de comunicaţii critice, dincolo de reţelele criptate ale comandamentelor NATO.

La exact şapte săptămâni după atacurile cibernetice împotriva Estoniei, la 14 iunie 2007, miniştrii aliaţi ai apărării s-au întâlnit, experţii NATO întocmind cu această ocazie un raport de „lecţii învăţate" care a stat la baza planului de lucrări necesare în domeniul apărării cibernetice. La întâlnirea lor, din octombrie 2007, miniştrilor aliaţi ai apărării le-a fost prezentat un raport mai detaliat, care analiza în amănunt apărarea cibernetică în cadrul Alianţei. Raportul a recomandat adoptarea unor acţiuni specifice în cadrul Alianţei, precum şi implementarea unor noi măsuri destinate să îmbunătăţească protecţia împotriva atacurilor din spaţiul cibernetic.

Raportul a cerut, de asemenea, dezvoltarea unei politici de apărare cibernetică în cadrul NATO, politică ce a fost aprobată în ianuarie 2008 şi semnată de către şefii de stat şi de guvern la Summitul de la Bucureşti, din aprilie acelaşi an. Rapiditatea cu care a fost adoptată politica NATO de apărare cibernetică evidenţiază largul consens politic din rândul membrilor Alianţei, seriozitatea ameninţărilor cibernetice, precum şi valoarea potenţială a rolului NATO în acest domeniu. Organismele militare şi tehnice principale ale Alianţei sunt, în prezent, angajate în implementarea acestei politici şi, în egală măsură, fiecare stat membru NATO în parte.

Deşi detaliile exacte ale politicii NATO referitoare la apărarea cibernetică rămân clasificate, înfiinţarea Centrului de excelenţă pentru cooperare în apărarea cibernetică la 14 mai 2008 reprezintă un pas notabil, de concretizare a acestei politici. Destinată a fi principala sursă de expertiză pentru NATO în problemele legate de apărarea cibernetică, această instituţie are următoarele sarcini principale:

- asigurarea doctrinelor şi conceptelor Alianţei în domeniul spaţiului cibernetic;

- găzduirea şi dessfăşurarea atelierelor de lucru, cursurilor şi exerciţiilor din domeniu pentru statele membre NATO;
- desfăşurarea activităţilor de cercetare şi dezvoltare în domeniul spaţiului cibernetic;
- studierea atacurilor cibernetice desfăşurate, precum şi a celor în curs de desfăşurare pentru a stabili lecţiile învăţate;
- asigurarea consultanţei, dacă este solicitată, pe timpul desfăşurării atacurilor cibernetice[8].

Pe lângă înfiinţarea Centrului de excelenţă pentru cooperare în apărarea cibernetică, oficialii NATO au dezvăluit, de asemenea, crearea Autorităţii de management a apărării cibernetice (CDMA – Cyber Defence Management Authority), ca element constitutiv al politicii NATO de apărare cibernetică. Aşa cum îi arată şi numele, CDMA este o autoritate NATO însărcinată cu iniţierea şi coordonarea unor acţiuni de apărare cibernetică imediate şi eficiente atunci când este necesar. Autoritatea serveşte drept comandament central pentru eforturile statelor membre ale Alianţei pentru eforturile politice, tehnice şi de informare şi are menirea de a conduce şi de a gestiona entităţile de apărare cibernetică existente ale NATO. La cerere, CDMA este pregătită şi capabilă să asigure coordonare şi asistenţă în cadrul unui efort concentrat dacă unul sau mai multe state membre suportă un atac semnificativ în spaţiul cibernetic.

La Summitul NATO din aprilie 2009, statele membre au pledat pentru accelerarea achiziţionării de noi mijloace de apărare cibernetică, integrarea apărării spaţiului cibernetic în desfăşurarea exerciţiilor NATO şi întărirea legăturilor dintre statele membre şi partenere NATO în domeniul protecţiei împotriva atacurilor cibernetice.

Mai recent, oficialii NATO au confirmat înfiinţarea unor echipe de reacţie rapidă care sunt disponibile statelor membre pentru contracararea atacurilor cibernetice. Programate a fi complet operaţionale, în anul 2012, aceste echipe de reacţie rapidă vor fi formate din experţi şi personal de stat major din statele membre NATO. Dacă vor fi solicitate să intre în acţiune, echipele de reacţie rapidă vor lucra sub directa îndrumare a statului atacat.

Măsuri tehnice de asigurare a protecţiei infrastructurii critice de informaţie

În urma analizării a mai multor rapoarte asupra securităţii spaţiului cibernetic şi a lecţiilor învăţate rezultate în urma atacurilor cibernetice, apreciem ca

[8] Sverre Myrli (Norway) – Rapporteur, *NATO and Cyber Defence*, NATO Parliamentary Assembly, 027 DSCFC 2009 E, p.5

fiind de maximă importanţă adoptarea următoarelor măsuri tehnice pentru asigurarea protecţiei infrastructurii critice de informaţie:

- **Tehnologiile de autentificare** – schemele de autentificare pentru elemente constitutive ale reţelelor, cum ar echipamentele hardware, aplicaţiile software, datele şi utilizatorii sunt necesare pentru o largă varietate de scopuri, ce includ identificarea, autentificarea şi verificarea integrităţii datelor. Aceste scheme trebuie să îşi dovedească siguranţa, să fie uşor de verificat, să poată fi utilizate de o multitudine de componente şi să fie executabile rapid. Metodele de criptografiere tradiţională s-au concentrat pe asigurarea securităţii, dar acestea nu pot fi suficient de eficiente în cazul utilizării extinse, în medii în care, de exemplu, un singur ruter de reţea trebuie să autentifice milioane de pachete de date pe secundă. Rezultate mult mai bune au fost obţinute cu protocoalele criptografice. Dar cerinţa ca protocoalele să poată fi utilizate într-un mediu cum este internetul impune dezvoltarea unor noi tipuri de protocoale. În cadrul acestei măsuri sunt luate în considerare mai multe tendinţe de dezvoltare, după cum urmează:
  - cercetarea infrastructurii şi protocoalelor pentru distribuţia şi managementul de chei pe scară largă, pentru public;
  - managementul certificării şi revocării certificatelor;
  - integrarea token-urilor fizice şi a dispozitivelor biometrice;
  - separarea procesului de autentificare de cel de identificare pentru a rezolva problemele de confidenţialitate.
- **Securizarea protocoalelor de bază** – puţine dintre protocoalele ce guvernează funcţionarea internetului au un grad de securitate adecvat. De exemplu, pentru a devia traficul de date pe un site alternativ, un atacator poate păcăli cu uşurinţă protocoale cum este şi Border Gateway Protocol (BGP) (care controlează traseele urmate de pachetele de date în circulaţia acestora pe internet) sau servicii de tipul Domain Name System (DNS) (care controlează destinaţia pachetelor de date). Astfel de atacatori pot intercepta, monitoriza, altera sau manipula traficul pe internet, adeseori fără a putea fi detectaţi. Pentru ca internetul să devină un mediu de comunicaţie de încredere, trebuie dezvoltate versiunile securizate ale protocoalelor de bază care să contracareze ameninţări cum ar fi: interzicerea de servicii, alterarea datelor şi inducerea în eroare. Mai mult, apreciem că trebuie securizate protocoalele de bază împotriva atacurilor de incapacitare, care exploatează slăbiciunile protocoalelor. Pentru această măsură considerăm că trebuie luate în considerare următoarele tendinţe de dezvoltare:
  - securizarea protocolului voce prin internet (VoIP), a comunicaţiilor wireless, a Web-ului şi a reţelelor private virtuale (VPN – Virtual Private Network), fiecare dintre aceste protocoale fiind mai complexe decât

protocoalele de bază ale internetului, iar niciunul dintre acestea nu este securizat în mod adecvat;
- securizarea protocoalelor chiar şi atunci când acestea sunt executate şi partajate cu utilizatori nesecurizaţi;
- adoptarea unor compromisuri între securitate şi performanţă

- **Securizarea ingineriei software şi a asigurării software** – ingineria aplicaţiilor software comerciale suferă de lipsa unor controale stiinţifice riguroase, necesare pentru producerea unor aplicaţii de calitate, securizate, la un cost acceptabil. Practicile de inginerie software obişnuite permit apariţia unor erori periculoase, care permit multor programe de atac să compromită, în fiecare an, funcţionarea a milioane de calculatoare. De la evitarea erorilor în programarea de bază şi până la dezvoltarea unor sisteme masive care să rămână securizate, chiar dacă părţi din software-ul de sistem sunt compromise, trebuie să beneficieze de cercetare în următoarele direcţii:
  - includerea caracteristicilor de securitate de bază în sistemele şi limbajele de programare;
  - codurile portabile sau reutilizabile care să rămână securizate atunci când sunt dislocate în medii diferite;
  - rezolvarea problemelor de securitate prin tehnologii care să verifice eficient şi economic dacă codurile de calculator nu conţin caracteristici nedocumentate sau nedorite care să poată fi exploatate de atacatori.

- **Securitatea holistică a sistemului** – securitatea eficientă într-o infrastructură globală, stratificată şi complexă, cum este internetul şi nodurile sale, impune mai mult decât securizarea componentelor sale. Realizarea unor metode clare de autentificare, protocoale de securitate pentru operaţiunile Web de bază, precum şi îmbunătăţirea ingineriei software fac parte din ecuaţia care trebuie să rezolve problema securităţii pe internet. Cu toate acestea, cel mai important aspect pe care cercetătorii trebuie să îl ia în consideraţie îl reprezintă abordarea arhitecturală *end-to-end* a securităţii întregului, care transcede securitatea fiecărui element în parte. Cercetarea fundamentală trebuie să dezvolte arhitecturi de securitate holistică cu totul noi, care să includă echipamentele hardware, sistemele de operare, reţelele şi aplicaţiile software. Acest deziderat se poate realiza prin:
  - reducerea proactivă a vulnerabilităţilor;
  - securizarea sistemelor la care pot avea acces adversarii;
  - contracararea problemei ameninţărilor interne;
  - modelarea şi analizarea defecţiunilor care apar în sistemele complexe;
  - ingineria factorilor umani, cum ar fi interfeţele care promovează securitatea şi care conştientizează utilizatorul asupra importanţei ei;
  - sprijinirea confidenţialităţii în conjuncţie cu îmbunătăţirea securităţii.

- **Monitorizarea şi detectarea** – indiferent de progresul realizat în cercetare, tot pot apărea evenimente neanticipate. Atunci când se întâmplă aşa ceva, sunt necesare instrumente care să permită monitorizarea şi înţelegerea evenimentului, precum şi adoptarea măsurilor defensive corespunzătoare. Capacitatea instrumentelor curente care monitorizează activităţile anormale din reţea de a identifica rapid cauzele este primitivă. Avantajul pe care îl au în prezent atacatorii va creşte pe măsură ce aceştia se perfecţionează, iar internetul devine tot mai vast şi mai complex. Această măsură tehnică poate fi îmbunătăţită prin:
  - introducerea unei protecţii dinamice care să poată reacţiona atunci când sunt detectate atacurile;
  - monitorizarea şi detecţia intruziunii pe scară globală;
  - monitorizarea sistemelor pentru a avea certitudinea că respectă politicile de securitate declarate;
  - realizarea unor instrumente mai bune bazate pe modele îmbunătăţite de caracterizare a comportamentului normal în reţea;
  - analizarea, colectarea şi stocarea datelor în timp real pe timpul crizelor;
  - interfeţele de prezentare eficiente care să permită operatorilor să înţeleagă mai bine incidentele care sunt în curs de desfăşurare.

– **Metodologiile de atenuare a efectelor atacurilor şi de recuperare** – sistemele securizate trebuie să fie astfel proiectate încât să răspundă rapid la atacuri şi evenimente neprevăzute şi să aibă capacitatea de recuperare în urma oricărei avarii rezultate, o sarcină cu atât mai provocatoare atunci când este cazul unui sistem de amploarea şi complexitatea internetului şi nodurilor sale. Această problemă a fost abordată în sisteme de extraordinară complexitate, cum este cazul navetelor spaţiale, prin realizarea unor investiţii substanţiale pentru obţinerea unor fiabilităţi şi redundanţe maxime. Niciun efort comparabil nu a fost investit în dezvoltarea metodelor de fiabilizare a internetului şi a sistemelor de calculatoare în faţa atacurilor. Elemente de aplicare a acestei măsuri includ:
  - descoperirea automată şi rapidă a defecţiunilor şi atacurilor prin monitorizarea datelor;
  - realizarea unor noi arhitecturi de sisteme care să permită recuperarea rapidă în urma defecţiunilor şi atacurilor;
  - simplificarea sistemelor pentru creşterea rolului operaţiunilor automate, pentru reducerea erorilor şi atacurilor interne cauzate de operatorii umani, în special la actualizarea configuraţiilor şi aplicaţiilor software;
  - toleranţă sporită la erori şi atenuarea automată a efectelor unui atac.

– **Prinderea atacatorilor şi descurajarea activităţilor informatice ilegale** – arestarea şi condamnarea rapidă a atacatorilor constituie principalul obiectiv al aplicării legii şi serveşte, în egală măsură, şi ca o metodă de descurajare

a activităţilor informatice ilegale. Capabilităţile curente de investigare a infracţiunilor informatice, identificarea făptaşilor, adunarea şi prezentarea probelor şi condamnarea atacatorilor sunt necorespunzătoare. Pentru rezolvarea acestei probleme sunt necesare:

- identificarea originii atacurilor cibernetice, inclusiv urmărirea traficului de reţea desfăşurat;
- identificarea atacurilor pe baza comportamentului acestora;
- colectarea dovezilor din medii de reţea ostile;
- depistarea informaţiilor furate, fraudelor, furtului de identitate, furtului de proprietate intelectuală, inclusiv realizarea de protocoale şi instrumente pentru recuperarea dovezilor de urme de pe suporţi media informatici volatili sau incomplet şterşi, discuri, telefoane mobile, PDA şi sisteme încorporate.

– **Modelarea şi bancurile de probe pentru noile tehnologii** – una dintre barierele în calea dezvoltării rapide a noilor produse de securitate cibernetică o reprezintă insuficienţa modelelor realiste şi a bancurilor de probă pentru testarea celor mai avansate tehnologii într-un mediu similar celui din realitate. Până acum au fost realizate unele cercetări de modelare a internetului, dar au fost oarecum rudimentare şi cu un impact mic în practică. Problema este de mare dificultate din cauza complexităţii şi mărimii internetului. Apreciem ca fiind utile următoarele direcţii de dezvoltare:

- realizarea unor medii de simulare a sistemelor;
- validarea simulărilor cu reprezentarea a milioane de noduri;
- culegerea şi sintetizarea unui mare volum de date;
- proiectarea unui banc de probe care să menţină confidenţialitatea datelor.

– **Problemele nontehnologice** ce pot compromite securitatea cibernetică – un mare număr de factori nontehnologici – psihologici, societali, instituţionali, legali şi economici – pot compromite securitatea cibernetică într-un mod ce nu poate fi rezolvat doar de reţea sau ingineria software. Instalarea tehnologiilor ce nu ţine cont de aceşti factori poate agrava problemele ce se intenţionează a fi rezolvate. Cercetarea asupra aspectelor umane şi organizaţionale ale infrastructurii critice de informaţie poate explora soluţii ce vizează comportamentul uman. Pentru această situaţie, apreciem că vor trebui adoptate următoarele:

- strategii pentru schimbarea percepţiei că o securitate de reţea mai bună nu merită efortul financiar la nivel de individ sau companie;
- modalităţi de îmbunătăţire a percepţiei valorii protecţiei confidenţialităţii şi încrederii în infrastructura TIC, cu implicaţii în analiza de risc şi managementul riscului;

- studiul interacţionării dintre oameni şi infrastructura TIC, cu accent pe etică, cultură, comportament şi alţi factori ce pot conduce la breşe de securitate nontehnologice;
- studii ale fenomenelor sociologice şi comportamentale ce pot determina oamenii să comită infracţiuni cibernetice;
- analize ale standardelor şi legilor internaţionale şi impactul acestora asupra politicilor şi tehnologiilor de securitate cibernetică;
- identificarea problemelor de securitate naţionale şi de afaceri în cazul transferului de tehnologii de securitate cibernetică din import.

Concluzii

Protecţia infrastructurii critice de informaţie a ajuns pe agenda internaţională de securitate. Întrucât majoritatea infrastructurilor critice sunt bazate sau monitorizate şi controlate pe sisteme TOC vulnerabile, infrastructura de informaţie a devenit punctul focal al politicilor de protecţie a infrastructurilor critice.

Atacurile îndreptate împotriva infrastructurii critice de informaţie pot include:

- accesul neautorizat la informaţii confidenţiale sau sensibile;
- distrugerea, modificarea sau sustragerea de aplicaţii software necesare nubei funcţionări a infrastructurilor critice;
- limitarea accesului agenţilor responsabili cu prevenirea atacurilor şi cu micşorarea efectelor acestora.

Consecinţele posibile ale acestor atacuri pentru infrastructurile critice sunt:

- blocarea mijloacelor de transport, alimentării cu apă, electricitate şi gaze, comunicaţiilor, transmisiilor de date, controlului traficului aerian, centralelor nucleare electrice;
- falimentarea structurilor comerciale şi a sistemelor financiare, alterarea tranzacţiilor financiare internaţionale, destabilizarea pieţelor şi instituţiilor financiare:
- pierderea proprietăţii intelectuale sau reputaţiei;
- victimele umane sau pierderi materiale cauzate de folosirea distructivă a unor elemente ale infrastructurilor critice (sabotaj cibernetic în industria alimentară, transportul aerian sau pe căile ferate);
- accesul neautorizat şi/sau modificarea datelor personale;

- posibilitatea imputării actelor teroriste unor state sau guverne şi agravarea tensiunilor în relaţiile internaţionale[9].

În timp ce refacerea infrastructurii critice de informaţie este adeseori o sarcină rapidă şi uşoară, efectele indirecte pot fi resimţite timp îndelungat. Atacurile asupra infrastructurii critice de informaţie pot submina serios încrederea mediului de afaceri şi a publicului în comerţul electronic sau în iniţiativele guvernamentale. Costurile umane şi economice asociate cu recuperarea sau cu strategiile de diminuare a efectelor atacului cibernetic sunt enorme.

Protecţia infrastructurii critice de informaţie are trei obiective strategice:

- prevenirea atacurilor cibernetice împotriva infrastructurilor critice;
- reducerea vulnerabilităţilor naţionale la atacurile cibernetice;
- micşorarea efectelor şi a timpului de recuperare după producerea atacurilor cibernetice.

În scopul îndeplinirii acestor obiective este necesară o nouă strategie, care să includă, pe lângă elementele de natură tehnologică, măsuri preventive la toate nivelele, îmbunătăţirea capabilităţilor de detectare timpurie şi de reacţie rapidă, limitarea impactului atacurilor la nivelul guvernului şi societăţii, precum şi modalităţi de menţinere în funcţiune a sistemelor afectate sau recuperare a acestora în cel mai scurt timp posibil. Ameninţările şi vulnerabilităţile constau în componente, informaţionale, fizice şi psihologice, care impun un dialog deschis neierarhizat pentru definirea măsurilor de protecţie corespunzătoare.

Cadrul pentru protecţia infrastructurii critice de informaţie la nivel naţional trebuie abordat într-un context mai larg, al mediilor de afaceri, social şi tehnic. Protecţia infrastructurii critice de informaţie necesită un răspuns multidisciplinar, ce trebuie să încorporeze soluţii tehnice, de management şi educaţionale, presupunând totodată o abordare interdepartamentală, la nivelul industriei, administraţiei publice şi guvernului.

[9] Cf. Eugene NICKOLOV, *Critical Information Infrastructure Protection: Analysis, Evaluation and Expectations*, INFORMATION & SECURITY. An International Journal, Vol.17, 2005, p.108.

INFRASTRUCTURI CRITICE ÎN CEL DE-AL DOILEA RĂZBOI MONDIAL ŞI INFLUENȚA LOR ASUPRA ACȚIUNILOR MILITARE

General de brigadă (r) prof. univ. dr. Nicolae CIOBANU

Comunicarea prezintă sintetic modul cum infrastructurile critice au influențat pregătirea şi desfăşurarea acțiunilor militare, cu precădere a operațiilor de amploare operativ-strategică. Sunt analizate o serie de structuri ca sistemul de comunicație rutier şi feroviar, sistemele hidroenergetice, rețeaua de transmisiuni, comunicațiile pe apă etc. Am pus accent pe rolul ce revine factorilor de decizie privind protejarea structurilor critice împotriva acțiunilor de diversiune şi teroriste.

În încheiere am subliniat rolul deosebit pentru buna desfăşurare a acțiunilor militare deținut de infrastructurile critice.

Cel de-al Doilea Război Mondial s-a desfăşurat pe spații imense de circa 22.000.000 km^2, areal, acțiunile militare s-au derulat pe trei continente, Europa, Asia şi Africa. Aceste teritorii aveau o variată rețea de infrastructuri, aşa cum era rețeaua de comunicații (şosele, autostrăzi, canale navigabile sau nu, rețea de căi ferate, transporturi cu feriboturi, cărări în interiorul junglei, cursuri de apă navigabile etc.).

O altă categorie de infrastructuri ce şi-a pus amprenta asupra acțiunilor de luptă a constat din existența unui mare număr de aerodromuri permanente, existente din timp de pace sub forma aeroporturilor naționale şi internaționale, porturi de mare capacitate folosite deseori şi ca baze maritime militare, căi de navigație de lungimi considerabile, uneori asigurând legăturile de la țărmurile unui

continent la alt continent, puncte obligate de trecere, strâmtori, trecători în zonele montane, viaducte şi poduri, tunele, noduri feroviare, aerodromuri de campanie.

De mare însemnătate pentru buna desfăşurare a acţiunilor militare sunt sistemele de legături telefonice, telegrafice, televiziune sau mai recent, legăturile radio, telefonia mobilă, internetul.

De mare însemnătate sunt liniile pentru transportul energiei electrice, sistemul de transport prin conducte a gazelor, ţiţeiului, produselor petroliere şi nu în ultimul rând, conductele pentru transportarea apei potabile sau celei industriale.

Analizând, fie şi pe scurt, rolul unor infrastructuri critice, vom constata importanţa fiecărui sistem, mai mult sau mai puţin critic, în pregătirea şi în ducerea acţiunilor de luptă. Astfel, reţeaua de căi ferate existentă pe teritoriul Germaniei naziste, Italiei fasciste şi Japoniei militariste era bine dezvoltată cu un număr important de mijloace de tracţiune (locomotive de varii puteri), dar şi o cantitate de vagoane de marfă şi personal suficiente să asigure o rapidă deplasare a forţelor şi mijloacelor de pe un front pe altul sau chiar de pe un teatru de operaţii pe un alt teatru de acţiuni militare.

Existenţa reţelei de cale ferată a permis Germaniei o rapidă transportare a forţelor şi mijloacelor, în iarna anului 1940, de pe teritoriul ocupat al Poloniei spre centrul Europei, ca apoi, la scurt timp, să declanşeze agresiunea împotriva Norvegiei şi a Danemarcei, folosind, mai ales, căile ferate, după care, restructurându-şi rapid dispozitivul strategic, prin ample manevre, ce au impus numeroase transferuri din zonele de concentrare spre viitoarele fronturi să constituie cele trei grupuri de armate cu care, la 10 iunie 1940, să declanşeze ampla operaţie de invazie a Belgiei, Olandei şi Franţei, concomitent cu ducerea unei ample ofensive aeriene asupra teritoriului Marii Britanii.

La puţin timp după ocuparea Belgiei, Olandei, Luxemburgului, dar şi celei mai mari părţi din teritoriul Franţei, forţele de ocupaţie să simtă efectul acţiunilor mişcării de rezistenţă prin aruncarea în aer a unor porţiuni de cale ferată, producând deraierea unor garnituri feroviare, deteriorarea acelor de cale ferată – macazurile – care, de asemenea, produceau, prin devierea circulaţiei ciocnirea unor garnituri feroviare. O atenţie deosebită s-a acordat punctelor de trecere obligatorie: noduri feroviare, poduri, tunele, viaducte.

Dacă ne-am referi la sistemul de comunicaţii feroviar existent pe teritoriul Uniunii Sovietice, constatăm unele particularităţi ale acestuia faţă de cele din Europa. Astfel, ecartamentul căii ferate ruseşti era diferit faţă de cel al statelor vecine, fiind mult mai mare. Aceasta presupunea executarea transbordării bunurilor

la frontiera sovietică sau măsuri care să permită trecerea directă din reţeaua europeană în cea rusească (respectiv sovietică).

Lungimea reţelei feroviare sovietice era enormă, dar raportată la suprafaţa teritoriului Uniunii Sovietice, era inferioară faţă de cea din Europa, vorbind de numărul de kilometri de cale ferată pe kilometrul pătrat.

Podurile, tunelele, viaductele sunt elemente de infrastructură deosebit de sensibile, şi mai ales, uşor de scos din funcţiune. Distrugerea unui pod de însemnătate strategică, precum cel aflat peste un curs de apă mare, de regulă, fluviu, poate duce la implicaţii deosebite asupra trecerii cursului respectiv. Distrugerea unor poduri, cum au fost cele de peste fluviile Nipru, Rin, Main, Dunăre etc. au avut urmări deosebite asupra ritmului ofensivei, forţarea unor asemenea cursuri de apă necesitând pregătiri şi o asigurare materială deosebită. Podurile, viaductele, tunelurile bine apărare împotriva loviturilor din aer de către aviaţie sunt în general greu de distrus. Aşa, spre exemplu, pentru distrugerea unui pod de peste Rin, forţele aliate au consumat o cantitate de aproximativ 2.500 tone de bombe în aproape 160-170 de ieşiri avion, aviaţia fiind nevoită să acţioneze de la mare înălţime. Când, însă, obiectivul este mascat prin ceaţă artificială sau fumizare, lovirea obiectivului este posibilă doar din întâmplare. În condiţiile actuale, având în vedere perfecţionarea armamentului de înaltă precizie, aceste elemente de infrastructură critică devin şi mai sensibile, mai uşor de lovit.

O mare atenţie trebuie acordată prevenirii acţiunii elementelor de cercetare-diversiune sau grupurilor teroriste. Un grup de 2-3 luptători special instruiţi în acte de diversiune poate scoate din funcţiune, de regulă, destul de uşor asemenea obiective.

Cucerirea unor poduri, tunele sau viaducte intacte influenţează pozitiv mersul acţiunilor de luptă. Aşa, spre exemplu, cucerirea podului "Ludendorf" de peste Rin, situat în apropierea oraşului Remagen, surprins intact de către trupele de cercetare-diversiune americane, au permis Armatei 9 americane să realizeze în scurt timp, un cap de pod cu o dezvoltare frontală de 48 km şi o adâncime de 16 km.

Împotriva reţelei feroviare, într-o serie de teritorii cum au fost cel al Uniunii Sovietice, Olandei, Iugoslaviei, Chinei, Birmaniei, Filipinelor, dar şi altele, s-a desfăşurat un adevărat *război al şinelor de cale ferată.*

Blocarea unor garnituri de tren cu muniţie, medicamente, echipament, furaje, combustibili, mai ales, benzină, au pus într-o situaţie dificilă Grupul de armate german, "Centru" care din cauza unor lipsuri materiale a fost nevoit să adopte un ritm de ofensivă scăzut, ceea ce a făcut să întârzie ofensiva pentru

cucerirea Moscovei, ajungând în faţa acesteia atunci când termometrele indicau -35^{0}C, iar militarii germani suferiseră încă din cea de-a doua decadă a lunii noiembrie degerături grave.

În timp ce trupele germane îngheţau efectiv în faţa Moscovei, la distanţe de zeci şi zeci de kilometri, zăceau imobilizate garniturile feroviare încărcate cu vagoane cu ţinuta de paradă a trupelor ce urmau a defila în faţa Kremlinului, cu alte zeci de vagoane pline cu sticle din cea mai bună şampanie franţuzească pentru sărbătorirea victoriei cuceririi Moscovei.

Asupra reţelei feroviare dinapoia frontului sovieto-german acţionau mii de grupuri şi detaşamente de partizani care, în perioada iulie 1941 – aprilie 1944, au aruncat în aer sute de trenuri ale armatei germane şi acoliţilor acesteia. Sunt bine cunoscute procedeele de deraiere a trenurilor prin slăbirea joncţiunii între două şine de cale ferată, înlocuirea unor şine metalice cu "şină" din lemn, pentru a nu mai aminti de folosirea diferitelor materiale explozive.

Modul de dispunere (traversarea unor cursuri de apă mari, a unor păduri sau locuri greu accesibile) face din reţeaua de căi ferate o suprastructură critică, uşor de scos din funcţiune, prin acţiuni ale partizanilor sau grupurilor de cercetare-diversiune.

În cursul celui de-al Doilea Război Mondial tracţiunea garniturilor feroviare se asigura de către locomotive cu abur, tracţiunea electrică fiind la începuturile afirmării sale. Existenţa locomotivelor cu abur prezenta o superioritate netă faţă de tracţiunea cu locomotive electrice, legate, exclusiv, de reţeaua electrică. Folosirea treptată a locomotivelor cu tracţiune Diesel şi, mai apoi electrice, au scos, după încheierea războiului, din 1947, tracţiunea cu abur. Locomotivele cu abur au fost, însă, conservate în marea majoritate a statelor atât pentru existenţa combustibilului în cantităţi suficiente, cât şi pentru asigurarea independenţei deplasării, nefiind legate de reţeaua electrică.

Existenţa, mai ales, în ţările puternic industrializate, a numeroase linii pentru transportul energiei electrice, face din acest sistem de infrastructură un element foarte sensibil, uşor de scos din funcţiune, dat fiind faptul că reţelele electrice pentru transportul energiei electrice măsoară sute de mii de kilometri, ceea ce face practic imposibilă paza şi siguranţa acestora. Deosebit de sensibile sunt transformatoarele electrice de mare capacitate. Prin distrugerea unui asemenea obiectiv este practic paralizat transportul energiei electrice pe spaţii întinse. La fel de sensibile sunt parcurile ce asigură conectarea diferitelor linii de înaltă tensiune.

Legat de sursele de energie electrică, barajele sistemelor hidroenergetice sunt, de asemenea, elemente de infrastructură deosebit de critice, mai ales faţă de

acţiunile grupurilor de diversiune, sabotori sau partizani. Lovirea unor asemenea obiective cu aviaţie necesită un mare consum de bombe şi, de regulă, cere timp îndelungat, iar mascarea acestora prin diferite forme şi procedee face şi mai dificilă distrugerea lor. Mai indicată în acest scop este folosirea armamentului de mare precizie.

Distrugerea unui baraj hidroenergetic se repercutează negativ asupra acţiunilor militare sub două aspecte. pe de o parte, paralizarea sistemului energetic prin încetarea furnizării de energie electrică de către hidrocentrala respectivă, pe de altă parte prin inundaţiile catastrofale ce se vor produce în aval de baraj, inundaţii care pot "spăla" tot ce le iese în cale pe distanţe impresionante. Aşa s-au petrecut lucrurile în cursul celui de-al Doilea Război Mondial, când trupele germane au distrus un baraj în regiunea Rinului creând pe sute de kilometri pătraţi îmlăştinarea terenului (căi de comunicaţie de tot felul, semănături, localităţi).

Telecomunicaţiile sunt, de asemenea, deosebit de uşor de scos din funcţiune, mai ales comunicaţiile prin fir şi radio. Distrugerea unor centrale telefonice pot paraliza zeci şi zeci de localităţi, nemaivorbind de distrugerea unor posturi de emisie radio. În acelaşi scop, de a le face inutile, se pot folosi şi mijloace mai sofisticate, cum ar fi bruierea emisiunilor etc.

În ceea ce priveşte transportul prin conducte este deosebit de vulnerabil la acţiunile distructive. Dacă ne-am referi doar la apeductele ce asigură aprovizionarea cu apă a unor centre urbane, distrugerea unei asemenea conducte poate avea urmări deosebite asupra locuitorilor prin lipsa de apă. În acest sens sunt grăitoare căderea garnizoanei italiano-germane de la Tobruk sau a garnizoanei britanice de la Singapore în timpul celui de-al Doilea Război Mondial. Lipsa apei a determinat încetarea ostilităţilor şi predarea garnizoanelor respective. Britanicii au pierdut 10.000 de militari morţi şi circa 70.000 de militari prizonieri.

De asemenea, sursele de apă transportată prin apeducte, cât şi staţiile lor de pompare, este necesar să fie temeinic păzite, iar calitatea apei verificată, cât mai des, pentru a se preveni introducerea unor microbi, bacterii sau substanţe toxice otrăvitoare cu urmări greu de prevăzut asupra locuitorilor, cât şi a unităţilor militare.

În cazul conductelor ce transportă gaze sau produse petroliere este necesară o bună supraveghere a staţiilor de pompare, atât la instalaţiile speciale existente la locul de pornire a conductelor, cât şi la staţiile finale.

În localităţile mari, în care există sisteme de transport prin trenuri subterane, inclusiv cele de tip metrou, o mare atenţie se impune a fi dată gurilor de

acces în subteran, iar în cursul acţiunilor militare, liniile de metrou pot fi folosite pentru executarea unor manevre în timp foarte scurt şi perfect mascate.

În situaţiile critice, metroul poate fi inundat şi făcut impracticabil pentru forţele agresoare. Aşa, spre exemplu, în aprilie 1945, din ordinul lui Hitler, metroul din Berlin a fost inundat între staţiile Leipzigerplatz şi Unter der Linden, murind mii şi mii de bătrâni, femei şi copii.

Am prezentat câteva aspecte ale situaţiei unor structuri critice în cursul celui de-al Doilea Război Mondial. Cunoaşterea acestor aspecte permit, în condiţiile ducerii unui conflict armat, fie el numai local, folosirea experienţei din această Mare Conflagraţie a secolului XX.

Desigur, în condiţiile actuale ale dezvoltării nivelului tehnicii de observare şi lovire, a creşterii gradului de precizie a loviturilor se impun măsuri noi de contracarare a efectelor acţiunilor adverse şi menţinerii acestor suprastructuri în funcţiune, fie chiar şi parţial.

PROTECȚIA INFRASTRUCTURII INFORMAȚIONALE CRITICE

Colonel (r) prof. univ. dr. Gruia TIMOFTE

Natura riscurilor şi vulnerabilităţilor în societăţile moderne devine astăzi din ce în ce mai transnaţională. Un dialog deschis şi non-ierarhic despre nou recunoscutele vulnerabilităţi la nivele fizice, virtuale şi psihologice este necesar pentru a crea noi cunoştinţe şi o înţelegere mai bună a noilor riscuri şi a cauzelor lor, a interacţiunilor, probabilităţilor şi a costurilor. Fie că este o concurenţă sau o colaborare cu ceilalţi, conexiunea dintre oameni este o realitate în întreaga lume. Cyberspaţiul a contribuit la această realitate prin revoluţia internetului şi a telecomunicaţiilor. Sectoarele critice ale societăţii moderne, şi anume: energia, transporturile, aplicarea legii, TIC (Tehnologia Informaţiei şi Comunicaţiilor), sectorul financiar, sănătatea publică etc, pentru a-şi îmbunătăţi eficienţa şi eficacitatea, devin din ce în ce mai dependente de structurile TIC.

O infrastructură critică (IC) este aceea în care incapacitatea de funcţionare sau distrugerea acesteia au un impact serios asupra securităţii naţionale sau economiei şi bunăstării unei naţiuni. Concepţiile privind protecţia infrastructurilor şi obiectivelor de importanţă strategică au făcut parte din planurile naţionale de apărare timp de zeci de ani, cu diferite niveluri de importanţă.

Infrastructura informaţională critică (IIC) cuprinde multe elemente din IC, aşa cum tehnologia informaţiei şi comunicaţiilor a fost integrată în celelalte elemente, conectând alte sisteme din infrastructură şi făcându-le interrelaţionate şi interdependente. IC oferă o gamă de servicii de care depind atât indivizii, cât şi societatea în ansamblu. Orice distrugere sau întrerupere în funcţionare determină o serie de repercusiuni în sistemele tehnice şi sociale, care se produceau şi în trecut,

dar care se manifestă mai pregnant în zilele noastre datorită interdependenţelor dintre elementele componente ale IC. Atacarea acestor infrastructuri are rol de forţă multiplicatoare a efectelor, care permite realizarea unui impact major şi în cazul atacurilor de anvergură redusă. Din acest considerent, structurile şi reţelele din IIC s-au dovedit atractive pentru o gamă largă de actori.[1]

În zilele noastre, devine din ce în ce mai importantă îmbunătăţirea securităţii reţelelor de comunicaţii şi sistemelor informatice, unele fiind mai importante decât altele şi, de aceea, sunt denumite IIC. Această ierarhizare este determinată de valoarea lor inestimabilă şi de creşterea rolului acestora în sectorul economic, poziţia de liant între diferitele sectoare ale infrastructurii şi au rol esenţial în funcţionarea multor servicii critice esenţiale pentru buna funcţionare a societăţilor dezvoltate. În timp ce protecţia infrastructurii critice (PIC) cuprinde toate sectoarele critice ale infrastructurii unei naţiuni, protecţia infrastructurii informaţionale critice (PIIC) reprezintă un segment al efortului de protecţie comprehensiv, concentrându-se asupra acesteia din urmă. PIIC este analizat din perspectiva mai multor puncte de vedere şi al diferitelor caracteristici. Ca urmare, diferenţele dintre sectoarele guvernamentale şi cele private, complică partajarea rolurilor şi responsabilităţilor acestora. Mai mult decât atât, limitele dintre diferite perspective de analiză se suprapun. Printre cele mai importante puncte de vedere pot fi enumerate următoarele tipuri ideale simplificate: nivelul sistemic sau tehnic; cel al afacerilor; cel privind impunerea legii; cel al securităţii naţionale. Faptul că 85% din IC este în proprietate privată sau a unor actori în unele ţări, nu face decât să agraveze şi mai mult această problemă. Reducerea riscurilor la adresa IC solicită eforturi pentru a contracara sau întrerupe sursele de ameninţare prin educaţie, acţiuni civile, combaterea criminalităţii sau acţiune de cercetare. În plus, este esenţial să se identifice vulnerabilităţile prin studiul acestora şi reducerea impactului unui atac prin realizarea avertizărilor, îmbunătăţirea capacităţii de refacere şi recuperare în urma dezastrelor. În final, analiza tendinţelor rezultate din raportarea incidentelor, schimbul de informaţii şi dialogul cu proprietarii de infrastructuri reprezintă, de asemenea, elemente importante pentru politica integratoare a PIIC. De aceea, guvernele trebuie să acorde o atenţie specială următoarelor probleme: înţelegerea naturii riscurilor şi a ameninţărilor, precum şi a vulnerabilităţilor rezultate; îmbunătăţirea procesului de detectare şi răspuns la vulnerabilităţi; promovarea unor produse şi servicii mult mai sigure şi sprijinul activităţii de cercetare şi dezvoltare; creşterea nivelului de cunoaştere a situaţiei şi distribuţie a informaţiilor aferente; dezvoltarea unui cadru legal adecvat; pregătirea pentru situaţiile de urgenţă şi de management al crizelor.[2]

Geneza şi definirea conceptelor privind PIC reprezintă rezultatul inter-relaţionării şi potenţării reciproce a doi factori în expansiune: extinderea spectrului

ameninţărilor, în special a software-ului rău intenţionat (*malicious*) şi a capacităţilor asociate acestuia; apariţia unui nou tip de vulnerabilităţi datorită dependenţei societăţii moderne de sisteme informaţionale nesigure. Ca urmare a acestor riscuri difuze şi a dificultăţilor în localizare şi identificare, o parte din obiectivele politicilor de securitate s-au îndepărtat de actori, capabilităţi şi motivaţii spre vulnerabilităţile generale ale întregii societăţi. Aceste elemente au fost definite ca infrastructuri critice deoarece funcţionarea defectuoasă sau distrugerea lor au un impact important asupra securităţii naţionale, bunăstării economice şi sociale. Teama faţă de acţiunile asimetrice împotriva unor asemenea „ţinte soft" este agravată de cel de-al doilea factor: aşa-numita revoluţie informaţională. Cele mai multe IC se bazează pe o gamă de sisteme de control bazate pe software pentru operaţiuni continue, fiabile şi fără neregularităţi. În multe cazuri, tehnologia informaţiei şi comunicaţiilor (TIC) a devenit atotcuprinzătoare, conectând alte sisteme ale infrastructurii şi făcându-le interrelaţionate şi interdependente. În acelaşi timp, răspândirea TIC creează condiţii pentru realizarea mai facilă a atacurilor asimetrice, pe care le produceau altă dată sistemele de armament specializate sau forţele militare. Graniţele, deja penetrabile în multe modalităţi în lumea reală, sunt inexistente în spaţiul cibernetic.[3]

Există o gamă largă de opţiuni de atac, de la cele ale hacker-ilor la distrugerea fizică a instalaţiilor civile sau militare. Principalul obiectiv al eforturilor iniţiale privind PIC l-au constituit diversele riscuri provenite din spaţiul cibernetic: infrastructura informaţională globală părea să faciliteze atacuri anonime din orice punct de pe globul pamântesc şi în acelaşi timp servind ca o sursă de instrumente pentru pentru orice hacker. În SUA, PIC a devenit un element esenţial al Departamentului Securităţii Interne şi este abordată, în mod curent, din punct de vedere al dezvoltării strategiilor de luptă împotriva terorismului.[4] Distincţia dintre PIC şi PIIC va continua să se concentreze pe *protecţia infrastructurii informaţionale critice.* În documentele oficiale, termenul PIC este utilizat în mod frecvent doar dacă acestea se referă numai la aspectele informaţionale ale domeniului abordat. Motivaţia o reprezintă faptul că aceşti doi termeni nu pot şi nu ar trebui discutaţi ca şi concepte complet separate. PIC reprezintă mai mult decât PIIC, dar PIIC reprezintă o parte esenţială a PIC. O concentrare exclusivă pe ameninţările cibernetice care ignoră ameninţările fizice tradiţionale importante este la fel de dăunătoare ca şi neglijarea dimensiunii virtuale, fapt ce este necesar într-o abordare raţională a ambelor concepte interrelaţionate. Oricum, există cel puţin o caracteristică care le distinge: în timp ce PIC cuprinde toate sectoarele critice din infrastructura unei naţiuni, PIIC reprezintă numai un subset al efortului de protecţie complet şi se concentrează pe măsurile de securitate ale *infrastructurii informaţionale critice*. În general, PIC reprezintă partea din infrastructura

informaţională globală sau naţională necesară şi esenţială pentru asigurarea continuităţii serviciilor infrastructurii critice ale unei ţări. PIC, în sens larg, constă din sectorul de informaţii şi telecomunicaţii şi cuprinde componente ca: telecomunicaţiile; calculatoarele şi software-ul; internetul; sateliţii, fibra optică etc. Termenul este, de asemenea, utilizat pentru desemnarea totalităţii calculatoarelor şi reţelelor interconectate, precum şi a fluxurilor informaţionale critice din cadrul acestora. Acestea sunt privite ca reţea de bază pentru infrastructurile critice, asigurând un schimb neîntrerupt de date, esenţial pentru utilizarea infrastructurilor în general şi a serviciilor pe care le furnizează. Este bine cunoscut că ameninţările pentru PIC / PIIC nu respectă limitele funcţionale sau geografice şi diferitele sectoare partajează vulnerabilităţile şi interdependenţele la nivelul graniţelor (de exemplu: infrastructurile care se bazează pe telecomunicaţii şi energie pentru funcţionare).

Securitatea spaţiului cibernetic a devenit un element esenţial în multe ţări, iar guvernele din întreaga lume fac eforturi deosebite în acest domeniu. În SUA, infrastructurile critice sunt definite în concordanţă cu Actul pentru Unitatea şi Întărirea Americii prin Asigurarea Instrumentelor Adecvate Necesare pentru Descoperirea şi Obstrucţionarea Terorismului, secţiunea 1016 (e) din 2001 care prevede că: „…termenul de „infrastructură critică” reprezintă sisteme şi mijloace, fizice sau virtuale, atât de vitale pentru SUA încât incapacitatea funcţională sau distrugerea lor au un impact serios asupra securităţii naţionale, securităţii economice naţionale, sănătăţii publice naţionale sau siguranţei, sau o combinaţie a acestor elemente.” Pe baza acestei definiţii, Departamentul pentru Securitate Internă a identificat 17 infrastructuri critice şi resurse esenţiale şi a delimitat rolul şi responsabilităţile pentru protecţia acestor sectoare. În timp ce alte modificări sau adăugiri sunt posibile, următoarele sectoare erau, la acel moment, definite ca infrastructuri critice şi resurse importante: tehnologia informaţiei, telecomunicaţiile, produsele chimice, facilităţile comerciale, barajele, reactoarele nucleare comerciale (inclusiv materialele şi deşeurile nucleare), amplasamentele guvernamentale, sistemele de transport, serviciile de urgenţă, serviciile poştale şi de transport cargo, agricultura şi alimentaţia, sănătatea publică şi serviciile specifice, sistemele de asigurare a apei potabile şi cele de tratare a apei uzate, sistemele energetice, inclusiv cele de producere, rafinare, stocare şi distribuţie a petrolului, gazului şi energiei electrice, băncile şi finanţele, monumentele şi simbolurile naţionale, baza industrială pentru apărare, produsele critice de larg consum.[5]

Uniunea Europeană (UE) reprezintă un organism esenţial la nivel internaţional care se preocupă de asigurarea informaţională. PIIC, societatea informaţională şi securitatea informaţiei sunt considerate probleme importante la nivelul acesteia. De aceea, UE a lansat iniţiative şi programe de cercetare pentru a

studia aspecte diverse ale revoluţiei informaţionale şi impactul acestora asupra educaţiei, afacerilor, sănătăţii şi comunicaţiilor. În domeniul comunicaţiilor, IC sunt definite după cum urmează: „Infrastructurile critice constau din acele facilităţi fizice şi de tehnologia informaţiei, reţele, servicii şi mijloace care, dacă sunt întrerupte din funcţionare sau distruse vor avea un serios impact asupra sănătăţii, siguranţei, securităţii sau bunăstării economice a cetăţenilor sau în funcţionarea eficientă a guvernelor statelor membre. PIIC este definită astfel: „Programele şi activităţile proprietarilor de infrastructură, operatorilor, producătorilor, utilizatorilor şi autorităţilor de reglementare care vizează menţinerea performanţelor PIIC în caz de defecţiuni, atacuri sau accidente mai mari decât un set minim de servicii şi urmăreşte minimizarea distrugerilor şi timpului de refacere. PIIC trebuie văzută ca un fenomen intersectorial şi nu ca unul limitat la anumite sectoare specifice. PIIC trebuie strâns coordonată cu PIC într-o perspectivă holistică". În mod particular, obiectivul cercetărilor din TIC în cadrul UE este acela de a îmbunătăţi competitivitatea Europei la toate nivelurile prin concentrarea pe următoarele trei zone importante ale TIC: productivitatea şi inovaţia prin facilitarea creativităţii şi managementului; modernizarea serviciilor publice precum sănătatea, educaţia şi transportul; dezvoltările în ştiinţă şi tehnologie prin sprijinul cooperării şi accesului la informaţie.[6]

Pentru proiectele în domeniul cercetărilor în securitate au fost identificate ca priorităţi nurmătoarele misiuni: optimizarea securităţii şi protecţiei sistemelor interconectate; protecţia IC împotriva terorismului (inclusiv bio-terorismul şi incidentele care implică substanţele biologice, chimice etc.); îmbunătăţirea managementului crizelor (inclusiv evacuarea, operaţiile de căutare şi salvare, control şi refacere); asigurarea interoperabilităţii şi integrării sistemelor din punct de vedere al informaţiei şi comunicaţiilor; îmbunătăţirea cunoaşterii situaţiei (de exemplu: în managementul crizelor, activităţile antiteroriste sau de control al graniţelor).

UE a stabilit un comitet ad-hoc pentru a explora măsurile luate de statele membre pentru combaterea ameninţărilor cibernetice împotriva infrastructurii critice. Ca parte a proiectului UE CI2RCO (Coordonarea Cercetării Infrastructurii Informaţionale Critice), anunţat în aprilie 2005, comitetul urmărea să identifice grupuri de cercetare şi programe concentrându-se pe securitatea tehnologiei informaţiei în infrastructurile critice, precum reţelele de telecomunicaţii şi electrice.[7]

Obiectivele principale ale proiectului CI2RCO sunt următoarele:

• de a încuraja o Europă larg concentrată pe cercetarea şi dezvoltarea PIIC;

• de a stabili un sistem de programe de cercetare ştiinţifică (ERA – European Research Area) pentru PIIC ca parte a obiectivului strategic mai larg al

TIC privind integrarea şi întărirea ERA în ceea ce priveşte capacitatea de a-şi îndeplini funcţiile cerute ($t_d/(t_d+t_c)$; unde: t_d – timpul disponibil; t_c – timpul cerut) şi securitatea;

• CI2RCO se concentrează asupra activităţilor şi acţiunilor statelor membre şi candidate. Printre alte informaţii, site-ul Web al CI2RCO caracterizează PIIC europeană.

În martie 2006 [8], Parlamentul şi Consiliul European emitea Directiva privind Reţinerea Datelor prelucrate privind asigurarea serviciilor publice de comunicaţii prin mijloace electronice sau ale reţelelor publice de comunicaţii. Directiva armonizează legislaţia naţională a statelor membre privind reţinerea datelor referitoare la accesul la internet, telefonia pe internet şi poşta electronică. Directiva se aplică la traficul şi localizarea datelor despre entităţile legale şi persoanele fizice, precum şi la datele necesare pentru identificarea abonatului sau utilizatorului înregistrat. Aceasta nu se aplică privitor la conţinutul datelor, inclusiv la informaţiile consultate prin utilizarea reţelelor de comunicaţii. Statele membre trebuie să se asigure că furnizorii de comunicaţii reţin datele pentru perioade între 6 luni şi 2 ani de la momentul efectuării comunicaţiei. Măsurile luate de Marea Britanie după atacurile teroriste de la Londra, din iulie 2005, impun companiilor de telecomunicaţii să păstreze o mare varietate de date, astfel: numerele de telefon, care iniţiază comunicaţia şi cele care recepţionează; durata convorbirilor telefonice; date privind modul de urmărire a apelurilor de la telefoanele fixe şi mobile; informaţii despre textul mesajelor; adresele IP prin care se determină locaţia calculatoarelor pe internet; timpii de conectare şi deconectare la/de la internet; detalii despre traficul prin poşta electronică, fără a accesa conţinutul mesajelor. Datele despre apelurile efectuate dar fără răspuns, care pot fi utilizate pentru a transmite semnale complicilor la crime sau pentru detonarea bombelor vor fi arhivate şi păstrate. Autorităţi independente sunt desemnate să monitorizeze utilizarea acestor date, care vor fi şterse la expirarea termenului de păstrare, în afara situaţiilor când sunt păstrate pentru investigaţii antiteroriste. Până la 15 septembrie 2010, Comisia Europeană este solicitată să prezinte o evaluare privind aplicarea acestei directive şi impactului acesteia asupra operatorilor economici şi consumatorilor, luându-se în considerare dezvoltările viitoare în tehnologia comunicaţiilor prin mijloace electronice şi statisticile prezentate Comisiei care să stabilească dacă este necesară amendarea acestei directive, în special privind lista datelor şi perioadelor de păstrare. Următoarele categorii de date trebuie păstrate privind telefonia fixă şi mobilă, accesul la internet, poşta electronică şi telefonia pe internet: cele necesare pentru urmărirea şi identificarea sursei comunicaţiei, destinaţia acesteia, timpul şi durata comunicării, tipul comunicaţiei, mijlocul de comunicaţie şi locaţia echipamentului de comunicaţii mobil.

Tratatul de la Lisabona, semnat de şefii de stat sau de guvern ai 27 de state membre, în Lisabona, pe 13 decembrie 2007, care a fost planificat să intre în vigoare la 1 ianuarie 2009, în scopul de a reforma cadrul constituțional al UE, include şi prevederile, privind protecția datelor personale. Tratatul reafirmă „dreptul de protecție al datelor personale”.[9]

Membrii G8 s-au întâlnit la Paris, în martie 2003, pentru prima întrunire multilaterală dedicată PIC / PIIC. Aceştia au definit clar principiile PIIC care au fost adoptate pe 5 mai 2003 de către miniştrii de interne şi de justiție. Acestea acoperă următoarele aspecte din țările membre [10]: necesitatea de a avea rețele de avertizare de urgență privind vulnerabilitățile, amenințările şi incidentele cibernetice; de a creşte nivelul de cunoaştere al situației pentru a facilita înțelegerea de către companii a naturii şi scopului IIC proprii, precum şi rolului pe care fiecare trebuie să-l aibă în protecția lor; să examineze infrastructurile lor şi interdependențele dintre acestea, întărind protecția lor; să promoveze parteneriatul dintre companiile publice şi private, să partajeze şi analizeze informațiile despre infrastructurile critice în scopul de a preveni, investiga şi răspunde la distrugerile sau atacurile asupra acestor infrastructuri; de a creea şi de a menține în funcțiune rețele de comunicații pentru situații de criză şi să le testeze pentru a se asigura că acestea rămân sigure şi stabile în situațiile de urgență; să se asigure că politicile privind disponibilitatea datelor iau în considerație necesitatea de protecție a IIC; să urmărească atacurile la adresa IIC şi, când este necesar, să transmită rezultatele şi altor țări; să conducă instruirea şi exercițiile pentru creşterea capabilităților de răspuns şi să elaboreze planurile pentru situații de urgență în caz de atac a IIC, precum şi să convingă proprietarii să se angajeze în activități similare; să se asigure că au proceduri legale adecvate, precum cele prevăzute în Convenția Consiliului Europei privind crimele cibernetice, din 23 noiembrie 2001, şi personal pregătit să investigheze şi să judece atacurile asupra IIC şi să coordoneze aceste investigații cu alte țări atunci când este cazul; să se angajeze în cooperarea internațională pentru securizarea IIC prin dezvoltarea şi coordonarea sistemelor de avertizare de urgență, partajarea şi analiza informațiilor privind vulnerabilitățile, amenințările şi incidentele, precum şi coordonarea investigațiilor privind atacurile asupra unor asemenea infrastructuri în concodanță cu prevederile legilor naționale; să promoveze cercetarea şi dezvoltarea națională şi să încurajeze aplicarea securității tehnologiilor în conformitate cu standardele naționale.

PIC rămâne una dintre preocupările importante a *Planificării Urgențelor Civile (PUC) în cadrul NATO*. Ghidul Ministerial pentru Planificarea Urgențelor Civile în NATO pentru anii 2007-2008 cuprinde câteva elemente referitoare la PIC, în timp ce Planul de Acțiune privind Actualizarea PUC cuprinde câteva acțiuni referitoare la PIC, precum şi unele măsuri de pregătire împotriva posibilelor atacuri

chimice, biologice, radiologice şi nucleare. Comitetul pentru Planificarea Comunicaţiilor Civile (CPCC) răspunde de verificarea infrastructurilor de comunicaţii publice şi private existente şi planificate să se dezvolte, serviciile oferite, facilităţile asociate, serviciile poştale şi alte servicii suplimentare pentru satisfacerea cerinţelor utilizatorilor importanţi, civili şi militari, pe timpul situaţiilor de urgenţă. Naţiunilor li s-au făcut recomandări să ia în considerare noile tehnologii şi pe cele care vor apărea, aranjamentele şi legislaţia naţională, precum şi rolul organizaţiilor internaţionale în acest domeniu.[11] CPCC a publicat o serie de documente şi studii despre infrastructura de telecomunicaţii, ca de exemplu: protecţia infrastrucurii critice de telecomunicaţii; consecinţele asupra PUC în cazul întreruperii funcţionării infrastructurii critice poştale; noile riscuri şi ameninţări la adresa telecomunicaţiilor civile; cerinţele PUC privind coordonarea măsurilor de reglementare a telecomunicaţiilor naţionale; noile riscuri şi ameninţări la adresa serviciilor poştale.

În plus, CPCC a contribuit la „Planul de Acţiune al Consiliului Nord-Atlantic privind Apărarea Cibernetică, astfel:

• consecinţele asupra PUC determinate de introducerea Echipelor de Răspuns la Urgenţele privind Calculatoarele şi a celor determinate de atacurile cibernetice şi războiul informaţional asupra infrastructurii de comunicaţii civile critice.

• identificarea şi analiza influenţelor altor infrastructuri critice asupra reţelelor de comunicaţii civile.

• impactul dezvoltării societăţii informaţionale şi a altor oportunităţi aferente asupra PUC în cadrul NATO.

În declaraţia summit-ului de la Bucureşti din 2008, la paragraful 47 se menţionează că „NATO rămâne angajat în întărirea sistemelor informaţionale ale Alianţei împotriva atacurilor cibernetice. Noi am adoptat recent o Politică privind Apărarea Cibernetică cu structuri şi autorităţi care s-o poată îndeplini. Politica noastră privind Apărarea Cibernetică evidenţiază cerinţele NATO şi ale naţiunilor de a proteja sistemele informaţionale în concordanţă cu responsabilităţile acestora; de a partaja cele mai bune practici şi a asigure o capabilitate de asistare a capabilităţilor Alianţei, la cerere, pentru contracararea unui atac cibernetic. Noi urmărim în continuare dezvoltarea capabilităţilor de apărare cibernetică ale NATO şi să întărim legăturile dintre NATO şi autorităţile naţionale”.[12]

Sistemele de avertizare timpurie sunt destinate să îndeplinească următoarele obiective: înţelegerea şi clasificarea pericolelor; monitorizarea şi prevederea evenimentelor viitoare; prelucrarea şi diseminarea avertizărilor clare autorităţilor politice şi populaţiei; întreprinderea celor mai adecvate şi oportune acţiuni ca urmare a avertizărilor primite. În PIIC, avertizarea timpurie se

concentrează, în principal, pe incidentele privind securitatea tehnologiei infirmaţiei. Următoarele elemente reprezintă aspectele comune discutate în contextul procedurilor legislative ale ţărilor membre: protecţia şi securitatea datelor în comunicaţiile prin mijloace electronice (inclusiv transmiterea datelor, stocarea sigură a datelor etc.); securitatea tehnologiei informaţiei şi cerinţele privind securitatea informaţiei; utilizarea frauduloasă a calculatoarelor şi reţelelor de calculatoare, distrugerea sau falsificarea datelor, precum şi alte atacuri similare; protecţia şi confidenţialitatea datelor personale; identificarea şi semnăturile digitale; responsabilităţile în comerţul şi afacerile derulate prin mediul electronic; armonizarea internaţională a legislaţiei privind criminalitatea cibernetică; standardele minime pentru securitatea informaţională în scopul guvernării electronice, furnizorii de servicii, operatorii, inclusiv implementarea standardelor de securitate; infrastructură cu chei publice şi managementul acesteia. Dincolo de toate graniţele, există 2 factori principali care influenţează şi uneori perturbă eficienţa impunerii legii – unul naţional şi celălalt internaţional.

Există 4 posibile categorii de iniţiative care pot fi lansate de actorii multipli: descurajarea, prevenirea, detectarea şi reacţia.[13]

• Descurajarea – sau concentrarea pe utilizarea legislaţiei împotriva crimelor cibernetice: iniţiative multilaterale pentru a descuraja utilizarea spaţiului cibernetic în scopuri rău intenţionate, care cuprind acţiuni de armonizare a legilaţiei împotriva crimelor cibernetice şi de a promova pedepse mai severe şi îmbunătăţirea legislaţiei comerţului electronic.

• Prevenirea – sau proiectarea şi utilizarea mai multor sisteme sigure cu un management performant al securităţii şi promovarea mai multor mecanisme de securitate: utilizarea unor sisteme informaţionale cu niveluri de securitate sporite, atât în mediul public, cât şi cel privat.

• Detecţia – sau politicile de cooperare şi avertizarea timpurie multilaterale privind atacurile cibernetice prin întărirea cooperării, avertizarea timpurie, schimburile de informaţii între sectorul public şi cel privat.

• Reacţia – sau proiectarea unor infrastructuri informaţionale puternice a unor programe de management al crizelor, a unor politici specifice şi eforturi juridice adecvate.

Orice politică de protecţie adecvată care se extinde până la infrastructura informaţională strategică necesită soluţii transnaţionale. Divergenţele dintre politicile naţionale privind PIIC sunt obstrucţii majore în dezvoltarea unor organisme de reglementare internaţionale, deoarece acestea trebuie să se bazeze pe o minimă convergenţă a aşteptărilor şi intereselor actorilor naţionali importanţi. De aceea, în spiritul intereselor economice şi de securitate, statele industrializate

conlucrează pentru a depăşi aceste obstacole temporare în scopul de a realiza convenţii şi mecanisme solide care să protejeze mediul informaţional global.

NOTE BIBLIOGRAFICE

[1] Office of Critical Infrastructure Protection and Emergency Preparedness (OCIPEP). *Threat Analysis No. TA03-001* (2003). http://www.ocipep-bpiepc.gc.ca/opsprods/other/TA03-001_e.pdf.

[2] Myriam Dunn and Victor Mauer (eds.), International CIIP Handbook, Vol. II, *Analyzing Issues, Challenges, and Prospects*, Center for Security Studies, ETH Zurich, 2006, pp.60-62.

[3] Joseph Glebocki, Jr., *DoD Computer Network Operations: Time to Hit the Send Button*, US Army War College, Carlisle Barracks, Pennsylvania, 2008, pp.13-16.

[4] Department of Homeland Security. "*National Infrastructure Protection Plan*", Washington, D.C., 2006, p.3.

[5] The White House. "*Homeland Security Presidential Directive/HSPD-7*", Washington, D.C., 17 December 2003, Section 15.

[6] Commission of the European Communities. *Green Paper on a European Programme for Critical Infrastructure Protection* (Brussels, 17 November 2005), COM(2005) 576 final, pp.19-20.

http://www.libertysecurity.org/IMG/pdf/EC_-_Green_Paper_on_CI_-_17.11.2005.pdf.

[7] http://www.attrition.org/pipermail/isn/2005-April/001454.html.

[8] *Directive on Data Retention 2006* (2006/24/EC, following Commission proposal COM(2005)0438). http://eur-lex.europa.eu/LexUriServ/LexUriServ.

[9] http://europa.eu/lisbon_treaty/full_text/index_en.htm.

[10] Elgin M. Brunner and Manuel Suter, International CIIP Handbook 2008 / 2009, *An Inventory of 25 National and 7 International Critical Information Infrastructure Protection Policies*, Center for Security Studies, ETH Zurich, 2009, pp.490-492.

[11] Ibid., pp.496-497.

[12] Bucharest Summit Declaration Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Bucharest on 3 April 2008. http://www.summitbucharest.ro/en/doc_201.html.

[13] Elgin M. Brunner and Manuel Suter, op.cit., pp.541-543.

COOPERAREA STRUCTURATĂ PERMANENTĂ ÎN DOMENIUL APĂRĂRII – PROVOCĂRI ŞI OPORTUNITĂȚI –

Dragoş ILINCA

Noutățile aduse de Tratatul de la Lisabona sunt, cu siguranță, ambiții de o mare importanță pentru apărarea europeană. Unul dintre articolele principale ale pachetului de la Lisabona este Cooperarea Structurată Permanentă, care oferă posibilitatea legală pentru o cooperare intensă în domeniul apărării între țările doritoare. Preambulul protocolului ataşat Tratatului, care subliniază obiectivele Cooperării Structurate Permanente şi criteriile de participare, vorbeşte despre „un rol mai hotărât al Uniunii în problemele de securitate şi apărare" şi chiar despre „investirea pe o nouă treaptă de dezvoltare a politicii de securitate şi apărare europeană". Cu toate acestea, Cooperarea Structurată Permanentă nu este „glonțul de argint" care va rezolva problema situației militare din Europa, dar făcând parte din Tratat şi Statele Membre, trebuie luat în considerare dacă şi cum să fie folosit, întrucât reprezintă o oportunitate pentru politica de securitate şi apărare europeană comună în viitor.

Prin intermediul Tratatului de la Lisabona unul dintre principalele elemente de noutate ale inventarului instituțional aferent Politicii Comune de Securitate şi Apărare (PCSA) îl reprezintă posibilitatea inițierii *Cooperării Structurate Permenente* (CSP) în domeniul apărării între statele membre care doresc acest lucru. Ca parte a segmentului inovator pe care noul Tratat îl aduce, acest tip de formulă a stârnit o amplă gamă de reacții, majoritatea acestora fiind cantonată în perimetrul dezbaterii privind eterna problemă a „*Europei cu mai multe viteze*".

În cazul dimensiunii de apărare, translatarea acestui principiu a căpătat accente suplimentare şi, în egală măsură specifice, date fiind coordonatele tradiţionale pe care a evoluat PCSA, anume cel al menţinerii prerogativelor extinse ale statelor membre în orientarea procesului de articulare a componentei de securitate şi apărare a Uniunii Europene.

Din această perspectivă, dezbaterea privind posibilitatea realizării unui cadru normativ care să permită implementarea unor astfel de formule la nivel european nu a fost însoţită, până în momentul adoptării Tratatului de la Lisabona, de exprimări concrete în plan instituţional. Istoria recentă a procesului de dezvoltare a PCSA a consemnat, în schimb, o serie de tentative iniţiate în acest sens, majoritatea acestora repurtând, însă, eşecuri lamentabile. La nivelul cauzelor care au condus la această situaţie se regăsesc factori aferenţi lipsei de coeziune politică privind asumarea unui astfel de obiectiv. În strânsă legătură cu acest aspect se plasează şi modalitatea de „orchestrare" a demersurilor iniţiate pe acest domeniu, mai precis corelaţia obiectivelor politice cu stadiul de dezvoltare al PCSA.

Pe această dimensiune, momentul apariţiei unor astfel de preocupări se regăseşte în contextul creat prin consensul franco-britanic asupra necesităţii unui profil mult mai robust al Uniunii Europene în domeniul securităţii şi apărării, aspect consemnat în cadrul reuniunii de la St-Malo, din decembrie 1998[1]. Practic, summit-ul franco-britanic a deschis o adevărată „Cutie a Pandorei" în ceea ce priveşte diversele idei şi iniţiative menite să contribuie la dezvoltarea instrumentelor europene de gestionare a crizelor, inclusiv cele militare.

Episodul, de departe cel mai relevant, l-a reprezentat aşa-numitul „Mini-summit al apărării"[2], organizat de Franţa, Germania, Belgia şi Luxemburg, derulat la începutul anului 2003, în plină criză transatlantică generată ca urmare a disputelor vizând lansarea campaniei împotriva regimului condus de Saddam Hussein. Iniţiativa celor patru state a reprezentat prima exprimare a preocupărilor

[1] Pentru detalii privind concluziile Summit-ului franco-britanic de la St.Malo a se vedea comunicatul acestei reuniunii la adresa http://www.fco.gov.uk/resources/en/news/2002/02/--8216-uk-french-summit-new05620.

[2] Cunoscut şi sub numele de „Summit-ul de ciocolată" reuniunea celor 4 state s-a finalizat cu adoptarea unei declaraţii de intenţie în cadrul căreia se regăseau iniţiative menite să contribuie la accelerarea procesului de dezvoltare a componentei de securitate şi apărare a UE, printre care: crearea Agenţiei Europene de Apărare, introducerea unei clauze de solidaritate în domeniul apărării, crearea Comandamentului Operaţional Autonom al UE etc., European Defence Meeting – Tervuren, Bruxelles, 29 aprilie 2003 în *From Copenhagen to Brussels. European Defence: core documents vol.IV*, European Union Institute for Security Studies, Paris, 2003, pp.76-81.

existente la nivelul Uniunii Europene, vizând articularea unui demers comun de lansare a unor iniţiative menite să accelereze procesul de operaţionalizare a componentei europene de apărare.

Deşi eşuat din punct de vedere instituţional, mini-summit-ul celor patru state a reuşit să contribuie în mod semnificativ la consolidarea tendinţelor apărute în contextul reuniunii de la St-Malo vizând preocuparea de articulare a unei agende europene de apărare, în sens autonomist, marcată chiar şi de accente radicale. Exprimări de acest gen aveau să se regăsească şi la nivelul dezbaterilor iniţiate în cadrul „Convenţiei pentru viitorul Europei”[3], conducând, finalmente, la reluarea ideilor avangardiste în ceea ce priveşte viitorul apărării europene în cadrul Constituţiei Europene. Practic, întregul pachet vizând componenta de apărare, codificat în textul constituţional, era marcat din plin de acest gen de abordări fiind socotit de majoritatea analiştilor ca fiind poate cel mai ambiţios proiect[4] la nivelul politicilor europene.

Relevanţa Tratatului Constituţional, deşi eşuat şi el, constă în faptul că pentru prima oară în istoria Uniunii Europene s-a reuşit agrearea la nivelul statelor membre a unei agende integraţioniste în domeniul apărării preluată, aproape în totalitate, la nivelul Tratatului de la Lisabona adoptat după evoluţii sinuoase la sfârşitul anului 2009.

Cu toate acestea, Cooperarea Structurată Permanentă reprezintă una dintre „enigmele” Tratatului de la Lisabona, în special, din perspectiva modalităţilor concrete de implementare la nivelul Uniunii Europene. Nu se poate exclude, însă, relevanţa pentru modul în care se PCSA, ritmul şi, mai ales, structura acesteia. În mod evident, CSP poate genera un moment favorabil pentru tendinţele existente deja la nivel european de a adânci cooperarea între statele membre pe diferite zone ale componentei de securitate şi apărare, precum cele vizând dezvoltarea capabilităţilor de apărare şi până la generarea de angajamente operaţionale.

Textul Tratatului nu oferă perspective extrem de clare asupra domeniilor pe care CSP le poate aborda, menţinând necesara ambiguitate constructivă menită să ofere posibilitatea avansării procesului de integrare în acest domeniu. Din

[3] Convenţia pentru viitorul Europei a fost înfiinţată prin decizia Consiliului European din decembrie 2001 pentru a elabora textul Tratatului privind instituirea Consituţiei Europene, mult mai cunoscut sub numele de Tratatul Constituţional. Lucrările acestui for s-au încheiat în iulie 2003 prin elaborarea acestui document supus ulterior referendumurilor din statele membre UE. După cum se cunoaşte acest process a înregistrat două eşecuri răsunătoare în Franţa şi Olanda ceea ce a condus la abandonarea Tratatului Constituţional şi, ulterior, elaborarea Tratatului de la Lisabona.

[4] Textul Tratatului Constituţional disponibil în forma electronic la adresa http://www.europa.eu.

perspectivă scolastică, prevederile Tratatului de la Lisabona oferă doar un set de orientări care la prima vedere pot părea extrem de generale, dar care se adresează elementelor definitorii ale sistemului de planificare în domeniul apărării, utilizat de toate statele membre UE.

În acest context se stipulează ca principiu fundamental al formulelor de cooperare structurată necesitatea realizării unei convergenţe reale între demersurile statelor membre implicate în acest gen de mecanisme. Importanţa acestui aspect merită, fără îndoială, o serie de clarificări. Practic, încă din momentul iniţierii PCSA, problema abordărilor divergente ale statelor membre a reprezentat principala provocare cu care Uniunea Europeană s-a confruntat. Percepţiile diferite asupra modului în care componenta europeană de securitate şi apărare trebuia să se dezvolte nu a permis identificarea acelui numitor comun care să poată întruni setul extins de exprimări naţionale şi, prin urmare, să se califice drept platformă de orientare pentru politica europeană în domeniu.

Cooperarea structurată şi procesul de dezvoltare a capabilităţilor de apărare

În cazul procesului de dezvoltare a capabilităţilor de apărare, problema convergenţei s-a dovedit a fi cu atât mai dificilă, în condiţiile unei fragmentări excesive a abordărilor naţionale. Acestui extrem de complicat subiect i s-a găsit o rezolvare parţială, prin intermediul stabilirii unui set comun de obiective, asumate în mod consensual de către statele membre în vederea depăşirii unor deficienţe din domeniul capabilităţilor de apărare. Soluţia identificată s-a concretizat prin intermediul adoptării Planului de Dezvoltare a Capabilităţilor (PDC)[5], care întruneşte un număr limitat de domenii identificate ca fiind deficite comune, asupra cărora s-a reuşit realizarea consensului statelor membre.

În ciuda acestui demers, salutar în esenţa sa, finalizarea procesului trenează. Principala cauză o reprezintă, ca şi în multe alte cazuri consemnate la nivelul componentei de securitate şi apărare, abordarea interguvernamentalistă a acestei politici la adăpostul căreia statele membre îşi pot permite opţiunea de a evita translatarea obiectivelor asumate în cadrul european la nivelul proceselor naţionale. Riscul major al menţinerii acestei situaţii îl reprezintă „consolidarea" caracterului orientativ al deciziilor adoptate la nivel european şi, în consecinţă, reducerea şanselor de implementare a unei abordări integrate la nivelul Uniunii Europene. Este explicabilă, astfel, necesitatea codificării la nivelul legislaţiei primare a Uniunii Europene, a posibilităţii implementării unei abordări convergente la nivelul componentei de securitate şi apărare, ca unică modalitate de a surmonta

[5] *Future treds from the Capability Development Plan*, http://www.eda.europa.eu.

racilele evidente ale sistemului interguvernamental. În acest context trebuie plasată apariţia prevederilor vizând introducerea CSP în domeniul apărării. Planul de Dezvoltare a Capabilităţilor este doar unul dintre subiectele care făceau necesară o abordare integrată, de valenţă europeană, care să poată fi extinsă la nivelul tuturor statelor membre, în scopul articulării unei viziuni strategice comune.

Conform Articolului 1 al Protocolului nr.4[6], anexă la Tratatul de la Lisabona, CSP vizează şi dimensiunea instituţională responsabilă pentru gestionarea procesului de dezvoltare a capabilităţilor de apărare. Din această perspectivă, unul dintre instrumentele esenţiale îl reprezintă Agenţia Europeană de Apărare al cărei rol în monitorizarea formulelor de cooperare structurată ce s-ar putea dezvolta este de departe cel mai important.

Dincolo de acest aspect, raţiunea introducerii Agenţiei a vizat adoptarea unei noi abordări în valorizarea diverselor iniţiative derulate până în prezent pe dimensiunea capabilităţilor europene de apărare, cu precădere cele derulate sub egida acestei structuri a Uniunii Europene. Şi în acest caz, CSP oferă oportunităţi de avansare a abordării comunitare, integraţioniste, prin replasarea programelor de cooperare într-o nouă formulă instituţională, mult mai constrângătoare în a fi respectată de statele membre. Astfel, prevederile Tratatului de la Lisabona în ceea ce priveşte criteriile pe care statele interesate de participarea în cadrul CSP trebuie să le îndeplinească, înglobează programele majore de înzestrare derulate la nivel european, precum şi cele care se află în gestiunea exclusivă a Agenţiei.

Este evident faptul că şi din această perspectivă, cooperarea structurată permanentă vine să contribuie la eliminarea fragmentării cu care cadrul european de dezvoltare a capabilităţilor de apărare se confruntă. În avansarea formulelor de cooperare structurată baza va fi furnizată de inventarul existent. Diferenţa notabilă o reprezintă posibilitatea unei mai bune conectări a programelor majore de înzestrare iniţiate prin participarea unor state membre, dar plasate în afara cadrului instituţional al Uniunii Europene. Din această perspectivă, contribuţia CSP poate fi apreciată ca fiind extrem de benefică în sensul în care prin intermediul acestui instrument se asigură conexiunea care a lipsit, până în prezent, între componenta instituţională de securitate şi apărare a Uniunii şi diversele iniţiative în domeniul capabilităţilor, inclusiv pe dimensiunea de producţie.

Nu trebuie neglijat şi impactul favorabil pe care această relaţie îl poate avea asupra eficienţei programelor *per se*, putându-se anticipa o revigorare a

[6] Treaty on the Reform of European Union, Protocol on Permanent Structured Cooperation established by the Article 28A of the Treaty on the European Union,http:///europa.eu/lisbon_treaty/full_text/index_en.htm.

acestora. În mod evident, programe majore, precum A400M[7], vor căpăta relevanţe suplimentare, permiţând, avansarea unor formule de cooperare în cadrul acestora care să capaciteze interesul statelor membre.

În acelaşi timp, analiza implicaţiilor CSP pentru problematica generală a capabilităţilor de apărare include şi o semnificativă componentă economico-comercială. Pe acest segment, demersurile[8] repetate ale Agenţiei Europene de Apărare vizând crearea unei pieţe europene comune în domeniul echipamentelor de apărare, precum şi în zona industrială pot beneficia de o susţinere suplimentară. Până în prezent acest demers nu a depăşit nivelul cadrului doctrinar, capacitarea segmentului industrial neputându-se realiza într-o manieră consolidată. Cauza fundamentală a reprezentat-o tocmai absenţa unei conexiuni directe cu PCSA şi, în egală măsură, atractivă pentru companiile europene de profil. Din această perspectivă, CSP oferă oportunităţi semnificative de eliminare a acestui vid stabilind o mai bună sinergie acţională între cele două componente.

Cooperarea structurată şi angajamentele operaţionale

Dintr-o perspectivă similară, anume cea a tentativei de a adânci integrarea pe componenta de apărare la nivel european, cel de-al doilea set de criterii se adresează dimensiunii capabilităţilor europene care pot face obiectul angajării în operaţiile de management al crizelor conduse de Uniune. Deşi referirile explicite la demersurile operaţionale nu se regăsesc în cadrul prevederilor CSP, obiectivul vizând accelerarea procesului de eliminare a deficienţelor şi, mai ales, de valorificare a oportunităţilor existente transpare cu extrem de multă claritate[9].

În egală măsură, se poate vorbi de o nouă etapă în cadrul procesului de generare a capabilităţilor operaţionale, orientată, primordial, în sensul utilizării inventarului existent, în susţinerea angajamentelor operaţionale. Binînţeles, principalul aspect vizează participarea statelor în cadrul Grupurilor de Luptă a căror menţionare explicită în ansamblul criteriilor CSP conduce la ideea unei largi disponibilităţi de utilizare a acestor structuri. Este, de asemenea, o consecinţă logică a evoluţiilor[10] înregistrate în cadrul procesului de generare a unor astfel de

[7] Programul A400M vizează producţia de către concernul EADS a primului avion de transport strategic european. În data de 12 ianuarie 2010, a avut loc zborul de inaugurare al acestui tip de avion. Pentru detalii http://www.a400m.com

[8] *Baza Europeană Industrială şi Tehnologică în domeniul Apărării* (European Defence technologial and Industrial Base - EDTIB), http://www.eda.europa.eu.

[9] Treaty on the Reform of European Union, Protocol on Permanent Structured Cooperation, Art.1, para.(b), http:///europa.eu/lisbon_treaty/full_text/index_en.htm.

[10] Începând cu 1 ianuarie 2007, Grupurile de Luptă ale Uniunii Europene au fost declarate operaţionale, putând fi utilizate în cadrul operaţiilor de management al crizelor derulate de

capacităţi de reacţie rapidă, dar şi o prelungire firească a dezbaterilor intraeuropene privind necesitatea utilizării în cadrul operaţiilor de management al crizelor în condiţiile în care adeseori aceastea înregistrează sincope majore în acoperirea inventarului de forţe şi capacităţi. Nu în ultimul rând, această abordare este orientată în scopul evitării pericolului de plasare a acestor instrumente, considerate a fi unele de „lux", în desuetudine şi, implicit, de slăbire a coerenţei operaţionale, acest din urmă aspect fiind, practic, esenţa valorii adăugate pe care Grupurile de Luptă o aduc în mediul de securitate contemporan.

În ciuda faptului că includerea Grupurilor de Luptă în cadrul Tratatului poate părea oarecum insolită, acest tip de abordare este perfect justificabil în condiţiile în care acestea reprezintă poate singurul proiect cu adevărat „european" care a reuşit să capaciteze toate statele membre, indiferent de opţiunea de raportare a acestora faţă de PCSA. Prin urmare, codificarea acestor structuri la nivelul legislaţiei primare europene reprezintă, întâi de toate, o modalitate de reafirmare a credibilităţii proiectului european de optimizare a angajamentului Uniunii în domeniul managementului crizelor.

De asemenea, prezenţa Grupurilor de Luptă în acest context oferă o serie de indicii asupra viitorului profil pe care formulele de cooperare structurată îl pot avea. Se poate anticipa, prin urmare, că acesta va fi orientat în scopul susţinerii de angajamente operaţionale cu caracter pronunţat expediţionar. Dacă această tendinţă, deja prezentă la nivelul unora dintre statele membre, se va regăsi într-un profil mult mai robust al PCSA este dificil de opinat la acest moment, dar ea nu trebuie exclusă din ansamblul cursurilor posibile de evoluţie.

În acelaşi timp, discuţia pe palierul privind generarea de capacităţi pentru operaţii include şi aspectele privind nivelul de operaţionalizare a forţelor puse la dispoziţia Uniunii Europene de către statele membre. După cum istoria recentă atestă, această problemă a reprezentat principalul element de critică la adresa membrilor UE, nivelul înregistrat de aceştia în raport cu cerinţele operaţionale ale agendei de securitate europeană fiind unul relativ scăzut, situaţie[11] consemnată şi în contextul NATO pentru aceleaşi state, membre ale celor două organizaţii. Şi în acest caz, CSP poate contribui în mod substanţial la eliminarea deficienţelor în utilizarea forţelor alocate operaţiunilor europene. Se poate vorbi de posibilitatea

---

Uniunea Europeană. Până în prezent, au fost structurate un număr de 14 Grupuri de Luptă, în diverse configuraţii. Pentru detalii vizând Grupurile de Luptă UE http://www.consilium.europa.eu/uedocs/cmsUpload/Battlegroups.pdf.

[11] Conform parametrilor agreaţi la nivelul NATO, disponibilitatea forţelor puse la dispoziţie de statele membre trebuie să îndeplinească următorii parametrii: 40% din totalul forţelor terestre dislocabile iar din cadrul acestora 8% sustenabile în teatrul de operaţii. http://www.nato.int/docu/speech/2005/s050414c.htm.

unei abordări cu valenţe comune evidente care poate contrabalansa avatarurile generate de menţinerea prerogativelor exclusive în ceea ce priveşte procesul de planificare şi generare a forţelor.

Agenda Cooperării Structurate Permanente

Abordarea utilizată la nivelul criteriilor de eligibilitate pentru participarea în cadrul formulelor de cooperare structurată se regăseşte şi în inventarul agendei pe care statele membre interesate vor trebui să şi-o asume. Elementul fundamental îl reprezintă implementarea abordării integrate în cadrul căreia opţiunile naţionale vor trebui să se armonizeze. Diversitatea aspectelor, care pot face obiectul acestei agende, a generat şi în acest caz necesitatea unei ambiguităţi constructive la nivelul codificării în textul Tratatului cu scopul evident de a permite o marjă de manevră sufiecientă care să permită stabilirea realistă a unor obiective posibil a fi îndeplinite.

Relevanţa constă, însă, în tendinţa pe care agenda de cooperare o conturează, anume aceea a unui caracter permanent al iniţiativelor care pot face obiectul formulelor de cooperare structurată. Acest demers vine, ca şi în cazul criteriilor de eligibilitate, să atenueze accentuata stare de fragmentare pe care componenta de securitate şi apărare o resimte şi, implicit, să conducă la atenuarea particularităţilor naţionale, în favoarea unei abordări europene integrate.

Din această perspectivă, inventarul de subiecte include, în primul rând, spinoasa problemă a armonizării alocaţiilor bugetare pentru apărare, pe care statele participante în cadrul cooperării structurate vor trebui să-i găsească o rezolvare. Pe acest segment, peisajul european oferă un tablou extrem de divers, modalităţile de raportare a statelor membre fiind dintre cele mai variate, acoperind o plajă largă de plafoane[12], adeseori extrem de reduse în raport cu ceea ce este considerat a fi nivelul adecvat de finanţare, anume cel de 2% din PIB.

Includerea acestui aspect vine ca urmare a unei necesităţi stringente pe care Europa o resimte, cu atât mai pronunţată în actualele condiţii ale crizei economico-financiare. Tocmai în aceste condiţii, este evident faptul că îndeplinirea unui astfel de obiectiv se va dovedi extrem de dificilă în condiţiile în care elementul de raportare va fi, în mod absolut sigur, plafonul alocaţiilor bugetare ale statelor mari din Uniunea Europeană, precum Franţa, Germania, Marea Britanie sau Italia, ţinte

[12] Se poate constata existenţa unui grup de state ale căror alocaţii bugetare se ridică la un nivel de peste 2%, considerat a fi un prag minimal de susţinere a unei capacităţi de apărare credibile. Zona majoritară o reprezintă statele membre ale căror alocaţii bugetare se înscriu sub acest prag, dar nu coboară sub 1%. Trebuie subliniat însă faptul că pe acest segment majoritatea[12] coboară spre jumătatea inferioară, beneficiind de alocaţii bugetare apropiate de acest procent. Pentru detalii *EDA Facts&Figures-2008,* http://www.eda.europa.eu.

aproape imposibil de atins de statele mici şi medii. Acest aspect conduce, în mod automat, la presupunerea unui semnificativ caracter exclusivist al viitoarelor formule de cooperare structurată, problemă cu care statele, având capacităţi financiare mai reduse, se vor confrunta în perioada imediat următoare implementării prevederilor Tratatului de la Lisabona.

Cu toate acestea nu trebuie omise potenţialele avantaje pe care armonizarea nivelului cheltuielilor pentru apărare le oferă. Principalul aspect care merită a fi subliniat este acela relativ la componenta aferentă finanţării programelor de dezvoltare a capabilităţilor de apărare, în special componenta europeană a acestora. Până în prezent, nu s-a reuşit armonizarea acestora în sensul stabilit[13], în mod consensual, la nivelul Agenţiei Europene de Apărare, discrepanţele între statele membre fiind extrem de mari, ceea ce nu permite, în consecinţă, implementarea unei abordări comune pe acest palier.

În acelaşi spirit, efectele benefice se extind şi la nivelul relaţiei cu segmentul industrial şi de cercetare din domeniul securităţii şi apărării, canalizarea alocaţiilor bugetare în susţinerea programelor „comunitare" fiind de natură să confere un caracter de predictibilitate al modului de dezvoltare a PSCA, sporindu-i, de asemenea, atractivitatea. Cu toate acestea, un astfel de demers nu se poate realiza în absenţa unei abordări comune în ceea ce priveşte identificarea cerinţelor. În consecinţă, agenda CSP include obligativitatea armonizării pe această dimensiune între statele membre participante în cadrul unor astfel de mecanisme.

Din aceeaşi perspectivă, prevederile Tratatului de la Lisabona, relativ la dezvoltarea acestui tip de formule de cooperare, includ şi problematica specializării ca element definitoriu al agendei de lucru. Este, în mod evident, o consecinţă firească a unei situaţii reale la nivel european, generată de incapacitatea statelor membre de a disponibiliza alocaţii financiare suficiente pentru menţinerea şi dezvoltarea unui set extins de capabilităţi. De asemenea, specializarea pe dimensiunea apărării reprezintă o prelungire firească a filosofiei ce a animat întregul proces de construcţie a arhitecturii europene, celelalte componente ale constructului european fiind marcate de această abordare cu mult timp în urmă.

---

[13] În mod concret, toate aceste aspecte erau reunite, conform deciziei miniştrilor apărării din noiembrie 2007, într-un set de repere colective care vizau pragurile pe care statele membre erau chemate să le îndeplinească: 2% din totalul cheltuielilor de apărare pentru cercetare şi tehnologii; asigurarea unui nivel de minim 20% din totalul cheltuielilor de apărare pentru programele de înzestrare; 35% din totalul cheltuielilor bugetare pentru programele europene de cooperare în domeniul înzestrării; 20% din totalul cheltuielilor bugetare pentru programele europene de cooperare în domeniul cercettării şi tehnologiilor. (Decizia Comitetului Director EDA la nivelul miniştrilor apărării din noiembrie 2007, http://www.eda.europa.eu).

În egală măsură, problema specializării a reprezentat unul dintre elementele constante ale dezbaterilor intra şi extrainstituţionale ale ultimului deceniu. Trebuie precizat faptul că soluţia a întârziat să apară, progresele înregistrate, în special, la nivelul Alianţei Nord-Atlantice, nefiind suficient de vizibile pentru a justifica o concluzie pozitivă. Rămâne de văzut în ce măsură implementarea acestui principiu la nivel european va funcţiona. Particularitatea cadrului european, în raport cu al NATO, poate să genereze oportunităţi suplimentare în implementarea cu succes a unui astfel de demers.

Alături de aceste aspecte, inventarul problemelor care vor alcătui agenda cooperării structurate include şi palierul angajamentelor operaţionale, mai precis parametrii forţelor alocate pentru operaţiilor UE. Şi în acest caz, la nivel european se constată o amplă fragmentare, pornind de la nivele superioare ale procesului de planificare şi până la zonele de detaliu ale procesului de generare a forţelor. Ca şi în cazul celorlalte aspecte aferente cooperării structurate, obiectivul pe acest palier îl vizează armonizarea procedurilor naţionale, menţionată explicit[14] în textul Tratatului, aspect de o importanţă majoră pentru statele implicate. În acest context, trebuie menţionat faptul că elemente iniţiale ale unei abordări standardizate au fost deja implementate la nivelul procedurilor naţionale ca urmare a necesităţii de a gestiona criteriile reclamate prin operaţionalizarea Grupurilor de Luptă. Acestea sunt, însă, limitate doar la palierul decizional, privind angajarea în cadrul unei operaţii, dar se poate anticipa o extindere a acestui tip de abordare în contextul apariţiei formulelor de cooperare structurată.

Concluzii

Este evident faptul că apariţia Tratatului de la Lisabona va influenţa în mod semnificativ procesul de dezvoltare a componentei de securitate şi apărare a Uniunii Europene. Inovaţiile introduse prin intermediul noului Tratat sunt de natură să contribuie la „rafinarea" acestui proces. În acest context, Cooperarea Structurată Permanentă reprezintă unul dintre instrumentele prin intermediul căruia valenţele integratoare ale procesului menţionat se vor contura într-un mod mult mai pronunţat ca până acum.

Stadiul incipient al procesului de implementare a noilor prevederi ale Tratatului de la Lisabona nu permit, încă, o evaluare exhaustivă asupra întregului set de implicaţii pe care acestea le vor genera. În ceea ce priveşte formulele de cooperare structurată, aceste aspecte sunt departe de a fi clarificate, putând fi anticipate doar o serie relativ limitată de implicaţii, detalierea procedurală a

[14] Treaty on the Reform of European Union, Protocol on Permanent Structured Cooperation, Art.2, para.(c), http:///europa.eu/lisbon_treaty/full_text/index_en.htm.

prevderilor aferente acestui instrument urmând să ofere elementele suplimentare de analiză.

Cu toate acestea, analiza cadrului conceptual furnizat prin intermediul Tratatului oferă o perspectivă clară asupra scopului formulelor de cooperare structurată, anume acela de a contribui la consolidarea dimensiunii „europene" a procesului de articulare a componentei de securitate şi apărare a Uniunii. În acest cadru, inventarul de obiective oferă, chiar şi în linii generale, un tablou extrem de ambiţios al viitoarelor preocupări legate de definirea profilului acestei componente.

În egală măsură, apariţia cooperării structurate vine să răspundă unei necesităţi evidente pe care stadiul actual al procesului de dezvoltare a Politicii Comune de Securitate şi Apărare o reclamă, în condiţiile în care menţinerea sistemului interguvernamental comportă o serie de riscuri şi provocări majore. Din această perspectivă, Cooperarea Structurată poate fi considerată ca fiind un element catalizator al preocupărilor statelor membre în domeniul securităţii şi apărării europene care poate susţine acea masă critică necesară pentru promovarea unor iniţiative suplimentare.

Este evident faptul că implementarea unor astfel de formule nu va putea surmonta întregul set de deficienţe care afectează, în prezent, procesul de dezvoltare a PCSA. Cooperarea structurată este orientată, mai degrabă, asupra remedierii unor deficienţe de nivel strategic fiind, în acelaşi timp, un instrument menit să asigure continuitatea şi predictibilitatea procesului de dezvoltare a acestei politici.

Elementul de o importanţă deosebită este reprezentat de modalitatea concretă prin care se va asigura implementarea unei astfel de agende, acest aspect fiind definitoriu, de asemenea, pentru articularea profilului viitoarelor formule de cooperare structurată. Traiectoria pe care acestea se vor plasa este marcată de provocări şi, în egală măsură, de riscuri. În acest cadru, principala problemă o reprezintă identificarea modalităţilor de combatere a percepţiilor negative la adresa principiilor de bază ale acestui tip de formulă de cooperare. În mod evident, implementarea unor astfel de formule consacră o nouă realitate la nivelul Uniunii Europene, anume aceea a „*Europei cu mai multe viteze*" care se extinde, astfel, şi în domeniul securităţii şi apărării. Aceasta, însă, incumbă şi o doză substanţială de exclusivism, în special în ceea ce priveşte criteriile pe care statele care doresc să participe la acest gen de cooperare trebuie să le îndeplinească. Limitarea acestora, doar la un club elitist, este de departe riscul major pe care acest gen de formule îl presupun. Din această perspectivă, abordarea optimă trebuie să fie aceea a menţinerii caracterului transparent al acestor mecanisme, opţiune posibilă doar prin adaptarea setului de criterii de eligibilitate la realităţile şi experienţei componentei de securitate şi apărare a Uniunii Europene.

Fără îndoială, problema criteriilor este extrem de importantă în special din perspectiva modului de raportare a statelor membre faţă de inovaţiile Tratatului de la Lisabona, inclusiv cele relative la cooperarea structurată permanentă. În mod evident, elementul fundamental care a stat la baza adoptării acestei platforme a fost reprezentat de sprijinul politic al statelor membre, în special cele cu un profil consolidat în ceea ce priveşte dezvoltarea componentei de securitate şi apărare. Din această perspectivă, se poate anticipa o atitudine pozitivă a acestora în ceea ce priveşte articularea formulelor de cooperare structurată.

În egală măsură, pentru statele medii şi mici ale Uniunii Europene participarea în cadrul procesului aferent dezvoltării acestui tip de cooperare va reprezenta unul dintre obiectivele fundamentale, opţiunea neparticipării nefiind de natură să genereze avantaje de susţinere a propriilor interese de securitate. Din această perspectivă, problema criteriilor de eligibilitate comportă semnificaţii suplimentare pentru acest tip de state membre.

Din perspectiva României, în calitate de membru, relativ nou al Uniunii Europene, problema participării în cadrul formulelor de cooperare structurată va constitui un demers natural, o etapă logică a participării consistente în cadrul procesului de dezvoltare a componentei europene de securitate şi apărare, încă din etapele sale iniţiale. Contribuţiilor cu forţe şi capacităţi pe care România le-a pus la dispoziţia Uniunii Europene, inclusiv în cadrul diferitelor operaţii de management al crizelor derulate de aceasta, li se adaugă participarea în cadrul procesului de reflecţie vizând adoptarea cadrului strategic de orientare a PSCA. În acest context, România a fost unul dintre principalii susţinători ai Tratatului de la Lisabona, inclusiv în ceea ce priveşte componenta de securitate şi apărare.

Toate aceste aspecte sunt de natură să ofere elementul de susţinere al unei implicări de substanţă a României în procesul de implementare a prevederilor Tratatului de la Lisabona, inclusiv în ceea ce priveşte reconfigurarea instituţională a noii arhitecturi a Uniunii Europene.

BIBLIOGRAFIE

BISCOP, Sven, *Permanent Structured Cooperation and the Future of ESDP*, Egmont Papers No.20, Royal Institute for International Relations, Bruxelles, 2008.

BISCOP, Sven&ALGERI, Franco, *The Lisbon Treaty and ESDP: Transformation and Integration*, Egmont Papers No.24, Royal Institute for International Relations, Bruxelles, 2008.

ERICKSEN, Olaf, *Developing a Constitution for Europe,* Routledge, Londra, 2004
HOWORTH, John, *The Security and Defence Policy in the European Union*, Palgrave Macmillan, Londra, 2007.
LAURSEN, Finne, *The Rise and Fall of the EU's Constitutional Treaty*, Leiden Nijhoff, 2008.
LINDSTROM, Gustav, *Enter The EU Battlegroups,* Institute for Security Studies, European Union, Paris, 2007.
Treaty on the Reform of European Union, http://www.europa.eu
Treaty Establishing a Constitution for Europe, http://www.european-convention.eu.int
European Defence: core documents (vol. I-IV), European Union Security Studies Institute, Paris.

Revista de Ştiinţe Militare

EDITOR
Secţia de Ştiinţe Militare
a
Academiei Oamenilor de Ştiinţă
din România

CONSILIUL EDITORIAL
PREŞEDINTE DE ONOARE
general (r.) prof. univ. dr. H.C. Vasile CÂNDEA

PREŞEDINTE
general (r.) prof. univ. dr. Eugen BĂDĂLAN

VICEPREŞEDINTE
general-locotenent prof. univ. dr. Teodor FRUNZETI

REFERENŢI ŞTIINŢIFICI
general-locotenent prof. univ. dr. Teodor FRUNZETI
general de brigadă (r.) prof. univ. dr. Viorel BUŢA
contraamiral fl. (r) prof. univ. dr. Marius HANGANU

MEMBRI
amiral prof. univ. dr. Gheorghe MARIN
general (r) prof. univ. dr. Anghel ANDREESCU
general de flotilă aeriană prof. univ. dr. Florian RĂPAN
general de brigadă (r.) prof. univ. dr. Viorel BUŢA
locotenent-colonel dr. Cristophe MIDAN, Franţa
colonel (r) dr. Costinel PETRACHE
general (r) prof. univ. dr. Mircea MUREŞAN
general (r) dr. Mihail POPESCU
general (r) conf. univ. dr. Constantin DEGERATU
dr. Karina MARCZUK, Polonia
prof. univ. dr. Adrian GHEORGHE, SUA
colonel (r) prof. univ. dr. ing. Eugen SITEANU

COLEGIUL DE REDACŢIE
Redactor-şef
Colonel drd. Vasile ANGHEL
editura@unap.ro

Secretar general de redacţie
Locotenent-colonel Liviu-Vasile STAN

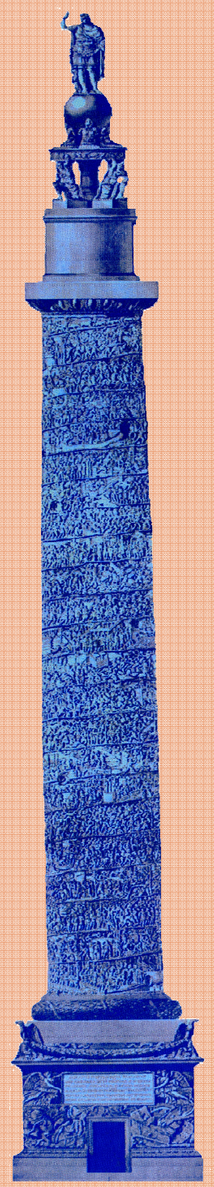
Redactori
Laura MÎNDRICAN
Mariana ROŞCA
Carmen IRIMIA

Tehnoredactor
Liliana ILIE

Tipar executat
la Editura Universităţii Naţionale de Apărare "Carol I"
Şoseaua Panduri, nr. 68-72, sector 5, Bucureşti
e-mail: editura@unap.ro
Tel./Fax: 319.59.69; 319.48.80/0215; 0307

Revista de Ştiinţe Militare *apare trimestrial*

COPYRIGHT: sunt autorizate orice reproduceri,
fără perceperea taxelor aferente, cu condiţia indicării
precise a numărului şi datei apariţiei revistei din care provin.



ÎN ATENŢIA COLABORATORILOR

Pentru o mai bună procesare a articolelor, dorim respectarea următoarelor reguli de tehnoredactare:

1. ***Textul.*** Se introduce în Microsoft Word, folosind fontul Times New Roman şi tastatura standard românească. Nu sunt acceptate fonturile care au mapări neobişnuite (în care caracterele cu diacritice - ş, ţ, ă, î şi Ş, Ţ, Ă, Î - înlocuiesc alte caractere - [,], @, ~, \ ş.a.m.d.). Textul în limba română trebuie să aibă în mod obligatoriu diacritice. Articolul trebuie cules, pur şi simplu, fără nicio altă formatare în afara sublinierilor, acolo unde este cazul, folosind bold şi italic. Paragrafele vor fi delimitate de un Enter, părţile articolului fiind separate între ele prin două-trei paragrafe goale.

2. ***Ecuaţiile.*** Indiferent de locul pe care îl ocupă în cadrul articolului, ecuaţiile se introduc numai în Microsoft Equation Editor. La limită, se acceptă ecuaţii scrise de mână, numerotate şi trimise separat de restul articolului).

3. ***Figurile.*** Sunt acceptate formatele vectoriale standard. în cazul figurilor produse cu o altă aplicaţie decât Microsoft Word (de exemplu, Corel Draw sau în AutoCAD), fişierele respectivelor aplicaţii vor fi trimise împreună cu restul articolului. Figurile trimise în format electronic vor fi desenate la dimensiunile la care pot fi tipărite, iar dimensiunea textului trebuie să fie între 8 şi 12 puncte tipografice. Sunt acceptate şi figuri desenate de mână, pe foi separate de restul articolului, cu condiţia ca desenele să fie clare şi să poată fi uşor identificat locul din cadrul articolului în care trebuie să se regăsească.

4. ***Imaginile.*** Imaginile scanate trebuie incluse atât în documentul Microsoft Word, cât şi trimise separat. Nu se recomandă folosirea imaginilor preluate de pe Internet, deoarece acestea nu satisfac cerinţele necesare pentru tipărirea lor (având o rezoluţie mult inferioară celei necesare pentru un tipar de calitate). Imaginile de calitate au o rezoluţie de minimum 200 dpi. Pentru formatele JPEG şi GIF, aveţi în vedere ca, în urma compresiei, calitatea imaginii să devină rezonabilă.

5. ***Numerotarea.*** Ecuaţiile, figurile, tabelele, titlurile din bibliografie vor fi numerotate cu cifre arabe, astfel:

- între paranteze pătrate pentru bibliografie;
- între paranteze rotunde pentru formule;
- prin exponent, în cazul notelor de subsol;
- precedate de denumire, în cazul observaţiilor, figurilor, tabelelor etc.

Rugăm autorii să redacteze articolele atât în limba română, cât şi în limba engleză.

Vă mulţumim ! *Redacţia*

Pentru publicarea de materiale promoţionale în cuprinsul revistei,
rugăm agenţii economici şi pe toţi cei interesaţi să se adreseze redacţiei
pentru a conveni forma de colaborare.

Coperta I: Dimitrie Cantemir, domnitor al Moldovei între anii 1710-1711
Sursă: enciclopedia wikipedia
Coperta II: *Columna lui Traian*. Sursă: Muzeul Militar Naţional,
prin amabilitatea domnului Neculai Moghior, şeful Secţiei Documentare.
Coperta IV: Fotografii reprezentându-l pe inginerul român Henri Coandă şi invenţia sa, primul avion cu motor aeroreactiv
Sursă: enciclopedia wikipedia

B. 989/2010 C. 301/2010