MANAGEMENTUL SECURITĂŢII INFRASTRUCTURILOR CRITICE

CRITICAL INFRASTRUCTURE SECURITY MANAGEMENT

Colonel (r) prof. univ. dr. Eugen SITEANU*
Colonel (drd.) Nicolae Zavergiu**

***Rezumat**: Războiul hibrid din Ucraina a readus în atenţie problema securităţii în Zona Extinsă a Mării Negre şi, evident, a porturilor din această zonă. Cercetarea noastră îşi propune să analizeze securitatea IC în noile condiţii ale mediului de securitate, în care câteva state membre ale UE manifestă o atitudine de apropriere de Federaţia Rusă, ceea ce a produs îngrijorarea statelor din Zona Extinsă a Mării Negre.*

***Cuvinte-cheie:** securitatea IC, analiza, riscuri, ameninţări şi pericole*

***Abstract**: Hybris War in Ucraine has brought again into the spotlight the security issue in the Extended Black Sea Area and, certainly, the security of critical infrastructure in this area. Our research aims at performing an analysis of critical infrastructure security in the new circumstances of the security environment, in which a few European Union member states manifest an attitude of closeness to the Russian Federation, triggering the deep concern of the states in the Extended Black Sea Area.*

***Keywords:** critical infrastructure security, analysis, risks, threats and dangers*

Managementul securităţii identifică ameninţările, analizează vulnerabilităţile infrastructurilor critice, înţelege modalităţile de producere a acţiunilor criminale şi a altor evenimente insecurizante şi acţionează diferenţiat, oportun şi eficace conform figurii nr. 1.

* Prof. univ. dr., membru corespondent al Academiei Oamenilor de Ştiinţă din România, consilier al preşedintelui Asociaţiei Naţionale a Cadrelor Militare în Rezervă şi în Retragere „Alexandru Ioan Cuza", vicepreşedintele Asociaţiei Absolvenţilor Universităţii Naţionale de Apărare „Carol I", membru în consiliul editorial şi redactor şef al Revistei de Ştiinţe Militare.

** Şef Birou Siguranţă - Midia, Compania Naţională Administraţia Porturilor Maritime SA, Constanţa, 0730.019.398, email: nzavergiu@constantza-port.ro

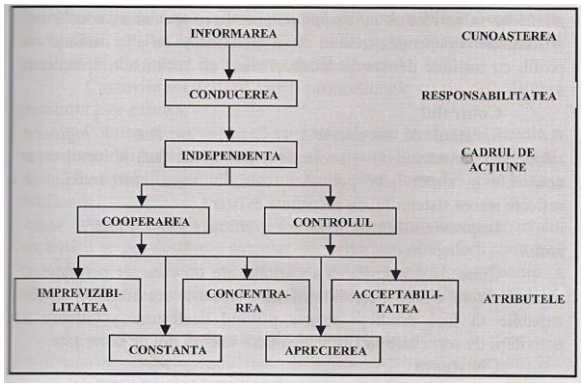

Figura nr. 1. Principiile de organizare a managementului securităţii

Din figura nr. 1 reiese că managementul securităţii trebuie să cuprindă: informarea, conducerea, independenţa (activitatea personalului de securitate este independentă de ierarhia obişnuită a instituţiei), cooperarea, controlul, imprevizibilitatea (confidenţialitatea perfecţionării securităţii), constanţa, concentrarea, aprecierea (evaluarea) şi acceptabilitatea.

Orice IC* poate fi considerată sau tratată/analizată ca un sistem în conformitate cu teoria generală a sistemelor. În procesul de construire şi dezvoltare a IC, în funcţie de cerinţele care trebuie să le satisfacă şi condiţiile impuse acestora, apare un decalaj între momentul construcţiei sau un moment al dezvoltării lor şi cel al datei curente/actuale; decalajul este cu atât mai mare cu cât între primul moment şi ultimul există o diferenţă mai mare de timp. Decalajul este o consecinţă de tehnologie, timp şi a altor factori care determină comportări periculoase ale sistemului (IC) dacă asupra sa acţionează forţe perturbatoare/distrugătoare care pot afecta oamenii, instalaţiile şi alte echipamente sau materiale. Aceste forţe perturbatoare/distrugătoare nu acţionează numai în viaţa reală, ci şi în mediul (realitatea) virtual(ă), adică în mediul digital (cibernetic), dar efectele lor se manifestă tot în realitate.

De aceea este necesară analiza specială a securităţii sistemelor (IC) pe baza teoriei fiabilităţii şi viabilităţii IC şi unor metode noi.

În literatura de specialitate apar multe concepte de securitate: „securitatea oportună *(opportune security),* securitate suficientă (*sufficient security),* securitate totală *(total security),* securitate, maximală *(maximum security),* securitate absolută *(absolute security),* securitate durabilă *(durable security)* sau securitate vitală *(vital security)* - ca o extensie a conceptului de dezvoltare durabilă *(vitală)* -

* IC-infrastructură critică (infrastructuri critice)

securitate optimală *(optimum security),* securitate minimală *(minimum_security)* sau securitate obligatorie *(obligatory security)* şi altele.[1]

Securitatea IC este o problemă atât funcţională, cât şi socială, deoarece insecuritatea poate produce pagube, dar şi sustrageri sau denaturări ale informaţiilor.

Trebuie să se înţeleagă că scopul realizării unei IC nu este doar obţinerea unei structuri în sine, ci a structurii care să asigure capacitatea operaţională de a realiza, în securitate/siguranţă, efectele tehnico-economice-sociale şi militare proiectate/dorite. Dar trebuie să avem mereu în vedere faptul că încă nu se poate asigura o protecţie integrală împotriva acţiunilor teroriste pentru o IC, dar se pot micşora efectele unor atacuri teroriste cu un consum rezonabil de resurse şi în primul rând cu un consum de resurse financiare. Depistarea locurilor vulnerabile/slabe, păstrarea unei vigilenţe permanente şi cunoaşterea perfectă a măsurilor de securitate pot asigura creşterea nivelului de securitate a IC.

Nicolae Dolghin, Alexandra Sarcinschi şi Mihai Dinu, în lucrarea Riscuri şi ameninţări la adresa securităţii României. Actualitate şi perspectivă, apărută în anul 2004, consideră că sunt trei categorii de riscuri şi ameninţări la adresa securităţii naţionale, militare şi riscuri asimetrice şi transnaţionale.

Prin conceptul de fiabilitate se înţelege capacitatea unei IC de a-şi îndeplini funcţiunile specificate în timp, dacă este utilizată în condiţii pentru care a fost construită (şi modernizată) şi este întreţinută şi reparată corect. Rezultă că fiabilitatea (F) unei IC are două componente: siguranţa în funcţionare (S) şi mentenanţă (M); matematic aceasta se scrie[2]:

$$F=S+M, \tag{1}$$

Fiabilitatea este analizată în funcţie de conexiunile, cauzele, factorii care o influenţează, efectele şi comportarea subsistemelor componente şi de interacţiunile dintre ele.

Pe baza teoriei fiabilităţii şi Teoriei Generale a Sistemelor (TGS) se poate deduce relaţia:[3]

$$F = \sum_{i=1}^{K} p_i \cdot F_i + F' \tag{2}$$

unde:

k – nr. subsistemelor componente;

F_i – fiabilitatea subsistemului i;

[1] Gheorghe Ilie, *Risc şi securitate,* volumul I, Editura UTI Press, Bucureşti, 2015, p. 11.

[2] Eugen Siteanu, Bedros Năianu, Gheorghe Ilie, *Fiabilitatea produselor tehnice*, Ed. AISTEDA, Buc., 2000, p. 125.

[3] Gheorghe Ilie, *Risc şi securitate,* volumul I, Editura UTI Press, Bucureşti, 2015, p. 17.

p_i – ponderea funcţională a subsistemului i;
F' – o componentă datorită organizării sistemului

Rezultă că fiabilitatea este o caracteristică de calitate a oricărei IC şi depinde de influenţa tuturor subsistemelor componente, dar şi de sinergia organizării IC; defectarea unui subsistem poate produce un defect al IC (o întrerupere a funcţionării, sau o eroare funcţională).

Între calitatea şi fiabilitatea IC este o conexiune organică întrucât calitatea înseamnă suma proprietăţilor necesare folosirii conform destinaţiei IC, iar fiabilitatea este capacitatea sa de a-şi menţine calitatea în timp (cu trecerea timpului). Rezultă că valoarea optimă a fiabilităţii corespunde costurilor minime destinate menţinerii Fiabilităţii (figura nr. 2).

Pe baza Fiabilităţii IC se defineşte Viabilitatea (V) acesteia astfel: „Capacitatea acesteia de a-şi conserva caracteristicile (funcţionale, de operativitate şi relaţional-informaţionale), în cazurile în care variaţiile mărimilor sale de intrare, perturbaţiile externe sau interne determină schimbări majore (sau consecinţe similare) ale condiţiilor pentru care a fost proiectată" [1].

Prin schimbări majore se înţeleg situaţiile (cazurile) de funcţionare în condiţii de excepţie (care au ca efecte întreruperile în funcţionare, erori de funcţionare sau excepţii). Excepţiile sunt unele abateri de la valorile normale ale parametrilor de funcţionare, iar deviaţiile de la acestea sunt considerate erori.

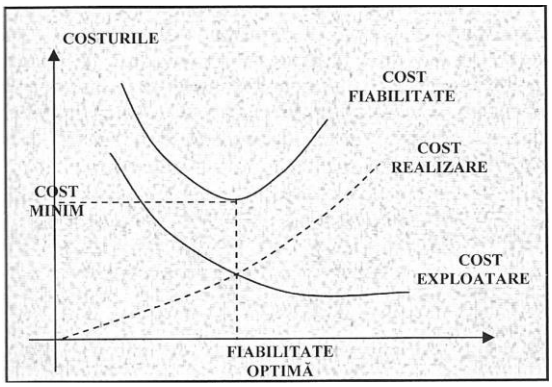

Figura nr. 2. Determinarea fiabilităţii optime a IC
Sursa: Gheorghe Ilie, Risc şi securitate, articole, comunicări, prelegeri, volumul 1, Articole publicate în revista Alarma, 2005-2011, Editura UTI Press, Bucureşti, 2015.

[1]Gheorghe Ilie, *Risc şi securitate,* volumul I, Editura UTI Press, Bucureşti, 2015, p. 19.

Viabilitatea (V) reprezintă suma reconfigurării/readaptării (Ra) şi rezervei de funcţionare (M') care este similară Mentenanţei (M) şi are expresia matematică[1]:

$$V=Ra+M' \quad (3)$$

sau: $$V = \sum_{i=1}^{K} q_i \cdot V_i + V' \quad (4)$$

unde:

V- viabilitatea sistemului;

k - nr. subsistemelor componente;

V_i- viabilitatea subsistemului i;

q_i - ponderea subsistemului i;

V' - o componentă datorată organizării sistemului

Între viabilitate şi fiabilitate există o legătură organică, la fel cum există între securitate şi viabilitate deoarece securitatea reprezintă proprietatea calitativa esenţială a sistemelor si organizaţiilor şi trebuie tratată pe baza tehnicilor de F şi V[2].

Securitatea este proprietatea calitativă esenţială a sistemelor (IC), capacitatea acestora de siguranţă în funcţionare, de a-şi conserva caracteristicile funcţionale împotriva riscurilor, ameninţărilor şi pericolelor prin evitare, atenuare sau remodelare şi de a se readapta[3] funcţional.[4]

Dar riscurile, ameninţările şi pericolele acţionează atât în realitate (viaţa reală), cât şi în mediul digital (cibernetic), efectele acestora manifestându-se însă asupra infrastructurilor critice.

În opinia noastră, securitatea IC reprezintă proprietatea calităţii esenţiale a sistemelor (IC), capacitatea acestora de a-şi conserva caracteristicile funcţionale împotriva riscurilor, ameninţărilor şi pericolelor prin evitare, atenuare sau Remodelare (Cv), de siguranţă în funcţionare (s) şi de a se readapta funcţional (Ra) la noile condiţii ale mediului de securitate.

Deci,

$$Sec = Cv+Ra+S \quad (5)$$

---

[1] Eugen Siteanu, Bedros Năianu, Gheorghe Ilie, *Fiabilitatea produselor tehnice*, Ed. AISTEDA, Buc., 2000, p. 128.

[2] Eugen Siteanu, Bedros Năianu, Gheorghe Ilie, *Fiabilitatea produselor tehnice*, Ed. AISTEDA, Buc., 2000, p. 123.

[3] Eugen Siteanu, Bedros Năianu, Gheorghe Ilie, *Fiabilitatea produselor tehnice*, Ed. AISTEDA, Buc., 2000, p. 130.

[4] Gheorghe Ilie, *Risc şi securitate, articole, comunicări, prelegeri,* volumul 1, Articole publicate în revista Alarma, 2005-2011, Editura UTI Press, Bucureşti, 2015, p. 22.

Cu cât riscul operaţional asumat (Ri) este mai mic, valoarea de prag optim economic (A) a sistemului de securitate este mai mare şi de asemenea valoarea securităţii IC este mai mare (R=1-A).

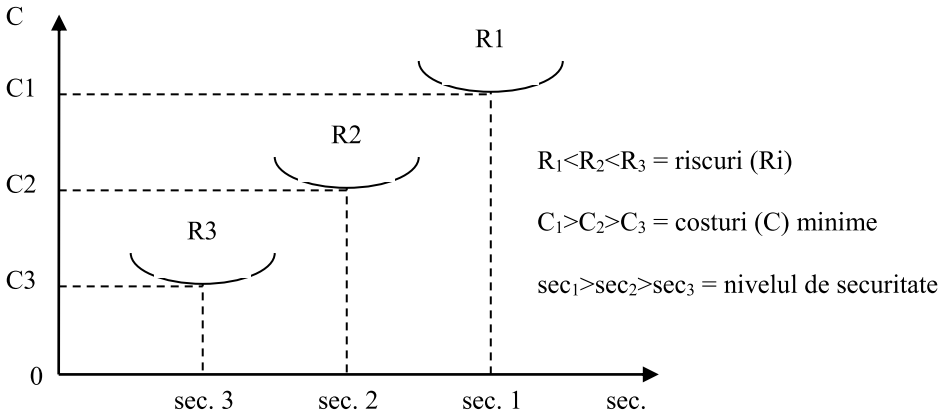

Figura nr. 3. Determinarea securităţii optime a IC

De asemenea, securitatea IC se mai poate exprima astfel[1]:

$$Sec = \sum_{i=1}^{n} m_i \cdot S_i + Sc \qquad (6)$$

unde:

n = numărul domeniilor care contribuie la securitatea IC (economic, social, cultural, religios, politic, militar, medical, tehnic, ştiinţific, alimentar, energetic etc.)

S_i = securitatea domeniului i

m_i = ponderea domeniului i;

Sc = componenta datorată caracteristicilor sistemului de securitate;

Dacă se iau în consideraţie numai acele domenii care contribuie la securitatea IC, rezultă că securitatea fiecărui domeniu (subsistem) influenţează securitatea IC cu o anumită pondere (care este determinată de locul pe care aceasta îl deţine în sistemul de securitate). Excepţiile de la funcţionarea normală a sistemului (IC) sau erorile, indiferent de natura acestora, pot produce defecţiuni, deteriorări şi disfuncţii ale IC.

[1] Ibidem, p. 23.

La fel ca şi în cazul fiabilităţii şi viabilităţii, valoarea securităţii IC depinde de costuri (cheltuielile destinate securităţii), putându-se determina o valoare optimă a acesteia (pentru costurile minime), în funcţie de costuri şi riscul asumat.

Rezultă că în funcţie de costuri şi de riscurile asumate, dinamica securităţii corespunde curbelor din figura nr.2.

Analiza securităţii IC ne-a condus la concluzia că măsurile şi mecanismele de securitate sunt perisabile în timp din cauza uzurilor sau îmbătrânirii morale a tehnologiilor utilizate astfel încât, dacă nu se iau periodic măsuri de mentenanţă şi de înlocuire a vechilor tehnologii, orice mecanism sau sistem de securitate poate fi la un moment dat compromis.

BIBLIOGRAFIE

SITEANU Eugen, NĂIANU Bedros, ILIE Gheorghe, *Fiabilitatea produselor tehnice*, Ed. AISTEDA, Bucureşti, 2000.

ILIE Gheorghe, *Risc şi securitate, articole, comunicări, prelegeri,* volumul 1, Articole publicate în revista Alarma, 2005-2011, Editura UTI Press, Bucureşti, 2015.

ILIE Gheorghe, *Risc şi securitate,* volumul I, Editura UTI Press, Bucureşti, 2015.