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

MILITARY AND SPECIAL COMMUNICATIONS AND INFORMATION SYSTEMS AND NETWORKS, AS VITAL PART OF ROMANIAN CRITICAL INFRASTRUCTURES. PROVIDING THEIR PHYSICAL AND INFORMATIONAL PROTECTION

Gl. mr. (r) prof. cons. dr. Constantin MINCU*

Rezumat: *În articol autorul prezintă, pe scurt, câteva argumente privind necesitatea studierii teoretice şi aplicative a problematicii infrastructurilor critice în România, incluzând desigur şi sistemele şi reţelele de comunicaţii militare şi speciale, cu rol vital în asigurarea securităţii şi apărării naţionale într-o lume tot mai agitată.*

Sunt prezentate într-o manieră concisă câteva sisteme, precum şi locul şi rolul acestora în conducerea şi administrarea ţării şi a structurilor militare naţionale.

Autorul insistă asupra problematicii complexe a protecţiei fizice şi informaţionale a sistemelor menţionate, în condiţiile creşterii vertiginoase a vulnerabilităţilor şi ameninţărilor interne şi externe din zilele noastre.

Sunt formulate şi câteva concluzii şi propuneri pentru decidenţii politici şi militari actuali şi pentru cei din viitorul apropiat.

Cuvinte-cheie*: Infrastructuri critice; sisteme de comunicaţii; sisteme informatice; război informaţional; NATO; Uniunea Europeană.*

Abstract: *In this article, the author briefly presents some arguments on the need for theoretical and application study of Romanian critical infrastructures topic also including the military and special communication systems and networks vital for the provisioning of national security and defence in the increasingly dynamic world.*

There are presented in a concise manner some systems, as well as their place and role in the leadership and management of the country and the national military structures.

* Membru titular al Academiei Oamenilor de Ştiinţă din România, Membru în Consiliul Onorific al AOŞ-R, secretar ştiinţific al Secţiei de Ştiinţe Militare, Tel.: 0722.303.015, E-mail: mincu_constantin@yahoo.com.

The author insists on complex issue of physical and informational protection of the above mentioned systems under the circumstances of emergent growth of internal and external vulnerabilities and threats in the recent days.

There are also formulated some conclusions and proposals for actual and future political and military decision-makers.

Keywords: *critical Infrastructures; communications systems; information systems; informational war; NATO; European Union.*

1. Argument pentru abordarea temei

Infrastructuri critice sunt 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 făcând obiectul studiilor, planurilor şi acţiunilor unor organizaţii internaţionale (ONU, NATO, UE).

Conceptul **„infrastructura 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 inter-relaţionate[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” s-a dovedit 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 Strategia Naţională de Securitate a Spaţiului Cibernetic (The National Strategy 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].

[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.

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 industrializate, 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 propune decidenţilor politici şi celor din administraţie elaborarea unui cadru normativ (legi, Hotărâri de Guvern etc.), urmat de punerea, cât mai urgentă 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.

În cele ce urmează mă voi referi numai la **sistemele informaţionale militare şi speciale existente în România,** în sensul cunoaşterii, la modul general al acestora, protecţiei fizice şi informaţionale în situaţiile unor atacuri, calamităţi naturale majore sau altor situaţii periculoase.

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],** care are loc tot timpul la pace, criză sau război, cu efecte grave asupra funcţionării lor in siguranţă, fapt care induce în mod direct dereglarea sau compromiterea totală a altor sisteme (subsisteme) servite: conducerea politică şi administrativă, apărarea naţională,

[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,* Editura Militară, Bucureşti, 2009; Teodor Frunzeti, *Securitatea naţională şi războiul modern,* Editura 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 vulnerabilitate pentru infrastructurile critice ale societăţii informatice – societatea cunoaşterii.*

siguranţa ţării şi a populaţiei, sistemele economice, financiar-bancare şi cele care privesc utilităţile vitale (energie, apă, alimente etc.). În acest context trebuie subliniate şi analizate elementele războiului informaţional în contextul crizei din Ucraina.

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

a. Sistemele de comunicaţii şi informatice militare

Sistemele de comunicaţii şi informatice militare au constituit şi continuă să constituie **elemente vitale în exercitarea comenzii şi controlului** la toate eşaloanele armatei, începând cu nivelul strategic şi până la luptător. Numeroşi autori, în principal militari, au produs 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, avere care trebuie protejată fizic şi informaţional faţă de multiple vulnerabilităţi şi ameninţări, se cuvine să reamintim câteva aspecte, să le spunem teoretice şi metodologice:

- **Sistemele C4I (+variante)** şi fiecare din acestea 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.

Fără a intra în detalii vom prezenta principalele subsisteme componente ale C4I (+variante). Acest lucru îl consider potrivit deoarece în „Revista de Ştiinţe Militare" au fost explicate pe larg componentele, funcţiile şi modul de folosire al acestor subsisteme:

- comandă şi control;
- comunicaţii;
- informatic (hardware şi software);
- informaţii (cercetare)
- ISR (diverşi senzori interconectaţi la centrele de comandă şi la sistemele de arme).

- **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 1990-2014, atât cât s-a putut în condiţii politice şi economice dificile şi de multe ori ostile. Aceste infrastructuri extrem de importante pentru apărarea ţării vor fi prezentate, pe scurt, în capitolul următor.

b. Sistemele de comunicaţii şi informatice speciale

Telecomunicaţiile speciale reprezintă **un segment** a ceea ce se numesc **telecomunicaţiile de stat** destinate asigurării unor comunicaţii securizate de voce şi date pentru autorităţile publice ale statului român Parlament, Preşedinţie, Guvern etc.:

Aceste sisteme şi reţele speciale se caracterizează prin acoperire naţională, un înalt 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.

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

3.1. 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 inter-categorii şi inter-forţe, 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).

Consider că o ameninţare majoră o reprezintă iresponsabilitatea unor decidenţi politici şi militari din M.Ap.N. care au lipsit de resurse minime de mentenanţă reţeaua mentenanţă, în perioada 2008-2014 (poate fi socotită o subminare a capacităţii de apărare a ţării cu iz penal).

Se pot face analize de risc de ordin general şi punctual şi propune măsuri concrete de protecţie (parte din ele vor fi prezentate în cap. 4).

- **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.

3.2. 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.

- **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 telefonice 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 Preşedinţie, Guvernul României şi Instituţia Prefectului.

- **Infrastructura sTESTA** 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.

4. 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

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

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 constea, cu precădere, în distrugerea totală a tehnicii, armamentului sau forţei vii a adversarului ci, mai ales, în neutralizarea şi dezintegrarea 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[8] 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 (o mare atenţie trebuie acordată propriului personal);

- afectarea infrastructurii informaţionale, ceea ce determină dificultăţi în managementul acesteia, imposibilitatea detectării accesului fraudulos la informaţii şi favorizarea atacurilor cibernetice (în ultimii doi ani atacurile cibernetice împotriva României s-au intensificat);

- 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

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

reţelele de comunicaţii ale acestora, ceea ce favorizează acţiunile teroriste şi criminalitatea organizată împotriva ţării noastre (acţiuni asupra unor instituţii ale statului, asupra sistemelor financiar-bancare);

- dependenţa infrastructurii sistemelor informaţionale pentru securitatea naţională de infrastructura informaţională comercială a ţării, ceea ce creează condiţii pentru acces fraudulos şi dezinformare (Statul Major General trebuie să analizeze gradul de dependenţă);.

- 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. Consider necesar ca decidenţii politico-militari să dezvolte capacităţi de comandă şi control pentru situaţia în care sistemele automatizate complexe vor cădea;

- 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 si 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 (sunt multe state care dispun de aceste capabilităţi);

- 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 (Statul Islamic îşi planifică şi conduce acţiunile prin Internet);

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

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

- 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 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 (în Armata Română se înţelege mai greu această realitate).

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 (încă suntem în epoca de pionerat);

- 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 (din nou – mare atenţie);

- securitatea redusă a datelor şi informaţiilor pe timpul transmiterii, memorării, prelucrării şi afişării acestora, accesul neautorizat 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, regulamente 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 si 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 în-greuierea 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;

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

- 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. Să luăm act că în conflictul din Ucraina, Federaţia Rusă a folosit, pe larg şi eficient, mare parte din acţiunile radioelectronice şi cibernetice, inclusiv atacul psihologic.

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 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, arrne 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.

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

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.

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.

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

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 si 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.

Fig. 1. *Principalele măsuri de protecţie a informaţiilor în sistemele informaţionale*

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 si zona administrativă.

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

Se va organiza o evidenţă strictă asupra documentelor clasificate si 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;
- remanenta 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;
- 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 permanentă şi corectă, 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 electrică 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 principală a tuturor specialiştilor din domeniile informaţiilor, comunicaţiilor şi informaticii, întrucât globalizarea ameninţărilor la adresa acestora poate produce efecte dezastruoase, ce afectează grav securitatea naţională.

De aceea, proiecţia sistemelor informaţionale privind securitatea naţională trebuie să aibă în vedere ansamblul mijloacelor tehnice al 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, datorită 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

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

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 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 măsura defensivă absolut necesară în toate situaţiile.

5. 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 din 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.

- studierea acţiunilor de război informaţional desfăşurate în ultimele conflicte, inclusiv în cazul crizei din Ucraina cu implicarea masivă a Federaţiei Ruse.

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, 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, Bucureşti, 2006;

ANDERSON H. Robert, *Physical Vulnerabilities of Critical US Information Systems* (internet, Iaver May 03.pdf);

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.

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.

MINCU Constantin, GREU Victor, ROTARIU Costel, *Salt de frecvenţă şi contrasalt de frecvenţă*, Editura Militară, Bucureşti, 1998;

MUREŞAN M., VĂDUVA Gh., *Războiul viitorului, viitorul războiului,* Editura UNAp, Bucureşti, 2005;

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:

Gândirea Militară Românească, anii 2001-2014;

Buletinul Universităţii Naţionale de Apărare "Carol I", 2008-2014;

Revista Forţelor Terestre, anii 2005-2014;

Impact Strategic, anii 2006-2014;

Revista de ştiinţe militare, anii 2006 – 2014;

Romanian Military Thinking Journal, anii 2005 – 2014.