



**SISTEME ȘI REȚELE DE COMUNICAȚII ȘI INFORMATICI
MILITARE ȘI SPECIALE, CA PARTE VITALĂ
A INFRASTRUCTURILOR CRITICE ALE ROMÂNIEI.
ASIGURAREA PROTECȚIEI FIZICE ȘI INFORMAȚIONALE
A ACESTORA**

**MILITARY AND SPECIAL COMMUNICATION AND
INFORMATICS SYSTEMS AND NETWORKS AS VITAL PART OF
CRITICAL INFRASTRUCTURE OF ROMANIA. THEIR PHYSICAL
AND INFORMATIONAL PROTECTION**

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

Rezumat: *Articolul prezintă argumente privind necesitatea de a studia infrastructura critică din România, incluzând diverse sisteme (rețele), precum și comunicațiile militare speciale. Totodată, subliniază rolul și locul unor astfel de sisteme și rețele pentru apărarea și securitatea națională și scoate în evidență riscurile și vulnerabilitățile cu care se confruntă aceste infrastructuri, precum și unele măsuri necesare a fi luate pentru protecția fizică și informațională, în cazul acțiunilor militare ostile, dezastre naturale sau alte fenomene negative.*

În final, sunt formulate câteva concluzii și propuneri.

Cuvinte-cheie: *infrastructuri critice, sisteme, rețele de comunicații, protecție fizică, protecție informațională.*

Abstract: *The article presents some arguments on the necessity to study the critical infrastructure in Romania including different systems (networks), as well as special military communications. Although, it underlines the role and place of such systems and networks used for the national defence and security and emphasizes the risks and vulnerabilities these infrastructures confront with as well as some measures needed for the physical and informational protection in situations of hostile military actions, natural disasters or other negative phenomena.*

At the end, there are formulated some conclusions and propositions

Keywords: *critical infrastructures, systems, communication networks, physical protection, informational protection.*

* Membru Titular al Academiei Oamenilor de Știință din România, membru al Consiliului Onorific al Academiei Oamenilor de Știință din România, secretar științific al Secției de Științe Militare. Telefon: 0722.303.015, E-mail: mincu_constantin@yahoo.com.



Argumente pentru abordarea temei

Infrastructurile critice – resurse vitale pentru buna funcționare a societății (asigurarea siguranței vieții cetățenilor, a bunurilor materiale de bază, a serviciilor publice cele mai importante) sunt de câțiva ani buni în atenția responsabililor politici, economici și militari din mai multe țări ale lumii și face obiectul studiilor, planurilor și acțiunilor unor organizații internaționale (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 Protecția Infrastructurilor Critice (Executive Order Critical Infrastructure Protection).

Apreciindu-se că securitatea, economia și chiar supraviețuirea lumii industrializate ar fi esențial dependente de trei elemente strâns interrelaționate¹: **energia, comunicațiile și computerele** – actul normativ explica și definea atunci infrastructura critică² ca fiind „parte din infrastructura națională care este atât de vitală încât distrugerea sau punerea ei în incapacitate de funcționare poate să diminueze grav apărarea sau economia SUA³”.

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

În **Strategia Națională de Securitate a Spațiului Cibernetic** (The National Strategy to Secure Cyberspace) sunt nominalizate **la infrastructuri critice**: „instituiții publice și private din sectoarele agriculturii, alimentației, aprovizionării cu apă, sănătății publice, serviciilor de urgență, guvernării, **industrii de apărare, informațiilor și telecomunicațiilor**, energiei, transporturilor, sistemelor bancare și financiare, chimice și a materialelor periculoase, precum și cele poștale și de navigație”⁴.

Și la nivelul **NATO** și al **Uniunii Europene** sunt preocupări concrete pentru a defini infrastructurile critice și pentru a propune soluții concrete de protecție a acestora în fața unor atacuri ostile sau a unor calamități naturale de amploare.

Problematica infrastructurilor critice a fost și este dezbătută în continuare de numeroși specialiști civili și militari, din multe țări ale lumii industrializate,

¹ http://en.wikipedia.org/wiki/critical_infrastructure_protection

² <http://www.whitehouse.gov/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



rămânând o problemă deschisă, atât pentru analiză și fundamentare teoretică, cât și pentru acțiune practică, în actele de bună guvernare.

Trebuie să remarc că și numeroși specialiști români s-au aplecat cu convingere, cu bune rezultate în plan științific și acțional, pentru a defini concepte, pentru a inventaria cu acuratețe infrastructurile critice ale României și pentru a propune decidenților politici și celor din administrație elaborarea unui cadru normativ (legi, hotărâri de Guvern etc.), urmat de punerea, cât mai urgent în practică a măsurilor principale, în mod deosebit pentru rețelele vitale (energie, apă, sisteme informaționale, sisteme de transport, sisteme financiar-bancare)⁵.

Atât specialiștii străini, cât și cei români, civili și militari, care au analizat domeniul infrastructurilor critice, au acordat o mare atenție rolului și locului sistemelor informaționale complexe (globale, zonale, naționale, militare, speciale, comerciale, private etc.) în asigurarea vieții normale a populației, în funcționarea economiilor, a sistemelor financiar-bancare, a securității și apărării naționale și a conducerii politice și administrative a unui stat, alianțe sau uniuni politico-economice.

Trebuie să arăt că acest gen de sisteme și rețele de comunicații și informatice sunt tratate de mulți autori ca **subiect al războiului informațional**⁶, la pace, criză sau război, cu efecte grave asupra funcționării lor în siguranță, fapt care induce în mod direct dereglarea sau compromiterea totală a altor sisteme (subsisteme) servite: conducerea politică și administrativă, apărarea națională, siguranța țării și a populației, sistemele economice, financiar-bancare și cele care privesc utilitățile vitale (energie, apă, alimente etc.).

⁵ Autori și lucrări:

Dr. Grigore Alexandrescu, Dr. Gheroghe Văduva, *Infrastructuri critice, pericole, amenințări la adresa acestora, sisteme de protecție*, Editura U.N.Ap. Carol I, București, 2006;

George Dediu, Alexandru Manafu, *Protecția infrastructurilor critice – o nouă provocare*, Editura U.N.Ap. Carol I, București, 2006;

Dr. Constantin-Gheorghe Balaban, *Infrastructurile critice, un domeniu care se cere investigat*, Revista Geopolitică, Anul VI – nr. 27, pp. 49-55.

⁶ Autori și lucrări:

Radu Dan Septimiu Popa, *Războiul informațional și securitatea națională*, Ed. Militară, București, 2009;

Teodor Frunzeti, *Securitatea națională și războiul modern*, Ed. Militară, București, 1999;

M. Mureșan, Gh. Văduva, *Războiul viitorului, viitorul războiului*, Editura U.N.Ap. Carol I, București, 2006;

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

Adrian V. Gheorghe, *Analiza de risc și de vulnabilitate pentru infrastructurile critice ale societății informatice – societatea cunoașterii*.



Locul și rolul sistemelor de comunicații și informatice militare și speciale în cadrul infrastructurii critice

a. Sistemele de comunicații și informatice militare au constituit și continuă să constituie elemente vitale în exercitarea comenzii și controlului la toate eșaloanele armatei, începând cu nivelul strategic și până la cel luptător. Numeroși autori, în principal militari, au elaborat cărți, studii, analize, proiecte, manuale și articole în care au demonstrat locul și rolul sistemelor complexe de tipul C4I (+ variante) într-un război modern, demonstrând totodată, pe lângă calitățile lor tehnice și operaționale și vulnerabilități reale ce decurg din metodele și procedeele războiului informațional modern, dar și cele care sunt create de calamități naturale majore, accidente grave, erori de proiectare și realizare sau erori umane.

Pentru a înțelege mai bine care este „averea” disponibilă în acest moment în armata noastră care trebuie protejată fizic și informațional față de multiple vulnerabilități și amenințări, se cuvine să reamintim câteva aspecte, să le spunem teoretice și metodologice.

- **Sistem C4I (+variante)** nu este privit ca un singur sistem, ci mai mult ca un **sistem de sisteme** în care fiecare sistem produce și/sau consumă servicii. C4ISR reprezintă integrarea doctrinelor, procedurilor, structurilor organizaționale, personalului, echipamentelor tehnice și produselor software, facilităților, comunicațiilor și cercetării pentru a sprijini abilitatea comandantului de a realiza comanda și controlul de-a lungul întregii game de operații militare. C4ISR asigură comandanții cu date oportune și precise și sisteme pentru planificare, monitorizare, conducere, control și raportarea desfășurării operațiilor.

- **Subsistemul de comandă și control** constă din facilitățile, echipamentele, procedurile și personalul esențiale pentru un comandant în planificarea, comanda și controlul forțelor subordonate și primite în sprijin pentru îndeplinirea misiunii.

- **Subsistemul de comunicații** reprezintă un ansamblu de echipamente, metode, proceduri și personal (dacă e necesar), organizat pentru a îndeplini funcțiile de transfer a informațiilor. Cuprinde sisteme de transmisie, de comutație și de utilizator. Poate îndeplini și funcții de stocare și prelucrare în sprijinul transferului de informații.

- **Subsistemul informatic (de calculatoare)** constituie un ansamblu de echipamente, metode, proceduri și personal (dacă e necesar), organizat pentru a îndeplini funcțiile de prelucrare a informațiilor. Poate transfera informații în sprijinul funcțiilor de prelucrare (de exemplu: în cadrul rețelelor locale de calculatoare).

- **Sistemul de informații (cercetare)** – echipamente, metode, proceduri și personal pentru realizarea produselor informative prin colectarea, prelucrarea,



integrarea, evaluarea, analiza și interpretarea informațiilor la dispoziție privind forțele ostile sau potențial ostile, zonele actuale sau potențiale de acțiune.

- **ISR** – sistem care colectează și prelucrează informații pentru realizarea produselor informative despre amenințări și mediu pe timpul operațiilor, precum și informații pentru identificarea, urmărirea și angajarea țintelor.

- **Arhitectura sistemelor C4ISR** trebuie să fie abordată din trei puncte de vedere (operațional, sistemic și tehnic) concomitent cu relațiile dintre ele. **Din punct de vedere operațional**, arhitectura se referă la centrele rețelei, misiunilor și sarcinile realizate, informațiile care trebuie vehiculate pentru îndeplinirea misiunii (tipul, frecvența, misiunile și activitățile sprijinite, natura acestora). **Din punct de vedere sistemic** sunt analizate: sistemul în ansamblu, serviciile și funcționalitatea interconectării asigurate pentru sprijinul activităților operaționale prin schimbul de informații între centrele rețelei. **Din punct de vedere tehnic** este analizat setul minim de reguli care guvernează organizarea, interacțiunile și interdependențele dintre părțile (elementele) sistemului în scopul satisfacerii cerințelor operaționale. Aceasta cuprinde o serie de standarde tehnice, rutine de implementare, selecția standardelor, regulilor și criteriilor care pot fi organizate, în ce gestionează sistemul sau serviciile elementelor pentru o arhitectură dată.

- **Sistemele menționate**, cu funcțiile lor prezentate pe scurt, sunt reprezentate pe teren de o serie de rețele și facilități tehnice și operaționale realizate în perioada 1990-2010, atât cât s-a putut în condiții politice și economice dificile.

b. Sistemele de comunicații și informatice speciale

Telecomunicațiile speciale reprezintă un segment a ceea ce se numesc telecomunicațiile de stat (anexa nr. 1) destinate asigurării unor comunicații securizate de voce și date pentru autoritățile publice ale statului român:

- Parlamentul României;
- Președinția României;
- Guvernul României;
- instituțiile care desfășoară activități în domeniul apărării, siguranței naționale și ordinii publice;
- administrația publică centrală și locală;
- autoritatea judecătorească:
 - Curtea Supremă de Justiție;
 - Ministerul Public;
 - Consiliul Superior al Magistraturii;
- Curtea de Conturi;
- Curtea Constituțională;
- organele de conducere din cadrul organismelor guvernamentale și al unor organisme neguvernamentale de interes național.



Aceste sisteme și rețele speciale se caracterizează prin acoperire națională, un înalt grad de protecție și confidențialitate și prin măsuri fizice și informaționale de protecție față de diferite riscuri și situații potențial periculoase.

Denumirea de „telecomunicații speciale” a fost adoptată în 1993 din considerentul delimitării lor de sfera telecomunicațiilor publice ori private, precum și al particularizării acestora în cadrul telecomunicațiilor de stat.

Specificitatea rețelelor de telecomunicații speciale este dată atât de modul de organizare a infrastructurii, cât și de organizarea serviciilor.

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

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

Prezentarea, pe scurt, a unor sisteme și rețele de comunicații și informatice militare și speciale, cu rol vital în asigurarea securității și apărării țării

Infrastructura IT&C a M.Ap.N

În perioada 1991 – 2010 în armata României a fost proiectată, realizată și dezvoltată Rețeaua de Transmisiuni Permanentă (R.T.P) care reprezintă o rețea distribuită, încorporând, din punct de vedere operațional și tehnic, 253 de centre de comunicații cu diferite dezvoltări, de la cele nodale principale, până la modulele desfășurabile în teatrele de operații și extensiile externe pentru comunicațiile cu NATO și UE. Această rețea, parte principală a Sistemului de Transmisiuni al Armatei României (STAR), asigură infrastructura de bază (staționară) pentru comunicații multicanal (voce, date, videoconferință) pentru conducerea operațională și administrativă a tuturor structurilor armatei la pace, criză și război. Are o dezvoltare geografică națională, fiind extinsă în aproape toate orașele reședință de județ și în alte numeroase locații unde sunt unități și interese de ordin militar.

Rolul de **infrastructură critică** a acestei rețele derivă din funcțiile ei în folosul conducerii strategice, operative și tactice și din resursele puse la dispoziție pentru cooperarea intercategorii și interforțe, precum și cele necesare unor proiecte cu mare valoare militară pentru apărare (de exemplu pentru SCCAN și SCOMAR). Pe lângă aceste calități operaționale și tehnice rețeaua are și unele vulnerabilități în ceea ce privește asigurarea funcționării sigure și neîntrerupte în condițiile în care ar



putea fi supusă unor acțiuni ostile prin atacuri fizice sau radioelectronice, prin mijloacele cunoscute ale războiului informațional (cu toate formele sale active și pasive).

Se pot face analize de risc de ordin general și punctual și propune măsuri concrete de protecție.

Rețeaua de Comunicații de Sprijin de Campanie (R.C.S.C) asigură infrastructura mobilă pentru comunicații multicanal, fiind destinată pentru refacerea unor tronsoane RTP distruse sau scoase din funcțiune temporar sau/și pentru extinderea RTP în zone încă neacoperite pentru puncte de comandă.

Rețeaua Radio cu Servicii Integrate (R.R.S.I) asigură echipamentele și procedurile pentru comunicații monocanal utilizând stații radio HF și VHF cu salt de frecvență, cu dispozitive de criptare pentru voce și date.

Sistemul Criptat de Videoconferință (V.T.C) asigură servicii de videoconferință criptate utilizând ca suport de comunicații RTP/RMNC. Beneficiarii sunt structurile principale de conducere ale M.Ap.N. și S.M.G.

Sistemul de comunicații prin satelit (S.C.S) asigură suportul de comunicații în locații greu accesibile, izolate sau îndepărtate (în teatrele de operații din străinătate – Irak, Afganistan etc.).

Sistemul de comunicații și informatică desfășurabil (S.C.I.D) asigură servicii de voce și date pentru forțele dislocabile în teatrele de operații, precum și pentru conectarea acestora la Sistemul NATO General de Comunicații (N.G.C.S).

Sistemele de comunicații mobile Tetra Dimetra sunt destinate să asigure unele comunicații mobile pentru structurile centrale ale M.Ap.N și S.M.G, categoriile de forțe ale armatei și comandamentele operaționale și de armă precum și cooperarea cu structuri din sistemul național de apărare, îndeosebi în situații de urgență în baza prevederilor Legii nr. 363/2004.

Toate sistemele și rețelele menționate fac parte din infrastructura critică a M.Ap.N și, în consecință, trebuie luate măsuri de protecție fizică și informațională, potrivit standardelor actuale valabile în NATO și UE.

Infrastructura de comunicații speciale de conducere și cooperare din administrarea S.T.S

- **Infrastructura de telecomunicații integrate de capacitate mare, redundată, cu puncte de prezență în capitală și în reședințele de județ.** Aceasta se bazează pe echipamente profesionale în tehnologii moderne, care utilizează pentru transport rețelele de fibră optică și radiorelee.

Capacitățile de transport sunt suficiente pentru asigurarea comunicațiilor între reședințele de județ și București în perspectiva următorilor ani pentru toate nevoile exprimate de către autorități. Această infrastructură de telecomunicații integrate asigură servicii de comunicații pentru rețele de voce, date și video.



Într-un termen scurt infrastructura radioreleu proprie va fi extinsă până la nivelul municipiilor, orașelor și localităților în care există entități ale autorităților publice.

- **Infrastructura de radiocomunicații mobile** constă în rețelele locale convenționale și în sistemele profesionale în tehnologiile TETRAPOL și TETRA-DIMETRA și furnizează servicii în regim de mobilitate pentru autoritățile publice cu atribuții în domeniul siguranței cetățeanului și securității naționale.

În prezent, utilizatorii serviciilor platformei comune TETRA-DIMETRA sunt: Ministerul Administrației și Internelor (Poliția Română, Poliția de Frontieră, Inspectoratul General pentru Situații de Urgență, Jandarmeria Română, Instituția Prefectului), Serviciul Român de Informații, Ministerul Sănătății – serviciile medicale de urgență (serviciul de ambulanță, SMURD), Ministerul Finanțelor Publice (Autoritatea Națională a Vămirilor), primăriile (Poliția Comunitară), Ministerul Apărării Naționale și Serviciul de Protecție și Pază.

- **Infrastructura pentru servicii de comunicații de date**

Infrastructura rețelei integrate de mare capacitate permite realizarea unor rețele naționale securizate de arie extinsă pentru autorități. Beneficiari mai importanți: Ministerul Finanțelor Publice, Ministerul Justiției și Libertăților Cetățenești, Ministerul Administrației și Internelor, Ministerul Apărării Naționale, Ministerul Agriculturii, Pădurilor și Dezvoltării Rurale, Ministerul Mediului, Ministerul Afacerilor Externe și Ministerul Muncii, Familiei și Protecției Sociale. Rețeaua este securizată și criptată conform standardelor NATO.

- **Infrastructura pentru servicii Internet**

Dezvoltată în urma nevoilor exprese ale instituțiilor publice și componentelor SNAOPSN (Sistemul Național de Apărare, Ordine Publică și Siguranță Națională) în condițiile în care serviciile de Internet au devenit o componentă principală a funcționării oricărei instituții a statului.

- **Infrastructura pentru servicii satelitare**

A fost dezvoltată ca alternativă la serviciile oferite de infrastructura terestră și pentru asigurarea serviciilor de comunicații în cazul misiunilor temporare, în locurile unde infrastructura terestră nu oferă servicii. Prin intermediul acestei infrastructuri sunt asigurate în mod operativ serviciile de telecomunicații pentru gestionarea situațiilor de urgențe oriunde situația impune prezența autorităților și forțelor de intervenție, iar serviciile rețelelor terestre nu sunt disponibile.

Prin infrastructura satelitară se asigură continuitatea conducerii statului în situații de calamități sau dezastre, în situațiile în care rețele terestre nu mai sunt funcționale, precum și pe durata activităților oficiale în străinătate ale conducerii statului. Infrastructura este disponibilă pentru utilizarea de către componentele de urgență ale autorităților publice.



- **Infrastructura pentru servicii telefonice** include comutatoarele telefonice și rețeaua de cabluri telefonice proprii, prin care sunt oferite serviciile telefonice speciale „S” și „TO”, precum și serviciile de cooperare IC.

Aspectele care necesită acordarea unei atenții deosebite care privesc această infrastructură sunt cele generate de schimbarea tehnologiilor în rețelele de acces ale operatorilor care furnizează servicii conexe, de asigurare a protecției comunicațiilor în acest mediu public, precum și de costurile ridicate ale acestui tip de suport.

- **Infrastructura de servicii video** funcționează pe infrastructura de comunicații integrate și asigură serviciile de videoconferință securizată pentru Guvernul României și Instituția Prefectului.

- **Infrastructura TESTA** a fost dezvoltată în baza Deciziei nr. 387/2004 a Comisiei Europene, sub forma unei rețele destinate susținerii proiectelor de interes comun și pentru oferirea unei platforme de comunicații protejate și fiabile destinată schimbului de date între administrațiile publice la nivel european.

- **Infrastructura de chei publice (PKI)** realizată de S.T.S se adresează instituțiilor componente ale SNAOPSN și autorităților publice.

- **Infrastructura de protecție a telecomunicațiilor speciale** asigură serviciile de securitate a telecomunicațiilor speciale și de cooperare prin:

- descoperirea, identificarea, localizarea și înlăturarea surselor de perturbării accidentale (analiza problemelor de interferență) sau intenționate (emisii neautorizate) și asigurarea disponibilității frecvențelor radio din gestiunea S.T.S.;

- executarea de controale tehnice a rețelelor de telecomunicații speciale în vederea asigurării confidențialității comunicațiilor speciale;

- zonarea locațiilor pentru prevenirea scurgerii de informații clasificate secrete de stat prin intermediul radiațiilor electromagnetice compromițătoare emise de echipamentele S.T.S.

- **Sistemul național unic pentru situații de urgență – 112** extins până la nivelul tuturor municipiilor și orașelor din România.

Toate sistemele și rețelele menționate necesită un proces amănunțit de analiză a vulnerabilităților de ordin fizic și informațional în vederea identificării unor măsuri eficiente de protecție.

Protecția fizică și informațională a sistemelor și rețelelor militare și speciale în condițiile manifestării unor acțiuni de război informațional, producerii unor dezastre naturale și a altor fenomene negative

Vulnerabilități și amenințări informaționale pentru securitatea națională:

Ca în orice domeniu de activitate, și în cel privind informațiile și sistemele informaționale pentru securitatea națională există anumite vulnerabilități, adică părți mai puțin studiate și slăbiciuni ale sistemului, infrastructurii, mediului de



control sau proiectării rețelelor, care nu sunt generate de acțiunile adversarilor, ci de soluțiile proprii adoptate, ce pot fi atacate relativ ușor și exploatare pentru a deteriora integritatea aceluia stat.

Vulnerabilitățile informaționale constituie o componentă a **vulnerabilității de securitate**⁷, generată de stări de fapt, procese sau fenomene din viața internă a comunității naționale, care diminuează capacitatea de reacție a societății la riscurile existente ori potențiale de orice natură, inclusiv informaționale sau care favorizează apariția și dezvoltarea acestora, cu consecințe privind realizarea securității naționale.

În general, vulnerabilitățile informaționale sunt cu atât mai mari, cu cât rețelele informaționale și structura informațiilor sunt de complexitate mai mare, fiind greu de optimizat, administrat și protejat. De asemenea, vulnerabilitățile sporesc direct proporțional cu nivelul tehnologic implementat în construcția și funcționarea echipamentelor (mai ales digitale) sistemelor informaționale.

Rezultă că obiectivul principal al conflictelor militare contemporane nu trebuie să fie acela de distrugere totală a tehnicii, armamentului sau forței vii a adversarului, ci, mai ales, de neutralizare și dezintegrare a sistemelor complexe ale acestuia, în principal a sistemelor informaționale. În acest context, s-a impus tot mai mult conceptul de **infrastructuri critice ale țării** de care depind¹⁸ stabilitatea, siguranța și securitatea sistemelor și 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 securității, în funcționarea sistemelor și în derularea proceselor economice, sociale, politice, informaționale și militare. Caracterul critic al unor infrastructuri, în principal informaționale, este determinat, mai ales, de condiția de unicat a unui sistem sau proces, de rolul său în funcționarea stabilă a infrastructurii și de vulnerabilitățile acesteia.

Siguranța națională, apărarea țării și ordinea publică constituie domenii importante ale infrastructurilor critice, în care se mai regăsesc structurile aferente tehnologiei informației și comunicațiilor, rețelele administrației de stat, diplomatice, energetice, de transport, de alimentare cu apă, sistemul financiar și medical.

Principalele vulnerabilități ale infrastructurii informaționale privind securitatea națională, apreciem că ar putea fi următoarele:

- posibilitățile de interceptare a informațiilor din rețelele de comunicații și calculatoare atât de către utilizatori, cât și de adversar;

⁷ *Doctrina națională a informațiilor pentru securitate*, Editura SRI, București, 2004.

⁸ Gr. Alexandrescu, Gh. Văduva, *Infrastructuri critice. Pericole, amenințări la adresa acestora. Sisteme de protecție*, Editura UNAp, București, 2006



- volumul foarte mare de informații produse, vehiculate și prelucrate în sistemele informaționale, care pot fi supuse cercetării și atacului adversarilor potențiali, distruse, falsificate sau sustrase;

- afectarea infrastructurii informaționale, ceea ce determină dificultăți în managementul acesteia, imposibilitatea detectării accesului fraudulos la informații și favorizarea atacurilor cibernetice;

- folosirea aceluiași benzi de frecvență, modulații și regimuri de lucru la echipamentele bazate pe propagarea undelor electromagnetice, atât în rețelele de comunicații proprii, cât și în cele ale adversarilor potențiali;

- utilizarea de echipamente tehnice, componente software și baze de date cu structuri și exploatare standardizate (comerciale) în toate rețelele de calculatoare din organizațiile implicate în securitatea națională, eventual și în rețelele de comunicații ale acestora, ceea ce favorizează acțiunile teroriste și criminalitatea organizată împotriva țării noastre;

- dependența infrastructurii sistemelor informaționale pentru securitatea națională de infrastructura informațională comercială a țării, ceea ce creează condiții pentru acces fraudulos și dezinformare;

- posibilitatea încorporării (ascunderii) din timp, în echipamentele de calcul și de comunicații, de către firmele furnizoare de aparatură, a unor module software malițioase, care pot fi activate de către adversari la momente hotărâte de aceștia, creând dezordine și haos în rețelele informaționale și cele decizionale;

- prin conectarea la Internet, Intranet sau Extranet, organizațiile de care depinde securitatea națională devin vulnerabile la pătrunderi neautorizate (cu rea intenție sau din neatenție);

- existența unor rețele informaționale cu număr mare de noduri și cu o largă interconectivitate, greu de sincronizat și gestionat, ceea ce permite penetrarea acestora, accesul neautorizat, capturarea fizică a unor echipamente sau a unor noduri (centre) de comunicații în totalitate, interceptarea sau întreruperea unor fluxuri de informații importante și/sau introducerea de informații false care să afecteze procesele decizionale;

- digitalizarea exhaustivă a structurii informaționale a securității naționale are un impact contradictoriu: pe de o parte, omogenizează, sincronizează și sporește gradul de compatibilitate și interoperabilitate a rețelelor informaționale pentru sistemul securității naționale, iar, pe de altă parte, determină stăpânirea cu greutate a complexității și a nivelului deosebit de ridicat de tehnicitate al acestora, oferind condiții pentru atacul cibernetic de la distanță sau din interiorul lor;

- nerespectarea integrală a cerințelor și standardelor Uniunii Europene și NATO privind compatibilitatea și interoperabilitatea sistemelor informaționale, mai ales în ce privește schimbul de informații (formatul mesajelor), accesul la



bazele de date, criptarea automată a comunicărilor și caracteristicile canalelor pentru legătură;

- posibilitatea folosirii de către adversari potențiali a războiului electronic împotriva mijloacelor radioelectronice din principalele sisteme informatice și de comunicații, cu precădere asupra canalelor care asigură legătura surselor de informații cu organele centrale de fuziune și prelucrare a datelor;

- interceptarea de către adversar (forțele ostile) a comunicărilor transmise prin radio, decriptarea acestora în timp oportun în cazul folosirii unor sisteme criptografice neperformante și folosirea în scopuri proprii a acestor informații pentru obținerea superiorității informaționale asupra statului român;

- mijloacele tehnice actuale ale sistemelor informaționale nu au asigurată protecția deplină împotriva atacului fizic, electromagnetic și cibernetic, acestea putând fi distruse, deteriorate sau extrasă informația stocată;

- dispunerea în locuri necorespunzătoare, din punct de vedere funcțional și al securității fizice și electromagnetice a echipamentelor tehnice ale sistemelor informaționale, în principal a mijloacelor de comunicații și de calcul, ceea ce sporește vulnerabilitatea de interceptare a informațiilor și de atac fizic;

- utilizarea pentru exploatarea sistemelor informaționale privind securitatea națională a unor persoane insuficient verificate și neloiale, predispuse a fi racolate de către adversarii potențiali și determinate să efectueze acțiuni de sabotaj sau să furnizeze acestora informații obținute fraudulos;

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

- existența, la adversarii potențiali, a armelor electronice cu radiații infraacustice, bazate pe propagarea în spațiu a undelor subsonice, care acționează asupra personalului, determinând inactivarea acestuia anumite perioade de timp și, implicit, întreruperea funcționării sistemelor informaționale;

- instalarea antenelor mijloacelor de comunicații în câmp deschis sau în spații fără proprietăți naturale de protecție, ceea ce permite scoaterea lor ușoară din funcțiune și întreruperea legăturii, mai ales a celei cu stații radio și radioreleu de putere mare;

- suprimarea accesului la Internet al sistemelor informaționale privind securitatea națională, pentru izolarea acestora, în vederea împiedicării folosirii de către adversari și persoanele neautorizate a unor surse de documentare proprii, cuprinzând informații neclasificate;



- utilizarea Internetului pentru acțiuni teroriste⁹ de dezinformare și atac cibernetic asupra infrastructurii informaționale critice a securității naționale;
- proiectarea necorespunzătoare a infrastructurii, cu redundanță informațională redusă, centralizată excesiv și cu posibilități scăzute de replicare a informațiilor existente în bazele de date;
- preocuparea insuficientă pentru ascunderea și mascarea elementelor infrastructurii informaționale, măsuri neadecvate de pază și apărare a acestora;

Din prezentarea efectuată rezultă că există numeroase vulnerabilități, dar dintre acestea, esențiale sunt cele care împiedică: organizarea optimă a sistemelor informaționale, alegerea echipamentelor tehnice utilizate și a produselor software comerciale cu înalte performanțe funcționale, realizarea calitativă a programelor (software) de aplicații și a bazelor de date de către specialiștii organizațiilor privind securitatea națională, precum și a software-ului pentru criptarea automată, sigură, a informațiilor în sistemele informaționale, măsurile de securitate adoptate.

Organizarea optimă a sistemelor informaționale constituie condiția fundamentală pentru funcționarea eficientă a acestora pe timpul războiului informațional, iar reconfigurarea în timp real, mobilitatea și adaptabilitatea lor la mediul de informații în continuă dezvoltare și la situațiile și standardele ce trebuie avute în vedere, ca țară membră a Uniunii Europene și NATO, se impun a fi respectate în totalitate și aplicate cu fermitate pentru a se îndeplini condițiile de compatibilitate și interoperabilitate.

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

Adaptarea sistemelor la mediul de informații, mai ales în situații de criză și conflict militar, impune echiparea acestora cu mijloace tehnice capabile să suporte fluxuri informaționale de 2-3 ori mai mari decât în condiții normale de funcționare pe timp de pace.

Fiabilitatea sistemelor informaționale trebuie să fie proiectată astfel încât probabilitatea de funcționare fără defecțiuni a structurilor tehnice și informaționale să fie mai mare de 0.95, asigurându-se totodată o probabilitate redusă de detectare și interceptare a comunicărilor.

O atenție deosebită se va acorda organizării și exploatării optime a bazelor de date ale rețelelor de calculatoare.

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



Amenințări informaționale interne

Analiza efectuată evidențiază următorii factori interni, care pot constitui amenințări asupra sistemelor informaționale privind securitatea națională:

- lipsa de preocupare pentru dobândirea superiorității informaționale asupra statelor și forțelor potențial ostile;

- neconcordanța între cerințele de informații pentru luarea deciziilor și conducerea acțiunilor privind securitatea națională și posibilitățile reale de dobândire a acestora;

- proiectarea, organizarea sau funcționarea necorespunzătoare a sistemelor informaționale;

- dotarea sistemelor informaționale cu mijloace de culegere a datelor, comunicații și calculatoare neperformante, greu de exploatat și de asigurat protecția, utilizarea necorespunzătoare a acestora;

- influența mediului de securitate intern și internațional asupra proceselor informaționale ale structurilor de informații specializate ale statului și a cooperării acestora cu organe similare ale celorlalte țări membre ale Uniunii Europene și NATO;

- organizarea necorespunzătoare a bazelor de date, existența unor produse software neperformante sau cu erori intenționate pentru gestiunea, prelucrarea și afișarea informațiilor, lipsa de preocupare pentru utilizarea inteligenței artificiale, pentru realizarea activităților informaționale și a celor de management;

- slaba pregătire profesională și experiența redusă a personalului, implicat în organizarea, exploatarea și asigurarea funcționării sistemelor informaționale;

- clasificarea necorespunzătoare a categoriilor de informații și date privind securitatea națională și certificarea eronată a dreptului de acces la acestea a personalului;

- neloyalitatea unor persoane care exploatează echipamentele tehnice ale sistemelor informaționale;

- securitatea redusă a datelor și informațiilor pe timpul transmiterii, memorării, prelucrării și afișării acestora, accesul neautorizat al unor persoane străine.

Răspunderea pentru asigurarea superiorității informaționale asupra adversarilor potențiali și a altor forțe ostile revine șefilor structurilor de informații specializate, aceasta trebuind să fie urmărită cu consecvență atât pe timp de pace, cât și în situații de criză sau de conflict militar.

Fragilitatea superiorității informaționale este dată de calitatea informației de a fi obținută în timp real, cu forțele și mijloacele structurilor de informații specializate, precum și din surse deschise sau primite de la organele cu care cooperează. Caracterul nonlinear al acesteia determină ca mici intrări de informație



să poată produce efecte disproporționate 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 și instrucțiuni, a cerințelor de informații privind securitatea națională, diferențiat pe domenii de activitate și eșaloane ierarhice de conducere, a modalităților și răspunderilor pentru obținerea acestora, precum și a conținutului lor informațional, forma de prezentare și operațiile de prelucrare la care sunt supuse.

În acest sens, trebuie avut în vedere că implementarea tehnologiei moderne a informației și comunicațiilor, precum și a metodelor de management moderne constituie o componentă esențială a definirii forței.

Experiența dobândită privind asigurarea securității naționale a dovedit că organizarea necorespunzătoare a sistemelor informaționale, lipsa de preocupare pentru funcționarea acestora și înlăturarea defecțiunilor ce pot apărea, constituie cauza principală a lipsei de informații relevante și a imposibilității dobândirii superiorității informaționale. Trebuie să se aibă în vedere că informatica și comunicațiile moderne, deși au un rol hotărâtor, prezintă și numeroase vulnerabilități tehnologice care trebuie diminuate sau înlăturate prin măsuri organizatorice și tehnice adecvate.

Chiar dacă nu sunt supuse atacului informațional al adversarilor potențiali, bazele de date și software-urile pot crea neajunsuri serioase în cazul când nu sunt organizate, realizate și exploatate corespunzător. Principala răspundere pentru funcționarea lor eficientă revine personalului de specialitate din sistemul informațional, mai ales inginerilor, analiștilor și programatorilor, precum și operatorilor de la mijloacele de comunicații. Corelat cu aceasta, un impact major asupra informațiilor îl are realizarea unei securități reduse a informațiilor în toate verigile sistemelor informaționale, care creează posibilitatea de acces neautorizat și de transmitere la adversar a unor date, din cauza lipsei de loialitate a unor persoane care sunt implicate în vehicularea fluxurilor de informații.

Totodată, există și cauze tehnice care pot constitui amenințări informaționale interne, rezultate mai ales din dotarea necorespunzătoare cu echipamente moderne de culegere, transmitere și prelucrare a informației, precum și a unor loturi de rezervă pentru acestea.

Se impune, așadar, efectuarea unor cheltuieli importante pentru dotarea sistemelor informaționale cu tehnică modernă, pentru că succesul în realizarea securității naționale se obține cu un preț ridicat.

Amenințări informaționale externe

Amenințările informaționale externe cuprind ansamblul acțiunilor specifice, executate de adversarii potențiali și forțele ostile țării noastre pentru interzicerea sau îngreuierea executării funcțiilor decizionale și operaționale privind securitatea



națională. Acestea urmăresc limitarea sau excluderea activităților proprii privind culegerea de informații, deteriorarea sau distrugerea senzorilor și a altor surse de date și interzicerea funcțiilor informaționale privind securitatea națională.

Conform concluziilor formulate în literatura de specialitate¹⁰, principalele amenințări informaționale externe asupra structurilor decizionale și acționale privind securitatea națională sunt următoarele:

- atacul fizic împotriva surselor de date și a mijloacelor de transmitere, prelucrare și afișare a informațiilor;
- atacul electronic asupra mijloacelor de culegere, transmitere și prelucrare a informațiilor;
- atacul cibernetic împotriva sistemelor informaționale ale structurilor de informații pentru securitatea națională și cele ale organizațiilor economice, financiare, diplomatice etc.;
- pirateria software;
- atacul fizic și electronic asupra organelor decizionale ale statului nostru (președinție, parlament, guvern etc.) privind securitatea națională;
- atacul psihologic asupra tuturor structurilor decizionale și acționale ale țării noastre (politice, economice, sociale, de apărare etc.)

Aceste amenințări nu sunt noi, ele fiind generate de însăși dezvoltarea societății informaționale, dar trebuie cunoscute, studiate cu atenție și stabilite cu precizie măsurile corespunzătoare pentru combaterea lor.

Este cunoscut că obiectul culegerii de informații pentru securitatea națională constă în asigurarea cunoașterii exacte a situației internaționale, mai ales în zona de interes a României, Uniunii Europene și NATO, precum și a situației interne din țara noastră și din țările vecine, realizându-se astfel anticiparea acțiunilor agresive ale adversarilor potențiali sau ale unor grupuri ostile și prevenirea surprinderii.

În prezent¹¹ securitatea se identifică cu protecția a tot ceea ce afectează bazele înseși ale statului și organizațiilor internaționale la care am aderat și cu care executăm acțiuni în comun.

Această evoluție a modificat și obiectivele serviciilor de informații, care nu se mai concentrează atât de mult pe informații despre parametrii militari și strategici ai unor țări, cât mai ales pe aspecte și fenomene economice, sociale și politice a căror logică de acțiune răspunde unor modele și condiții diferite și, în special, cu mult mai imprevizibile decât în trecut.

Se dovedește că existența unor informații sigure, complete și oportune constituie suportul principal al conducerii și coerenței proceselor decizionale

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

¹¹ *Doctrina națională a informațiilor pentru securitate*, Editura SRI, București, 2004.



privind securitatea națională. De aceea, atacul fizic al adversarilor potențiali și grupurilor ostile împotriva surselor și mijloacelor pentru obținerea informațiilor constituie, probabil, principala vulnerabilitate pentru sistemele informaționale de orice natură, din țara noastră.

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

Apreciem că acest atac constituie amenințarea fizică principală asupra mijloacelor tehnice ale sistemelor informaționale existente la structurile de informații privind securitatea națională.

Protecția împotriva acestor arme, care atacă echipamentele tehnice și personalul sistemelor informaționale, are un rol hotărâtor pentru funcționarea neîntreruptă a mijloacelor electronice utilizate pentru culegerea, transmiterea, prelucrarea și diseminarea informațiilor.

Atacul cibernetic asupra structurii informaționale a securității naționale reprezintă o amenințare deosebit de importantă, care are în vedere „spațiul virtual” ce vizează mai ales produsele software și firmware, protocoalele și bazele de date ale sistemelor informatice utilizate în rețelele de calculatoare și de comunicații. Acțiunile externe specifice atacului cibernetic au în vedere reducerea însemnată a posibilităților de efectuare corectă a serviciilor în cadrul sistemului informațional, deteriorarea software-ului de aplicație ce are, de regulă, caracter confidențial sau secret, pentru a genera informații greșite din datele prelucrate.

Aceste amenințări externe sunt favorizate de neaplicarea unor reguli sigure de protecție și securizare a informațiilor pe timpul transmiterii și prelucrării datelor culese de către surse. Ele fructifică lacune și/sau slăbiciuni existente în structura sistemului de securitate a rețelelor proprii de comunicații și calculatoare.

Atacul cibernetic are legătură cu pirateria software¹², care poate fi desfășurată de agresori locali sau plasați în orice puncte din spațiul interconectat al informației și urmăresc, după caz, paralizarea completă a sistemelor informatice sau defectarea (căderea) lor intermitentă, la momente de timp dinainte stabilite.

Atacul cibernetic urmărește și deteriorarea programelor (sistemelor expert) folosite în procesele decizionale și acționale privind securitatea națională, ceea ce

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



depășește cu mult sfera informațională propriu-zisă și poate genera decizii greșite care, într-o formă sau alta, să avantajeze adversarii potențiali.

Atacul împotriva capacității de conducere a organelor centrale și locale ale țării urmărește neutralizarea sistemelor decizionale, personalului și tehnicii, precum și a comenzii structurilor operaționale subordonate acestora, pentru paralizarea activităților privind securitatea națională (siguranța cetățenilor, ordine publică, apărare, situații de urgență etc.) a celor economice, financiare, sociale etc. Este îndreptat asupra capacităților fizice și intelectuale ale conducătorilor, funcționarilor din administrația de stat și locală, personalului de ordine publică, apărare și intervenție în situații de urgență.

Ca metodă de acțiune, adversarii potențiali sau grupurile ostile pot folosi capturarea unora dintre persoanele de conducere, parlamentari, miniștri, diplomați, ofițeri superiori etc. pentru dezorganizarea diferitelor domenii de activitate și/sau atacul pentru influențarea stării biofizice a întregului personal pentru scoaterea lui definitivă sau temporară din activitățile desfășurate.

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

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

Existența în sistemele de asigurare a informațiilor și de comunicații ale sistemelor informaționale privind securitatea națională a unor radare, stații radio și radio-relee, care funcționează cu frecvențe radio de înaltă energie și folosesc antene cu câștig foarte mare, poate constitui un risc important pentru personalul de exploatare și unele categorii de aparatură electronică, în principal, calculatoare, din compunerea acestora. Rezultă că sistemele informaționale ale structurilor de stat privind securitatea națională pot avea unele vulnerabilități ce pot fi exploatare de către adversari sau grupuri ostile, dar și de persoane din interiorul acestora, rău intenționate.

Cunoașterea vulnerabilităților și amenințărilor informaționale permite luarea de măsuri severe, organizatorice și tehnice, pentru diminuarea sau înlăturarea completă a acestora.

Măsuri de protecție a sistemelor și rețelelor militare și speciale

Protecția sistemelor informaționale se referă la luarea unor măsuri speciale de apărare a datelor vehiculate prin acestea, prin intermediul echipamentelor de

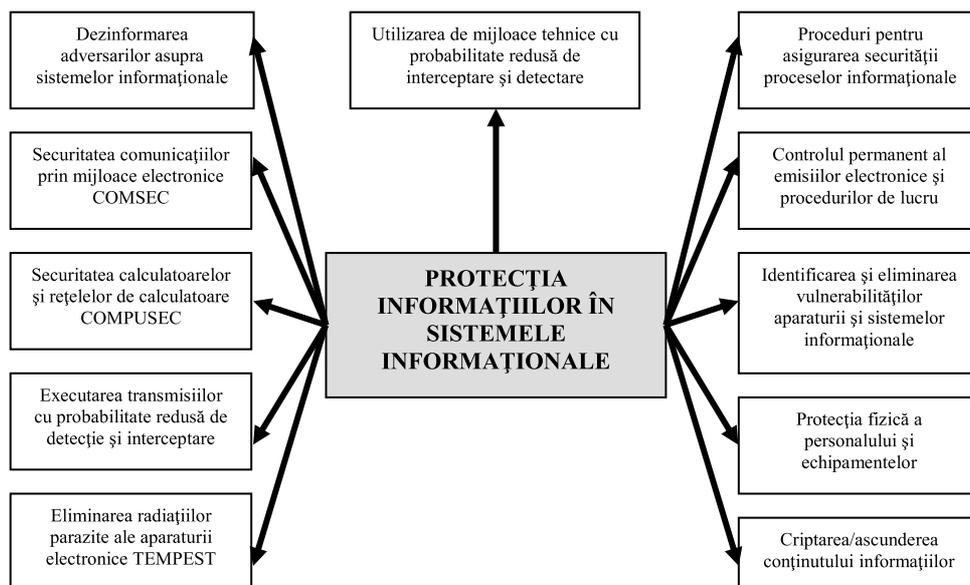


prelucrare automată a datelor, software de sistem și de aplicație, precum și al comunicațiilor.

Cinci valori patrimoniale ale sistemelor informaționale (echipamente, software, materiale, date, servicii) pot constitui ținta următoarelor amenințări: pierdere, respingere (nerecunoaștere), compromitere și corupere.

Securitatea sistemului informațional pentru securitatea națională depinde de dinamica sa, iar amenințările asupra acestuia sunt îndreptate împotriva structurilor organizatorice, echipamentelor, programelor de aplicație și sistemului de operare, materialelor utilizate în rețelele de calculatoare, informațiilor memorate pe diverse suporturi magnetice, hârtiilor de valoare aflate în sistem sau a serviciilor prestate de componentele acestuia.

Enumerarea principalelor măsuri de protecție a informațiilor¹³ în sistemele informaționale se prezintă în figura următoare:



În general¹⁴, amenințările privind securitatea sistemelor informaționale și a informațiilor vehiculate prin acestea pot fi grupate astfel:

- pierderea unor echipamente sau componente fizice;
- respingerea serviciilor;

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

¹⁴ D. Oprea, *op. cit.*, p. 38.



- folosirea neautorizată a echipamentelor;
- accesarea informațiilor clasificate;
- modificarea neautorizată a informațiilor;
- pierderea informațiilor;
- folosirea neautorizată a informațiilor;
- aflarea neautorizată a secretelor privind produsele software utilizate;
- modificarea neautorizată a programelor utilizatorilor;
- pierderea sau folosirea neautorizată a produselor software.

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

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

Preocupările pentru protecția informațiilor clasificate în sistemele informaționale s-au amplificat considerabil odată cu trecerea la prelucrarea automată a datelor, întrucât:

- densitatea informației este mult mai mare decât în sistemele clasice bazate pe hârtie, iar suporturile magnetice actuale (mai ales memory stick) cu capacități de ordinul zecilor de gigabaiți pot memora cantități foarte mari de informație, ce poate fi sustrasă cu relativă ușurință;

- dispărea transparența documentelor;

- accesarea datelor în sistemele de calcul moderne se poate efectua cu mai mare ușurință prin accesul neautorizat al unor persoane externe sau din cadrul organizației privind securitatea națională;

- eventualele atacuri cibernetice asupra sistemelor de calcul pe care sunt stocate informațiile sunt greu de depistat;

- remanența suporturilor magnetice, după ce au fost șterse, poate constitui o cale sigură de a reface informațiile înregistrate anterior;

- existența în memoriile calculatoarelor a informațiilor de sinteză (agregate) cu valoare decizională ridicată permite obținerea prin activități criminale a unor date utilizabile direct de către adversari;

- comunicațiile și rețelele de calculatoare au devenit tot mai performante, dar prezintă și vulnerabilități însemnate, ceea ce permite ca atacurile informaționale asupra acestora să se poată efectua în principal prin acțiuni cibernetice din orice loc de pe globul pământesc;



- standardele de securitate a informațiilor în sistemele informaționale existente nu permit o protecție sigură a acestora și necesită cheltuieli foarte mari și specialiști cu înaltă calificare, măsuri care sunt greu de realizat.

Mecanismele de protecție utilizate în sistemele informaționale trebuie să fie cât mai simple, ușor de întreținut, să ofere un număr cât mai mic de erori sau alarme false și să demonstreze completitudine, caracterizată printr-o funcționare normală la orice și corectitudine, prin oferirea răspunsurilor anticloate la înregistrarea unor intenții frauduloase. Mecanismul de protecție trebuie să aibă o perioadă cât mai mare de supraviețuire și să asigure permanent un nivel determinat al protecției. De asemenea, trebuie să ofere soluții de funcționare normală a echipamentelor sistemului informațional în situația întreruperii alimentării cu energie electrică a acestora, defectării sistemului de comunicații și variațiilor bruște ale temperaturii.

Apreciem că protecția componentelor sistemelor informaționale privind securitatea națională împotriva atacurilor informaționale, cu precădere împotriva celor electronice și cibernetice, trebuia să constituie preocuparea principală a tuturor specialiștilor din domeniile informațiilor, comunicațiilor și informaticii, întrucât globalizarea amenințărilor la adresa acestora poate produce efecte dezastruoase, ce afectează grav securitatea națională.

De aceea, proiecția sistemelor informaționale privind securitatea națională trebuie să aibă în vedere ansamblul mijloacelor tehnice a celor trei componente principale ale acestora, anume:

- subsistemul de asigurare a informațiilor;
- subsistemul de comunicații;
- subsistemul rețelelor de calculatoare (informatic).

Subsistemul de asigurare (culegere) a informațiilor este cel care dă semnificația și importanța sistemelor informaționale, întrucât el furnizează materia primă (date și informații) care privește securitatea națională.

Mijloacele tehnice moderne utilizate pentru culegerea informațiilor sunt numeroase și se bazează pe utilizarea celei mai înalte tehnologii rezultată din simbioza electronicii, comunicațiilor moderne și informaticii. Ca urmare, ele prezintă anumite vulnerabilități care pot fi exploatate în cadrul războiului informațional al adversarilor potențiali (reali), prin atacarea lor fizică, electromagnetică sau cibernetică.

Scoaterea din funcțiune a unora dintre acestea poate cauza întreruperea unor fluxuri informaționale, din cauza împiedicării funcționării surselor de informații, respectiv senzori, mijloace de ascultare și supraveghere, aparatură de goniometrare și de obținere a imaginilor etc. Principalul mijloc de protecție a acestora constă în



paza și apărarea lor neîntreruptă, precum și dispunerea echipamentelor în locuri (spații) protejate față de impulsurile electromagnetice și energiile de mare putere.

Protecția împotriva interceptării radiațiilor parazite

Radiațiile (emisiunile) compromițătoare sunt constituite din semnale neintenționate care, dacă sunt interceptate și analizate, asigură dezvăluirea conținutului informației transmise, recepționate, supuse prelucrării sau altor operațiuni în echipamentele sistemelor de comunicații și de calcul. Studiul efectuat asupra domeniului menționat este cunoscut sub denumirea de TEMPEST (Transient Electro Magnetic Pulse Emanation Standardizing), care definește ansamblul investigațiilor, studiilor și controlului asupra radiațiilor compromițătoare ale echipamentelor electronice.

Protecția¹⁵ împotriva interceptării și analizei radiațiilor parazite pe timpul funcționării acestora se realizează prin:

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

Protecția fizică a personalului și echipamentelor tehnice

Protecția fizică reprezintă o componentă importantă a managementului sistemului informațional, care se realizează prin monitorizarea umană și/sau electronică a zonei protejate, folosirea de bariere și proceduri standardizate, chei de control, documente de acces specializate, iluminări și alte soluții care interzic accesul neautorizat.

În general, protecția fizică trebuie să asigure:

- securitatea personalului și compartimentarea strictă a accesului la echipamentele de comunicații și de calcul;
- protecția împotriva acțiunilor de spionaj, sabotaj, defectare și furt;
- reducerea expunerii la amenințări care pot cauza refuzul serviciilor sau alterarea neautorizată a informațiilor;

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



- controlul și supravegherea continuă a echipamentelor și a locurilor de lucru ale personalului (monitorizarea video);

- reinscripționarea cheilor de criptare după fiecare oprire a echipamentelor criptografice;

- asigurarea pazei neîntrerupte și apărării punctelor cheie ale sistemelor de comunicații și rețelelor de calculatoare.

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

- selecția;

- verificarea prin prisma securității;

- supravegherea continuă;

- instruirea și conștientizarea.

Rezultă că protecția informațiilor și a sistemelor informaționale privind securitatea națională împotriva operațiilor informaționale ofensive ale adversarilor potențiali este o măsură defensivă absolut necesară în toate situațiile.

Concluzii și propuneri

Din tratarea teoretică a problematicii privind importanța doctrinară și acțională a războiului informațional în viziunea Alianței Nord-Atlantice și, implicit, în concepția de transformare a Armatei României, precum și a celei referitoare la asigurarea informațională a securității naționale rezultă, evident, unele concluzii, esențializarea acestora permițându-ne să apreciem că:

- informația este, fără îndoială, un element esențial al factorului de putere, oricare ar fi domeniul de manifestare, dar nu este suficientă deținerea ca atare a acesteia, utilizarea ei oportună confirmând, de fapt, eficacitatea și puterea utilizatorului informațional;

- în contextul extrem de alert al noii revoluții informaționale, revoluție care, practic, determină libertatea neîngrădită a cunoașterii în geopolitica globalizării, războiul informațional reprezintă componenta sau, după caz, dominantă oricărei confruntări, indiferent de domeniul în care se manifestă: social, militar, economic, fizic etc.;

- în actualul context informațional global, dar și al unei acerbe competiții desfășurate la nivelul tuturor subsistemelor sistemului social global, inclusiv, evident, a celui militar, războiul informațional este, deopotrivă, omniprezent, inevitabil și continuu;

- scopul organic al războiului informațional, în oricare dintre formele sub care se poate desfășura operațional-ofensiv sau defensiv, constă în dobândirea superiorității informaționale, cu consecințe în afirmarea superiorității/victoriei în domeniul căruia îi este subsumat, în cazul nostru, cel privind securitatea națională;



- imposibilitatea practică de a-l limita în vreun fel, ca arie de desfășurare, spațialitate și obiectivele urmărite, indiferent de domeniul în care se manifestă și în care este utilizat, conferă războiului informațional atributele spațiale ale globalizării, putând considera, pe drept cuvânt, că este, deopotrivă, vector și consecință a acesteia;

- în ceea ce privește armele și tehnicile utilizate în războiul informațional, acestea nu au nicidecum un caracter imuabil, dincolo de cele deja consacrate, fiind posibilă, în circumstanțe imprevizibile, apariția unor „arme”, instrumente și tehnici necunoscute încă de ducere a războiului informațional, inclusiv prin utilizarea unor noi principii ale fizicii;

- din perspectiva împlinirii tehnologiei postmoderne, războiul informațional pune în evidență atât virtuțile incontestabile ale revoluției informaționale, cât și limitele acesteia în contextul înfruntărilor care o exprimă deopotrivă;

- războiul informațional și informația, în sensul cognoscibil al practicii umane, sunt unii dintre vectorii cei mai determinanți ai noii revoluții în afacerile militare;

- în asigurarea informațională a securității naționale, resursele informaționale au un rol decisiv, calitatea și oportunitatea acestora relevând capacitatea structurilor de informații ale statului, precum și nivelul de racordare instituțională la rigorile aplicate ale revoluției informaționale;

- conținutul informațiilor care alimentează afirmarea complexă a securității naționale este extrem de eterogen, practic nedefinit și neprincipializat doctrinar, motiv pentru care, în perspectiva coagulării sistemice a acestei problematice, apreciem că este util să se procedeze la sistematizarea criterială coerentă a acestora;

- eficiența asigurării informaționale a securității naționale depinde, decisiv, de capabilitățile decizionale ale structurilor instituționale împuternicite cu asemenea responsabilități;

- explozia informațională, fără precedent, ca amploare și anvergură, în istoria umanității, îngreuiază obținerea conținutului util al informațiilor prin care asigurăm securitatea națională, realitate care impune utilizatorilor avizați ai informațiilor dobândite, un discernământ profesional desăvârșit;

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

- detalierea conceptului de război informațional, în accepțiunea utilizării sale pentru asigurarea securității naționale, în funcție de cele trei situații majore în care poate fi utilizat: la pace, în situații de criză și în caz de război;

- studiul sistematic al conținutului asigurării informaționale a securității naționale, cu luarea în considerație a tuturor domeniilor care contribuie la aceasta și



a necesităților lor de informare, comandă și control, precum și a măsurilor de protecție a rețelilor de comunicații și de calculatoare aferente;

- includerea securității informațiilor printre prioritățile naționale;
- problematica războiului informațional să devină disciplină obligatorie de studiu în toate structurile de învățământ ale instituțiilor care răspund pentru securitatea națională;

- în cadrul măsurilor privind pregătirea țării pentru apărare (exerciții, aplicații etc.) să fie incluse și acțiunile de descoperire și contracarare a amenințărilor informaționale privind securitatea națională;

- studiul temeinic al normelor și instrucțiunilor NATO privind războiul informațional, de către toate structurile privind securitatea națională, în părțile ce le privesc;

- pregătirea personalului de informatică care exploatează rețelele de calculatoare ale structurilor din sistemul securității naționale pentru prevenirea și lichidarea atacurilor cibernetice;

- corelarea doctrinară și operațională a războiului informațional, ca formă a luptei armate, cu principalele forme de luptă utilizate în prezent, dar și cu legile și principiile luptei armate, avându-se însă în vedere și posibilitățile de utilizare independentă a acestuia;

- protecția împotriva amenințărilor informaționale să constituie o preocupare continuă a tuturor structurilor care răspund de securitatea națională, dar și a celorlalte organizații atât pe timp de pace, dar mai ales în situații de criză și conflict militar;

- procurarea și dotarea cu mijloace moderne de război informațional defensive, dar și ofensive a principalelor structuri ale statului care răspund de securitatea națională.



BIBLIOGRAFIE

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

*** Doctrina națională a informațiilor pentru securitate, Editura SRI, Buc., 2004

*** Doctrina pentru informații, contrainformații și securitate a armatei, Buc., 2005

*** Legea protecției informațiilor clasificate, nr. 182/2002, în M.Of. nr. 248/2002



- *** Legea privind securitatea națională a României nr. 51/1991, publicată în M. Of. Nr. 163/1991
- *** Securitatea informațiilor, Centrul de Expertiză în Domeniul Securității, București, 2008
- *** Sisteme informaționale – Sesiunea anuală de comunicări științifice cu participare internațională, Editura UNAp. "Carol I", București, 2007
- *** Strategia de securitate națională a României, București, 2007
- ALEXANDRESCU C. și alții, *Supremația electromagnetică*, Editura UNAp, București, 1999
- ALEXANDRESCU C., *Amenințări informaționale asupra sistemelor de comandă și control în acțiunile militare moderne "SI-2007"*
- ALEXANDRESCU C., TEODORESCU C., *Războiul electronic contemporan*, Editura Sylvi, 1999
- ALEXANDRESCU C., ILINA D., MINCU C., *Bazele matematice ale organizării sistemelor de transmisiuni*, Ed. Militară, București, 1994
- ALEXANDRESCU Gr., VĂDUVA Gh., *Infrastructuri critice: Pericole, amenințări la adresa acestora*: Ed. UNAp. "Carol I", Buc., 2006
- ANDERSON Robert H., *Physical Vulnerabilities of Critical US Information Systems* (internet, Iaver May 03.pdf)
- BĂDĂLAN Eugen, *Securitatea României, actualitate și perspective*, Editura Militară, București, 2001
- ENSA Risk Management/Risk Assessment (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 națională și războiul modern*, Ed. Mil., Buc., 1999
- HLIHOR C., *Geopolitica și geostrategia în analiza relațiilor internaționale contemporane*, Editura UNAp, București, 2005
- ILIE Gh., STOIAN I., Ciobanu V., *Securitatea informațiilor*, Ed. Mil., Buc., 1996
- ISO/IEC 27001 Information Technology. Security Technique. Information Security Management Systems – Requirements



- MINCU Constantin, GREU Victor, ROTARIU Costel, *Salt de frecvență și contrasalt de frecvență*, Editura Militară, București, 1998
- MINCU Constantin, TIMOFTE Gruia, *Compatibilitatea Sistemelor Radioelectronice*, Editura Olimp, București, 1999
- MUREȘAN M., VĂDUVA Gh., *Războiul viitorului*, viitorul războiului, Editura UNAp, București, 2005
- TOFFLER Alvin și Heidi, *Război și anti-război*, Editura Antet, București, 1995
- TOFFLER Alvin, *Powershift, puterea în mișcare*, Editura Antet, București, 1995

Reviste de specialitate:

1. Gândirea Militară Românească, anii 2001-2015;
2. Buletinul Universității Naționale de Apărare „Carol I”, 2008-2015;
3. Revista Forțelor Terestre, anii 2005-2015;
4. Impact Strategic, anii 2006-2015;
5. Revista de Științe Militare, anii 2006 – 2015;
6. Romanian Military Thinking Journal, anii 2005 – 2015.

