DUPĂ DOUĂZECI DE ANI. REALIZĂRI NOTABILE ŞI PROIECTE ABANDONATE SAU AMÂNATE ÎN DOMENIUL SISTEMELOR DE COMUNICAŢII ŞI INFORMATICE ALE ARMATEI ROMÂNIEI (1997-2017)

TWENTY YEARS LATER. NOTABLE ACHIEVEMENTS AND ABANDONED AND POSTPONED PROJECTS IN THE FIELD OF COMMUNICATION AND INFORMATICS SYSTEMS OF ROMANIAN ARMED FORCES (1997-2017)

Gl. - mr. (r) prof. asoc. 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 ameninţări externe ale sistemelor şi reţelelor de comunicaţii şi informatice militare dezvoltate în Armata Română, începând cu anul 1997.*

Sunt aduse în atenţie evoluţiile, în condiţii de austeritate şi ostilitate, a principalelor segmente operaţionale şi tehnice ale STAR (RTP/RMNC), precum şi influenţele noilor tehnologii în domeniul sistemelor C4I asupra planificării şi ducerii operaţiei (luptei).

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 ameninţări externe ale acestora, identificate în urma unei analize atente. Se remarcă, din păcate, proiectele abandonate sau amânate din diverse motive.

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 vulnerabilities and external threats of the military communication and informatics systems and networks developed in the Romanian Armed Forces since 1997.*

There are exposed the evolutions in austerity and hostility conditions of the main operational and technical sequels of the Romanian Armed Forces Transmissions System - STAR (RTP/RMNC), as well the influences of new technologies in the C4I systems on the planning and conductment of operation (battle).

* Membru titular al Academiei Oamenilor de Ştiinţă din România, membru al Consiliului Onorific al Academiei Oamenilor de Ştiinţă din România, secretar ştiinţific al Secţiei de Ştiinţe Militare, Telefon: 0722.303.015, email: mincu_constantin@yahoo.com.

Furthermore there are presented some strong points of the achieved systems and principles taken into account in the modernization and transformation effort (regarding the NATO criteria and requirements), as well as their internal vulnerabilities and external threats identified following a thorough analysis. Unfortunately, we can see the projects remain abandoned or postponed by different reasons.

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

1. Introducere

Consider, pe baza unui set de argumente complexe aflat, dacă se doreşte, la îndemâna actualilor decidenţi civili şi militari din Ministerul Apărării Naţionale, că o revedere critică a realizărilor şi restanţelor în domeniul sistemelor de comunicaţii şi informatice (CIS) în ultimii douăzeci de ani este de maximă actualitate şi utilitate în contextul geopolitic zonal şi global actual.

Este necesar să observăm atent şi să luăm act că în zona sistemelor tehnice pentru comanda şi controlul forţelor şi pentru utilizarea acestora, în timp real sau aproape real, a crescut aproape exponenţial rolul integrator al sistemelor C4I, pe baza unor progrese tehnologice şi operaţionale înregistrate, în ultimii ani, în armatele importante ale unor ţări NATO şi non NATO, dintre care menţionăm:

- Dezvoltările tehnologice rapide în producţia echipamentelor de comunicaţii şi a celor informatice;
- Creşterea uluitoare a performanţelor computerelor, în ultimii 25-30 de ani;
- Dezvoltarea performanţelor microprocesoarelor[1] ca element de bază pentru viteza de operare şi pentru eforturile de miniaturizare;
- Unirea conceptuală, tehnologică şi operaţională a echipamentelor şi a reţelelor de comunicaţii digitale cu echipamentele de calcul electronic şi aplicaţiilor software;
- Creşterea presiunii asupra structurilor militare de comandă şi control pentru scurtarea continuă a ciclului conducerii şi pentru efectuarea corectă şi rapidă a unei anaalize multicriteriale a unui volum uriaş de date şi informaţii necesare planificării şi ducerii operaţiei (luptei);
- Perfecţionarea senzorilor opto-electronici integraţi în toate sistemele şi platformele de arme şi echipamente;
- Apariţia şi dezvoltarea hărţilor digitale şi a integrării acestora în sistemele GPS;
- Apariţia şi dezvoltarea conceptuală şi acţională a „războiului informaţional", care, în zilele noastre se manifestă tot mai violent;

[1] http://wikipedia.org/wiki/central_processing_unit

- Elaborarea unor noi concepte privind ducerea războiului, cum sunt: „războiul bazat pe reţea", „conflicte militare asimetrice", „războiul cibernetic", „lupta împotriva terorismului", „războiul hibrid" etc.

La toate punctele enumerate mai sus se pot face dezvoltări şi analize comparative, inclusiv între unele sisteme din armatele moderne şi cele din Armata României, cu concluzii clare privind paşii de urmat, dacă există voinţa politică şi instituţională necesară şi dacă, se acordă resursele umane şi financiare necesare.

2.Unele influenţe ale noilor dezvoltări ştiinţifice şi tehnologice asupra sistemelor şi echipamentelor de comunicaţii şi informatică cu efecte directe în planificarea şi ducerea acţiunilor militare moderne.

Specialiştii şi analiştii din domeniul militar[2] sunt unanimi în a aprecia că dezvoltarea fără precedent a tehnicii şi a tehnologiilor, apariţia unor noi produse şi servicii performante cu o dezvoltare accelerată – mă refer în special la tehnologia informaţiei, tehnologiile speciale, sistemele de comunicaţii digitale, aplicaţiile software dedicate planificării şi ducerii operaţiei (luptei), precum şi la cele implementate în sistemele de arme – au un impact major asupra tuturor categoriilor de forţe, arme, sisteme de armamente şi implicit asupra rezultatelor scontate ale acţiunilor în situaţii de criză sau de război.

Este de înţeles că nu vom putea, în spaţiul rezervat, să identificăm şi să prezentăm toate influenţele posibile (sunt foarte numeroase şi în continuă dezvoltare). Voi încerca să aduc în atenţia celor interesaţi doar câteva, care mi se par mai importante şi mai vizibile astăzi.

Astfel, în domeniul resurselor umane militare şi civile şi a performanţelor aşteptate de la sistemele militare se pot identifica:

- cerinţe noi şi dure în pregătirea profesională, psihică şi în dezvoltarea calităţilor morale pentru a face faţă unor sisteme din ce în ce mai complexe şi mai greu de gestionat;
- necesitatea înţelegerii, de la general la soldat, a noilor „unelte" ale erei informaţionale în toată complexitatea lor tehnică şi operaţională, în scopul utilizării lor în mod firesc, natural, fără sincope datorate stresului tehnologic (de către toţi combatanţii, indiferent de funcţie, grad sau armă);
- aprecierea justă a limitelor sistemelor C4ISR (+ variante) în condiţiile unui război informaţional dur, dus cu toate mijloacele moderne. În acest scop militarii trebuie să rămână capabili ca la nevoie să poată acţiona fără aceste mijloace, care

[2] *Lucrările Simpozionului Jubiliar AFCEA,* Washington DC, 18-19 iunie 2006, cu intervenţiile: Amiralului Edmund P. Giambastini Jr., Vicepreşedinte (la acea dată) al Statului Major Întrunit al Armatei SUA şi ale Generalului (ret.) Colin L. Powell (fost secretar de stat).

pot intra în congestie sau chiar în colaps (acest lucru s-a înţeles deja chiar şi în cele mai tehnologizate armate, cum este cea a SUA);

- testarea, la aplicaţii şi exerciţii, în condiţii cât mai apropiate de realităţile câmpului de luptă modern, a modului de relaţionare a luptătorilor cu sistemele de arme complexe, asistate de computere sau integrate în complexe tehnice şi operaţionale de tipul C4ISR;
- pregătirea specifică şi luarea măsurilor necesare pentru protejarea luptătorilor faţă de acţiunile de război psihologic utilizate de inamic pe timp de pace, în situaţii de criză şi la război.

În exercitarea comenzii şi controlului de la nivelul strategic şi până la soldat:

- amplificarea posibilităţilor comandanţilor, statelor majore şi luptătorilor de a cunoaşte inamicul şi intenţiile acestuia în timp real (cvasireal) prin utilizarea posibilităţilor sistemelor C4ISR (acolo unde acestea există);
- analiza rapidă, multicriterială, a situaţiilor complexe, utilizând computerele şi programele software specifice şi prin aceasta scurtarea timpului afectat tuturor activităţilor de comandament şi stat major (ciclul conducerii);
- stocarea datelor şi informaţiilor detaliate despre toate aspectele operaţiei (luptei) în cronologia desfăşurării acestora şi desprinderea, prin analiză, a unor lecţii pentru viitor;
- replicarea şi stocarea automată a datelor şi a informaţiilor din punctul de comandă de bază (principal) în alte 1-2 puncte de comandă proprii, în unele puncte de comandă ale eşaloanelor subordonate şi în punctele de comandă ale eşalonului superior;
- numirea unor înalţi comandanţi după criterii cât mai dure privind profesionalismul, pregătirea psihomorală şi rezistenţa în condiţii de stres, în condiţiile în care aceştia exercită managementul unor sisteme umane şi tehnice complexe şi cu o largă desfăşurare spaţială (se înţelege de la sine că numirile politice clientelare tot mai numeroase în ultimii ani, în România, sunt destinate, din start, distrugerii coeziunii şi eficienţei structurilor militare din oricare armată modernă);
- prin aportul noilor tehnologii au fost posibile micşorarea numărului şi gabaritului mijloacelor de comunicaţii şi informatice, precum şi a celulelor de comandă, în unele situaţii de aproape zece ori. Acest fapt a dus la creşterea gradului de mobilitate şi de protecţie a tuturor punctelor de comandă.

În domeniul integrării subsistemelor de senzori ISR în complexele sisteme C4ISR:

- se desprinde clar ideea că sistemele de comunicaţii şi informatică nu pot fi un diferenţiator puternic în acţiuni militare complexe fără o integrare operaţională şi tehnică a unei largi clase de senzori opto-electronici (sisteme radar, senzori cu

infraroşii, senzori optici, senzori acustici, sisteme de marcare şi ochire laser etc.) în ceea ce înţelegem astăzi prin sisteme înalt integrate de tipul C4ISR (+variante);

- crearea pe baza tuturor informaţiilor şi datelor culese prin mijloace tehnice moderne (inclusiv satelitare) şi umane a unei imagini comune asupra spaţiului de desfăşurare a acţiunilor militare, punerea acestora la dispoziţia celor cu drept de cunoaştere, în timp real sau aproape real;
- crearea posibilităţilor operaţionale şi tehnice de a „vedea" mai departe şi mai repede decât inamicul, prin performanţele reunite ale senzorilor, oamenilor şi computerelor;
- luarea unor măsuri tehnice şi organizatorice de protejare a senzorilor faţă de contramăsurile posibile ale inamicului;
- posibilitatea reală ca fiecare luptător să devină el însuşi un senzor integrat în sistem, prin mijloace de comunicaţii, microcomputerele şi senzorii pe care îi poartă în luptă, indiferent de mediul şi locul în care se află la un moment dat.

Ca o concluzie la acest capitol se poate afirma că noile mijloace tehnice (comunicaţii, computere, aplicaţii software, senzori) determină, în mod direct, o eficienţă şi o rapiditate sporite actelor de comandă şi control, aducând totodată noi riscuri şi vulnerabilităţi interne şi externe, care trebuie cunoscute şi contracarate.

3. Evoluţia sistemelor de comunicaţii şi informatică în Armata României în perioada 1950-2017

Apreciez că dezvoltarea transmisiunilor Armatei României după cel de-al Doilea Război Mondial este foarte bine sintetizată în capitolul comunicaţii şi informatică (pp. 408 - 441) din *Enciclopedia Armatei României*, publicată în anul 2009, capitol republicat de C.Trs. şi în Revista Comunicaţiilor şi Informaticii nr. 2 (10) din 2009.

Este, cred, necesar să readucem în atenţie câteva aspecte mai importante şi cu efecte pozitive sau negative în timp (unele prelungindu-se până astăzi):

- Din 1950 până în 1968 putem vorbi despre transmisiuni la limita de jos a unei armate europene, cu tehnică exclusiv analogică, majoritatea importată din URSS, de regulă, cu cel puţin zece ani în urmă faţă de dotarea forţelor armate ale aliatului de atunci;
- Evenimentele din august 1968 i-au trezit la realitate pe decidenţii politici şi militari români (nu pentru mult timp) care au realizat precaritatea cantitativă şi calitativă a structurilor şi a mijloacelor tehnice pentru exercitarea conducerii trupelor în acea perioadă. S-a pus accentul pe proiectarea şi fabricarea în ţară a unor tipuri de tehnică şi echipamente cu performanţe acceptabile, adaptate la nevoile de conducere a trupelor pe teritoriul naţional.

• În anul 1978, Comandamentul Trupelor de Transmisiuni (CTT) a întocmit *„Studiul de dezvoltare a armei transmisiuni”* care a propus, în principal, măsuri pentru perfecţionarea transmisiunilor armatei în scopul evitării stagnărilor, învechirii materiale şi morale a tehnicii, scăderii capacităţii de reacţie a conducerii în situaţii deosebite.

• Au existat unele progrese, mai ales în producerea tehnicii pentru eşaloanele tactice, dar la mijlocul anilor ’80 entuziasmul s-a topit. Măsurile excesive de economisire impuse armatei de către conducerea politică de atunci au făcut ca dinamica încurajatoare a eforturilor de perfecţionare a mijloacelor şi a forţelor de transmisiuni să nu determine îmbunătăţiri evidente, anul 1989 găsind sistemul de transmisiuni al armatei la nivelul unuia analogic, echipat cu tehnică eterogenă învechită, cu foarte multe elemente de risc tehnic, fără forme evidente de tranzit către digitalizare, informatizare şi automatizare.

• Începând cu anul 1990 a demarat un nou proces de modernizare a transmisiunilor militare, sub toate aspectele sale (resurse umane, structuri organizatorice, sisteme şi echipamente tehnice), proces care s-a dovedit şi se dovedeşte lung şi anevoios, desfăşurat adesea în condiţii de ostilitate, mai ales din partea acelora care au obligaţia legală de a aloca un minim de resurse financiare:

o Până la începutul lunii februarie 1993 în Comandamentul Transmisiunilor, Informaticii şi Electronicii (CTIE) a fost definitivată forma finală a *„Concepţiei de organizare şi realizare a Sistemului de Transmisiuni al Armatei României – STAR”;*

o Concepţia menţionată a fost analizată şi aprobată în şedinţa CSAT din data de 09.06.1993.

Este necesar să menţionez că la baza concepţiei unitare aprobate prin Hotărârea nr. 0031 din 09.06.1993 au stat:

o experienţa proprie din Armata României acumulată de-a lungul anilor în domeniul proiectării, realizării şi utilizării sistemelor de transmisiuni militare;

o experienţa şi tehnologiile avansate în unele armate din ţări NATO (SUA, Marea Britanie, Franţa, Italia, Germania, Belgia) transmise armatei noastre prin publicaţii, cărţi de specialitate, studii, analize, întâlniri directe etc.;

o structura proiectată a forţelor armatei noastre în perspectiva anilor 2005-2015;

o organizarea conducerii armatei pe întreaga scară ierarhică la pace, criză şi război;

o asigurarea în deplină siguranţă şi acurateţe tehnică a relaţiilor informaţionale, pe baza unor reguli puse de acord cu celelalte instituţii ale statului cu atribuţii în domeniul securităţii, apărării naţionale şi ordinii publice, utilizând

resursele existente şi pe cele ce vor fi implementate în mod gradual (conceptul de „reţea de reţele", pe baza unor soluţii organizatorice şi tehnice de interoperabilitate).

• **Începând cu anul 1994** s-a trecut la fundamentarea conceptuală şi tehnică a *Proiectului STAR* (RTP şi Programul radio HF şi VHF cu staţii cu salt de frecvenţă), pe baza consolidării cunoştinţelor şi accesului la informaţii privind experienţa şi tehnologiile unor armate moderne occidentale şi în urma învăţămintelor desprinse pe timpul participării unor specialişti români la seria de aplicaţii *„Combined Endeavor"* şi la activităţi organizate de Cartierul General al NATO (după ianuarie 1995) şi la unele armate ale alianţei (SUA, Marea Britanie, Germania, Italia, Belgia etc.). Un rol important l-a avut şi efortul de îndeplinire a obiectivelor de interoperabilitate în domeniul comunicaţiilor şi informaticii stabilite cu NATO în procesul de pregătire pentru aderare (1995-2002). De implementarea cerinţelor acestor obiective a depins, în mod clar şi fără echivoc, invitarea ţării noastre, în octombrie 2002, de a intra în alianţă cu drepturi şi obligaţii depline.

• Fără a intra în prea multe detalii[3] se poate afirma că până acum au fost făcuţi paşi importanţi în consolidarea unor sisteme de comunicaţii şi informatică moderne, fără să se ajungă încă la nivelul sistemelor puternic integrate de tipul C4ISR (+ variante), îndeosebi din lipsa resurselor financiare alocate.

• Specialiştii militari şi civili familiarizaţi cu evoluţiile din România în perioada 1990-2017 apreciază aproape în unanimitate fenomenele produse:

o starea precară a ceea ce a mai rămas din aşa-zisa „industrie de apărare";

o politicile greşite aplicate în perioada 1990-2017 în păstrarea şi în consolidarea unor subdomenii cu potenţial tehnologic şi ştiinţific în România;

o aplicarea unui management defectuos şi uneori fraudulos, care a contribuit din plin la falimentarea unor unităţi productive;

o existenţa unor interese nelegitime privind acapararea terenurilor pe care au fost şi sunt amplasate unităţile de producţie ale echipamentelor şi tehnicii de luptă (acţiunile continuă);

o descurajarea firmelor private care au apărut în România, cu produse şi servicii pentru apărare, şi apelarea, uneori fără argumente, numai la importuri;

o nepăsarea factorilor politici faţă de înzestrarea armatei şi subfinanţarea proiectelor importante, efectuarea rectificărilor de buget exclusiv negative şi instituirea unor puternice bariere birocratice şi de altă natură, care să ducă la începerea procedurilor de licitaţie abia în lunile septembrie – octombrie ale fiecărui an, cu pierderea finanţării din lipsă de timp (acţiunea pare chiar programatică);

[3] *Revista Comunicaţiilor şi Informaticii,* nr. 2 (10)/2009, pp. 30-36.

o pierderea unor specialişti de mare valoare, unii cu specializări unicat, care, din lipsă de resurse şi perspectivă, au fost nevoiţi să plece în alte domenii sau chiar să emigreze;

o indiferenţa totală a factorilor politici cu responsabilităţi în securitatea naţională şi apărare pentru exportul de echipamente şi servicii, din domeniul apărării, pe pieţele pe care România le-a avut şi pentru acele produse care au rămas sau care puteau fi făcute competitive (exportul s-a diminuat de la 800 de milioane USD pe an, în perioada 1985-1989, la 50 de milioane USD pe an, în prezent). Explicaţiile care se dau sunt fără argumente credibile şi, în consecinţă, neconvingătoare.

- Transformarea procesului de planificare a înzestrării Armatei (celebrul PAAP) într-o adevărată farsă, astfel: Să presupunem că militarii, cu argumente, stabilesc nevoile de înzestrare pentru anul următor la 100 de lei. Guvernul spune că este criză şi nu alocă decât 10 lei, ministrul apărării şi generalii raportează că sunt fericiţi şi se vor descurca şi cu 8 lei. În luna decembrie a anului respectiv se constată că au primit în mod real (prin acţiuni deliberate) doar doi lei. Este clar că România va avea o apărare de doar doi lei.

- În contextul celor prezentate mai sus prezentăm un fragment dintr-un interviu acordat de George Friedman, fondatorul STRATFOR, ziaristei Anne-Marie Blajar, hot_news.ro, 16 noiembrie 2010, referitoare la situaţia României (decidenţii politici şi militari români ar putea studia întregul interviu cu creionul în mână):

„[...] Un alt lucru pe care trebuie să-l aibă (România) este o armată. Nu eşti ascultat cu atenţie în lumea asta dacă nu ai o armată. Veţi zice că e costisitoare. Iar eu vă voi spune să vă uitaţi la secolul trecut: 5% din PIB ar fi o sursă colosală, dar ce aţi fi plătit să evitaţi ruşii şi germanii. Dacă voi credeţi că nu mai există ameninţări şi nu vor mai exista, atunci sunteţi într-o poziţie foarte raţională. Pe de altă parte, trebuie să vă gândiţi că în această parte de lume nu a fost un secol fără vreo tragedie. Şi în aceste condiţii 5% nu înseamnă atât de mult.

Polonia credea în 1939 că are o relaţie cu germanii şi cu ruşii, care a făcut nenecesară radicala modernizare a armatei sale.

Sunt două chestiuni: nu poţi ajuta o ţară care se prăbuşeşte într-o săptămână. Şi în al doilea rând, în această lume nimeni nu ajută o ţară care nu se poate ajuta singură. Ideea că germanii vor trimite tinerii să lupte şi să moară în interesul României nu e raţională. Poţi argumenta că Rusia nu va fi agresivă, poate că nu va fi, dar în trecut, de fiecare dată când o ţară est-europeană a pariat că o alta nu va fi agresivă, a pierdut. Dacă îţi construieşti apărarea şi nu sunt agresivi ai irosit ceva bani. Dacă îţi construieşti apărarea şi de aceea nu sunt agresivi, nu vei şti niciodată. Dar dacă îţi construieşti apărarea şi vor veni, atunci alianţele înseamnă ceva. Nimeni nu îşi va trimite copiii să vă apere. Am doi copii în armata americană: fiica

mea a fost în Irak, timp de 25 de luni, fiul meu este în aviaţie. Ei nu vin aici să apere românii.

Dacă e în interesul nostru, e o altă problemă. Un lucru asupra căruia trebuie românii, ca o naţiune matură, să îşi pună întrebarea este cum să fac să transform asta în interesul americanilor? ..."

4. Puncte tari ale sistemelor CIS din Armata României bazate pe principii dezvoltate şi aplicate, în armatele ţărilor membre NATO

În titlul articolului mă refer la ultimii douăzeci de ani (1997-2017) pentru că în 1997 au avut loc o serie de evenimente importante pentru Armată, în general, şi pentru comunicaţii în special:

- La 30 aprilie 1997 se înfiinţează Direcţia de Comunicaţii şi Informatică din Statul Major General (DCI/SMG);
- În primăvara aceluiaşi an se instalează după lungi eforturi teoretice şi practice, desfăşurate într-o atmosferă de ostilitate şi atacuri continui (1993-1997), primele trei centre din Reţeaua de Transmisiuni Permanente (RTP), partea principală a noului Sistem de Transmisiuni al Armatei României (STAR). În anul 2002 RTP va ajunge la 60% din prevederile Proiectului, iar în 2010 la 100%.
- Sistemele radio HF şi VHF cu salt de frecvenţă au ajuns la 50% în 2002.

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, astfel:

- 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 similitare 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 cinci sute 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.

5. Vulnerabilităţile interne, nerealizări, proiecte abandonate sau amânate

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[4], 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.[5]

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: 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 2010-2017 nu au fost realizate activităţile minimale de mentenanţă, decât pentru 12% din centre.

[4] 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.

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

- repararea unor echipamente şi module a fost practic abandonată, în depozite, se află sute de elemente defecte.
- în ultimii patru ani unele lucrări de mentenanţă au fost atribuite clientelar pe baza presiunilor unor politicieni 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:**

o 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;

o 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 CBRN.

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 protecţia, 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.

Trebuie să menţionăm în acest context amânarea sau abandonarea unor sisteme vitale pentru Armata României, cum sunt:

- sistemele tactice C4I pentru eşaloanele tactice (companie, batalion, brigadă, divizie), din subordinea SMFT;
- realizarea doar a unor insule cu rol nesemnificativ în conducerea forţelor;
- întârzieri nerezonabile pentru sistemele specifice ale SMFA şi SMFN;
- nerealizarea gestiunii automatizate a spectrului de frecvenţe radioelectronice.

Se invocă permanent lipsa de resurse financiare, dar dacă nimeni nu cere (mai hotărât), factorul politic şi Guvernul nu alocă nici un ban, ei având alte „priorităţi”.

6. Vulnerabilităţi şi ameninţări externe asupra sistemelor C4I

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[6], principalele vulnerabilităţi şi ameninţări sunt următoarele:

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

7. Câteva concluzii

Afirmaţiile Generalului (ret.) Colin L. Powell (AFCEA, 2006, Washington DC):

- oamenilor de stat civili şi militari le revin înalte responsabilităţi politice şi morale faţă de luptătorii trimişi în teatrele de operaţii;

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

- soldaţii (în sensul extins de luptători) nu pot fi obiectul acţiunilor propagandistice şi politicianiste, al lacrimilor de crocodil, exprimate în mass-media, după ce s-au întâmplat nenorociri, soldate cu pierderi de vieţi tinere;
- înzestrarea cu armament, echipamente IT&C şi mijloace de protecţie pentru militari trebuie să fie prioritatea zero a Armatei SUA (n.a. – şi a oricărei alte armate);
- războaiele şi conflictele moderne au dovedit, fără tăgadă, că a crescut exponenţial importanţa sistemelor C4ISR, de la nivel strategic şi până la soldat, aceasta însemnând vizualizarea, în timp real, a spaţiului de operaţii (luptă), informaţie pertinentă pentru luptători, aspect care salvează vieţile mai mult decât grosimea blindajelor.

Evoluţiile domeniului (CIS, C4ISR etc.) continuă în ritm alert în armatele NATO şi non NATO (Rusia, China, India etc.) în competiţia dură pentru câştigarea şi menţinerea superiorităţii informaţionale.

Rapiditatea schimbărilor este evidentă în domeniul computerelor şi al aplicaţiilor software, în dezvoltarea tehnologiilor spaţiale, în miniaturizarea componentelor şi echipamentelor, fapt care contribuie direct la sporirea mobilităţii şi a protecţiei trupelor.

Microelectronica, informatica, robotica, nanotehnologia, contribuie la dezvoltarea unor noi sisteme de arme din ce în ce mai ucigătoare.

Armata României s-a mişcat corespunzător (în condiţiile unor limitări financiare dure) în perioada 1994-2006, dar după această dată, practic, a abandonat programele şi proiectele de modernizare în domeniul C4ISR, principala structură care are de suferit fiind Statul Major al Forţelor Terestre, marile unităţi şi unităţile din subordine. În prezent nu sunt identificate posibilităţi reale de schimbare în bine.

BIBLIOGRAFIE

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

*** *Doctrina pentru Informaţii, Constrainformaţii şi Securitate a Armatei*, Bucureşti, 2005;

*** ENSA Risk Management/Risk Assesment (European Network on Information Security Agency);

*** *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;

*** *Strategia de Securitate Naţională a României*, Bucureşti, 2014;

ALBERTS, S. D., HAYES E. R., *Planning – Complex Endeavours, CCRP.*

ALEXANDRESCU C, *Ameninţări informaţionale asupra sistemelor de comandă şi control în acţiunile militare moderne*, „SI-2007";

ALEXANDRESCU G., VĂDUVA G., *Infrastructuri critice. Pericole, ameninţări la adresa acestora. Sisteme de protecţie,* Editura Universităţii Naţionale de Apărare „Carol I", Bucureşti, 2006.

ANDERSON H.R., *Physical Vulnerabilities of Critical US Information Systems* (Internet, IaverMay03.pdf);

GANSLER J.S., BINNENDJIC H., *Information Assurance, Trend in Vulnerabilities, Thret and Technologies.*

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.