PUNCTE TARI ŞI VULNERABILITĂŢI INTERNE ŞI EXTERNE ALE SISTEMELOR ŞI REŢELELOR DE COMUNICAŢII ŞI INFORMATICE MILITARE DEZVOLTATE ÎN ARMATA ROMÂNĂ, ÎN CONDIŢIILE PROVOCĂRILOR DE SECURITATE ACTUALE

STRONG POINTS AND INTERNAL AND EXTERNAL VULNERABILITIES OF THE MILITARY COMMUNICATIONS AND INFORMATICS SYSTEMS AND NETWORKS DEVELOPED IN THE ROMANIAN ARMED FORCES UNDER THE CIRCUMSTANCES OF THE CURRENT SECURITY CHALLENGES

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

Rezumat: *Autorul prezintă într-o manieră succintă o serie de aspecte, de mare actualitate în contextul geopolitic actual, privind unele puncte tari, dar şi vulnerabilităţi interne şi externe ale sistemelor şi reţelelor de comunicaţii şi informatice militare dezvoltate în Armata Română, începând cu anul 1997.*

Sunt aduse în atenţie, la punctul 2 evoluţiile, în condiţii de austeritate şi ostilitate, a principalelor segmente operaţionale şi tehnice ale STAR (RTP/RMNC).

În continuare sunt prezentate unele puncte tari ale sistemelor realizate şi principiile de care s-a ţinut seama în efortul de modernizare şi transformare (având în vedere criteriile şi cerinţele NATO), precum şi vulnerabilităţile interne şi externe ale acestora, identificate în urma unei analize atente.

Cuvinte-cheie*: comunicaţii, RTP/RMNC, STAR, NATO.*

Abstract: *The author briefly presents a series of recent aspects in the current geopolitical context on some strong points as well as internal and external vulnerabilities of the military communication and informatics systems and networks developed in the Romanian Armed Forces since 1997.*

Point 2, presents the evolutions, in austerity and hostility conditions of the main operational and technical sequels of the Romanian Armed Forces Transmissions System - STAR (RTP/RMNC).

Furthermore the article presents some strong points of the systems achieved and principles taken into account in the modernization and transformation effort (regarding the

* 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.

NATO criteria and requirements), as well as their internal and external vulnerabilities identified by means of a thorough analysis.

Keywords: *communications, RTP/RMNC, STAR, NATO.*

1. Introducere

Consider, pe baza unui set de argumente complex aflat, dacă se doreşte, la îndemâna actualilor decidenţi civili şi militari din Ministerul Apărării Naţionale, că tema propusă este de maximă actualitate în contextul geopolitic zonal şi global actual.

Cred că este cazul să reiau ce am publicat în Revista de Ştiinţe Militare nr. 1/2008, cu scopul de a explica demersul meu şi al altor autori în domeniul apărării:

„Plecând de la realitatea că apărarea ţării, precum şi armata sunt de drept public şi nu privat, iar prevederi clare din Constituţie şi din legislaţia specifică dau dreptul fiecărui cetăţean al ţării de a contribui direct sau indirect la întărirea capacităţii României de a se apăra, în caz de nevoie, am considerat că este potrivit ca acţiunile şi procesele specifice să fie analizate şi dezbătute şi în cadrul Secţiei de Ştiinţe Militare a Academiei Oamenilor de Ştiinţă din România (AOŞR). Precizările sunt necesare pentru a răspunde nedumeririi şi anxietăţii posibile, în rândul unor oficiali civili şi militari, din unele instituţii ale statului, care, considerându-se singurii deţinători ai adevărului, mai întreabă uneori: „De ce se amestecă rezerviştii ăştia?". Răspunsul este simplu - se amestecă pentru că încă mai sunt cetăţeni români, cu drepturi şi îndatoriri cetăţeneşti şi, în mod sigur le pasă. Iar în cazul special al membrilor Secţiei de Ştiinţe Militare a AOŞ-R se adaugă cel puţin un motiv: printre membri se află trei foşti şefi ai Statului Major General, şefi de direcţii, profesori la instituţii civile şi militare de învăţământ superior şi unii oficiali în funcţii importante ale statului român (Ministerul Apărării Naţionale, Ministerul Administraţiei şi Internelor, Preşedinţia României, etc.).

Adăugând faptul că toţi deţin titlul de doctor şi au ca experienţă o activitate profesională şi o operă importantă (cărţi, manuale, studii, articole) atribute care le conferă capacitatea de analiză critică şi expertiză în domeniul securităţii naţionale şi apărării ţării, aceştia pot oferi puncte de vedere obiective, nevirusate de influenţa intereselor politice şi economice conjuncturale ale unor grupuri, mai mult sau mai puţin interesate de soarta ţării."

Consider că din 2008 şi până astăzi (2015) autismul şi nepăsarea responsabililor civili şi militari aflaţi în funcţii, s-a accentuat, iar în cazul special al celor din comunicaţii şi informatică a depăşit, cel puţin după 2010, orice limită logică şi de bun simţ.

2. Scurt istoric

Au trecut mai bine de 25 de ani de la primele demersuri teoretice şi practice pentru realizarea a ceea ce numim **„Sistemul de transmisiuni al Armatei României - STAR”** (cu mai multe componente) şi mulţi din cei de astăzi nu mai cunosc sau nu vor să mai cunoască demersurile şi paşii făcuţi, în condiţii de maximă austeritate şi într-o atmosferă de ostilitate (detalii poate cu o altă ocazie). De aceea o readucere în atenţie, pe scurt, cred că poate fi utilă:

- **Preocupări concrete** (studii, rapoarte) pentru modernizarea organizatorică, structurală şi tehnică de fond a sistemului de transmisiuni au fost numeroase, începând din anul 1970. Din lipsă de înţelegere şi în oarecare măsură de resurse nu s-a făcut mare lucru.
- **În 17 iulie 1991** Inspectoratul General al Transmisiunilor (denumirea nefericită de atunci a actualului Comandament al Comunicaţiilor şi Informaticii) a înaintat la Marele Stat Major un studiu complet şi bine documentat, privind modernizarea majoră a sistemului de transmisiuni. Problema de bază prevăzută era realizarea unei reţele strategice, pe întregul teritoriu naţional (numită până în 2006 – Reţeaua de Transmisiuni Permanentă – RTP, iar după 2006 Reţeaua Militară Naţională de Comunicaţii - RMNC). Studiul a fost înapoiat fără să se întreprindă nici o măsură.
- **În perioada august 1991 - 30 ianuarie 1993** un grup restrâns de specialişti de transmisiuni din I. G. Trs. împreună cu un Colectiv special destinat au întocmit, în mai multe forme succesive „Concepţia organizării şi realizării sistemului de transmisiuni al Armatei Române (STAR)” având la bază:
  - analiza critică severă a sistemului de transmisiuni existent;
  - experienţa, în domeniu, a armatelor moderne (au fost studiate câteva zeci de cărţi de specialitate, manuale, sute de articole şi materiale documentare obţinute pe diferite căi);
  - necesităţi reale (cu o bază de calcul matematică) ale tuturor eşaloanelor şi tipurilor de unităţi militare din armata noastră;
  - consultarea strânsă şi permanentă cu specialiştii de transmisiuni din întreaga armată;
  - consultarea cu specialiştii din organele centrale ale M.Ap.N. şi din academiile militare;
  - alte numeroase considerente de ordin strategic, operativ şi tactic.
- **„Concepţia organizării şi realizării sistemului de transmisiuni al Armatei Române (STAR)”** în forma finală a fost definitivată la 30 ianuarie 1993 şi înaintată conducerii M.Ap.N. la începutul lunii februarie 1993, cu propunerea de a fi supusă aprobării C.S.A.T., dat fiind importanţa problemei, nevoile financiare

deosebite şi precaritatea actualului sistem (cu totul şi cu totul depăşit tehnic şi organizatoric), fiind situat la nivelul anului 1960.

• **Concepţia menţionată** a fost însuşită de conducerea M.Ap.N. şi a fost înaintată C.S.A.T. la sfârşitul lunii martie 1993.

• Documentul a fost discutat în şedinţa CSAT din 9 iunie 1993, luându-se hotărârea de a **se aproba** realizarea sistemului.

• **După şedinţa din iunie 1993** au urmat tot felul de atacuri şi intervenţii din partea unor reprezentanţi ai instituţiilor din sistemul de apărare, ordine publică şi siguranţă naţională şi din partea a doi ofiţeri din armată fapt care adus la întârzieri, reanalizarea problemei în alte şedinţe CSAT (nu le mai amintim aici) şi la declanşarea unei virulente campanii de presă cu autori cunoscuţi şi interesaţi, din motive diferite, de blocarea programelor.

• **Ca urmare a situaţiei** create s-a propus şi s-a aprobat constituirea unui „Colectiv". Interdepartamental format din specialişti din M.Ap.N., MAI, SRI, SIE, Ministerul Comunicaţiilor şi S.T.S. (16.09.1993). „Colectivul" finalizează documentul **„Concluziile privind compatibilitatea în lucru şi posibilităţile utilizării în comun, de către componentele Sistemului Naţional de Apărare şi Ministerului Comunicaţiilor a RTP/STAR"**. Acest document a fost semnat şi asumat de toţi reprezentanţii instituţiilor menţionate. Cu toate acestea atacurile nefondate au continuat, astfel că, primele centre se vor instala abia în primăvara anului 1997, iar configurarea a 50% din reţea în anul 2002 (argument puternic pentru integrarea în NATO), iar finalizarea s-a prelungit până în 2010 (motive subiective şi obiective, între care finanţarea la întâmplare şi fără nici un fel de responsabilitate).

• **Sunt şi alte argumente şi detalii** care din motive de înţeles nu pot şi făcute publice.

3. Puncte tari bazate pe principii dezvoltate şi aplicate în armatele ţărilor membre NATO

În abordarea acestui punct este necesară o analiză temeinică şi extinsă asupra unor chestiuni de ordin strategic, operativ şi tactic privind: structura forţelor, dispunerea la pace şi posibile variante la război, organizarea comenzii şi controlului (resurse umane, tehnologie de ultimă generaţie, numărul şi dispunerea punctelor de conducere pe întreaga scară ierarhică, rezervarea conducerii etc.).

Astfel s-au concretizat următoarele principii, care pot fi considerate puncte tari:

• **Sistemul este militar,** cu conducere unică realizată de organele de specialitate ale S.M.G. (Direcţia Comunicaţii şi Informatică şi Comandamentul Comunicaţiilor şi Informaticii). Acest sistem funcţionează după principii militare,

la pace şi la război, diferite de cele ale altor sisteme comerciale sau speciale. Se impun preponderenţa cerinţelor de ordin strategic, operativ şi tactic în faţa cerinţelor de ordin tehnic.

- **Este automatizat,** secretizat şi multiplu rezervat.
- **Este realizat după standarde şi cerinţe militare,** ca o condiţie de interoperabilitate cu sistemele mobile tactice şi cu cele ale NATO şi armatelor aliate.
- **Sistemul este permanent în stare de pregătire** (de luptă) prin serviciul de management şi operare asigurat de specialişti bine pregătiţi şi motivaţi.
- **Se asigură (sau ar trebui) un secret desăvârşit** al structurilor sistemului existent la pace şi dezvoltat la război.
- **Structura STAR** are capacitatea reală de a asigura o anumită independenţă faţă de dispunerea actuală şi viitoare a punctelor de comandă şi a elementelor de dispozitiv.
- **A avut şi are loc,** în continuare, schimbarea radicală a ponderii transmiterilor în sistem – restrângerea procentuală a transmiterilor de voce în favoarea transmiterilor de date.
- **Se asigură** posibilitatea de reconfigurare rapidă a sistemului de transmisiuni, în raport cu condiţiile complexe ale unui eventual război:
  - reţeaua de transmisiuni permanentă la pace RTP/RMNC;
  - reţeaua de transmisiuni strategică la război, prin adăugarea de noi centre mobile şi fixe în RTP/RMNC.
- **O independenţă** sporită (necesară acum) faţă de reţelele comerciale (canalele asigurate prin acestea devin complementare).
- **Fiabilitate ridicată** (a se vedea cărţile şi studiile pe această temă) care să asigure legătura neîntreruptă şi în situaţia scoaterii din funcţiune permanentă sau temporară de până la 50% din elementele sale.
- **Elementele RTP/RMNC** sunt dispuse în teritoriu astfel încât să poată fi apărate de unităţile armatei aflate în zonă.
- **Asigurarea cu echipamente** radioreleu şi radio cu agilitate de frecvenţă (posibilitatea de a „fugi" de bruiajul şi interceptarea inamicului).
- **Asigură interoperabilitatea,** fără probleme organizatorice şi tehnice cu sistemele similire ale NATO.
- **Realizarea** unei soluţii de interconectare cu alte sisteme speciale pe baza convenirii unor porţi de acces bidirecţional, fără a exista o relaţie de subordonare a sistemului armatei şi de dependenţă exagerată faţă de administratorii acestora. Aici funcţionează principiul militar potrivit căruia conducătorul operaţiei (luptei) se bazează în primul rând, pe resursele umane şi tehnice proprii şi nu trebuie să umble

cu căciula în mână pentru a cere comunicaţii de la alţii, oricât de bună credinţă se presupune că ar fi aceştia.

Aceste puncte tari (principii) prezente în concepţia STAR, în Proiectul Tehnic şi în documentele conexe (peste o sută de mii de file şi care au fost aprobate prin mai multe Hotărâri CSAT, ordine ale Ministrului Apărării şi ale Şefului Statului Major General, nu pot fi obiect al liberului arbitru (fără argumente de ordin operaţional şi tehnic) al câtorva ofiţeri din Direcţia Comunicaţii şi Informatică şi Comandamentul Comunicaţiilor şi Informaticii, care după anul 2010 le ignoră sau le distrug, din considerente pur comerciale, făcând pe plac unor furnizori **„anume desemnaţi"** şi care contribuie, din plin, la transformarea sistemelor într-un jalnic ghiveci călugăresc.

Dacă vor să schimbe totul trebuie să obţină aprobarea de la aceleaşi foruri (CSAT, Ministrul Apărării, Şeful Statului Major General). Dacă nu, ar putea în situaţii de criză sau la război, să suporte consecinţe chiar penale.

Vom vedea (evident tot pe scurt) în capitolul vulnerabilităţi la ce pericole sunt expuse aceste sisteme din considerente, în primul rând interne şi apoi externe.

4. Vulnerabilităţi interne

În mod cât se poate de justificat, cu argumente de ordin operaţional şi tehnic, sistemele de comunicaţii şi informatice militare sunt o parte vitală a infrastructurilor critice ale României. Pe acest subiect am publicat în anul 2010 un articol[1], cu unele probleme privind asigurarea protecţiei fizice şi informaţionale a acestora, în contextul ameninţărilor în continuă creştere. Sunt şi alţi autori care au publicat studii şi articole pe acest subiect, cu intenţia clară de a sensibiliza decidenţii politici şi militari, şi iniţierea unor măsuri concrete de dezvoltare şi protecţie.[2]

Din păcate aceste măsuri lipsesc cu desăvârşire, iar planificatorii, realizatorii şi utilizatorii de sisteme de comunicaţii militare ignoră, cu seninătate, orice aplecare asupra acestei problematici complexe şi greu de gestionat.

În cele ce urmează nu am să reiau ce am scris în 2010, ci mă voi referi la unele chestiuni concrete, care, pe termen scurt şi mediu, vor crea situaţii periculoase pentru capacitatea de apărare a ţării.

Mă voi referi, în principal, la starea în care a ajuns RTP/RMNC prin abandonarea totală a lucrărilor normale de mentenanţă şi reparaţii începând cu anul 2010. În ceea ce mă priveşte cred că situaţia se datorează unui mix de cauze:

---

[1] Constantin Mincu, *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,* Revista de Ştiinţe Militare a Academiei Oamenilor de Ştiinţă din România, nr. 2/2010.

[2] Gr. Alexandrescu, Ghe. Văduva, *Infrastrucruri critice. Pericole, ameninţări la adresa acestora. Sisteme de protecţie,* Editura UNAp, Bucureşti, 2006.

iresponsabilitate crasă, lipsă de profesionalism, pregătire precară în domeniul cunoştinţelor de nivel strategic şi operativ, rea credinţă şi servilism faţă de persoane care emit ordine aberante, toate acestea având ca rezultat subminarea capacităţii de apărare a ţării, putând fi documentată şi calificată, inclusiv penal. Să ne explicăm:

- **în perioada 2010-2015** nu au fost realizate activităţile minimale de mentenanţă, decât pentru 12% din centre.
- **repararea unor echipamente** şi module a fost practic abandonată, în depozite, se află sute de elemente defecte.
- **în ultimii doi ani unele** lucrări de mentenanţă au fost atribuite clientelar politici şi pe baza unui unic criteriu – „preţul de dumping" unor firme care n-au nici o legătură de ordin operaţional şi tehnic cu o asemenea reţea naţională complexă care este încă RTP/RMNC. Efectul este distrugerea acestui bun naţional şi militar, în cel mai scurt timp. Să explicăm efectele care deja se manifestă:

- blocarea convorbirilor telefonice şi a traficului de date pentru aplicaţiile specifice M.Ap.N., generate de întreruperea unor legături la nivelul interfeţelor de capacitate mare fapt care determină concentrarea traficului pe legături de capacitate mică (2 Mbps), fenomen care produce saturarea acestora.

- **Anomalii în funcţionarea** proceselor de sincronizare de bit care se desfăşoară între echipamentele de comunicaţii, cu repercusiuni evidente în ceea ce priveşte calitatea legăturilor de voce şi date, anomalii generate de starea necorespunzătoare a echipamentelor interconectate (comutatoare TDM şi ATM, multiplexoare, radiorelee etc.);

- Imposibilitatea de a se extinde, implementarea ultimei versiuni de software;

- Funcţionarea defectuoasă/neconformă a nivelelor ATM şi TDM din cadrul RTP/RMNC, această situaţie fiind determinată de lipsa modulelor, submodulelor, a subansamblurilor de schimb şi a materialelor conexe, datorată neexecutării la timp a lucrărilor de reparaţii în laboratoare specializate.

- **Au fost identificate şi diagnosticate** unele cauze în funcţionarea cu performanţe scăzute a RTP/RMNC:

- existenţa unor configuraţii incomplete ale echipamentelor;

- resetări repetate ale echipamentelor, fapt ce generează alterarea pachetelor software.

- defectarea unităţilor de abonat cauzată de scurtcircuite accidentale, atingeri întâmplătoare ale terminaţiilor, utilizării inadecvate a terminalelor de linie şi/sau de canal;

- deteriorarea reţelei de sincronizare de bit datorată defectării modulelor sursă de ceas;

• **Funcţionarea cu performanţe scăzute** a sistemului de management al RTP/RMNC, conduce la:

- imposibilitatea de a se ţine la zi baza de date globală a reţelei;
- imposibilitatea actualizării centrelor de comunicaţii într-o manieră centralizată;
- imposibilitatea gestionării alarmelor generate de echipamente şi, pe baza acestora, imposibilitatea de a se lua măsurile necesare corectării inadvertenţelor apărute.

• **Degradarea rapidă şi ireversibilă** a ghidurilor de undă mergându-se până la întreruperi ale legăturilor radioreleu, generate de către lipsa/defectarea echipamentelor de presurizare a ghidurilor de undă, coroborată cu distrugerea membranei excitatorului.

• **Ieşirea din parametrii de temperatură** a tuturor echipamentelor, fapt determinat de lipsa/defectarea sistemelor de climatizare din incinte.

• Funcţionarea defectuoasă a sistemelor de electroalimentare/împământare, fapt ce poate conduce la defectarea echipamentelor din centre.

• Funcţionarea necorespunzătoare a sistemelor radiante (una din cauze fiind dezalinierea antenelor) fapt care generează întreruperea unor fluxuri de mare capacitate.

Menţionez că în condiţiile apariţiei unor deranjamente majore în RTP/RMNC va fi afectat grav suportul de comunicaţii pentru sistemele şi aplicaţiile de date care tranzitează reţeaua, cum sunt:

• comunicaţiile de voce şi date pentru toţi utilizatorii;
• INTRAMAN;
• SCCAN (Poliţie Aeriană, FDEX, SIMIN, RAP, LAP etc.);
• Video-conferinţa M.Ap.N.
• CRONOS
• Legăturile de comunicaţii cu teatrele de operaţii;
• Legăturile de comunicaţii cu sistemele NATO şi UE;
• Sistemul de Supraveghere şi Avertizare CBRNe.

La cele prezentate mai sus mai pot fi adăugate şi alte ameninţări şi vulnerabilităţi interne:

-lipsa de preocupare pentru dobândirea şi menţinerea superiorităţii informaţionale;

-neconcordanţa, adesea flagrantă, 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 protecţie, utilizarea necorespunzătoare a acestora (a se vedea mixul de echipamente comerciale neperformante introduse în RTP/RMNC în ultimii ani);

-lipsa de înţelegere a mediului de securitate intern şi internaţional şi influenţa acestuia asupra proceselor informaţionale ale structurilor militare;

-organizarea necorespunzătoare a bazelor de date, existenţa unor produse software neperformante sau cu erori intenţionate;

-slaba pregătire profesională şi experienţa redusă a personalului implicat în organizarea, exploatarea şi asigurarea funcţionării sistemelor informaţionale (în opinia mea acest fenomen se regăseşte pe toată scara ierarhică actuală);

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

-neloialitatea (din ce în ce mai evidentă) a unor persoane care exploatează echipamentele tehnice ale sistemelor informaţionale;

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

Apreciez şi, în această fază, rog pe responsabilii civili şi militari care au o tangenţă mai mare sau mai mică cu sistemele de comunicaţii şi informatice militare că ar trebui să facă o analiză chirurgicală, punct cu punct, să identifice măsurile de repunere în stare operativă a sistemelor şi să ia măsurile cuvenite de protecţie fizică şi informaţională ca urmare a ameninţărilor şi vulnerabilităţilor reale prezentate şi a altora care pot apare.

5. Vulnerabilităţi şi ameninţări externe

Ameninţările informaţionale externe cuprind ansamblul acţiunilor specifice executate de adversari potenţiali şi forţele ostile ţării noastre pentru interzicerea sau îngreuierea executării funcţiilor decizionale şi operaţionale privind securitatea naţională.

Conform concluziilor formulate în literatura de specialitate[3], principalele vulnerabilităţi şi ameninţări sunt următoarele:

-atacul fizic împotriva surselor de date şi a mijloacelor de transmitere, prelucrare şi afişare a informaţiilor;

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

-atacul electronic asupra mijloacelor de culegere, transmitere şi prelevare a informaţiilor;

-atacul cibernetic împotriva sistemelor informaţionale ale structurilor de informaţii pentru securitatea naţională şi cele ale organizaţiilor economice, financiare, diplomatice etc.;

-pirateria software;

-atacul fizic şi electronic asupra organelor decizionale ale statului nostru (preşedinţie, parlament, guvern, ministere etc.) privind securitatea naţională;

-atacul psihologic asupra tuturor structurilor decizionale şi acţionale ale ţării noastre (politice, economice, sociale, de apărare etc.).

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

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

Faţă de aceste ameninţări şi vulnerabilităţi prezentate mai sus se pot identifica şi multe altele studiind literatura de specialitate şi făcând studii de caz pe evenimente petrecute recent în zona noastră şi în lume.

Măsurile de prevenire şi protecţie trebuie să depăşească faza declarativă şi academică şi se impune ca factorii decidenţi de astăzi şi de mâine să ia măsuri concrete, vizibile şi verificabile, evident cu asigurarea resurselor umane şi financiare necesare. Asta dacă mai dorim să existăm ca stat, dacă nu, nu.

BIBLIOGRAFIE

*** *Concepţia de organizare şi realizare a STAR,* Comandamentul Comunicaţiilor şi Informaticii, Bucureşti, 1993;

*** *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;

*** ENSA Risk Management/Risk Assesment (European Network on Information Security Agency);
*** EUROCOM D/1 Tactical Communications Systems. Basic Parameters, 1986.
*** FM 3-13, Information Operations: Doctrine, Tactics, Techniques and procedures, US Army, 2003;
*** FM 34-1, Intelligence and Electronic Warfare Operations, Headquarters, Departament of the Army, Washington DC;
*** ISO/IEC 27001 Information Technology. Security Technique, Information Security Management – Requirements;
*** *Legea privind protecţia informaţiilor clasificate,* nr. 182/2002, publicată în Monitorul Oficial nr. 248/2002;
*** *Proiectul tehnic general al RTP/STAR*, Statul Major General, Bucureşti, 1996;
*** *Securitatea informaţiilor,* Centrul de Expertiză în Domeniul Securităţii, Bucureşti, 2008;
*** *Sisteme informaţionale*, Sesiunea anuală de comunicări ştiinţifice cu participare internaţională, Editura UNAp „Carol I", Bucureşti, 2007;
*** *Strategia de Securitate Naţională a României*, Bucureşti, 2014;
ALEXANDRESCU C şi alţii, *Supremaţie electromagnetică,* Editura Universităţii Naţionale de Apărare „Carol I", 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 Ghe., VĂDUVA Ghe., *Infrastructuri critice. Pericole, ameninţări la adresa acestora. Sisteme de protecţie,* Editura Universităţii Naţionale de Apărare „Carol I", Bucureşti, 2006.
ALEXANDRESCU C., ILINA D., MINCU C., *Bazele matematice ale organizării sistemelor de transmisiuni*, Editura Militară, Bucureşti, 1994;
ANDERSON H.R., *Physical Vulnerabilities of Critical US Information Systems* (Internet, IaverMay03.pdf);
BĂDĂLAN E., *Securitatea României, actualitate şi perspective,* Editura Militară, Bucureşti, 2001;
FRUNZETI T., *Securitatea naţională şi războiul modern*, Editura Militară, Bucureşti, 1999;
FRUNZETI T., ZODIAN V., (coordonatori), *LUMEA DE AZI 2015*, Editura RAO, Bucureşti, 2015;
GANSLER J.S., BINNENDJIC H., *Information Assurance, Trend in Vulnerabilities, Threats and Technologies.*

HLIHOR C., *Geopolitica şi Geostrategia în analiza relaţiilor internaţionale contemporane,* Editura Universităţii Naţionale de Apărare „Carol I", Bucureşti, 2005;
ILIE Ghe., STOIAN I., CIOBANU V., *Securitatea Informaţiilor,* Editura Militară, Bucureşti, 1996;
MINCU C., TIMOFTE G., *Compatibilitatea Sistemelor Radioelectronice,* Editura Olimp, Bucureşti, 1999;
MINCU C., GREU V., ROTARIU C., *Salt de frecvenţă şi contrasalt de frecvenţă,* Editura Militară, Bucureşti, 1998;
MINCU C., *Analiză privind realizarea Sistemului de Transmisiuni al Armatei României (STAR),* Comandamentul Comunicaţiilor şi Informaticii, Bucureşti, februarie 1997;
MINCU C., *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,* Revista de Ştiinţe Militare a Academiei Oamenilor de Ştiinţă din România, nr. 2/2010.
MUREŞAN M., VĂDUVA Ghe., *Războiul viitorului, viitorul războiului,* Editura Universităţii Naţionale de Apărare „Carol I", Bucureşti, 2005;
TOFFLER A., HEIDI, *Război şi anti-război,* Editura Antet, Bucureşti, 1995;
TOFFLER A., *Powershift, puterea în mişcare,* Editura Antet, Bucureşti, 1995;

Reviste de specialitate:
1. Gândirea Militară Românească, 1997-2014.
2. Buletinul Universităţii Naţionale de Apărare „Carol I", 2008-2015.
3. Revista de Ştiinţe Militare, 2006-2015.
4. Annals Series on Military Sciences, 2005-2015.