REVISTA COMUNICAȚIILOR ȘI INFORMATICII

Nr. 1/2011

TRANSMISIUNILE ARMATEI ROMÂNIEI LA CEAS ANIVERSAR

Colonel dr. Ionel CIOBANU
Comandamentul comunicaţiilor şi informaticii

Aşa cum se cunoaşte, la 14 Iulie 2011 se împlinesc 138 de ani de când, prin Înaltul Decret Regal nr. 1303/1873, a luat fiinţă prima subunitate de transmisiuni - secţia de telegrafie, moment ce a marcat actul de înfiinţare al transmisiunilor din Armata României.

De-a lungul acestor ani, transformările succesive suferite de moderna armă au fost constante, fiind în pas cu transformarea, modernizarea şi operaţionalizarea armatei, dar şi lucru foarte important, cu progresul uimitor al domeniului.

Nimic nu poate fi astăzi conceput fără a fi implicată tehnica, echipamentele şi sistemele de comunicaţii.

În acest scurt editorial nu doresc să fac o prezentare, pas cu pas, în sens istoric aşa cum de regulă se obişnuieşte al realizărilor şi neîmplinirilor diferitelor etape parcurse, nu doresc să prezint schimbările efemere de denumire şi nu doresc să intru în polemică pe tema: Transmisiuni sau comunicaţii; împreună cu sistemele informatice sau separate de acestea, deoarece subiectele stârnesc aprige dispute intelectuale şi râuri de cerneală.

Mi-am propus să prezint câteva din realizările colegilor noştrii ce sigur ne fac mândrie.

Printr-o susţinută activitate, prin implicarea tuturor factorilor de la eşaloanele strategice până la cele tactice, militarii transmisionişti pot raporta cu mândrie că au realizat, exploatat şi asigurat mentenanţa sistemului de comunicaţii şi informatic necesar Armatei României. Acest fapt poate fi uşor verificabil în activitatea cotidiană a marilor unităţi şi unităţi militare şi a comandamentelor. De asemenea, activitatea este cuantificabilă în teatrele de operaţii din Irak, Afganistan şi Kosovo, unde militarii noştrii au realizat sistemele de comunicaţii şi informatice necesare legăturilor elementelor luptătoare, necesare comunicării cu aliaţii şi cu ţara. Ne putem mândri cu faptul că în anul 2011 s-a reuşit pentru prima dată, ca numai cu forţe proprii să se configureze aparte sistemul de comunicaţii şi informatic din teatrul de operaţii Afganistan.

Capabilităţile existente în armată în acest domeniu au făcut posibile asigurarea serviciilor de comunicaţii şi informatice pentru comanda şi controlul forţelor la toate nivelurile ierarhice şi sprijinirea implementării programelor de comunicaţii şi informatice.

Folosind cu multă abilitate forţele şi mijloacele la dispoziţie, am făcut faţă realităţilor economico-financiare cu care s-a/se confruntă ţara şi implicit armata sa, reuşind să operaţionalizăm Modulul CIS dislocabil, să coordonăm şi să implementăm procesul de standardizare pe domeniul CIS şi să ne aducem contribuţia la elaborarea unei strategii şi concepţii, pe termen mediu, de dezvoltare şi realizare a capabilităţilor de tip CIS/C4ISR în Armata României.

În atenţia noastră a stat şi continuarea procesului de realizare a sistemului de comunicaţii şi informatic al reţelei naţionale integrate a punctelor de comandă pentru dispunerea elementelor de conducere strategică a RNI/PCS şi implementarea reţelei private de date a Ministerului Apărării Naţionale de nivel strict secret – INTRASS - şi asigurarea condiţiilor pentru extinderea celei de nivel secret de serviciu – INTRAMAN.

Este evident că la acest moment aniversar, ar fi foarte multe alte aspecte de remarcat în evoluţia şi activitatea specialiştilor de transmisiuni, dar închei focalizând atenţia noastră şi asupra domeniului deosebit de important al pregătirii resurselor umane. Diversitatea, complexitatea şi continua expansiune a domeniului a impus din partea colegilor noştrii o pregătire asiduă personală în primul rând, apoi prin instituţiile militare şi civile de învăţământ şi nu în ultimul rând prin participarea activă la îndeplinirea tuturor misiunilor primite în teatrele de operaţii şi la exerciţiile multinaţionale şi naţionale de profil.

Am încercat să prezint, pe scurt, frământările şi dorinţele noastre, iar în încheiere doresc în numele redacţiei să urez tuturor truditorilor în domeniu multă sănătate, fericire, alături de tradiţionalul “LA MULŢI ANI !”

ORIENTĂRI PRIVIND ELABORAREA CONCEPŢIEI DE DEZVOLTARE A CAPABILITĂŢILOR C4ISR ÎN ARMATA ROMÂNIEI

Colonel ing. Ovidiu TĂRPESCU
Colonel dr. Mihai BURLACU
Direcţia comunicaţii şi informatică

Transformările aflate în derulare reflectă provocările mediului curent de securitate şi operaţional spre operaţii mai flexibile, bazate pe coaliţii, care solicită o revedere atentă a definirii conceptuale a capabilităţilor generice C4ISR şi a cerinţelor operaţionale asociate. Aceste dezvoltări trebuie incluse în cadrul procedural reglementat necesar proiectării şi dobândirii abilităţii adecvate de a realiza superioritatea informaţională esenţială pentru succesul misiunilor întrunite.

Urmărind acest scop, capabilităţile C4ISR vor facilita superioritatea decizională ca o cale esenţială de a furniza efecte coerente şi precise în orice tip de operaţie militară.

În sinteză, acest set de obiective complexe ar putea fi realizate printr-o abordare arhitecturală şi evolutivă a celor mai eficace soluţii integrate pentru a sprijini comanda şi controlul în mediul static, la pace şi de a extinde serviciile informaţionale necesare oricând şi oriunde forţele naţionale vor fi desfăşurate.

Facilităţile şi complexitatea capabilităţii C4ISR trebuie să facă obiectul unei continue analize pentru a răspunde exigenţelor specifice şi de adaptare la cadrul operaţional. Din perspectiva echipamentului, întotdeauna este necesar ca acesta să fie în mod rapid dislocabil, scalabil, sigur, robust, interoperabil şi capabil să furnizeze serviciile relevante.

Dezvoltarea la nivel naţional a următoarei generaţii de sisteme şi servicii C4ISR trebuie să urmeze aceeaşi cale, pe baza unei abordări arhitecturale, de la definirea conceptuală la implementarea iterativă, pentru a fi în măsură să sprijine angajamentele anticipate şi nivelul prezent al ambiţiilor naţionale.

The ongoing transformational changes reflecting the challenges of the present security and operational environment to more flexible, coalition based operations require a thorough review of the current generic C4ISR concept definition and associated operational requirements. These developments should be referred as a formal framework to design and acquire the adequate ability to achieve the information superiority as critical for a successful joint mission.

Pursuing this aim the C4ISR capabilities will enable the desired decision superiority as an essential way of delivering precise and coherent effects in any type of military operation.

In summary this set of complex objectives could be achieved through an architectural and evolutionary approach of the most effective and integrated solution in order to support command and control within the static peace environment and to extend the required information services whenever and wherever the national forces are going to be deployed.

Further consideration should be given to the various nature and features of the C4ISR capability to be tailored and adapted to the operational framework. From the equipment perspective there is always a need to be rapidly deployable, scalable, secure, robust, interoperable and capable to provide the relevant service.

The national development of the next generation of C4ISR systems and services has to follow the same route, based on an architectural approach from concept definition to the spiral implementation in order to be able to support the envisaged commitments and the current level of national ambitions.

Complexitatea şi intensitatea transformărilor din mediul de securitate contemporan au determinat o revizuire fundamentală a scenariilor de desfăşurare a acţiunilor militare. Operaţiile întrunite impun angajamente internaţionale care solicită componentelor militare caracteristici deosebite de agilitate, flexibilitate, interoperabilitate şi mobilitate, ce reflectă profilul expediţionar al acestora. Sistemele C4ISR[1] trebuie să dispună de aceleaşi atribute de performanţă pentru a contribui esenţial la realizarea superiorităţii informaţionale şi decizionale. Implementarea principiilor teoriei „*capabilităţilor facilitate de reţea*” sprijină abilitatea de a genera efecte militare decisive şi precise, cu o viteză şi acurateţe neîntâlnite în trecut, prin interconectarea senzorilor, factorilor de decizie şi

[1] Comandă, control, comunicaţii, computere, informaţii, supraveghere şi recunoaştere.

sistemelor acţionale, oferind comandanţilor o mai bună înţelegere a situaţiei, încredere şi control.

Rolul central al reţelei determină o trecere de la schimbul informaţional punct la punct între sisteme eterogene, la un acces informaţional între surse multiple bazat pe mecanisme de modelare, identificare şi publicare a datelor într-un spaţiu colaborativ, geografic distribuit. Perfecţionarea sistemelor C4ISR în contextul acţiunilor militare întrunite reprezintă o condiţie esenţială nu numai pentru asigurarea succesului operaţional, ci şi pentru evitarea sau reducerea pierderilor proprii într-un spaţiu de luptă tot mai complex şi eterogen.

Modernizarea sistemelor C4ISR în Armata României este determinată de criteriile şi cerinţele minime de performanţă impuse de angajamentele politico-militare, fiind fundamentată pe abordările arhitecturale orientate spre servicii, cerinţele de interoperabilitate şi tehnologice adecvate noilor concepte referitoare la managementul informaţiilor şi la asigurarea comenzii şi controlului în timp aproape real.

Concepţia de dezvoltare a capabilităţilor C4ISR formulează direcţii şi opţiuni de perfecţionare, revizuire conceptuală şi dezvoltare coerentă în Armata României a acestei categorii de capabilităţi, în perspectiva apropiată, pe termen mediu şi lung.

1. Ipoteze de planificare

Comanda şi controlul se asigură în conformitate cu Concepţia privind comanda şi controlul structurii de forţe în Armata României, aprobată prin hotărârea CSAT nr.33/2010.

Sistemul de comandă şi control este realizat din timp de pace fiind completat în situaţii de criză şi război astfel încât la nivel strategic modificările şi restructurările sistemului de sprijin C4ISR să fie minime, realizându-se în principal pentru dezvoltarea şi integrarea componentelor dislocabile şi mobile.

Sistemul C4ISR se compune din sistemele de senzori şi de prelucrare a informaţiilor ISR, centrele de comandă şi sistemele acţionale, angajate în operaţii întrunite la nivel tactic, operativ şi strategic, interconectate în cadrul unei infrastructuri de reţea şi informaţionale capabile să asigure superioritatea informaţională şi decizională în conformitate cu principiile Capabilităţilor facilitate de reţea - NEC.

Capabilităţile facilitate de reţea reprezintă abilitatea cognitivă şi tehnică de a constitui o federaţie a diferitelor componente ale mediului operaţional de la nivelul strategic până la cel tactic, prin realizarea Infrastructurii de reţea şi informaţionale.

Sistemul C4ISR utilizează structuri şi baze de date, realizate într-un format compatibil NATO -JC3IEDM[2], specificat în Strategia datelor aprobată la nivelul MApN, precum şi aplicaţii specifice pentru sprijinul C2, implementând soluţii adecvate de modelare şi simulare pentru asistarea deciziei. Dezvoltarea acestora este abordată într-o arhitectură deschisă, ce se bazează pe o combinaţie a infrastructurilor pentru reţele de arie largă fixe, dislocabile temporar şi mobile, destinate asigurării serviciilor de transport, rutare, integrare, securitate, management, precum şi a celor evidenţiate ca aplicaţii comune sau specializate la nivelul utilizatorilor. În principal, aceaste infrastructuri sunt incluse şi realizate prin implementarea conceptului Infrastructurii comune criptate pentru transmisii de date - ICCTD. Sistemul de transmisiuni al ICCTD este asigurat prin servicii de transport centrale, de distribuţie şi acces, furnizate de operatori militari, guvernamentali şi comerciali astfel:

- Reţeaua militară naţională de comunicaţii – RMNC cu componentele sale în serviciu:

[2] Joint C3 Information Exchange Data Model

- Reţelele private de date ale MApN: Intraman şi INTRASS (în curs de implementare)
- Serviciile de comunicaţii electronice asigurate de Serviciul de Telecomunicaţii Speciale
- Serviciile de comunicaţii electronice asigurate de furnizori ai Infrastructurii comune de date a statului - Telecomunicaţii CFR, Teletrans, SNRadiocom.
- Serviciile de comunicaţii electronice comerciale asigurate de Romtelecom, RDS-RCS, Vodafone etc.

În vederea realizării acestei infrastructuri este necesară o estimare cât mai realistă, pornind de la dimensionarea cantitativă a resurselor de acest tip în locurile de dispunere permanentă a componentelor sistemului C4ISR.

Puncte de comandă (amplasamente fixe) Comandamente de nivel strategic şi operativ Medie – 100 utilizatori	Campusuri /garnizoane Medie >500 utilizatori	Campusuri /garnizoane Medie 300-500 utilizatori	Campusuri /garnizoane Medie 100-300 utilizatori	Unităţi în cazărmi independente, depozite, sisteme radar /garnizoane Medie < 50 utilizatori
8[3]	12	70	150	250

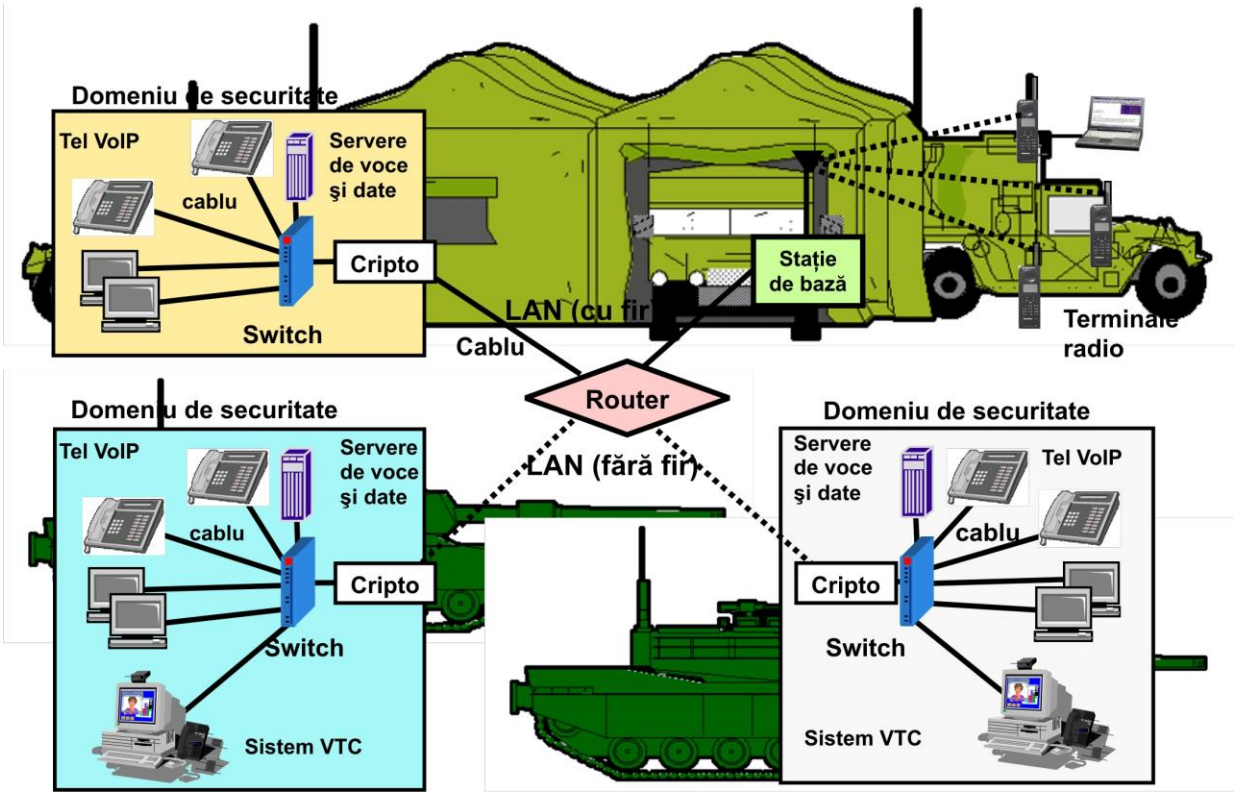
Deşi principalele aplicaţii vor folosi soluţii de tip portal şi arhitecturi orientate spre servicii în general bazate pe tehnologii web, traficul de mesaje cu fişiere ataşate va continua să reprezinte o cerinţă importantă. Folosind o repartiţie medie a volumului de trafic în 3 domenii de securitate separate fizic la nivelul reţelelor locale, putem estima 60-70% trafic în domeniul NESECRET (naţional şi echivalent internaţional), 20-25% trafic în domeniul SECRET DE SERVICIU (naţional şi echivalent internaţional), respectiv 5-20% trafic până la STRICT SECRET (naţional şi echivalent internaţional). Distribuţia geografică a acestuia este neomogenă şi dinamică în raport cu cerinţele misiunilor şi sarcinilor esenţiale ale utilizatorilor.

Pentru cei aproximativ 75-80000 de utilizatori activi care au prin intermediul staţiilor de bază individuale sau utilizate în comun acces la domeniul SECRET DE SERVICIU, în aproximativ 500 de campusuri, sunt în prezent necesare în medie 400 puncte de prezenţă sau interfeţe de acces la cele 3 infrastructuri asociate domeniilor de securitate mai sus menţionate.

Într-o dislocare temporară specifică unei operaţii de nivel întrunit desfăşurată pe teritoriul naţional, se estimează în zona de responsabilitate a unei divizii prezenţa unui total aproximat la 15-20000 utilizatori din care peste 1/3 pe platforme mobile, dispersaţi sau regrupaţi, cu următoarele cerinţe de conectivitate la o infrastructură comună.

Punctele de comandă ale D.I (de bază/rezervă/ logistic /înaintat) şi alte elemente de sprijin/logistice Medie – 75-100 u	Puncte de comandă 5-6 Cdm.Bg (de bază/rezervă/ logistic/înaintat) Medie-50-75 u	Puncte de comandă tactice 20-24 B şi entităţi C2 echivalente (de bază/rezervă/ logistic/înaintat) Medie 25-100 u	Alte entităţi tactice sub comandă operaţională Medie 50-100 u	Platforme mobile, sisteme de senzori Medie < 50 u
10	24	100	100	200

[3] 4 în Bucureşti



2. Perspective de abordare a capabilităţilor C4ISR

Având în vedere resursele disponibile şi planurile curente putem avea în vedere următoarele priorităţi:

A. Pe termen scurt 2012-2015

a. Realizarea capabilităţilor C4ISR pentru forţele dislocabile asigurând cu prioritate:

1. Interfeţe informaţionale pentru transfer între domeniile de reţea
2. Mesagerie organizaţională cu implementarea serviciilor X.500, compatibilă NATO
3. Implementarea unui sistem C2IS pentru componenta operaţională terestră
4. Infrastructură dislocabilă pentru 9-12 Sisteme de arie locală (LAS) /TOC-uri naţionale
5. Integrare date de la surse multiple, inclusiv UAS-uri, generare şi diseminare a datelor despre situaţia terestră - LGP/COP

b. Iniţierea Programului – Sistem de comunicaţii şi informatic pentru Reţeaua naţională integrată a punctelor de comandă pentru dispunerea elementelor de conducere strategică - CIS-RNI PCS

1. Instalarea capabilităţilor CIS proiectate în punctele de comandă de bază
2. Creşterea capacităţilor de conectare externă şi instalarea punctelor de prezenţă la punctele de comandă de rezervă

c. Implementarea Programului INTRASS

d. Extinderea Intraman până la unităţile luptătoare, de sprijin şi logistice terestre de nivel batalion.

e. Menţinerea în stare operaţională a SCCAN, finalizarea proiectelor NATINADS şi introducerea unor noi capabilităţi

f. Iniţierea implementării NAVCIS, complementar proiectului NATO - BRASS şi operaţionalizarea Link 11 la dezvoltarea prevăzută în planuri

g. Implementarea proiectelor C4ISR specifice mediului operaţional terestru

B. Pe termen mediu 2015-2020
   a. Dezvoltarea şi integrarea capabilităţilor ISR
   b. Implementarea Programului PC Bg/PC D
   c. Implementarea capabilităţii Link16/MIDS la nivel naţional concomitent cu viitoarele sisteme de apărare aeriană şi de management al spaţiului aerian
   d. Finalizarea punctelor de comanda de bază
      1. Realizarea capabilităţilor de generare şi diseminare ISI
      2. Activarea Centrelor de date/NOC în configuraţia finală
   e. Modernizarea RMNC
      1. Creşterea capacităţilor de bandă
      2. Convergenţă IP pentru nivelul central, de distribuţie şi acces
      3. Modernizarea soluţiilor de management şi introducerea acordurilor privind nivelul de servicii de tip SLA
   f. Iniţierea implementării unui sistem integrat de sprijin al acţiunilor militare folosind o soluţie de tip ERP
   g. Finalizarea implementării obiectivelor forţei relaţionate cu procesul de implementare a Capabilităţilor facilitate de reţea (NEC)

C. Pe termen lung - după 2020
   a. Integrarea infrastructurii de reţea şi informaţionale a apărării administrată de CCI ca operator guvernamental al MApN, în federaţia de reţele şi servicii naţionale şi internaţionale (NATO/UE) relevante pentru Armata României

3. Orientări privind dezvoltarea capabilităţilor C4ISR

Realizarea Infrastructurii de reţea şi informaţionale implică o viziune comună a tuturor beneficiarilor asupra îndeplinirii unui set minim de condiţii necesar integrării capabilităţilor, având în vedere sincronizarea dezvoltărilor în mediul cultural, al managementului informaţiilor şi al implementării noilor tehnologii.

Exercitarea funcţiilor de comandă şi control la nivel naţional solicită un sistem C4ISR robust, stabil, sigur, flexibil şi scalabil, cu componente şi servicii uşor de transportat, desfăşurat, configurat, utilizat, administrat şi menţinut, şi care să reclame în acest scop resurse minime umane şi materiale. Scopul său primordial este facilitarea înţelegerii spaţiului de operaţii, prin managementul eficient al informaţiilor, în vederea asigurării avertizărilor asupra situaţiei, producerii şi diseminării imaginii operaţionale comune, necesare angajării optime şi coerente a forţelor şi mijloacelor adecvate, pentru realizarea efectelor planificate.

Pornind de la structura capabilităţilor C4ISR rezultă că principalele direcţii de dezvoltare ar trebui să urmărească perfecţionarea componentelor sale: pregătirea personalului, managementul informaţiilor, procedurile şi angajarea soluţiilor tehnice şi tehnologice evolutive.

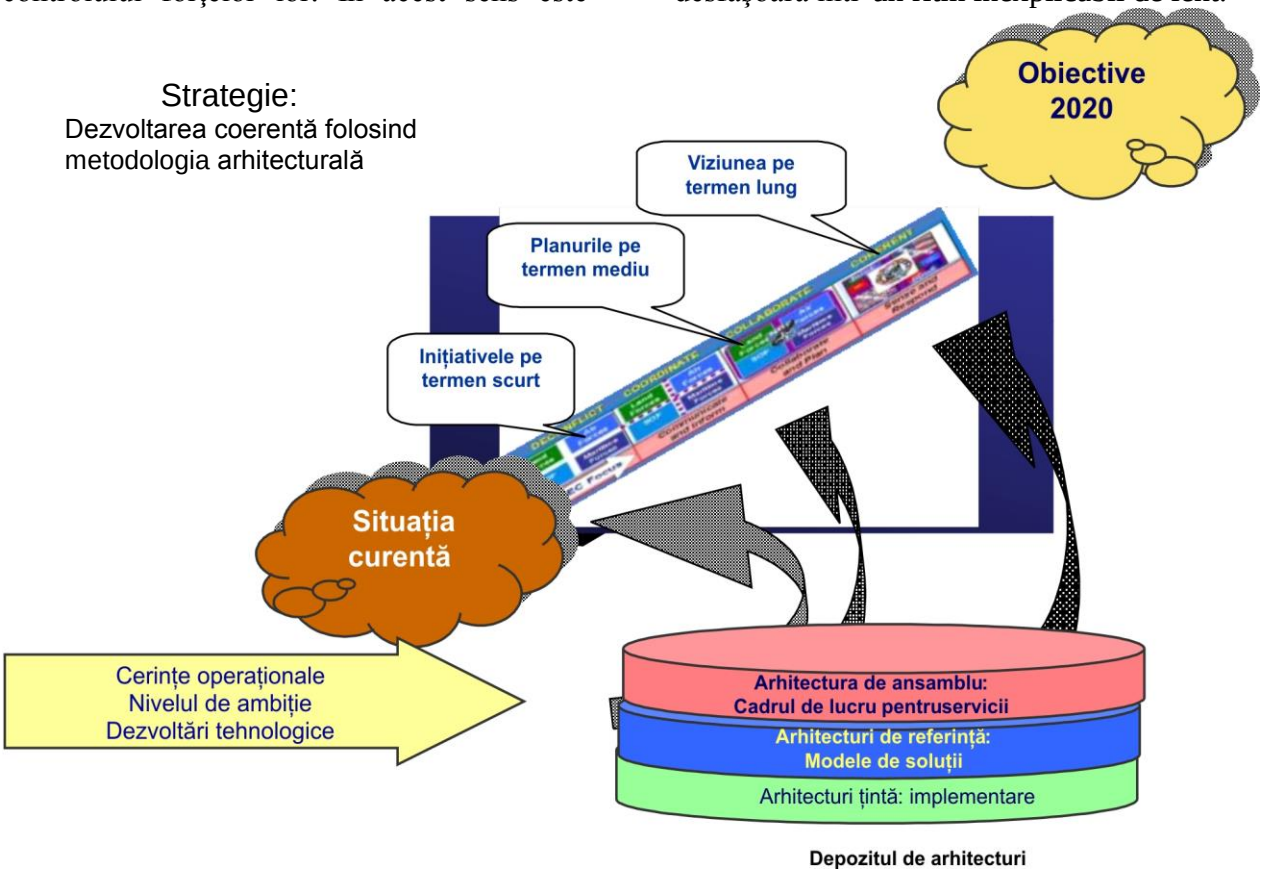
Sistemul trebuie să fie complet integrat, robust, flexibil şi să asigure secretul operaţiei, bazându-se pe o interconectare complexă în reţea a centrelor de fuziune a informaţiilor din punctele de comandă, precum şi pe integrarea serviciilor principale şi funcţionale într-o arhitectură client – server scalabilă. Totodată, pentru implementarea unui schimb de informaţii structurat, bazat pe tehnici de replicare automată a datelor este necesară folosirea unui model de date comun care să asigure construcţia şi distribuţia avertizărilor de

situaţie în cadrul imaginii operaţionale comune.

Necesitatea standardizării şi implementării procedurilor operaţionale permanente reprezintă o cerinţă imperativă pentru creşterea eficienţei şi a ritmului de derulare a proceselor operaţionale. Antrenarea personalului în aplicarea lor constituie baza optimizării proceselor C2.

Managementul informaţiilor, suportul analitic şi operarea sistemelor funcţionale depind, de asemenea, în egală măsură, de aspectele organizaţionale şi legale ale realizării sistemului C4ISR, care determină standarde procedurale ce pot facilita sau îngreuia desfăşurarea proceselor complexe de estimare, planificare, decizie şi evaluare, în cadrul desfăşurării operaţiilor întrunite. Comandanţii şi statele majore trebuie să beneficieze de un cadru juridic clar şi lipsit de echivoc pentru realizarea comenzii şi controlului forţelor lor. În acest sens este bineînţeles necesară definirea cu claritate a „lanţului de comandă" de la cele mai înalte autorităţi naţionale până la luptătorul dislocat în teatru, având în vedere cerinţele şi particularităţile scenariului operaţional, ale schimbului informaţional, regulile de angajare şi condiţiile transferului de autoritate. Este necesar totodată să se ia în considerare şi să se exerseze nivelurile de autoritate NATO pentru comandă şi control, precum şi modul de atribuire al acestora, prin reglementări naţionale care să vizeze şi sistemul propriu de pregătire al statelor majore.

O importanţă specială ar trebui acordată revederii unor aspecte doctrinare, în vederea preluării şi însuşirii principiilor « comenzii misiunii » şi al «descentralizării». Deşi această măsură ar avea un impact major asupra perfecţionării sistemelor de comandă şi control, asumarea şi aplicarea ei se desfăşoară într-un ritm inexplicabil de lent.



„Reducerea" distanţei dintre punctele de comandă, prin mijloace tehnice, permite experimentarea practică a conceptului de comandă distribuită care oferă flexibilitate maximă în reorganizarea sau adaptarea funcţională a comandamentelor pe principii modulare, pentru asigurarea redistribuirii sarcinilor şi orientării eficiente a controlului misiunii. O condiţie esenţială o constituie antrenarea entităţilor funcţionale, individual

şi în cadrul comandamentului, în vederea atingerii optimului funcţional şi a nivelului maxim de coeziune. Pregătirea ofiţerilor de stat major şi a specialiştilor trebuie corelată cu tehnologia asigurată pentru managementul informaţiilor. Lipsa pregătirii necesare organizării comenzii şi controlului şi prezenţa deficienţelor în asigurarea fluxurilor de informaţii pe verticală şi orizontală, precum şi în utilizarea ineficientă a sistemelor informatice poate afecta direct procesul de vizualizare, de producere şi distribuţie a imaginii operaţionale comune. Evaluarea pregătirii personalului pe timpul exercitării rolurilor şi funcţiunilor în cadrul comandamentelor trebuie să constituie baza pregătirii pentru operaţiile următoare precum şi pentru revederea procedurilor.

Tendinţele internaţionale privind dezvoltarea sistemelor C4ISR reflectă atât convergenţe generate de potenţialul tehnologic, tot mai dinamic în dezvoltările comerciale, cât şi modificări conceptuale substanţiale determinate de tipologia viitoarelor conflicte armate. Abordările operaţiilor bazate pe efecte solicită organizaţiile guvernamentale şi non-guvernamentale, mai mult ca oricând, să dezvolte o interacţiune complexă cu entităţile militare şi cele civile implicate într-o diversitate de scenarii operaţionale. Aceasta impune realizarea unei infrastructuri de reţea şi informaţionale comune, capabile să suporte aceste dezvoltări. În acest context, studiile de fezabilitate reclamă invariabil următoarele *obiective strategice* privind implementarea unei infrastructuri pentru servicii şi aplicaţii specifice constituită dintr-o federaţie complexă de sisteme şi resurse naţionale grupate sub sintagma C4ISR:

a) Infrastructura de comunicaţii caracterizată prin adoptarea şi utilizarea Protocolului internet (IP), ca mecanism comun şi viabil de transport pentru toate tipurile de informaţii şi medii de transmisiuni asociate fiecărui tip de transport. Această viziune este determinată în principal de cerinţele critice ale operaţiilor expediţionare care solicită, în cadrul unui proces de lungă durată, adoptarea şi implementarea IPv6, mai întâi în infrastructura reţelelor staţionare şi ulterior în extensiile lor mobile, pe baza standardizării interfeţelor pentru comunicaţii prin satelit, concomitent cu adaptarea şi optimizarea reţelelor mobile, în vederea asigurării traficului IP şi al implementării criptării IP, folosind un sistem adecvat de management criptografic, destinat să faciliteze realizarea unei aşa numite reţele nucleu cu identitate virtuală, capabilă să integreze servicii de voce şi date pentru domenii de utilizatori cu niveluri multiple de securitate a informaţiilor. Totodată, în vederea unei tranziţii rapide de la tehnologiile prezente în diferite sisteme tactice, la cele viitoare, este anticipat un progres rapid în identificarea soluţiilor care să permită transferul informaţional între reţelele IP şi non-IP, folosind mecanisme de interfaţă standardizate care vor asigura servicii informaţionale de proximitate pe nivelul infrastructurii de comunicaţii. *Pe termen scurt şi mediu,* primele soluţii aflate în curs de implementare vizează interfaţa reţelelor IP cu reţelele de date tactice (TDL). Adoptarea comună, pe scară largă, a mecanismelor de transport IP solicită un progres semnificativ şi continuu, în special pentru sprijinul utilizatorilor mobili, în zone de maxim interes cum ar fi: standardizarea formelor de undă; implementarea unor arhitecturi software comune pentru mijloacele radio tactice; utilizarea mai eficientă a spectrului de radiofrecvenţă şi a protocoalelor destinate funcţiilor de reţea în reţelele mobile. *Pe termen lung,* obiectivul principal în implementarea reţelelor IP mobile depinde de viteza de evoluţie a protocoalelor destinate aşa numitelor reţele mobile ad-hoc (MANET) care vor include soluţiile pentru suportul necesar calităţii serviciilor. Aceasta implică activităţi de cercetare, dezvoltare a concepţiei şi experimentare.

b) Componenta informatică şi de integrare este caracterizată prin utilizarea arhitecturilor orientate pe servicii (SOA), capabile să prezinte funcţiile software sub forma unor servicii care pot fi descoperite şi invocate oriunde în reţeaua globală. Utilizarea SOA uşurează accesul distribuit la

date şi aplicaţii, şi furnizează un mecanism flexibil pentru reutilizarea serviciilor existente, facilitând dezvoltarea unor servicii informaţionale noi. Un scop primar al abordării SOA este de a face resursele informaţionale disponibile tuturor „consumatorilor" din reţea şi de a sprijini descoperirea şi livrarea eficientă a acestor informaţii către beneficiari. Utilizarea abordării SOA solicită adoptarea unei strategii comune privind datele, centrată pe reţea, pentru a asigura informaţiilor vizibilitate, accesibilitate, inteligibilitate şi interoperabilitatea cu alte surse de informaţii. Asigurarea credibilităţii informaţiilor obţinute şi a capacităţii de a fi furnizate şi procesate corect, constituie un factor de succes. Abilitatea de a asigura accesul la informaţii într-un mod sigur, flexibil, bazat pe rolul funcţional al utilizatorilor, rapid configurabil în raport cu modificările politicilor de securitate şi informaţionale, reprezintă fundamentul succesului pe termen lung. Obţinerea beneficiilor prevăzute de abordarea SOA impune realizarea unui acord asupra unui set standardizat de servicii principale, care să acopere zone cum ar fi: securitatea serviciului de descoperire; managementul metadatelor; managementul identităţii; managementul serviciilor şi medierea. Utilizarea abordării SOA nu va ignora utilizatorii finali ai reţelelor non-IP. Progresul rapid în domeniul *„distribuţiei secretizate a informaţiilor bazate pe text"*, împreună cu progresul înregistrat în domeniul *„tehnologiilor facilitate de XML"* constituie direcţiile generale în dezvoltarea serviciilor informatice şi de integrare *pe termen scurt şi mediu*. Mesageria robustă şi secretizată de tip – e-mail, oficială, instantanee – constituie baza dezvoltării acestor servicii iar abilitatea de a asigura suportul schimbului de informaţii secretizat, bazat pe text, arată că informaţia codată XML poate fi, de asemenea, procesată şi schimbată în mod secretizat. Aceasta va sprijini, bineînţeles, interacţiunile între baze de date, aplicaţii şi utilizatori, pentru a facilita dezvoltarea unei game largi de servicii informaţionale secretizate şi interoperabile.

c) Elementele principale ale managementului şi controlului de sistem implică asigurarea acestor funcţii esenţiale, în mod secretizat, între utilizatorii finali, prin folosirea acordurilor asupra nivelului de serviciu de-a lungul unor federaţii de sisteme, administrate independent, incluzând suportul necesar asigurării calităţii serviciilor. Acordurile asupra nivelului de serviciu (SLA) joacă un rol vital în arhitectura globală prin garantarea nivelului adecvat de performanţă. Cererea pentru furnizarea nivelurilor adecvate de performanţă este adesea crucială în domeniul tactic, acolo unde capacitatea de bandă este în mod uzual limitată. Îndeplinirea acestei viziuni depinde de progresele tehnice care vor fi înregistrate în diferite sectoare cum ar fi: asigurarea unor capacităţi de bandă crescute utilizatorilor mobili, noi servicii de securitate şi corelarea dinamică a acordurilor de tip SLA între diferitele segmente de reţea administrate în prezent independent.

d) Elementele principale ale asigurării informaţionale se constituie în cadrul unor mecanisme care permit perfecta lor integrare în arhitectura generală, pentru asigurarea obiectivului primar de protecţie a informaţiilor atât în domeniul staţionar cât şi în condiţii de mobilitate. Aceste mecanisme au ca scop să garanteze că informaţia adecvată poate fi furnizată celor care au nevoie de ea, la momentul potrivit şi că această informaţie este credibilă şi veridică. Armonizarea abordării principiului *„datoriei de a distribui cu cel al nevoii de cunoaştere"* rezumă sintetic această intenţie. Se exprimă astfel dezideratul ca politicile, procedurile, serviciile şi sistemele C4ISR să fie dezvoltate şi implementate cu o capacitate inerentă de a distribui informaţiile, aplicând măsurile de securitate necesare pentru a garanta că numai utilizatorii autorizaţi pot avea acces la aceste informaţii. *Pe termen scurt* implementarea soluţiilor de criptare IP şi a infrastructurilor optimizate pentru managementul

criptografic reprezintă obiective critice. *Pe termen mediu,* infrastructura cu chei publice (PKI) şi tehnologiile XML pot facilita implementarea unor scheme de acces la informaţii dinamice, bazate pe rolul funcţional şi pe politicile de securitate şi informaţionale. Una din provocările majore o constituie abilitatea de a implementa o infrastructură PKI interoperabilă şi o schemă de management a identităţii care să asigure suportul schemelor de acces informaţional. Continuarea rapidă a dezvoltărilor tehnologice în zonele mai sus menţionate reprezintă o condiţie necesară pentru îndeplinirea aspiraţiilor pe termen lung privind securitatea informaţiilor aliniată la conceptul „securităţii informaţiilor bazate pe conţinut", în care se apreciază că informaţiile sunt protejate la nivelul „obiectului informaţional" iar accesul este controlat pe baza identităţii utilizatorilor şi a rolului pe care aceştia îl au în cadrul unei operaţii particulare. Performanţele din domeniul criptografic, al implementării unor noi soluţii referitoare la managementul criptografic şi la deciziile de acces rapid, bazate pe politici, necesită modificări majore de nivel tehnologic dar şi o revoluţie în domeniul cultural.

4. Direcţii generale de acţiune

În plan conceptual şi normativ este necesară*:*

- Definirea procesului de management al capabilităţilor C4ISR care coordonează proiectarea, implementarea (experimentarea, achiziţia, realizarea / configurarea, integrarea, testarea, validarea), operarea şi întreţinerea lor pe întregul ciclu de viaţă, abordând toate aspectele de dezvoltare a capabilităţii (pregătirea personalului, infrastructură, logistică proprie etc.).
- Aplicarea metodologiei şi a „Cadrului de lucru arhitectural NATO" în formularea cerinţelor operaţionale, definirea concepţiei de întrebuinţare şi în proiectarea soluţiilor tehnice.
- Adoptarea politicilor, strategiilor şi directivelor NATO în domeniul implementării măsurilor INFOSEC, concomitent cu dezvoltarea propriilor reglementări.
- Monitorizarea dezvoltărilor referitoare la implementarea „capabilităţilor facilitate de reţea" în statele NATO şi la nivelul Alianţei, focalizând cerinţele de interoperabilitate.

În plan tehnologic se va urmări:

- Asigurarea proceselor de adaptare, preluare şi implementare a recomandărilor de standardizare NATO, folosind arhitectura de referinţă pentru sisteme C4ISR dislocabile şi alte programe relevante.
- Implementarea unor soluţii şi mecanisme de interoperabilitate precum şi a politicilor de securitate a informaţiilor referitoare la interconectarea cu sistemul NATO (Bi-SC AIS) a elementelor dislocabile din structura forţelor naţionale, care ar putea fi desfăşurate în operaţii NATO. Definirea cerinţelor, elaborarea conceptului de operare, proiectarea şi realizarea unei soluţii „IEG Case B"[4] pentru schimbul informaţiilor între domeniile de securitate naţional şi NATO, indispensabilă asigurării unei infrastructuri C2 distribuite. Extinderea capacităţii de interconectare între sistemele naţionale şi NGCS / Bi-SC AIS constituie totodată o prioritate esenţială pentru participarea la operaţiile Alianţei.
- Implementarea la nivel naţional a unei soluţii de infrastructură şi transport pentru o reţea bazată pe IPv6, cu servicii integrate de date şi multimedia, ce poate fi extinsă prin satelit (X, C, Ku), folosind acorduri de servicii cu operatorii capabili să asigure zona de acoperire necesară. Această infrastructură critică trebuie să permită implementarea modulară şi coerentă a serviciilor şi aplicaţiilor comune şi funcţionale, în cadrul componentei staţionare şi mobile a subsistemului de comunicaţii şi informatic extins, din cadrul sistemului C4ISR, folosind soluţii comerciale.

[4] Information Exchange Gateway Case B (IEG Case B) – se referă la interconectarea Bi-SC AIS cu o reţea naţională acreditată NATO Secret pentru partajarea resurselor şi serviciilor necesare schimbului de informaţii în conformitate cu un acord.

- Dezvoltarea facilităţilor şi sistemelor informatice relevante pentru punctele de comandă prin realizarea unor module de comandament dislocabile, care să sprijine cerinţele schimbului informaţional şi accesul la resursele naţionale de comunicaţii disponibile la nivel strategic în orice zonă de operaţie.
- Implementarea capabilităţilor radio definite software (SDR) şi a soluţiilor Wi-LAN (cu aplicaţii de securitate integrate) precum şi a comunicaţiilor bazate pe standarde civile (de exemplu, TETRA, PRR).
- Proiectarea şi dezvoltarea unui sistem C4ISR folosind o arhitectură client-server, modulară şi capabilă să asigure serviciile generale (mesagerie oficială, web, colaborare, suport GIS, suport de stat major etc.) precum şi pe cele specifice zonelor funcţionale (imagini operaţionale, aplicaţii sau sub-sisteme şi servicii specifice) folosind implementarea evolutivă a produselor comerciale şi a soluţiilor de securitate militare, pentru extinderea sistemelor informatice strategice.

Din perspectivă procedurală:

- Implementarea unui model unitar pentru prelucrarea şi schimbul datelor, care să asigure proiectarea şi realizarea aplicaţiilor necesare managementului informaţional integrat, adaptabil la politicile şi strategiile NATO în domeniu, este esenţială pentru toate dezvoltările ulterioare. În acest context, se evidenţiază ca prioritară implementarea unei strategii privind administrarea datelor. Totodată, este necesară adaptarea naţională a mecanismelor de replicare a datelor şi funcţiilor colaborative definite în cadrul „Programului multilateral de interoperabilitate" (MIP Block 2) pe baza modelului LC2IEDM, nucleul modelului de referinţă NATO, (STANAG 5523 / ADatP-32), pentru a dezvolta interfeţe cu alte sisteme (C4ISR) atât la nivelul unor comandamente naţionale, NATO, cât şi pentru asigurarea unor soluţii de interoperabilitate în scenarii de coaliţie.
- Implementarea unor soluţii de administrare a reţelelor militare bazate pe concepte moderne de management al serviciilor şi implementare a noilor tehnologii specifice.

Din perspectivă organizaţională cele mai semnificative măsuri vizează:

- Introducerea în structurile organizatorice de stat major de la toate eşaloanele a rolului de ofiţer şef pentru managementul informaţional.
- Transformarea Comandamentului comunicaţiilor şi informaticii într-un operator şi furnizor militar de infrastructuri, reţele, sisteme şi servicii C4ISR la scară naţională, având ca obiectiv principal asigurarea calităţii, eficienţei şi eficacităţii acestor servicii pentru structura de comandă şi în sprijinul structurii de forţe a Armatei României.

Alte direcţii se referă la*:*

- Implementarea conceptelor şi procedurilor standard pentru C2 în timp real, care să asigure utilizarea serviciilor web, a mesajelor text în format NATO (ADatP-3) şi a comunicaţiilor de date tactice (Link 16, 22), pentru C2 şi generarea / administrarea imaginii recunoscute aeriene şi navale în vederea asigurării imaginii operaţionale comune întrunite.
- Implementarea sistemelor de monitorizare a dispunerii forţelor (avertizare asupra situaţiei) bazate pe tehnologii de localizare (GPS), identificare şi navigaţie moderne şi integrarea acestora în sistemul C4ISR naţional.
- Implementarea unor sisteme mobile de senzori pe platforme aeriene nedeservite (UAS), în configuraţia curentă a spaţiului operaţional, pentru asigurarea funcţiilor de detecţie, supraveghere, indicare şi achiziţie ţinte, pornind de la cerinţele domeniului tactic şi integrarea acestora în sistemul C4ISR naţional.
- Analiza unor parametri critici pentru funcţionarea sistemului C4ISR cum ar fi stabilitatea, disponibilitatea şi capacitatea de transmitere a acestuia, a criteriilor şi valorilor de prag pentru infrastructurile critice ale capabilităţilor C4ISR.

IMPLICAŢIILE CORELAŢIEI SPAŢIU, TIMP, TEHNOLOGIE ASUPRA PREGĂTIRII ŞI DESFAŞURĂRII OPERAŢIILOR ÎNTRUNITE ÎN RĂZBOIUL VIITORULUI

Colonel dr. Ionel CIOBANU
Comandamentul comunicaţiilor şi informaticii

Motto:
"Războiul nu s-a sfârşit. ... întrucât se pare că războiul este un însoţitor permanent al societăţii omeneşti....Există un război informaţional, un război economic, ...un război în ciberspaţiu"
Gen. dr. Mircea MUREŞAN, Gen.bg. dr. Gheorghe VĂDUVA
– Războiul viitorului, viitorul războiului –

Conflictele armate ale ultimului secol şi studiul doctrinelor armatelor moderne, atestă cu claritate *implicaţiile corelaţiei spaţiu, timp, tehnologie asupra pregătirii şi desfăşurării operaţiilor întrunite în războiul viitorului* şi ne arată foarte clar că sensul revoluţiei fenomenului militar în secolul 21, va fi dat de *mutarea centrului de greutate de pe dimensiunea cantitativă, pe cea calitativă care implică în cel mai înalt grad folosirea inteligenţei umane, ca bază esenţială a războiului informaţional şi ca supremă confirmare a rolului tehnologiei în războiul viitorului.*

În prezenta lucrare doresc sa emfazez, ca parte decisivă a corelaţiei tehnologie – operaţii întrunite în războiul viitorului, formele de bază ale războiului informaţional şi implicaţiile acestora in corelaţia spaţiu, timp, tehnologie ce acţionează în slujba luptătorului modern, în cadrul acţiunilor militare. În continuarea exerciţiului nostru ideatic vom prezenta unele aspecte ale acţiunilor militare şi legătura cu mediul informaţional.

Militarii nu pot opera într-un mediu informaţional complet izolat. Multiplele infrastructuri de comunicaţii care compun mediul informaţional actual sunt extrem de interdependente. Ca orice element viu, dinamic, şi formele războiului informaţional la nivel operativ comportă aprige dispute teoretice.

În principiu, analiştii militari definesc şi apreciază ca operaţionale, în acţiunile militare, şapte forme de bază ale războiului informaţional - care implică protecţia, manipularea, degradarea şi anularea informaţiei: *Războiul de comandă şi control (C2W- Command and Control Warfare); Războiul "supremaţiei informaţiilor" (IBW- Intelligence- Based Warfare); Războiul electronic(EW- Electronic Warfare); Războiul psihologic(PSIW- Pshyhological Warfare); Războiul hackerilor sau „pirateria software" (HW- Hacker Warfare); şi Războiul în spaţiul de luptă al realităţii virtuale (CybW- Cyber Warefare).*

În prezentul referat am optat pentru a dezvolta unele aplicaţii de noutate, aparţinând Războiului psihologic (PSYW - psychological warefare) şi Războiului informaţiilor economice (EIW- Economic Information Warefare), ce în opinia mea conţin multe elemente de modernitate în acţiunile militare.

1. RĂZBOIUL PSIHOLOGIC (PSIW- PSHYHOLOGICAL WARFARE)

În concepţia unor specialişti informaţia în războiul psihologic este utilizată pentru a modifica atitudinile şi opţiunile amicilor, neutrilor şi adversarilor, în funcţie de interesele existente, în aşa fel încât să fie afectată îndeplinirea

obiectivelor politico- militare ale acţiunilor militare.

Imaginile curente ale conflictelor desfaşurate pe diverse meridiane, pe care le vedem mediatizate în cadrul emisiunilor de ştiri, au devenit deja un lucru care nu mai şochează. Puţini dintre noi mai simt compasiunea şi empatia cu suferinţa victimelor, pentru că noi înşine am devenit un alt fel de victime, am devenit "publicul ţintă", victima informaţiilor prezentate cu un anumit înveliş pe care noi în vâltoarea vieţii de zi cu zi nu mai avem puterea să-l judecăm cu propriile minţi. Nu ni se cere decât să credem fără să cercetăm, pentru că mijloacele noastre sunt sumare sau chiar inexistente.

Cum putem să ne protejăm minţile de prejudecăţile proprii şi cum să decelăm adevărul de neadevăr? Probabil, este extrem de dificil, chiar şi asimilând mijloacele de protecţie, să susţinem cu tărie că am fi în posesia adevărului nealterat, dar putem să ne asigurăm un anumit grad de obiectivitate cultivându-ne minţile prin cunoaşterea acelor elemente folosite ca arme potenţiale pentru disimularea adevărului sau chiar schimbarea acestei valori în neadevăr.

Conflictele actuale indiferent de eşalon se desfăşoară cu alte forme decât cele convenţionale şi una dintre forme este cea a războiului informaţional, forma supremă şi superioară de desfăşurare a unei bătălii, care nu va fi transparentă în ştirile zilnice decât pentru cei ce ştiu să aprecieze valoarea informaţiilor, pentru cei ce ştiu şi doresc să vadă faptele din ambele ipostaze, de victimă şi de agresor. Fenomenul PSYW este unul dintre cele mai contestate fenomene pentru că argumentaţia este săracă şi greu de evaluat.

Acest lucru nu a împiedicat desfăşurarea unor programe ample în timpul Războiului Rece, între cele două superputeri reprezentante ale blocurilor militare aflate în război informaţional. Eşecul unor experimente însoţite de aspectul din ce în ce mai important, al potenţialelor încălcări ale drepturilor omului, au condus la sistarea acestor programe, principalul motiv fiind ignoranţa generală în ceea ce priveşte capacitatea minţii umane de a produce efecte materiale - *telekinezia* - sau nemateriale - *telepatia*.

În mod cert au existat probabil şi rezultate pozitive care nu au fost publicate. Această afirmaţie nu este gratuită, deoarece în cartea "Război şi anti-război" (Editura Antet, 1995), scrisă de Alvin şi Heidi Toffler, autorii menţionează posibilitatea surprinzătoare prezentată de Generalul Maior Sidney Schachnow de la Comandamentul de Operaţiuni Speciale ale SUA, în iulie 1992, a unei "linii temporale tehnologice" proiectată pâna în anul 2020, care preconiza dezvoltarea unor activităţi ca "mijloace de identificare ADN dobândite fraudulos", "înlocuire integrală a sângelui" şi chiar "telepatie sintetică".

O altă informaţie interesantă prezentată în aceeaşi carte este cuprinsă într-un citat al colonelului Craig Chidress, expert al Pentagonului în operaţiunile speciale, care spune "vom avea nevoie să folosim realitatea virtuală şi inteligenţa artificială" în repetiţii şi în lupta propriu-zisă; în acelaşi citat se face şi referirea asupra influenţării psihologice a adversarului "adăugând realităţii virtuale inteligenţa artificială" prin schimbarea realitaţii aparente, astfel "băieţii răi" să creadă că o uşă se deschide la dreapta când de fapt se deschide la stânga".

Totul pare desprins dintr-un scenariu SF sau a jocurilor video. Să nu uităm totuşi sursa acestor menţiuni. Dintotdeauna, oamenii au ridiculizat asemenea afirmaţii ce nu par a fi susţinute în realitate, dar această atitudine nu este generată decât de propria ignoranţă. *Cea mai bună atitudine este cea de tip platonician: "dar dacă totuşi ...".*

Dacă există asemenea informaţii, cu siguranţă există şi premisa materializării

mijloacelor de folosire a unor asemenea arme, la orice eşalon. Justificarea materializării lor este susţinută de zona în care există şi viitorii utilizatori ai acestor mijloace, şi anume oamenii implicaţi în "SPECIAL OPERATIONS" care argumentează că acestea "*sunt o armă rafinată care se poate folosi preventiv - pentru a decapita un conflict mai amplu, a sufoca războaiele mici, a distruge armele de nimicire în masă şi alte scopuri pozitive*". Eludând aspectul moral al utilizării lor, forma aceasta de război "*va deveni mai importantă fiindcă guvernele vor găsi în el o variantă relativ mai puţin costisitoare - în comparaţie cu scoaterea pe câmp a marilor forţe convenţionale - pentru a-şi atinge ţelurile*".

În ultima vreme, mai mult ca oricând trebuie ca toţi să ne acordăm respectul cuvenit faţă de propria fiinţă în primul rând şi apoi faţă de ceilalţi oameni, să reflectăm încrezători asupra cunoaşterii unor lucruri care par greu de înţeles sau desprinse de orice context.

În sprijinul aserţiunilor noastre vom încerca să prezentăm succint, câteva variante de acţiune a *războiului psihologic desfăşurate de către SUA şi Marea Britanie*. Facem precizarea că efectele PSYW sunt identice şi la nivel operativ cu cele ce vor fi prezentate de noi şi de asemenea simţim nevoia de a apela la elemente de noutate, ştiut fiind faptul că pe această linie există o abundentă literatură de specialitate.

Abilitatea de a gestiona şi a schimba percepţiile unui public ţintă este considerată al patrulea instrument al puterii în SUA, celelalte trei fiind puterile diplomatice, economice şi militare. Statele ce nu posedă capabilităţile pentru gestionarea percepţiilor şi pentru contracararea acestora, tind să devină vulnerabile la atacul forţelor externe ce au ca obiectiv distrugerea moralului şi a culturii şi schimbarea autorităţilor legal alese a ţării atacate.

Expresiile războiului psihologic (PSYW), gestionarea percepţiilor, propaganda precis dirijată se referă la aceleaşi tehnici de influenţare a minţii oamenilor. Această putere are două aspecte: unul „tare" şi celălalt „moale".

Aspectul *„tare"* vizează crearea în mintea oamenilor a unor percepţii negative la adresa statului, guvernului şi societăţii din care provin în măsură să sădească germenii înstrăinării.

Aspectul *„moale"* se referă la proiecţia în faţa audienţei ţintă, a unor imagini atractive a statului sau a grupului, direcţionând propaganda în măsură să creeze dorinţa acestora de a-şi urma conducătorii.

Ambele aspecte au ca scop final subminarea minţii auditoriului şi influenţarea acestuia pentru a acţiona inconştient, la comanda directă a propagandei statului sau a unui grup de influenţă. Dintre armele valide pentru acest exerciţiu al puterii enumerăm: pamflete şi cărţi editate, radio, TV, faxul şi telefonul, E-mail, CD-ROM şi Internetul.

Până la al II-lea Război Mondial, armele folosite au fost în special pamfletele editate. Radioul a devenit un instrument important al propagandei în timpul războiului. Forţele naziste au fost infrânte nu numai de către puternica superioritate militară a Aliaţilor, cât şi de „maşina" de propagandă mai bună a acestora, în special, de către BBC, care a subminat voinţa poporului german de a continua lupta.

În timpul Războiului Rece, maşina de propagandă a Lumii Vestice a fost direcţionată împotriva statelor comuniste din Estul Europei, Asia şi Cuba ca şi împotriva acelor state din Lumea a Treia, inclusiv India care dispuneau de mişcări puternice comuniste şi socialiste.

Un fapt puţin cunoscut este că în Actul Naţional de Securitate al SUA din 1947, sa dispus ca, Consiliu Naţional de Securitate şi CIA să îşi împartă responsabilităţile. CIA a primit misiunea să coordoneze funcţionarea organizaţiilor de informaţii ale diferitelor departamente ale guvernului şi să nu îşi permită transformarea

ei într-o independentă agenţie de colectare de informaţii.

Când importanţa războiului psihologic împotriva comunismului şi a socialismului a crescut, CIA, care deţinea majoritatea experţilor din domeniul informaţiilor şi a războiului psihologic din al II-lea Război Mondial, a fost rugată să îşi asume responsabilitatea pentru conducerea războiul psihologic. Mai târziu, când acţiunile acoperite împotriva statelor şi a indivizilor au devenit prioritare, agenţia şi-a sporit responsabilitatea şi asupra colectării informaţiilor.

Serviciul Secret de Informaţii (SIS) al Marii Britanii, idealişti cunoscuţi ca MI6, care reprezintă agenţia externă de informaţii a Marii Britanii, s-a distins de asemenea în războiul psihologic şi acţiuni sub acoperire în timpul războiului.

CIA şi MI6 au acţionat în tandem pentru rezolvarea operaţiilor războiului psihologic de-a lungul Războiului Rece, folosind mai multe metode.

1. *Metode tradiţionale*

Instrumentele iniţiale de bază folosite de agenţii, au fost pamfletele şi cărţile editate şi posturile de radio. CIA a înfiinţat două staţii de radio în Munchen – Gerania de Vest, numite „Radio Europa Liberă" şi „Radio Libertatea", ce emiteau spre ţările comuniste. „Vocea Americii", care era controlat de către Departamentul de Stat al SUA şi nu de către CIA, îşi coordona activitatea cu staţiile CIA de la Munchen. MI6 a continuat să controleze BBC.

Altă tehnică folosită cu succes pe timpul Război Rece a reprezentat-o cooptarea jurnaliştilor, autorităţilor şi editorilor pentru a ajuta agenţiile de informaţii.

Se poate evoca numărul mare al rapoartelor neîntemeiate legate de India privind acordarea facilităţilor de bază pentru forţele Navale Sovietice în Vizag şi în Andaman Nicobar, transmise de către noile agenţii ale SUA şi Marii Britanii către presă, în timpul vizitei primului ministru indian, doamna Indira Gandhi. Alt raport neîntemeiat dat publicităţii de către jurnaliştii din Vest, a fost cel vizând ataşarea unor experţi KGB pe lângă generalul indian Sunderji, pe timpul operaţiunii „BLUE STAR" din 1984. Aceste rapoarte au dispărut tot atât de misterios cum au apărut, după moartea Indirei Gandhi în 1984.

Urmând dezvăluirilor din mass-media, cabinetul britanic al lui John Major, a admis în 1995, că un număr de scriitori britanici, ale căror cărţi anti-comuniste au devenit best-seller-uri în timpul Războiului Rece, au cooperat cu Divizia de Publicitate Externă a Ministerului de Externe Britanic. În realitate ei au fost dirijaţi de MI6.

Această perioadă a fost marcată de apariţia, ca ciupercile după ploaie, cu fonduri furnizate de CIA, a unui mare număr de staţii radio private în Asia de Sud-Est. Multe din aceste staţii radio, având la faţadă organizaţii creştine, erau anti-comuniste şi anti-socialiste în conţinutul programelor.

Altă tehnică perfecţionată în timpul Războiului Rece şi incă folosită a fost cooptarea formatorilor de opinii politice sau sociologice, ca şi a academicienilor şi altor părţi ale elitei intelectuale din ţările Lumii a Treia, prin aranjarea unor călătorii ale acestora în Europa de Vest şi în SUA, diseminate sub forma unor studii de cercetare sau pentru participarea la seminarii ştiinţifice finanţate oficial de organizaţii non-guvernamentale.

Fondurile furnizate de agenţiile de informaţii erau dirijate direct către universităţile vestice, către mediile academice şi organizaţiile non-guvernamentale.

Fondurile indirecte constituite în aşa numita „A doua cale diplomatică" reprezintă o altă tehnică a războiului psihologic de dată recentă.

În afară de binecunoscutele organizaţii non-guvernamentale (NGO), care în trecut au fost în prim-planul primirii de fonduri financiare de la agenţiile de informaţii, mai sunt stipendiate organizaţiile „Amnesty Internaţional" din Marea Britanie

şi Comisia Internaţională a Juriştilor (CIJ) de la Geneva.

Amnesty Internaţional a fost chipurile îndreptăţită să primească fonduri de la guvernul Harold Wilson, ca răsplată pentru rolul său deosebit în deconspirarea violării drepturilor omului de către forţele britanice de securitate în Aden şi Zimbabwe, iar CIJ a primit fonduri de la o organizaţie privată de avocaţi din SUA (bineînţeles că fondurile au fost „donate" de CIA).

În concluzie putem aprecia că este posibil ca şi în fâşia de acţiune a marilor unităţi operative să ne confruntăm cu astfel de organizaţii sau situaţii. Numai printr-o conlucrare strânsă a tuturor factorilor implicaţi putem folosi în interes propriu metodele tradiţionale.

2. Folosirea televiziunii

Televiziunea a devenit un instrument principal în gestionarea percepţiilor din 1960. Rolul deosebit al imaginilor TV din Vietnam, în special în comunitatea grupurilor anti-război din Vest, împreună cu mişcările pentru pace, au avut un rol predominant în întoarcerea opiniei publice împotriva războiului şi întoarcerea luptătorilor în ţară.

„TV MARTI" staţia de televiziune a CIA, a transmis o multitudine de programe către poporul din Cuba, iar CIA a ajutat un important număr de oameni de afaceri privaţi, să înfiinţeze staţii pentru transmiterea programelor de televiziune către ţările comuniste din locaţii situate în Berlinul de Vest şi Hong Kong.

Instrumente ca pamfletele şi cărţile editate, staţiile de radio, telefonia şi faxul, E-mailul şi Internetul sunt bune pentru aspectul „tare" al războiului psihologic, pentru înstrăinarea mentală a poporului faţă de ţara lui şi pentru discreditarea statului în ochii propriului popor şi al lumii, dar pot fi numai limitat folosite pentru aspectul „moale" al proiecţiei puterii unui grup în cadrul războiului psihologic, într-o lumină atractivă şi creatoare a dorinţei de emulaţie a culturii şi a creşterii standardului de viaţă.

Aici ne apare televiziunea ca mijloc foarte valoros. Cu ajutorul unor producţii sofisticate şi prin grila de programe, se poate crea în mintea unei audienţe ţintă – în special din mediul urban şi în rândul tinerilor, o admiraţie nemărginită şi necriticabilă faţă de societatea democratică, să îmblânzească prejudecăţile lor faţă de capitalism şi să le stârnească dorinţa să îi imite. Pe această bază o mare parte din publicul ţintă îşi pierde încrederea în propria societate şi cultură.

În „ Washington Quarterly" în vara lui 1995, Gerald Segal, director al Institutului Internaţional pentru Studii Strategice din Londra, declara: „Nu este mult timp de când staţia TV a unui consorţiu multinaţional a început să emită prin satelit din Hong Kong, filme soap-opera" străine şi chinezeşti şi sport internaţional ce sunt văzute de milioane de oameni. Faptul că BBC World Service TV, proprietarul satelitului comercial a permis utilizarea acestuia, a permis o mare penetrare pe piaţă, dar în mod anecdotic este clar că auditorii din Asia, apreciază în special valorile Vestice, din programele de divertisment şi numai în trecere pentru „talk-show-uri"unde sunt dezbătute probleme de drepturi fundamentale ale omului.

Cele mai vizionate sunt filmele „Baywatch", „Dallas" sau „Kung-Fu", în mod sigur datorită faptului că sunt mult mai atractive decât emisiunile „cerebrale", aceste programe urmărind efectiv subminarea influenţei autorităţii şi controlului statului chinez.

Scriind despre CNN şi BBC, Segal concluziona „CNN şi pentru un timp BBC WSTV au adăugat imagini subversive la voci subversive ce proveneau de la „Vocea Americii" şi de la mai multe staţii radio din Europa". Exemplele cele mai citate sunt demolarea zidului Berlinului, revolta populară din România din 1989 şi mişcarea studenţească din Bangkok din 1992.

Digitalizarea şi canalele TV prin cablu DTHTV au adăugat necesitatea de a dispune de personal specializat.

Necesităţile strategice pentru 1995, enunţate de către Institutul Naţional pentru Studii Strategice din Washington, care funcţionează în cadrul Universităţii Naţionale de Apărare, coordonată de Pentagon clama:

„Mâine, antenele pot să-şi potenţeze capacităţile de a fi ascunse prin pereţi sau alte medii fizice, interzicând astfel posibilitatea descoperiri lor. Focalizarea electronică poate pune în dezavantaj staţiile terestre de bruiaj. Compresia video, care multiplică numărul de canale pentru a fi găzduit de către orice satelit, intensifică economia de frecvenţe fixe".

O investiţie de câteva miliarde de dolari SUA, permite achiziţionarea a mai mult de o sută de staţii TV digitale, care bine folosite, pot în schimb să aducă un profit de cel puţin 2 milioane de dolari SUA pe an. La acest preţ, oricare din grupurile naţionale sau politice nemulţumite – Kurzii, Şiiţi radicali, Sikh etc. – pot oferi spaţiu propagandistic emitent 24 de ore pe zi, cuprinzând întreg teritoriul vizat.

Canalele TV prin cablu conduse de elemente extremiste, dispunând de mari fonduri financiare provenite din narcotice şi agenţii de informaţii străine cu oportunităţi de închiriere a canalelor, ascunse sub masca unor companii de cablu şi folosind canalele TV, pot uşor prezenta imagini aranjate cu musulmani ucigând hinduşi sau creştini ori viceversa, ducând la sporirea tensiunilor sociale, religioase etc.

În „The Foreign Policy" din toamna lui 1997, John Dentch, director al CIA în timpul primului mandat Clinton, se referea la pericolul imaginilor şi a mesajelor contrafăcute introduse în sistemele radio şi TV ale unor state, ce împroaşcă minciuni şi incită populaţia la violenţă.

Până recent, în SUA, străinilor nu le era permis să aibă firme având ca obiect de activitate operatorii de telefonie şi televiziunea prin cablu. Murdoch a trebuit să îşi ia cetăţenia americană şi să aibă reşedinţă permanentă în State şi numai după aceea a putut solicita licenţă pentru televiziunea prin cablu. Dar, el a fost nevoit să renunţe la acest proiect datorită opoziţiei operatorilor locali din domeniu. În acest moment datorită faptului că a fost stipulat în documentele World Trade Organisation posibilitatea deschiderii serviciilor de telefonie de către străini, Congresul SUA a reanalizat condiţiile sub care cetăţenii altor ţări pot să primească licenţă. Una din condiţii stipulează posibilitatea ridicării licenţei, sau a refuzării acesteia în interes public, sau mai concret spus în cazul în care se atentează la securitatea naţională. Condiţii similare sunt prevăzute şi pentru operatorii de televiziune prin cablu de naţionalitate străină.

În sud-estul şi estul Asiei, numai Japonia permite cetăţenilor străini să obţină 25% din participarea în cadrul unor companii ce oferă servicii de televiziune prin cablu.

Scriind în jurnalul ce apare în SUA „Foreign Affairs", Joseph S.Nye, fostul preşedinte al Consiliului Naţional de Informaţii al SUA din cadrul Administraţiei Clinton şi Amiralul William A. Owens, fostul vice-preşedinte al Comitetului Şefilor de State Majore Întrunite ale armatei SUA tot în perioada sus-menţionată, enunţau următoarele idei: "Puterea „soft"- moale reprezintă abilitatea de a-ţi atinge scopurile şi dezideratele în afacerile internaţionale, prin atragere mai mult decât prin certitudine. Este mult mai indicat să îi convingi pe alţii să te urmeze, sau să fie de acord cu respectarea normelor şi instituţiilor care produc comportamentul dorit. Puterea „moale" poate lua o pauză în aşteptarea unei idei strălucite sau are abilitatea de a îşi planifica agenda în măsură să satisfacă şi propunerile altora.

Dacă un stat poate să îşi legitimeze puterea în percepţia altor state şi poate construi canale de legături cu instituţii internaţionale care să îl incurajeze, el nu va fi nevoit să îşi sporească tradiţionalele sale costuri economice sau resursele militare".

După colapsul regimurilor comuniste din Europa, direcţia maşini de război psihologice a SUA a fost îndreptată spre ASIA. În acest scop postul de radio Europa Liberă a fost mutat de la Műnchen la

Praga, cu scopul de a combate regimul anti-Saddam Hussein din Irak. Începând din septembrie 1996, a fost înfiinţat cu banii daţi de Congresul SUA, postul de radio Asia Liberă, având programe în limbile chineză, tibetană, thailandeză, vietnameză şi coreană. China a început bruierea acestui post din septembrie 1997.

3. Faxul, E-mailul, Cd-Rom-ul şi Internetul

Faxul, E-mailul, Cd-Rom-ul şi Internetul au plasat noi şi sofisticate instrumente ale războiului psihologic în mâinile agenţiilor de informaţii şi a organizaţiilor separatiste, extremiste şi teroriste. Aceste instrumente electronice au revoluţionat total conceptul de „PSYW".

În timp ce în trecut războiul psihologic era dus de state sau de grupuri de indivizi şi era direcţionat către o comunitate sau grup de oameni, aceste instrumente fac posibilă focalizarea războiului psihologic direct pe specialiştii aleşi individual din cadrul unei ţări sau populaţii ţintă, care se află în poziţiile de a influenţa pe ceilalţi.

Faxul, E-mailul, Cd-Rom-ul şi Internetul sunt foarte mult folosite de Amnesty International, Organizaţia de Apărare a Drepturilor Omului şi alte organizaţii neguvernamentale, de obicei acţionând din proprie iniţiativă sau la sugestia unor agenţii de informaţii, pentru a menţine două sau mai multe căi de comunicaţii deschise cu diferite grupări sau cu indivizi disidenţi, cu precădere din China şi Cuba. Christofer M. Centner, analist superior în cadrul Agenţiei de Informaţii a Apărării SUA, enunţa în primăvara 1997, în revista "Strategic Review": „Era modernă informaţională pune la dispoziţie mijloacele de persuasiune directă către indivizi influenţi şi către audienţa ţintă, fără a mai apela la mijloacele diplomatice şi propagandistice tradiţionale. Era diplomaţiei „stat la stat" este în declin accentuat. Era diplomaţiei „stat la individ (persoană) a început".

El mai adaugă: „ Noua mass-media informaţională-Internetul şi sistemele sale asociate, E-mailul, comunicaţiile prin satelit, computerele personale, CD-Rom-urile şi altele – permit statelor să dispună de mai multe oportunităţi pentru a se adresa cetăţenilor străini mai ales sub forma de bază „de la om la om". Manipularea datelor, folosirea utilităţilor oferite de E-mail, schimbarea în sensul dorit a resurselor inteligenţei umane, alterarea prin furnizarea de date false a auzului, video şi alte forme mass-media pot fi folosite. Alte surse informaţionale –individuale, companii private, agenţii specializate – care pot împiedica sau stânjeni acceptarea termenilor unei companii, o pot discredita, împreună cu alte mijloace, folosind „distribuirea" de informaţii false sau zvonuri, folosind fax-uri şi E-mail-uri pe timpul conferinţelor, pe site-urile World Wide Web(WWW).

Noua eră informaţională permite ghidarea cu precizie a propagandei, mai mult decât permite tehnologia modernă lansarea bombelor de mare precizie. Propaganda poate fi adresată indivizilor în particular, grupurilor şi facţiunilor de interese, potenţând favorabil probabilitatea de a obţine succesul în operaţiile operative şi în campanie. Este posibil ca produsele planificate şi executate de diferite organizaţii să poată „coordona o campanie" în sprijinul atingerii ţelurilor supreme de securitate naţională.

În acest moment, noi apreciem că odată intraţi în era tehnologiei informaţionale şi a războiului informaţional, este timpul re-examinării şi revederii ţelurilor propagandei naţionale. Cum informaţiile, mai bine spus deţinerea lor devine critică, decelarea acestora şi orchestrarea judicioasă a mijloacelor mass-media din acest domeniu, devine nu numai esenţială în atingerea ţelurilor naţionale, ci şi în menţinerea securităţii ţării.

4. Cum putem contracara războiul psihologic folosind mijloace electronice

Odată cu apariţia noilor instrumente electronice, agenţiile de informaţii au trebuit să facă faţă dificultăţilor în contracararea

războiului, aşa cum s-a văzut în unele ţări cum sunt China, Arabia Saudită, Egipt etc.

Ca exemplu amintim că s-au descoperit că există 15.000 site-uri WEB ce operează pe Internet cu ajutorul exilaţilor tibetani şi ai suporterilor acestora din toată lumea, prin care poporul din China, poate accesa guvernul Tibetan - din exil, Biblioteca Tibetană şi Arhivele, şi mişcarea Campania Internaţională pentru Eliberarea Tibetului.

În concluzie apreciez că cerinţele esenţiale ale unui război psihologic la pace şi pe timpul războiului, în corelaţia spaţiu, timp, tehnologie asupra pregătirii şi desfăşurării operaţiilor întrunite în războiul viitorului sunt bazate pe valabilitatea, accesibilitatea şi corectitudinea unei baze de date exhaustive cu detalii ale elementelor de sprijin şi false ale propagandei, conţinutul acesteia, determinarea tehnicilor etc. Construirea unei asemenea baze de date trebuie să constituie o prioritate de bază a comunităţii de informaţii a armatei României.

2. RĂZBOIUL INFORMAŢIILOR ECONOMICE (EIW – ECONOMIC INFORMATION WAREFARE)

Specialiştii militari apreciază că EIW reprezintă ansamblul activitaţilor coordonate de căutare, prelucrare şi difuzare a informaţiei despre mediul specific desfăşurării activităţilor de tip economic, asociind statul, întreprinderile şi structurile militare de la diferite eşaloane, incluzând aici şi cel operativ.

Acţiunile din sfera acestei forme de bază a războiului informaţional urmăreşte blocarea sau canalizarea informaţiilor, în scopul obţinerii supremaţiei economice. Conţinutul şi modul de acţiune al atacurilor în sfera informaţiilor economice, ne îndreptăţesc să afirmăm că ele se manifestă concentrat, atât la nivel operativ cât şi la nivel strategico-militar, fapt ce ne permite să prezentăm problemele exhaustiv, punctând numai acolo unde apreciem că este imperios necesar eşalonul operativ.

La o analiză atentă vom descoperi că mai nimic nu este ce pare la prima vedere, că interesul material, ascuns sub slogane variate, a stat la baza tuturor confruntărilor umane, începând din cele mai vechi timpuri şi până în zilele noastre.

Apreciem că nu este lipsit de importanţă să enumerăm pe scurt unele învăţături ale lui SUN TZI, perfect aplicabile războiului în sfera informaţiilor economice:

a) O naţiune coruptă şi imorală poate fi înfrântă uşor. Corupeţi şi semănaţi imoralitatea în rândul naţiunii adverse.

b) Peştele de la cap se împute. Corupeţi mai întâi liderii! Compromiteţi-i, şantajaţi-i, aduceţi-i la ascultare!

Direcţiile de acţiune în războiul infomaţiilor economice (parte esenţială a războiului informaţional), vizează schimbarea mentalităţilor, aspiraţiilor, ideilor, teoriilor, comportamentelor, moravurilor militarilor în domeniul economic.

Sunt folosite *metode de manipulare* foarte greu de depistat, bazate pe exploatarea instinctelor primare (de hrană, de apărare, de reproducere) şi a înclinaţiilor primitive din om:

1. inocularea şi dezvoltarea spiritului consumatorist, în dauna spiritului de economie, prin reclama manipulatorie, trezirea instinctelor acaparatorii, exploatarea orgoliului, uşurinţei (nechibzuinţei), superficialităţii, naivităţii şi altor trăsături negative de personalitate. Fiecare om are un complex de nevoi care-i asigură o viaţă normală. Agresorul din sfera informaţiilor economice îşi propune însă, să dezvolte în omul-ţintă şi în naţiunea-ţintă nevoi şi cerinţe artificiale, să-i smulgă ultimul bănuţ din buzunar sau din bancă, pentru a-l aduce în starea de falit, dependent de împrumuturi pe care tot el, manipulatorul, le oferă. Astfel că dacă individul ţintă nu rezistă tentaţiilor

abil construite, va ajunge sclav economic. Ce observăm în România la ora actuală? Multe persoane acuză că o duc rău cu banii dar consumă bunuri scumpe, de import, la care ar putea renunţa fără a suferi nimic (ţigări, alcool, dulciuri etc.)

2. abaterea atenţiei şi interesului cetăţenilor de la sectorul economic, material, producător de bunuri şi valori, către direcţii neproductive sau nocive. *Cele mai cunoscute manipulări spre direcţii inutile în România sunt:*
a. fetişizarea sectorului politic, concentrarea atenţiei opiniei publice naţionale pe acest sector neproductiv;

b. mistică, sub diferitele ei forme şi manifestări (oficială şi neoficială, "zeiască" sau "demonică", mai veche sau mai nouă etc.). În această acţiune invadatorii economici contează pe câteva elemente reale, cum ar fi: tendinţa celor slabi de a se refugia în mistică, la primul contact cu greutăţile vieţii sau cu fenomene necunoscute; fascinaţia pentru mister; înclinaţia spre credinţă în supranatural; speranţa salvării prin intervenţia miraculoasă a divinităţii; reminescenţe psihice primitive (teama de necunoscut sau de zei, de fenomene inexplicabile, tendinţa de a fabula mistic dincolo de realitatea demonstrată ştiintific, speranţa de a rezolva pe cale mistică, uşoară, fenomene rezolvabile pe cale naturală etc.);

c. preocupări dezumanizante de tipul aberaţiilor sexuale, pornografiei, violenţei, traiului în jocul hazardului (la întâmplare, fără planuri de viitor), necinstei, consumului de droguri, alcoolismului. Propaganda pentru îmbolnăvirea cu aceşti "viruşi sociali" se face direct, prin organisme specializate, ascunse sub lozinci umanitare.
d. o altă direcţie către care invadatorii economici încearcă să ne abată atenţia este : senzaţionalul (o categorie aparte constituind-o fenomenele paranormale);

3. crearea şi impunerea în conştiinţa (şi inconştienţa) naţiunii-ţintă a unor false valori umane şi tehnice, în scopul înlocuirii valorilor adevărate şi tradiţionale (naţionale);

1. orbirea, surzirea, distrugerea spirituală sau fizică a liderilor hotărâţi să lupte pentru înflorirea economică a naţiunii lor, doparea acestora cu informaţii false cu privire la domeniul pe care trebuie să-l conducă, la economie, în primul rând;
2. afectarea relaţiilor economice ale ţării respective cu alte state ori cu firme economice din diferite zone ale lumii. Pentru a atinge acest obiectiv sunt folosite măsuri complexe:

a. ideologizarea economică, prin care eşti făcut să crezi că poţi face afaceri bune numai cu o anumită tabără dominată de o anumită ideologie. Desigur, invadatorii economici fac afaceri cu toată lumea, indiferent de ideologie, religie etc. În războiul din sfera informaţiilor economice nu există altă ideologie decât a avantajului economic;

b. promovarea amatorismului în rândul liderilor economici;

c. denigrarea produselor şi serviciilor proprii, prin mijloace de luptă psihologică: propaganda neagră, zvonuri, bancuri, ştiri false sau denigratoare în mass- media etc.

6. spionajul economic şi confruntarea din sfera informaţiilor economice planetare moderne, a determinat apariţia unor noi forme de luptă economică:
a. lupta pentru impunerea standardelor pentru anumite categorii de produse. Fiecare creator şi producător este interesat să acapareze întreaga piaţă mondială, să elimine toţi concurenţii, prin obţinerea standardizării produsului sau (cazul luptei dintre sistemele de televiziune PAL şi SECAM; lupta pe piaţa informaticii dintre Microsoft şi alte companii de sisteme de operare) ;

b. devalorizarea forţată a valutelor naţionale, prin speculaţii financiar-bancare;

c. crearea dependenţei printr-un produs livrat foarte ieftin, dar al cărui preţ creşte pe măsură ce populaţia din ţara-piaţă devine dependenta de el.

Pentru a exemplifica pe scurt accerba luptă ce se dă în “mirificul” război al informaţiilor din sfera economicului, şi a

trage învăţămintele folositoare nouă ca cetăţeni ai României şi ca militari, vom prezenta două cazuri reprezentative – chiar şocante, pentru statele lumii a treia, intens mediatizate de presa naţională şi mondială:

1. CAZUL "COSTA RICA"

Înainte ca FMI şi Banca Mondială să fi restructurat politicile economice ale acestui stat, în numele atenuării poverii datoriei sale externe, Costa Rica era cunoscută în întreaga lume ca o societate mai egalitaristă decât cea din ţările vecine. Avea o bază puternică de mici fermieri şi foarte puţine din marile moşii tipice societăţilor latino-americane.

Politicile impuse de FMI şi Banca Mondială au lipsit producţia fermelor mici de stimulentele economice. Aceste ferme produceau hrana zilnică a populaţiei. Stimulentele au fost canalizate spre marile proprietăţi funciare care produc pentru export.

În consecinţă, mii de mici fermieri au fost dizlocaţi, pământurile lor au fost înglobate de marile ferme şi proprietăţi funciare care produc pentru export, iar decalajul în veniturile din Costa Rica a început să semene cu cel din alte ţări latino-americane. O creştere a criminalităţii şi violenţei a necesitat o sporire substanţială a bugetului forţelor de poliţie şi de siguranţă publică.

Acum ţara este dependentă de importuri pentru a satisface necesităţile alimentare vitale, iar datoria externă, pe care această restructurare economică şi socială ar fi trebuit s-o reducă, s-a dublat. În ciuda faptului că aceste consecinţe ale politicilor promovate de cele două instituţii internaţionale au fost catastrofale, ele consideră Costa Rica un exemplu al succesului restructurării economice şi sociale, deoarece creşterea economică a sporit, iar ţara este acum capabilă să facă faţă datoriei sale externe crescute.

2. CAZUL "ARGENTINA"

Presa şi canalele de ştiri din ţară şi mondiale prezentau cu lux de amănunte în 2002 criza economică şi socială de proporţii ce izbucnise în Argentina.

Înfometaţi, zeci de mii de oameni au luat cu asalt magazinele alimentare bilanţul fiind de 12 morţi, aproape 200 de răniţi, sute de arestaţi la Buenos Aires. Populaţia acuză FMI pentru falimentul economiei argentiniene. Zeci de mii de oameni au ieşit în stradă nemulţumiţi de condiţiile extrem de sărace de trai.

Planul de austeritate al Guvernului argentinian a eşuat, ţara aflându-se într-o gravă criză economică şi socială. Tensiunea pe străzile capitalei Buenos Aires a mai scăzut odată ce demisia ministrului argentinian al economiei, Domingo Cavallo, considerat cel mai vinovat de situaţia în care se afla Argentina, a fost acceptată. Premierul Christian Colombo le-a cerut şi celorlalţi membrii ai Guvernului să demisioneze. Manifestanţii au cerut şi demisia preşedintelui argentinian. Poliţia a arestat sute de manifestanţi. Preşedintele Fernando de la Rua a decretat stare de asediu pentru mai mult de o lună în întreaga ţară. Argentina, confruntată cu trei ani şi jumătate de recesiune şi restricţii, a ajuns în pragul falimentului financiar. Violenţele s-au înteţit în toate regiunile mari ale ţării. Protestatarii au devastat magazinele, au incendiat clădirea Ministerului Economiei, maşini, pneuri, şi au luat cu asalt Palatul Prezidenţial şi Clădirea Parlamentului. Forţele de ordine au format cordoane în jurul magazinelor şi baraje pe autostrăzile de acces către Buenos Aires. Poliţia a încercat să înăbuşe revoltele cu gaze lacrimogene şi gloanţe de cauciuc. Maşina care îl transporta pe şeful statului a fost ţinta pietrelor şi a loviturilor de picioare din partea manifestanţilor.

Potrivit CNN, protestatarii strigau că sunt flamânzi şi că vor de mâncare şi fugeau cu braţele încărcate de alimente furate din supermaketurile devastate. După trei ani de recesiune guvernul argentinian a lansat planul de austeritate. Dar Fondul Monetar Internaţional a refuzat să mai acorde Argentinei o ultimă tranşă de ajutor de peste 1 miliard de dolari, pentru că nu şi-a

echilibrat bugetul conform planului. Rata şomajului a depăşit 18%, în timp ce mai mult de 14% din populaţie lucrează cu jumătate de normă, ceea ce înseamnă că Argentina nu prea mai producea nimic. Agenţia "Standard and Poor's" a anunţat că Buenos Aires a fost declarat în stare de "încetare de plăţi", fiind în incapacitate de a-şi achita datoriile. Cancelaria prezidenţială a difuzat un mesaj al Papei Ioan Paul al II-lea care le-a cerut argentinienilor "să găsească o cale de înţelegere reciprocă".

Concluzia celor sus prezentate pentru domeniul militar, în particular vizând implicaţiile corelaţiei spaţiu, timp, tehnologie pentru operaţiile întrunite în războiul viitorului, apreciem noi că este clară – nu se poate discuta de planuri şi strategii operative de război, ignorând cu bună ştiinţă informaţiile ce trebuiesc cunoscute în domeniul economic. Mai mult apreciem că aceste planuri trebuie să fie puternic ancorate în realitatea economică a României.

În încheierea scurtei noastre prezentări a acestui domeniu, doresc să aduc în atenţie unele metode de luptă ce pot fi cu succes folosite în războiul în sfera informaţiilor economice:

1. Cea mai perversă metodă constă în ameninţarea cu forţa coercitivă directă (mai ales, cu armata) şi invadarea militară. Ocuparea militară a unei naţiuni poate fi efectuată deschis, prin atac armat clasic sau mascat prin lovituri de stat şi revoluţii. De regulă, prin invadări mascate se urmăresc următoarele:
   - ✪ păstrarea aparenţei de onestitate şi neamestec în treburile interne ale statului agresat de către statul agresor;
   - ✪ evitarea scandalurilor publice, prin mass-media şi demonstraţii populare;
   - ✪ impunerea în statul atacat a unor lideri favorabili agresorului, care ulterior îşi vor plăti datoriile prin înfeudarea economică a naţiunii lor.

2. A doua metodă vizează înrobirea economică prin schimbări fundamentale în psihologia naţională a poporului ţintă. Ceea ce este adevărat puternic şi etern într-o naţiune nu este ideologia socială, schimbătoare prin vremi, ci psihologia naţională, sufletul naţiunii, adică un ansamblu coerent şi puternic de credinţe, speranţe, idealuri, modele de comportament, obiceiuri, moravuri, stări volitive şi emoţionale, puternic implantate în subconştientul naţional.

Numai din cele sus prezentate, ne putem da seama că formele de bază ale războiul informaţional, reprezintă cele mai noi modalităţi de ducere a acţiunilor militare la nivel operativ iar importanţa lor deosebită ne îndreptăţesc să apreciem că studiul lor şi în viitor reprezintă o necesitate politico - militară.

BIBLIOGRAFIE SELECTIVĂ

Alvin Toffler	Al treilea val, Editura Politică, Bucureşti, 1983.
Alvin şi Heidi Toffler	Război şi antirăzboi, supravieţuirea în zorii secolului XXI, Editura Antet, Bucureşti, 1995.
Ionel Ciobanu	Formele de bază ale războiului informaţional.**C**orelarea şi influenţa acestora asupra desfăşurării acţiunilor militare de nivel operativ**,** Editura U.N.Ap., Bucureşti, 2005.
Sorin Topor	Aspecte teoretice ale războiului informaţional contemporan, Editura U.N.Ap., Bucureşti, 2004.
Sun Tzu	Arta războiului, Bucureşti, 1993.

UNELE CONCLUZII ŞI ÎNVĂŢĂMINTE PRIVIND DEZVOLTAREA SISTEMELOR DE COMUNICAŢII DIGITALE REZULTATE DIN OPERAŢIILE MILITARE MODERNE

Colonel dr. Aurel BUCUR
Locotenent-colonel drd. Daniel BRĂTULESCU
Direcţia comunicaţii şi informatică

În contextul militar contemporan, când este necesar să abordăm ameninţările asimetrice, adversarul tinde să înţeleagă şi să exploateze cu eficienţă sporită toate slăbiciunile fundamentale în abilitatea de a răspunde cu soluţii oportune. Pe scurt, este aproape imposibil de contracarat ceva ce evoluează şi se adaptează cu viteză foarte mare, deziderat care stă, de fapt, şi la baza acţiunii propriilor forţe. Dezvoltarea tehnologică, factorul uman şi situaţiile se schimbă de multe ori peste noapte, cu o viteză mult mai mare decât spirala obişnuită a ciclurilor de dezvoltare a sistemelor de arme.

Se elaborează cerinţele pentru viitor dar, în fapt, nu reuşim să prevedem cu mare acurateţe acel viitor şi nu există capacitatea financiară necesară pentru a face faţă tuturor situaţiilor care pot deriva din cea iniţială. Experienţa dobândită până în prezent ne arată că trebuie să dezvoltăm sistemele în mod progresiv, cu punct de plecare plecând de la acele soluţii care sunt disponibile într-o perioadă mai mică de trei ani, bazate pe un cadru arhitectural care permite adăugarea unor noi capabilităţi, în mod progresiv[1].

Se poate afirma că 80% dintr-o capabilitate realizată la timp este mult mai bună decât acumularea procentului de 100% mult prea târziu, astfel că viteza cu care sunt implementate cuceririle tehnologice tinde să devină un factor critic în obţinerea avantajului.

Realităţile evidente din teatrele de operaţiuni actuale l-au făcut pe actualul secretarul american al apărării, Robert GATES să recunoască că: *„în timp ce programele convenţionale de modernizare sunt îndreptate spre atingerea unui procent de soluţionare a cerinţelor de 99% într-o perioadă măsurată în ani, războaiele în care SUA sunt angrenate reclamă obţinerea a cel puţin 75% din cerinţe într-o perioadă măsurată în luni.* [2]”

Mediul de tip *net centric* în care se desfăşoară operaţiile militare oferă o flexibilitate deosebită statelor majore în planificarea şi realizarea misiunilor dar în acelaşi timp creează o imensă presiune asupra reţelelor de comunicaţii care facilitează acest mediu. O statistică arată că pe timpul conflictului din Golf din 1991 mai mult de 95% din ieşirile aeriene executate de forţele americane au avut ţinte stabilite, în timp ce pe timpul invaziei din 2003 aproape 99% din ieşiri nu aveau o ţintă specificată, aceasta fiind asignată cu rapiditate, funcţie de evoluţia situaţiei[3].

În timp ce facilitarea oferită de reţea reduce drastic timpul alocat unei misiuni şi măreşte determinant flexibilitatea la nivel tactic, este încă dificil de integrat informaţia vitală, primită din mai multe domenii (întrunit, interagenţii şi multinaţional), în cadrul unei imagini operaţionale recunoscute, în principal datorită incoerenţei setului de informaţii specific fiecărei ţinte. Pe de altă parte, se constată încărcări deosebite ale sistemelor de comunicaţii cu informaţii nesemnificative, neconfirmate şi de multe ori redundante, ce blochează capacităţile de transfer şi stocare ale acestora şi care nu au nici un fel de valoare operaţională pentru decident[4].

Se poate aprecia că aceasta reprezintă o provocare deosebită a conceptului războiului bazat de reţea şi că nu se întrevede, deocamdată, un mod concret de rezolvare. Un pas major către acest deziderat îl constituie distribuirea comenzii şi controlului pentru a optimiza

alocarea resurselor în cadrul spaţiului de luptă, integrarea senzorilor în reţea, în scopul obţinerii informaţiilor la timp şi în locul dorit şi facilitarea angajării eficace.

Toate programele de dezvoltare a viitoarelor capabilităţi trebuie să aibă la bază concepţia că senzorii, platformele şi chiar senzorii din cadrul acestora vor avea o adresă de reţea în cadrul viitorului Internet tactic militar, care va permite integrarea şi accesarea instantanee atunci când este necesar. Datele care astăzi sunt disponibile dar nu sunt accesibile ca facilităţi oferite de reţea, vor fi în viitor fundamentul pentru multiplicarea puterii.

Experienţa din conflictele ultimilor două decade arată că la nivelurile tactice mici, batalion sau grup de luptă, este generată o mare cantitate de informaţie valoroasă, care se referă în principal la informaţii asupra spaţiului de luptă, situaţia forţelor proprii/amice, locaţia acestora etc. Dacă nu se reuşeşte transmiterea acestor informaţii în timp oportun către eşaloanele superioare, care să confere posibilitatea construirii unei imagini operaţionale actualizată în permanenţă, există pericolul apariţiei a ceea ce specialiştii militari denumesc „ceaţa războiului”. În acest context, apariţia fratricidului devine doar o chestiune de timp şi nu de probabilitate a producerii lui.

Eforturi deosebite au fost făcute în ultimii ani pentru a implementa sisteme multimedia moderne de comunicaţii, care produc capacităţi de comandă şi control automatizate, şi care au transformat decisiv forţele militare, perfect sincronizate în cadrul *net centric*.

Pentru a sprijini comandanţii aflaţi în mişcare sau în poziţii avansate, punctele de comandă vehiculare trebuie dotate cu terminale de comunicaţii integrate, utilizând tehnologia *wireless* precum şi terminale mobile de satelit, care împreună satisfac nevoia de comunicaţii din mişcare pentru un comandant ce trebuie să-şi exercite în mod continuu atribuţiunile din domeniul comenzii şi controlului asupra întregii forţe la dispoziţie.

Sistemele radio actuale permit viteze de transfer a informaţiei de până la 16 Mbps, dar atunci când sunt necesare transmiterea de imagini sau fluxuri video, este obligatorie realizarea unor rate superioare, care pot fi obţinute de reţelele digitale moderne de mare capacitate. Serviciile oferite de către sistemele comerciale derivate din reţelele fără fir de arie locală (WLAN), de reţelele celulare sau de comunicaţiile de bandă largă prin satelit, bazate pe tehnologia Internet Protocol, pot elimina limitările din reţelele radio tradiţionale, dar nu pot încă realiza vitezele de până la 155 Mbps cu care sunt conectate centrele staţionare de comunicaţii la reţelele terestre, prin intermediul fibrei optice[5]. Reţelele de date de mare viteză *wireless* trebuie să integreze comunicaţiile dintre diferitele niveluri de comandă în jos, până la nivelul brigăzilor sau diviziilor[6].

Din punct de vedere operaţional se pot lua în considerare următoarele elemente:

- operaţia ”Iraqi Freedom” poate fi caracterizată ca una de tranziţie deoarece tehnologia la dispoziţie nu a fost desfăşurată integral, iar unele sisteme nu s-au dovedit prietenoase pentru utilizatori;
- adversarii recenţi ai SUA (Panama-1990, Irak-1991, Serbia-1999, Afganistan-2001, Irak - 2003) s-au dovedit a fi relativ slab pregătiţi din punct de vedere militar;
- în ceea ce priveşte reţelele de comunicaţii s-au constatat supraîncărcări informaţionale şi comunicarea cu întreruperi pe timpul deplasărilor;
- în domeniul senzorilor, sistemele de urmărire a forţelor proprii s-au dovedit eficiente. Cunoaşterea situaţiei la contact a fost însă incompletă;
- sateliţii au jucat un rol esenţial, dar uneori au fost saturaţi (banda maximă a fost de 3 Gb/s, oricum de 30 de ori mai mare decât la nivelul anului 1991), tabelul 1.

Tabelul 1

	Operaţia *Desert Shield/Storm*	**Operaţia *Noble Anvil***	**Operaţia *Enduring Freedom***	**Operaţia *Iraqi Freedom***
Total SATCOM folosiţi (Mbps)	100	250	750	2.400
Total forţe angajate	500.000	51.000	55.000	235.000
Număr de structuri angajate (echivalent 5.000 militari)	100	10.2	11	47
SATCOM folosiţi (Mbps) de o structură (echivalent 5.000 militari)	1	24,5	68,2	51,1

Eforturi deosebite sunt depuse de către naţiuni pentru a creşte semnificativ capacităţile ISR, conectate la reţea, care pot fi puse la dispoziţia trupelor de nivel tactic desfăşurate în teatre. Astfel, în 2010, o echipă de luptă de nivel brigadă din cadrul forţelor SUA va fi dotată pentru prima dată cu capabilităţi ISR, care vor cuprinde:

- Sisteme autonome terestre de mici dimensiuni, pentru misiuni de recunoaştere în situaţii dificile;
- UAV-uri de mici dimensiuni, pentru supravegherea zonelor apropiate, simultan cu producerea datelor despre ţinte;
- Senzori autonomi tereştri, pentru detectarea, localizarea, identificarea şi clasificarea ţintelor;
- Echipamente specifice pentru conectarea la reţea, care asigură sisteme de comunicaţii şi software-ul de comandă şi control pentru integrarea senzorilor şi transferul datelor de la aceştia.

Senzorii autonomi tereştri, pe care trupele îi au la dispoziţie de mai mulţi ani, trebuie să fie integraţi în reţea în scopul de a permite ca sute de utilizatori să poată avea acces la datele colectate. Principiul de împărţire a datelor presupune ca senzorii să transmită datele primare la cel mai apropiat vehicul care, la rândul său, le transmite către vehiculul comandantului de pluton. Prin sistemul de comandă şi control se materializează, în timp aproape real, situaţia pentru întregul pluton, aceasta fiind accesibilă pentru oricare din membrii săi. Prin intermediul unor produse software, datele pot fi transferate către eşaloanele superioare pentru valorificare. Dacă consideră necesar, comandantul de pluton poate dispune supravegherea zonei de către un UAV de mici dimensiuni, pentru colectarea de imagini în timp real despre ţintă.

Elementul cheie din acest întreg ciclu îl reprezintă asigurarea benzii necesare pentru canalele de comunicaţii, având în vedere cerinţele tot mai mari de imagini de înaltă definiţie. Soluţiile de comprimare a imaginilor existente în acest moment, folosite în mod succesiv, produc constant pierderi semnificative de rezoluţie, fapt ce a generat în câteva cazuri angajarea unor ţinte civile, care la o primă analiză erau considerate cu relevanţă militară. Pentru a rezolva această problemă, specialiştii militari se îndreaptă către utilizarea de comunicaţii tactice de date de nouă generaţie, care pot asigura capacitatea de bandă necesară.

O posibilă rezolvare poate consta în utilizarea sistemului avansat de comunicaţii de date pentru armamente (AWDL). Acesta permite, între altele, controlul vizual, în timp real al rachetelor aer-sol după ce acestea au fost lansate. Sistemul, care de altfel a beneficiat de o vizibilitate deosebită în cel de-al doilea război din Golf, oferă platformei care a lansat-o, imaginea în timp real a ţintei, obţinută de camera video instalată la bordul rachetei şi permite pilotului/operatorului să facă ajustările necesare pe ultima parte a zborului acesteia

spre ţintă, de la o distanţă de peste 150 de mile nautice de aceasta.

În scopul realizării sprijinului trupelor din teatre, specialiştii americani ai DARPA se află într-o fază avansată de testare a unei soluţii novatoare de criptare, care să faciliteze traficul în reţea şi să simplifice managementul acesteia. Soluţia, denumită *Stealth*, face posibilă împărţirea datelor în deplină securitate atunci când acestea sunt vehiculate în medii nesecurizate, constând într-un proces de criptare urmat de o segmentare a pachetelor transmise în reţea. Aplicaţia, care utilizează combinaţia dintre o soluţie de criptare în baza de 256 de biţi şi o tehnologie de segmentare a pachetelor, facilitează folosirea unei singure reţele pentru informaţii partajate şi segregate pe niveluri de clasificare de securitate. Tehnologia de segmentare constă în spargerea fiecărui pachet în blocuri aleatorii de date care sunt vehiculate în reţea. Utilizatorii trebuie să fie partajaţi în aşa numitele comunităţi de interese (CoI) pentru a fi în măsură să recompună datele. Fără configurările iniţiale specifice comunităţii, datele nu pot fi inteligibile, pachetele segmentate circulând fără restricţii în reţeaua comună.

Pe timpul operaţiei din Afganistan au fost folosite intens sistemele de poziţionare a trupelor proprii (BFT), care au suferit semnificative modernizări faţă de varianta, care a fost utilizată pentru prima dată, în Kosovo, în 2004. Aplicaţiile de comandă şi control ale principalelor armate moderne care participă la această operaţie includ aceste facilităţi BFT, fapt ce conferă posibilitatea integrării depline a situaţiei de avertizare în procesele de comandă şi control ale eşaloanelor tactice. Există însă şi o limitare majoră în utilizarea eficientă a acestor sisteme, generată în principal de timpul relativ lung de transmitere şi recepţie, prin intermediul canalelor de comunicaţii radio sau satelitare, către un punct unic de stocare, actualizare şi diseminare, care nu se găseşte în acest teatru. Astfel, actualizarea imaginii se face acum la 15 – 20 de minute, ceea ce pentru un eşalon de nivel companie sau batalion este mult prea mare. Printre soluţiile avute în vedere de specialiştii americani şi ai NATO pentru a elimina această limitare se numără dotarea cu echipamente de comunicaţii prin satelit care să lucreze din mişcare (SATCOM On The Move) şi care să asigure o bandă suficient de largă pentru a preîntâmpina congestionarea informaţiei. Această soluţie este abordată şi de specialiştii Ministerului Apărării Naţionale, care prevăd dotarea cu astfel de mijloace, inclusiv a maşinii de luptă a comandantului de companie.

O altă variantă este implementarea noii generaţii de echipamente BFT, de mare viteză, care ar putea asigura, conform testelor efectuate, o actualizare a situaţiei într-o perioadă de timp sub 2 minute. Cum deocamdată tehnologia nu este suficient maturizată, se apreciază că aceste echipamente vor fi disponibile de abia peste 2 – 3 ani.

Deosebit de importante în orice operaţie sunt aspectele privind managementul spectrului electromagnetic. La începutul operaţiei din Afganistan, deoarece forţele insurgente nu deţineau mijloace de comunicaţii sofisticate iar forţele coaliţiei multinaţionale nu erau extrem de numeroase, nu s-a înregistrat o congestionare a spectrului. Acest lucru însă a devenit evident odată cu creşterea numărului de naţiuni şi organizaţii implicate în conflict, spectrul electromagnetic devenind în perioada actuală resursa cea mai expusă la presiuni. Dacă principalul consumator de benzi de frecvenţă continuă să fie sistemele de comunicaţii, cu aproximativ 65% din existent, în ultima perioadă a crescut foarte mult cererea de alocare pentru sistemele de senzori şi cele de conducere/dirijare a armamentelor. Nu trebuie omis şi că mass media, organizaţiile non guvernamentale şi cele umanitare au propriile nevoi de comunicaţii, care trebuie coordonate cu mare atenţie.

O concluzie majoră desprinsă din derularea misiunii din Afganistan constă în reconsiderarea ambiţiilor privind realizarea unei interoperabilităţi satisfăcătoare între

sistemele de comunicaţii şi informatice ale naţiunilor. Astfel, existenţa în teatru a mai multor generaţii de echipamente, cu caracteristici mai mult sau mai puţin eterogene şi nu întotdeauna bazate pe standardele internaţionale, a condus la decizia de a dezvolta şi implementa, prin eforturile NATO, a unei federaţii de reţele, care să asigure, pe lângă interoperabilitatea vizată, şi cerinţele de securitate necesare fluxurilor informaţionale. Reţeaua Misiunii Afganistan (AMN), odată implementată, va avea caracteristicile unei reţele globale, fiind puternic fundamentată de aplicarea principiului *nevoia de a împărţi* informaţia partajată pe domeniile de clasificare.

Pe plan naţional, deşi au fost întreprinse eforturi intense pentru acoperirea tuturor nevoilor de sprijin în domeniul comunicaţii şi informatică a trupelor desfăşurate, acest lucru nu s-a putut realiza decât prin asistarea masivă de către partenerii din coaliţie. Lipsa mijloacelor financiare, care să fie asigurate ritmic, a împiedicat dotarea forţelor noastre cu aplicaţia de comandă control BC2A Cinetic, care a fost testată anterior la exerciţiile de interoperabilitate multinaţionale şi unde, s-a bucurat de o largă recunoaştere a valenţelor deosebite de interoperabilitate pe care le oferă. Acest lucru, conform planului aprobat, se va petrece în decursul anilor 2010 şi 2011, facilitând integrarea forţelor naţionale în cadrul celor ce deţin capabilităţi de tip *net centric*.

Se impune o nouă abordare a cerinţelor de asigurare a canalelor satelitare necesare echipamentelor de la nivel tactic (TACSAT), care să faciliteze accesul facil al trupelor proprii la aceste resurse. Ele nu sunt disponibile pe teritoriul naţional, fapt ce afectează semnificativ capacitatea de antrenare din perioada de pre desfăşurare şi sunt extrem de limitate în teatru, ceea ce ridică noi constrângeri în utilizare.

Participarea în teatrele de operaţii, alături de aliaţi şi parteneri, constituie un prilej deosebit şi unic de testare şi verificare a propriilor doctrine, tactici şi sisteme de armamente naţionale, precum şi a nivelului de pregătire şi a capacităţii operaţionale a trupelor. În acest context de coaliţie, nivelul şi calitatea asigurării sistemelor de comunicaţii şi informatice joacă un rol crucial, fără de care succesul în operaţie nu poate fi atins. Învăţămintele şi concluziile rezultate reprezintă motorul principal în proiectarea, dezvoltarea şi implementarea noilor sisteme şi reţele de comunicaţii şi informatice naţionale, în strânsă conformitate cu principiile războiului bazat pe reţea şi ale capabilităţilor facilitate de reaţea.

Bibliografie

[1]*Implementing NATO Network Enabled Capability Governance*, NATO HQ, Brussels, 2007, p. 9.

[2]*Secretary of Defence hearing before the Congress*, 2008, September 22nd , the Library of Congress, Washington, D.C., p. 5.

[3]*MC Guidance for the Strategic Commanders on Further Development of Alliance Transformation*, MCM-0054-2005, revised in 2006, Brussels, p.16.

[4]*NATO Network Centric Operational Needs and Implications for the Development of Net-centric Solutions*, vol.1, NATO HQ, Brussels, 2005, pp. 14-17.

[5]*TACOMS Post 2000, Final Study Report,* WP13202, Technology Independent Network Architecture, NC3A, The Hague, 2005, pp. 13-15.

[6]*Network-Centric Warfare: Background and Oversight Issues for Congress*, Congressional Research Service, Washington, D.C., 2005, p. 24.

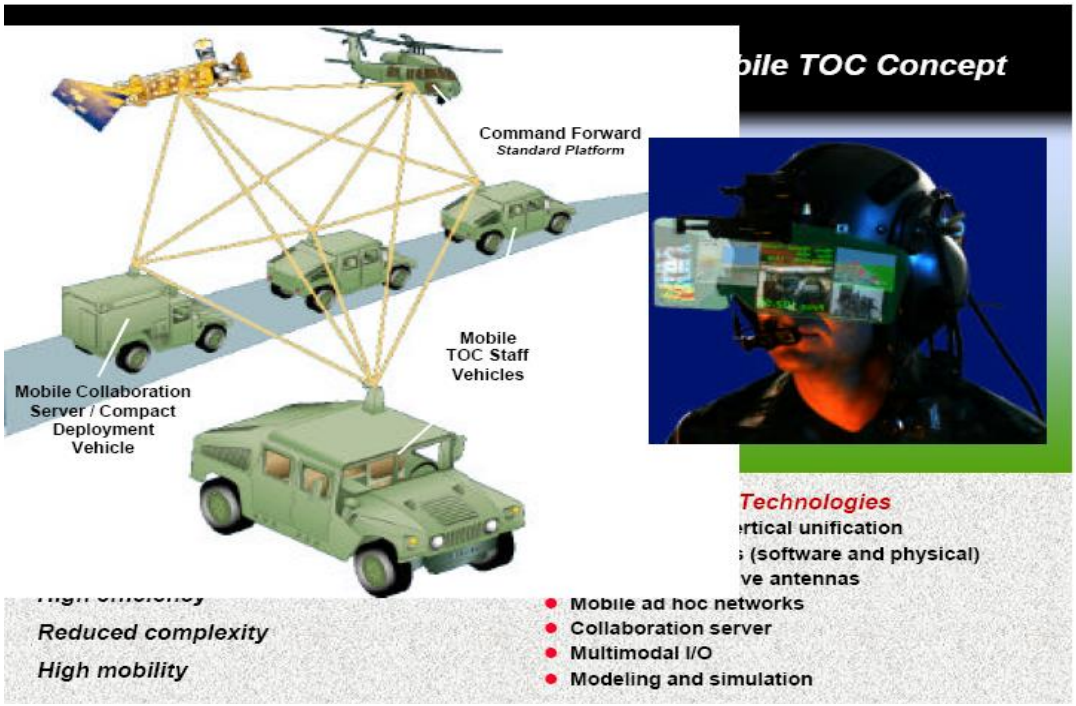
CONCEPTUL DE TOC MOBIL ÎN VIZIUNEA NATO

Colonel drd. Silviu PREDA
Comandamentul comunicaţiilor şi informaticii

În concepţia NATO, Centrul de operaţii tactice este element component al Centrului de operaţii şi are rolul de a realiza imaginea tactică comună a zonei de responsabilitate, prin monitorizarea tuturor acţiunilor şi evenimentelor/sau incidentelor importante şi de a oferi comandantului sprijinul necesar privind înţelegerea situaţiei curente din campul de luptă, precum şi estimări privind evoluţia ulterioară a acesteia. Centrul de operaţii tactice (Tactical Operations Center - TOC). este nodul central al fluxului de informaţii pentru toate rapoartele şi ordinele care intră şi ies în/din punctul de comandă al unei structurii de forţe.

La nivelul Alianţei există un puternic sentiment de nemuţumire privind constituirea şi funcţionalitatea actualelor centre de operaţii tactice. Această nemulţumire este cauzată de ineficienţa rezultatelor obţinute prin activitatea lor, de complexitatea majoră a activităţilor care se desfăşoară în cadrul acestora şi de lipsa lor de mobilitate. Problema imobilităţii se referă atât la incapacitatea de a opera din mişcare, precum şi la durata mare de timp necesară punerii în funcţiune între operaţiile executate din staţionare şi operaţiile mobile. Mărirea numărului de resuse hardware, software şi de resurse umane necesare pentru a opera un TOC şi dependenţa sa de comuncaţiile terestre limitează mobilitatea de care este nevoie pe câmpul de luptă, prezent şi viitor. Ca urmare, speciliştii în sisteme de comandă şi control au dezvoltat *conceptul de TOC mobil.*

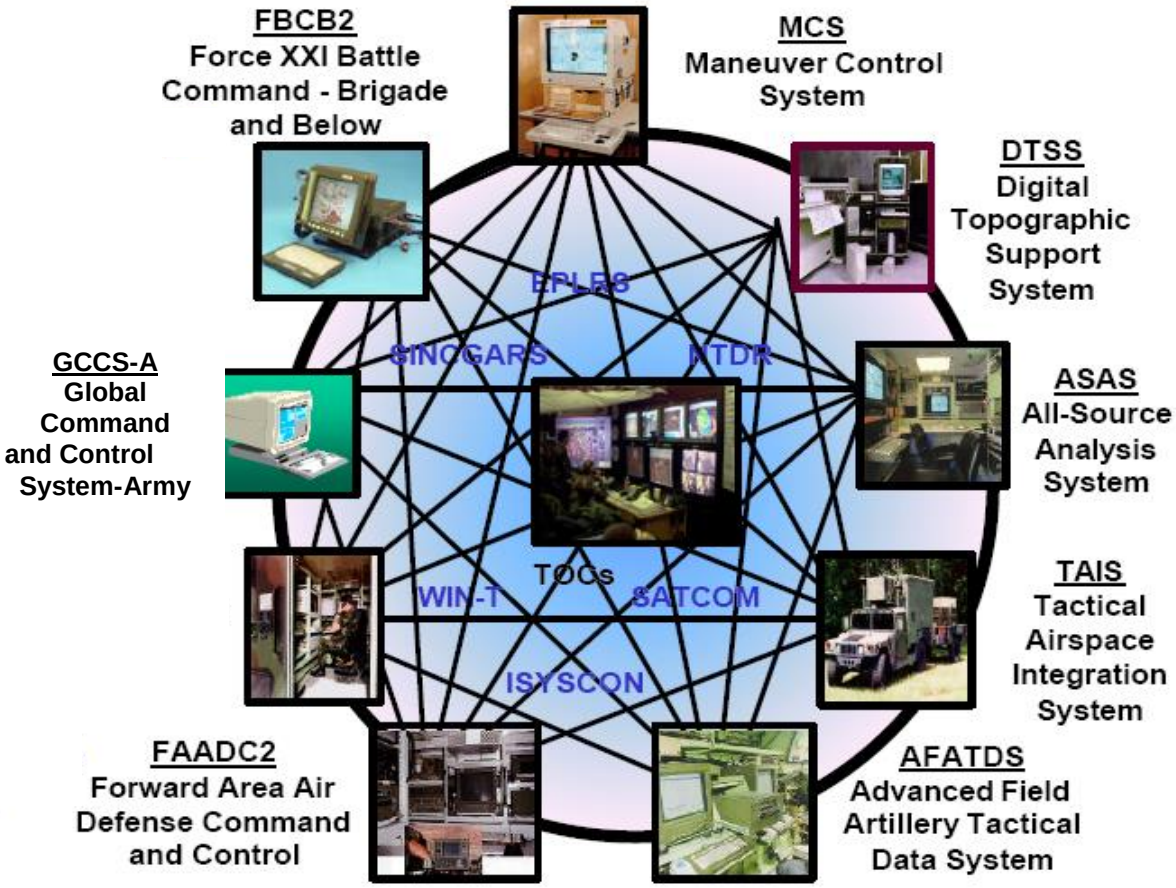
Esenţa Conceputului de TOC mobil o reprezintă *automatizarea TOC-ului* prin unificarea sistemului de arhitectură, intensificarea comunicaţiilor şi perfecţionarea software-ul agent de arhitectură şi a aplicaţiilor informatice necesare funcţionării, precum şi prin realizarea unei infrastructuri tehnologice bazată în principal pe echipamente de comunicaţii şi informatică dispuse pe patru platforme mobile de tip Hamvi interconectate între ele prin radio.



Cele 4 platforme mobile sunt de fapt 4 noduri de prelucrare a informaţiilor interconectate în principal prin reţele radio aeriene şi satelitare care au la bază folosirea benzilor largi multi-modale cu toate sistemele de senzori şi de observare existente în câmpul de luptă.

În condiţiile în care viitorul câmp de luptă este anticipat să fie mult mai dinamic şi non-liniar decât operaţiunile curente, nevoia de mobilitate a TOC-ului va creşte considerabil, însă *conceptul de TOC mobil* prin conţinutul său rezolvă această problemă. Automatizarea TOC-ului mobil, suplețea acestuia şi eliminarea legăturilor fir fac ca acesta să capete o mobilitate destul de mare şi în acelaşi timp să-şi poată îndeplini rolul chiar şi din mişcare.

Funcţionalitatea TOC-ului mobil este asigurată în principal de serverul mobil care centralizează şi integrează informaţiile furnizate de toate sistemele care asigură funcţionalitatea şi conectivitatea pentru o anumită zonă funcţională a actualului camp de luptă şi anume: sistemele de informaţii, sistemele de control ale manevrei, sistemele de apărare antiaeriană, sistemele de sprijin cu foc, sistemele de spijin şi ducere a luptei şi le pune apoi la dispoziţie tuturor entităţilor interconectate la el devenind astfel server comun pentru toate sistemele amintite anterior.

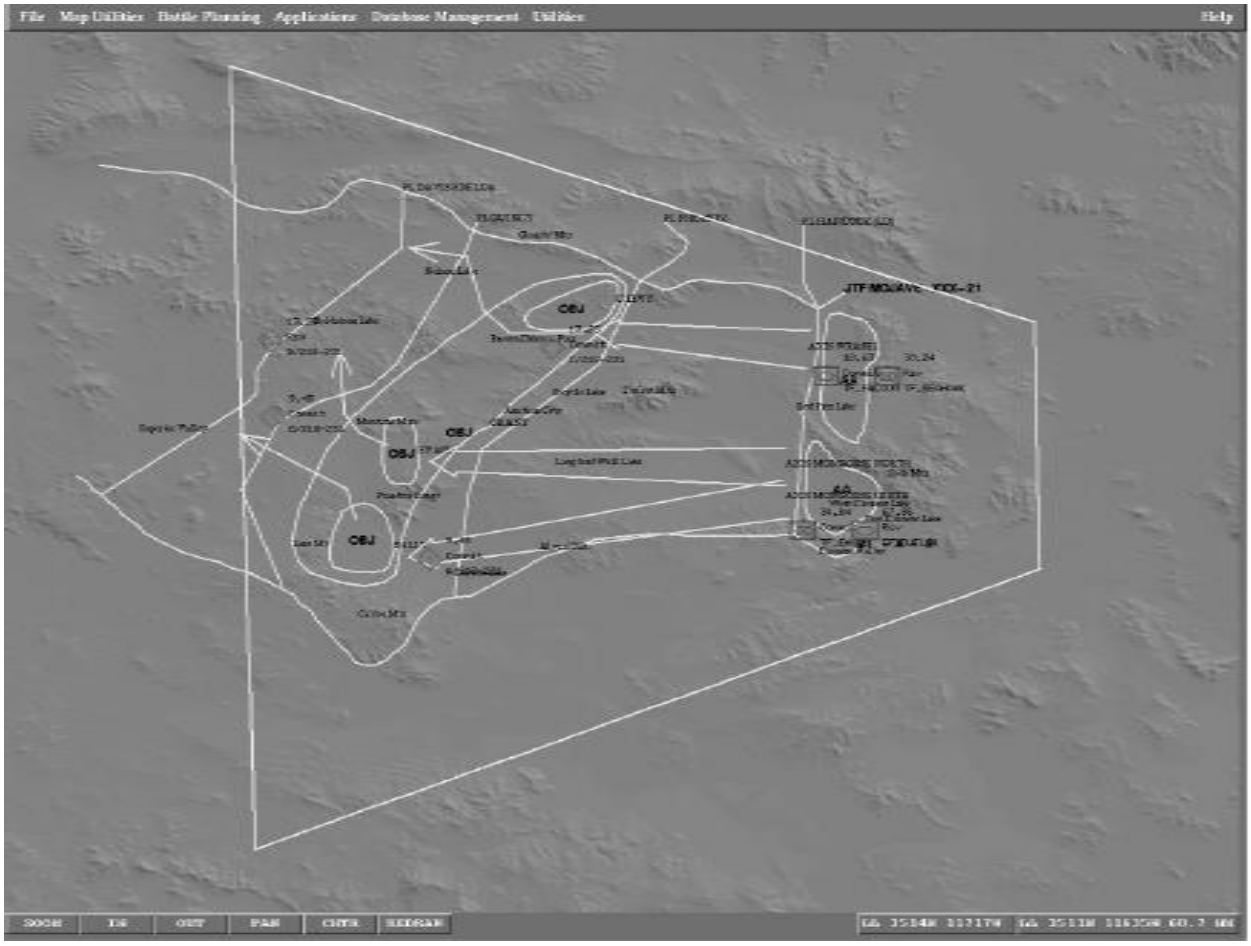


Totodată, funcţionalitatea TOC-ului mobil nu ar putea fi eficientă fără o infrastructură softwer care să asigure fuziunea tuturor informaţiilor despre inamic şi trupele proprii şi care să genereze imaginea tactică comună a câmpului de luptă, precum şi vizualizarea acestuia.

Infrastructura software a TOC-ului mobil este dată de programul de vizualizare a câmpului de luptă şi platforma software a agentului de arhitectură cu aplicaţiile informatice aferente fiecărui agent. Programul de vizualizare a câmpului de luptă, are rolul de a asigura o infrastructură globală multi-rezoluţie, cu capacitatea de a

vizualiza întregul câmp de luptă (caracteristicile şi particularităţile terenului, starea vremii, căile de comunicaţii, etc), la orice rezoluţie la care informaţiile sunt disponibile. Acest lucru permite comandantului să-şi formeze propriile puncte de vedre despre câmpul de luptă, precum şi o înaltă rezoluţie locală care îl spijină pe acesta în luarea deciziilor importante. Aceeaşi infrastructură oferă, posibilitatea vizualizării de înaltă fidelitate şi de pe platformele de manevră ale comandanţilor, precum şi, abilitatea de a vizualiza orice altă vedere locală din lume pentru a sprijini procesul de instruire sau de pregătire pentru dislocare. Platforma software a agentului de arhitectură este de fapt programul care asigură managementul tuturor informaţiilor care pentru fiecare zonă funcţională a câmpului de luptă are un agent de arhitectură care pe baza aplicaţiei de agent analizează informaţiile oferite.

Spre exemplu, această imagine ilustrează un curs al manevrei în cadrul planului de acţiune selectat de comandantul TOC-ului la nivel de brigadă, care necesită sincronizarea manevrei, angajarea inamicului şi asigurarea logistică a celor trei batalioane ale sale.



Planul a fost comunicat şi platformele de manevră au început executarea cursului acţiunii. Implementarea unui plan simplu stimulează activităţi importante ale agentului, atât în cadrul TOC-ului cât şi în cadrul platformelor de manevră. Un agent de monitorizare a planului global de manevră în TOC interacţionează cu agentul de monitorizare a sincronizării manevrelor executate de platforme. Agentul de monitorizare a sincronizării manevrelor executate de

platforme are sarcina de a-l atenţiona pe comandantul platformei în cazul în care "entitatea" nu este capabilă să execute planul manevrei. Acest agent va alerta de asemenea, si agentul de monitorizare a manevrelor din cadrul TOC-ului în legatură cu orice probleme privind execuţia. Un agent de informaţii monitorizează în continuu şi reactualizează orice informaţii pertinente privind inamicul, care ar putea afecta această operaţie. De exemplu, un radar al inamicului este detectat în apropierea unei zone în care era planificată a executa o manevră unul dintre batalioanele de manevră. Agentul de informaţii alertează atât agentul însărcinat cu planificarea manevrelor din cadrul TOC-ului cât şi agenţii de manevră şi de informaţii ai platformei care va fi afectată. În cadrul TOC-ului un agent însărcinat cu sprijinul de foc generează un plan de atac pentru a dezactiva senzorul activ al inamicului. Acest plan este prezentat comandantului TOC-ului şi este refuzat din cauza lipsei de sprijin cu foc disponibil. La platformele afectate este generat un plan de manevră reactiv şi, dacă este acceptat de comandantul local este executat. Un agent de monitorizare logistică a platformei ţine evidenţa resurselor locale (de combustibil, muniţie, piese de schimb, etc) şi distribuie aceste informaţii către agenţii logistici din cadrul TOC-ului. Agenţii logistici din cadrul TOC-ului monitorizează continuu planul de aporvizionare care spijină acest plan de angajare. În cazul în care punctele de realimentare devin inadecvate datorită timpului excesiv al angajamentului sau al manevrei, agenţii de logistică din cadrul TOC-ului replanifică punctele de aprovizionare. Această aplicaţie oferită drept exemplu indică nevoia existenţei agenţilor de monitorizare, de alertare, de diseminare şi de recepţionare a informaţiilor pentru fiecare din cele mai importante funcţii cum ar fi: manevra, funcţia de informaţii şi logistica, care există atât în cadrul TOC-ului cât şi în cadrul platformelor conducătoare.

UTILIZAREA SISTEMELOR DE IDENTIFICARE ÎN CÂMPUL DE LUPTĂ

Colonel Valentin DRĂGUŢ; col.ing. Valentin STEMATE
Direcţia comunicaţii şi informatică

În toate conflictele armate fratricidul a reprezentat o preocupare a tuturor părţilor implicate. Numărul incidentelor de fratricid a scăzut semnificativ pe măsură ce au fost dezvoltate sistemele de armament, s-au îmbunătăţit tehnicile, tacticile şi procedurile de întrebuinţare a acestora şi s-a optimizat cunoaşterea şi înţelegerea situaţiei (*SA - Situational Awareness*) din câmpul de luptă.

Cu toate acestea, fratricidul constituie încă o ameninţare majoră pentru trupele care desfăşoară astăzi operaţii în spaţiul de luptă. Acest fenomen a devenit un factor cu impact major strategic şi operaţional, care nu poate fi omis în mediile actuale internaţionale. Deşi au fost înbunătăţite doctrinele pentru operaţiile întrunite, au fost dezvoltate sisteme performante de comunicaţii de date (TDL – Tactical Data Link) şi sisteme de identificare în câmpul de luptă (CID - Combat Identification System), au fost perfecţionate metodele şi procedeele de instruire şi antrenare a personalului participant la operaţii militare în scopul prevenirii fratricidului, factorii umani în conjuncţie cu viteza şi nelinearitatea de ducere a operaţiilor combatante vor face ca eliminarea completă a fratricidului să fie imposibilă.

Informaţiile vehiculate în cadrul sistemelor de comandă, control, comunicaţii, computere, informaţii, supraveghere şi recunoaştere (C4ISR) constituie fluxuri informaţionale specifice care se realizează în cadrul sistemului şi urmăresc, dar nu se limitează la descoperirea, recunoaşterea, identificarea, localizarea şi intenţiile probabile, în mod oportun, a ţintelor sau a altor obiective sau fenomene cu relevanţă pentru domeniul acţiunilor militare (de exemplu: tehnică de luptă; non-combatanţi; condiţii de mediu; potenţiale pericole pentru forţele proprii etc.).

Asigurarea serviciilor de comunicaţii şi informatice, adecvate fiecărui utilizator sau comunităţi informaţionale, la locul şi momentul în care sunt solicitate, asigurând caracteristici şi performanţe ridicate de stabilitate, flexibilitate şi securitate, cu utilizarea eficientă a resurselor angajate şi la nivelul de calitate prevăzut, reprezintă obiectivul principal al activităţii structurilor specializate de comunicaţii şi informatică, de la fiecare nivel ierarhic, în Armata României.

Identificarea în câmpul de luptă reprezintă procesul prin care se obţine o caracterizare precisă a unei entităţi detectate prin orice acţiune sau mijloc, astfel încât să poată fi luată o decizie bazată pe informaţii de înaltă certitudine, în timp real, inclusiv în privinţa angajării sistemelor de armament. Caracteristicile detectate trebuie să certifice cu siguranţă dacă entitatea respectivă, persoana, obiectul sau fenomenul, este amic, inamic sau neutru şi necesită realizarea distincţiei asupra naturii sale militare sau civile şi să determine clasa, tipul, naţionalitatea sau intenţia. Obiectivul principal al identificării este de a amplifica cunoaşterea situaţiei reale şi de a estima pericolele şi riscurile pentru forţele proprii şi aliate, astfel încât să fie maximizată eficienţa operaţională, concomitent cu minimizarea fratricidului şi a pagubelor colaterale.

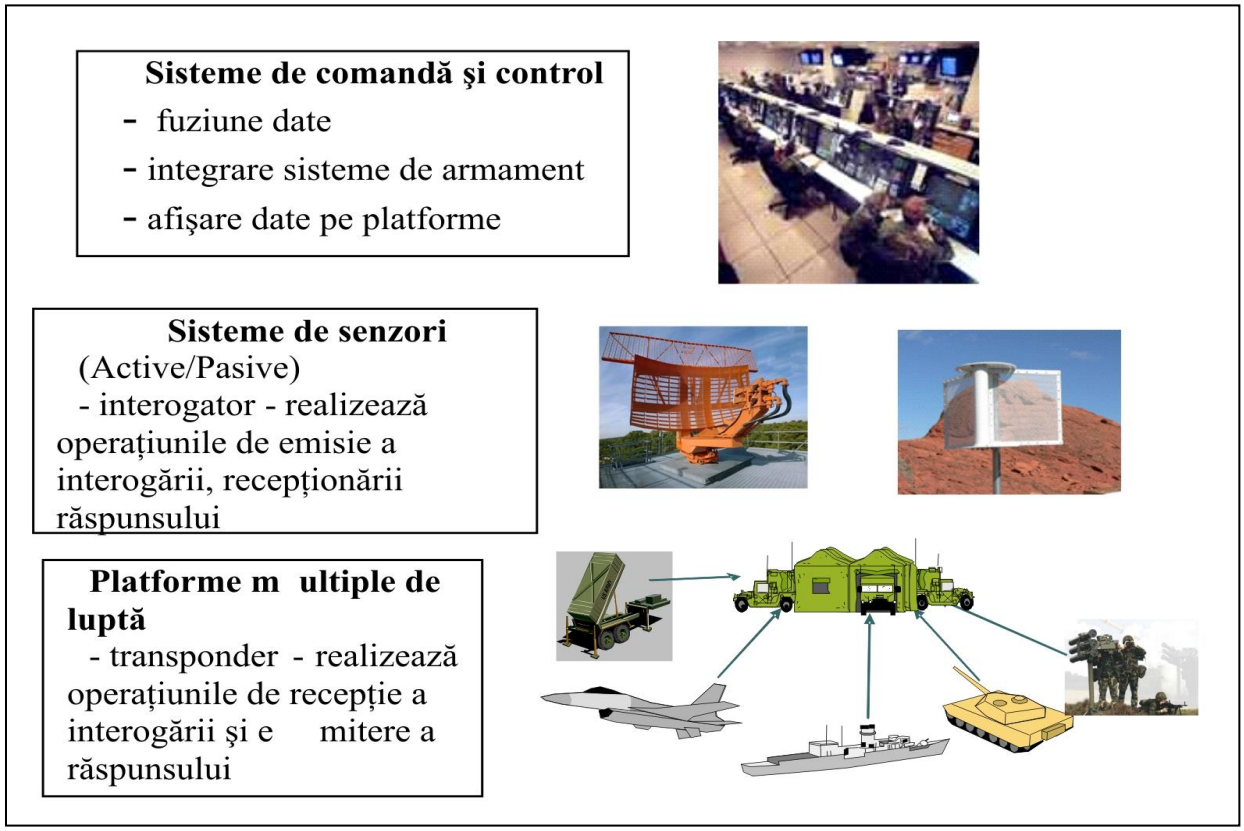
Identificarea în câmpul de luptă poate fi exprimată pe scurt ca mijloacele prin care entităţile militare disting elementele amice de cele inamice pe timpul operaţiilor şi cuprinde în principal trei elemente: cunoaşterea şi înţelegerea situaţiei (SA), identificarea ţintelor (TI - Target Identification) şi tacticile, tehnicile şi

procedurile pentru utilizarea combinată a primelor două elemente. SA reprezintă cunoaşterea şi înţelegerea relaţiilor dintre forţele participante la operaţie, statutul, misiunile şi intenţiile acestora în spaţiul de luptă şi are ca principal scop creşterea eficacităţii forţelor în operaţii. Identificarea ţintelor reprezintă procesul de determinare al caracterului de amic, neutru sau inamic al unei entităţi detectate, în scopul protejării forţelor proprii împotriva atacurilor forţelor aliate şi al iniţierii sau neiniţierii acţiunilor pentru distrugerea sau neutralizarea entităţii identificate.

Identificarea poate fi clasificată atât din punct de vedere al mediului desfăşurării operaţiei: suprafaţă-suprafaţă, suprafaţă-aer, aer-aer şi aer-suprafaţă, cât şi din punct al modului de executare a identificării: cooperantă / activă[5] şi non-cooperantă/ pasivă[6].

Operaţiile întrunite implică forţe terestre, maritime şi aeriene care acţionează la toate nivelurile, strategic, operativ şi tactic. Acest lucru a determinat dezvoltarea accelerată a sistemelor C4ISR şi implicit a uneia dintre componentele esenţiale ale acestora, identificarea în câmpul de luptă.

Principalele sisteme de identificare suprafaţă-aer şi aer-aer utilizate în Alianţa Nord-Atlantică sunt sistemele de identificare amic-inamic (IFF - Identification Friend or Foe) Mark X, Mark XII şi Mark XIIA, compatibile modurilor de lucru 1, 2, 3/A, C, 4 şi 5.



[5] Ex. mijloace de identificare a ţintelor în câmpul de luptă, mijloace portabile de identificare a militarilor combatanţi, sisteme de identificare de luptă prin radio, marcatoare de radio frecvenţă şi sisteme de identificare amic-inamic IFF.

[6] Ex. radare optice sintetice de identificare în luptă, sisteme ajutătoare de recunoaştere a ţintelor, sisteme cu program de obţinere a imaginilor prin laser .

Utilizarea acestor sisteme se efectuează de către platforme multiple de luptă (capacităţi de apărare anti/aeriană, avioane, nave maritime), sisteme de senzori (radare) şi sisteme de comandă şi control şi este prezentată în figura 1. Radarele de supraveghere secundare (SSR - Secondary Surveillance Radar) reprezintă echivalentul civil al sistemelor militare IFF şi sunt utilizate atât de organizaţiile civile cât şi de cele militare, pentru identificarea şi controlul propriilor platforme aeriene de către furnizorii de servicii de trafic aerian şi de către unităţile responsabile de realizarea şi interpretarea imaginii aeriene recunoscute (RAP). Atât sistemele IFF cât şi cele SSR sunt considerate sisteme de siguranţă aeriană critice pentru controlul traficului aerian şi pentru exercitarea comenzii şi controlului aerian.

Autorităţile aeronautice civile au decis tranziţia către SSR în modul de lucru "S" (Select) pentru utilizare în spaţiul aerian european, cu implicaţii majore asupra plaformelor militare care nu au posibilitatea de utilizare a acestui mod de lucru.

Sistemul IFF Mk XII(A) (Mod 5) reprezintă performanţe sporite faţă de sistemul precedent IFF Mk XII, dispunând de perfecţionări semnificative din punct de vedere operaţional şi al performanţelor, prin utilizarea unui nou mod de identificare, Mod 5. Acesta asigură îmbunătăţirea securităţii şi creşterea capacităţii sistemului şi soluţionează majoritatea deficienţelor semnalate la sistemele existente IFF Mk XII, inclusiv deformarea răspunsurilor şi replicărilor platformelor apropiate în spaţiu. Principalele beneficii operaţionale ale sistemelor IFF Mod 5, sunt:

a. compatibilitatea cu modul civil de lucru „S" (IFF Mod 5 dispune şi de capacitatea de interogare, răspuns şi interpretare a datelor în modul de lucru „S");

b. creşterea performanţelor transponderului şi a capabilităţii acestuia de a nu fi influenţat de semnale de dezinformare, de interferenţe cu alte interogatoare şi creşterea rezistenţei la bruiaj;

c. creşterea controlului emisiilor radio;

d. creşterea performanţelor razei de acţiune;

e. reducerea efectelor de variaţie a puterii semnalelor radio (*multipath fadding*[7]);

f. eliminarea replicilor distorsionate emise de aeronavele apropiate în spaţiu;

g. creşterea capacităţii şi a posibilităţilor de lucru ale sistemului;

h. îmbunătăţirea corelării semnalelor IFF recepţionate de la ţintele detectate;

i. creşterea capacităţii de transmitere de date;

j. creşterea performanţelor de securitate a datelor transmise/recepţionate;

k. sporirea compatibilităţii electromagnetice;

l. reducerea numărului de operaţiuni pe care le efectuează operatorul.

Pentru asigurarea interoperabilităţii şi creşterea capacităţilor operaţionale în domeniul sistemelor de identificare amic-neutru-inamic, în Armata României urmează să se integreze sistemele IFF Mark XIIA pe platformele terestre, aeriene şi navale dislocabile cu nivel ridicat de operativitate.

Localizarea şi identificarea suprafaţă-suprafaţă, corectă şi precisă a ţintei (TI) reprezintă elemente esenţiale pentru diminuarea fratricidului.

[7] Fluctuaţia puterii semnalului radio, datorată variaţiilor produse în mediile de transmitere ale acestuia.

Fig. 2 – Sistem FFT

În prezent se manifestă un interes deosebit pentru îmbunătăţirea realizării şi diseminării SA, în special prin dezvoltarea şi realizarea interoperabilităţii sistemelor de identificare a forţelor proprii/aliate (FFT - *Friendly Force Tracking*). În figura 2 este prezentat un sistem FFT şi imaginea realizată/afişată de acesta. SA şi TI se realizează atât pe baza integrării sistemelor FFT cât şi prin completarea datelor prin utilizarea informaţiilor furnizate prin alte echipamente şi sisteme, în special prin cele de voce, din reţelele tactice satelitare, prin echipamentele radio VHF/FM şi prin diferite reţele de comandă şi control. FFT reprezintă capabilitatea de a monitoriza locaţia precisă a forţelor proprii şi aliate care dispun de astfel de sisteme, în timp aproape real şi de a exercita comanda şi controlul acestor forţe, la nevoie. Acestea dispun de un receptor GPS, un emiţător şi un computer/display care afişează simbolurile forţelor individuale proprii şi ale unităţilor aliate. Pentru realizarea interoperabilităţii sistemelor FFT a fost validat operaţional un standard al interfeţei de transfer a datelor/informaţiilor.

Una dintre priorităţile din domeniul identificării este dezvoltarea serviciului de transfer a datelor colectate/centralizate de sistemele FFT prin intermediul sistemului multifuncţional de distribuţie a informaţiilor, Link 16, în vederea realizării imaginii operaţionale comune şi pentru prevenirea fratricidiului. Acest serviciu va fi extins în vederea transferului datelor relevante FFT, prin intermediul sistemului de comandă-control maritim către capabilităţile navale şi prin intermediul sistemului de comandă-control aerian, către capabilităţile aeriene.

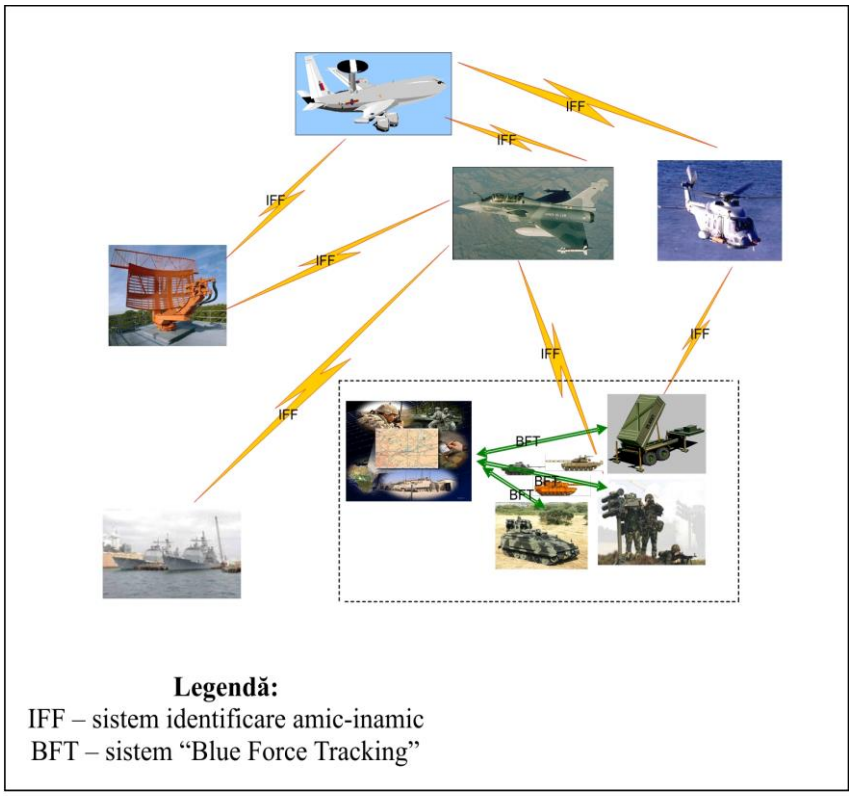


Fig. 3 Sisteme de identificare în operaţii întrunite

Principalele preocupări actuale în domeniul CID (SA şi TI) rămân schimbul de date şi informaţii între sisteme compatibile, standardizate şi diseminarea acestora pentru realizarea imaginii operaţionale comune, a imaginilor aeriene, terestre şi maritime recunoscute, schimbul de date şi informaţii combinate, a datelor de identificare a ţintelor şi a schimbului de date video.

Este cunoscut faptul că de-a lungul timpului trei întrebări simple referitoare la locaţia geografică au constituit factori esenţiali în desfăşurarea conflictelor armate, pentru comandanţi şi forţele participante:

- Care este poziţia mea şi a unităţii din care fac parte?
- Unde se află forţele de care aparţin şi forţele aliate?
- Unde este adversarul şi care este calea optimă pentru mine de a-l ataca şi învinge?

Cunoaşterea şi interpretarea corectă a situaţiei şi identificarea precisă a ţintelor sunt factori esenţiali în formularea unor răspunsuri pertinente la aceste întrebări.

În concluzie, identificarea în câmpul de luptă reduce producerea fratricidului şi a pagubelor colaterale, datorate în principal erorilor în localizarea ţintelor, când muniţia trasă împotriva adversarului loveşte forţele proprii şi a erorilor de identificare, când forţele aliate sau neutre sunt atacate din greşeală, pe baza considerentului că acestea sunt forţe ostile/inamice. În prezent şi cu certitudine în toate operaţiile militare viitoare, identificarea în câmpul de luptă va fi unul dintre factorii esenţiali ai obţinerii supremaţiei informaţionale şi implicit a succesului în câmpul de luptă.

Bibliografie

[1] The US Training and Doctrine Command (TRADOC) definition for fratricide.
[2] Friendly fire From Wikipedia, the free encyclopedia (INTERNET);
[3] Defense Technology Objectives for JWSTP - USD(A&T) (INTERNET);
[4] Guidance for the Operational Introduction of SSR Mode S - European Organisation For The Safety Of Air Navigation (INTERNET)

MENTENANŢA ECHIPAMENTELOR DE COMUNICAŢII ŞI INFORMATICĂ

Colonel ing. Ştefan DIMITRIU
Comandamentul comunicaţiilor şi informaticii

Activitatea de mentenanţă în cadrul Comandamentului comunicaţiilor şi informaticii

Mentenanţa cuprinde totalitatea acţiunilor întreprinse pentru menţinerea sau restabilirea echipamentelor la caracteristicile specifice de funcţionare.

O importanţă vitală pentru desfăşurarea în bune condiţii a mentenanţei o au resursele financiare, care sunt cele stabilite prin buget şi au la bază estimarea necesarului de fonduri băneşti, pentru echipamentele generale şi specifice aflate în dotarea unităţilor militare, în vederea executării mentenanţei în sistemul propriu şi externalizat.

În sistemul propriu, estimarea fondurilor la categoriile de echipamente, aflate deja în dotarea armatei, se face pe baza planului de mentenanţă, din care se extrage numărul necesar de reparaţii pentru echipamentele din dotare. Pentru echipamentele tehnice, la care estimările depăşesc 60% din valoarea de înlocuire a acestora, se dispune scoaterea din funcţionare şi valorificarea în conformitate cu prevederile legale în vigoare. Pentru echipamentele tehnice care nu se mai fabrică, se foloseşte ca valoare de înlocuire, valoarea echipamentelor cu caracteristici tehnice similare. În cazuri speciale, când anumite tipuri de echipamente tehnice sunt unicat sau sunt absolut necesare, cu aprobarea ministrului apărării, acestea pot fi reparate chiar dacă costul reparaţiei este mai mare de 60% din valoarea de înlocuire.

În varianta externalizată, estimarea fondurilor necesare se face având în vedere raportul dintre valoarea orei de muncă practicată de operatorii economici specializaţi şi valoarea orei de muncă, realizată în sistemul propriu de mentenanţă, înmulţit cu valoarea fondurilor estimate în varianta clasică, la care se adaugă valoarea estimată, statistic, a pieselor de schimb.

Conceptul de mentenanţă redefinit, în funcţie de starea echipamentelor şi momentul efectuării lucrărilor, are două componente: preventivă şi corectivă.

Mentenanţa preventivă cuprinde un ansamblu de activităţi întreprinse pentru menţinerea sistemelor tehnicii în condiţii normale de funcţionare, prin înlocuirea sistematică a elementelor şi executarea unor lucrări de revizie periodică, reglaj, diagnosticare şi control, planificate la intervale stabilite în funcţie de durata de utilizare.

Mentenanţa corectivă cuprinde activităţi desfăşurate pentru restabilirea capacităţii normale de funcţionare a sistemelor defecte cum ar fi reparaţiile de mică, medie sau mare amploare, care au ca scop repunerea în stare de funcţionare a tehnicii defecte şi/sau deteriorate, ca urmare a uzurii normale sau participării la acţiunile militare. Astfel de activităţi de mentenanţă cuprind operaţii, cum sunt testarea/diagnoza, localizarea şi remedierea defecţiunilor prin înlocuirea sau repararea elementelor defecte, verificarea şi executarea reglajelor .

Nivelurile de mentenanţă, pe care este structurat sistemul de mentenanţă a echipamentelor militare, stabilite în funcţie de complexitatea lucrărilor, durata de imobilizare, dotarea cu echipamente specifice, aparatură, utilaje şi S.D.V. - uri specifice, calificarea personalului şi condiţiile de lucru, sunt următoarele:

- Nivelul de bază – cuprinde intervenţiile de mentenanţă preventive şi corective, cu imobilizări ale tehnicii, de scurtă durată, control tehnic înaintea misiunii, control tehnic pe parcurs, întreţineri tehnice curente, întreţineri tehnice

şi inspecţii periodice, revizii, reparaţii;

- Nivelul intermediar – cuprinde intervenţiile de mentenanţă preventive şi corective, cu imobilizări ale tehnicii, pe durată medie de timp, testare, clasificare operaţională, revizii, reparaţii;
- Nivelul general – cuprinde interveneţiile de mentenanţă preventive şi corective, cu imobilizări ale tehnicii, pe durată de timp relativ mare.

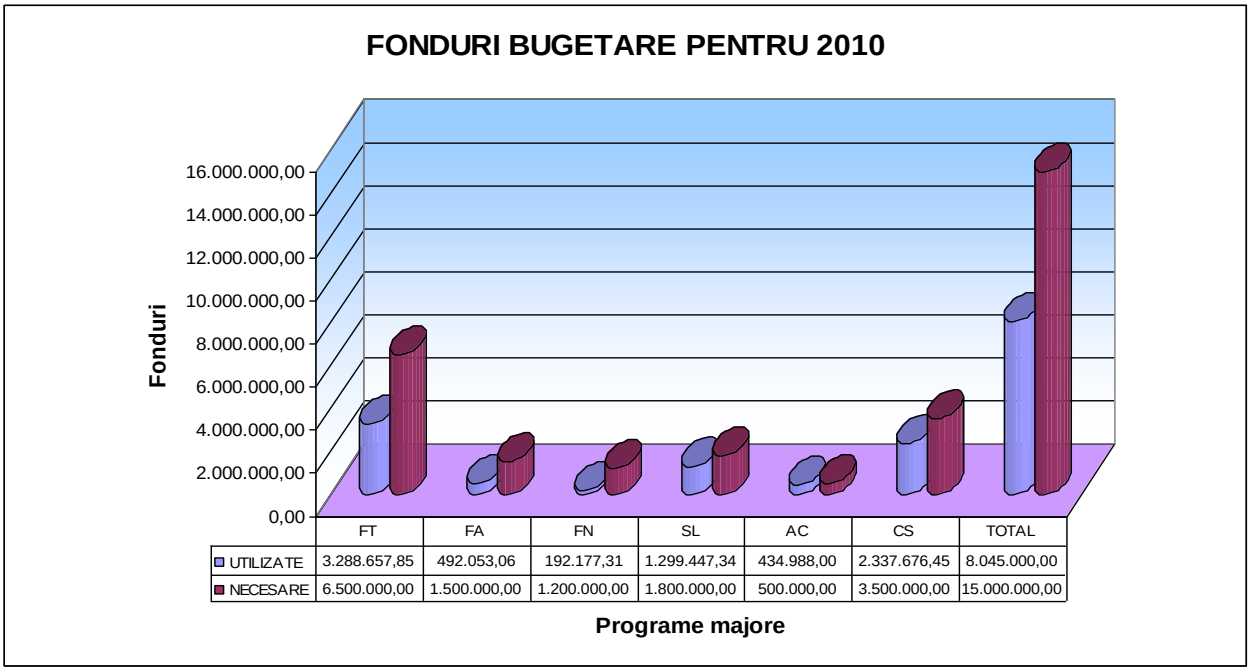
În funcţie de tipul tehnicii, gradul de uzură şi volumul de manoperă, de regulă, la tehnică se execută reparaţii, care pot fi;

- reparaţii curente şi de complexitate redusă – RC;
- reparaţii de complexitate medie – RM;
- reparaţii de complexitate ridicată, - RR.

Duratele acestor tipuri de reparaţii sunt reglementate prin norme specifice armei, elaborate de către structurile cu atribuţii în domeniu, din cadrul categoriilor de forţe ale armatei şi comandamentelor de arme.

În sprijinul activităţii de mentenanţă, atât pentru partea de planificare, cât şi pentru partea de execuţie, au fost actualizate sau elaborate o serie de acte normative, cele mai importante fiind Normele tehnice de reparare a echipamentelor din dotarea M.Ap.N. şi Catalogul costurilor de mentenanţă pentru echipamentele militare.

După o perioadă în care tendinţa a fost pentru externalizarea a cât mai multe din activităţile de mentenanţă, după o analiză atentă, coroborată şi cu realitatea alocării fondurilor financiare pentru activităţi de mentenanţă, sub valorile necesare (*figura nr. 1*), s-a ajuns la implementarea unui sistem de mentenanţă combinat. Aceasta implică executarea în sistem propiu a tuturor activităţilor de mentenanţă care se pot executa în condiţiile existente de resurse şi specialişti, iar în sistem externalizat numai a activităţilor care nu pot fi executate în sistem propiu, dar în limita fondurilor băneşti existente.



	FT	FA	FN	SL	AC	CS	TOTAL
UTILIZATE	3.288.657,85	492.053,06	192.177,31	1.299.447,34	434.988,00	2.337.676,45	8.045.000,00
NECESARE	6.500.000,00	1.500.000,00	1.200.000,00	1.800.000,00	500.000,00	3.500.000,00	15.000.000,00

REGÂNDIREA SECURITĂŢII INFORMAŢIILOR PENTRU A ÎMBUNĂTĂŢI FUNCŢIONAREA ORGANIZAŢIILOR

Locotenent-colonel ing.Constantin PĂNOIU
Centrul de instruire pentru comunicaţii şi informatică „Decebal”

Utilizarea unei noi abordări trebuie să ajute la crearea de soluţii inovatoare în condiţiile reducerii riscurilor de securitate.

Prezentare generală

Pentru a permite adoptarea rapidă a noilor tehnologii şi modele de utilizare şi a oferi

protecţie într-un context evolutiv al ameninţărilor-IT Intel s-a angajat la o reproiectare radicală, de cinci ani, a arhitecturii de securitate a informaţiilor.

Se consideră că această arhitectură, gândită să sprijine iniţiativele-cheie, cum ar fi consumerizarea IT şi cloud computing, reprezintă o abordare noua pentru securitatea organizaţiilor. Aceasta face controale de securitate mai flexibile, mai dinamice, şi granulare în comparaţie cu modele tradiţionale. De exemplu, arhitectura este concepută pentru a ajusta dinamic privilegiile de acces ale utilizatorului în funcţie de schimbările riscurilor, depinzând de factori ca localizarea şi tipul de dispozitiv utilizat: un PC securizat sau un smartphone nesecurizat. Arhitectura, de asemenea, se concentrează foarte mult pe supravieţuire, pe baza presupunerii că o compromitere este inevitabilă.

Nouă arhitectură se bazează pe patru piloni:

• **Calcul de încredere** (Trust calculation). Acest calcul determină dinamic dacă un utilizator

trebuie să aibă acces la anumite resurse şi de tipul de acces care va furnizat. Se bazează pe factori cum ar dispozitivul şi locaţia client a utilizatorului, tipul de resurse solicitate, precum şi controalele de securitate care sunt disponibile.

• **Zonele de securitate** (Security zones). Mediul este împărţit în zone, variind de la zone de încredere care conţin date critice, cu acces controlat strict, la zone cu nivel de încredere scăzut, care conţin date mai puţin valoroase şi care permit un acces mai larg. Comunicarea între zone este controlată şi monitorizată; dacă una din zone este compromisă, aceasta previne răspândirea problemei la alte zone.

• **Controale echilibrate** (Balanced controls). Pentru a creşte flexibilitatea şi capacitatea de a se recupera după un atac cu succes , modelul de securitate subliniază nevoia pentru un echilibru al controalelor de detectare/corectare, la care să se adauge controalelor preventive implementate prin firewall-uri.

• **Perimetre de utilizator şi de date** (User and data perimeters). Recunoscând că protejarea limitelor reţelei organizaţiei nu mai este adecvată,trebuie să se definească perimetre de utilizatori şi date şi acestea să fie protejate în consecinţă.

Nu toate tehnologiile de securitate necesare pentru implementarea completă a acestui model există astăzi; se încurajarea în mod activ dezvoltarea tehnologiei pentru a susţine capabilităţi, cum ar fi calculul de încredere.

Intel a început punerea în aplicare a acestei arhitecturi şi plănuieşte adoptarea în întreaga organizaţie a arhitecturii de securitate peste aproximativ cinci ani. Utilizarea acestei abordări a dat deja rezultate, ajutându-i prin oferirea de soluţii inovatoare în reducerea eficientă a riscurilor.

Provocarea

Cerinţele de securitate ale tuturor organizaţiilor se schimbă şi extind rapid. Acest lucru se datorează adoptării de noi modelele de utilizare, cum ar fi cloud computing şi consumerizării IT-ului, dar în

aceeaşi măsură şi evoluţiei rapide a ameninţărilor.

Profilul de risc al lui Intel este prezentat în figura 1. Tendinţe cheie includ:

Consumerizarea IT-ului

Mulţi dintre angajaţii extrem de mobili ai Intel doresc să-şi utilizeze propriile dispozitive, cum ar smartphone-urile, pentru muncă. Acest lucru creşte productivitatea angajaţilor pentru că li se permite colaborarea, precum şi accesul la informaţii, de oriunde, în orice moment. Pentru a sprijini acest lucru, se oferă deja un acces limitat la datele organizaţiei, cum ar fi e-mailul, prin intermediul smartphone-urilor şi tabletelor deţinute de angajat.

Deoarece această tendinţă creşte, va fi nevoie să se ofere angajaţilor un anumit nivel de acces la resursele organizaţiei de la un număr din ce în ce mai divers de dispozitive client, unele având controale de securitate mai slabe decât PC-urile mobile de afaceri.

Este nevoie de o arhitectura de securitate care să permită să se ofere suport dispozitivelor noi, să se ofere acces la o gamă mai largă de aplicaţii şi de date, fără a creste riscurile organizaţiei.

Trebuie să existe capacitatea de ajustare dinamică a nivelurilor de acces oferite şi a nivelului de monitorizare, în funcţie de controalele de securitate ale dispozitivului client. De exemplu, un angajat ar trebui să aibă acces limitat la resursele mai valoroase ale organizaţiilor, atunci când se utilizează un dispozitiv mai puţin sigur, cum ar fi un smartphone, în comparaţie cu situaţia când se utilizează un sistem sigur, un PC administrat.

Noi nevoi pentru afaceri

Intel se extinde pe noi pieţe, prin atât prin creştere cât şi prin achiziţii, şi îşi dezvoltă sisteme de colaborare online cu partenerii de afaceri. Ca urmare, au nevoie de a oferi acces la o gamă mai largă de utilizatori, mulţi dintre ei nefiind angajaţi ai Intel.

Pentru a sprijini şi a alimenta această creştere să vor implementa noi sisteme, cum ar fi un portal online de vânzări, care să ofere datele Intel noilor clienţi. De asemenea, trebuie să

integreze bine companiile achiziţionate şi să le asigure acces la resursele de care au nevoie. În general, trebuie să permită Intel accesul rapid către noi utilizatori, reducând la minimum riscul şi să ofere acces controlat şi selectiv numai la resursele de care aceştia au nevoie.

Cloud Computing

Intel IT implementează un nor privat bazat pe o infrastructură virtualizată, de asemenea, iar noi se studiază implementarea serviciilor externe de nor pentru aplicaţii non-critice. În aceste medii tip nor,sistemele şi datele lor sunt virtualizate şi pot migra dinamic către locaţii de reţea logică sau fizică diferite.

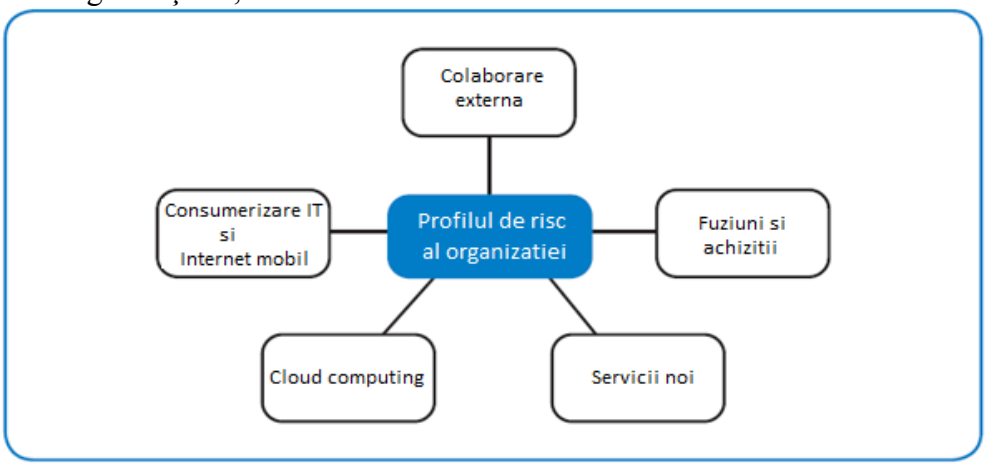


Figura 1. Evoluţia cerinţelor de securitate conduc către nevoia unei noi arhitecturi de securitate.

Acest lucru face dificilă restricţionarea în mod eficient a accesului folosind controalele de securitate tradiţionale ca firewall-uri, care presupune că locaţiile sistemelor şi a datelor pe care acestea le conţin sunt statice. Este nevoie de controale mult mai granulare şi dinamice, care să fie legate de resurse şi nu doar de locaţia în reţea. Este nevoie de o tehnologie de securitate, care să ofere protecţie mai bună platformei şi o mai bună protecţie a datelor, atât celor stocate cât şi în timpul procesării sau transferărilor; Intel evaluează o astfel de tehnologie bazată pe server-e.

Schimbarea peisajului ameninţărilor

Peisajul ameninţărilor evoluează foarte rapid. Din ce în ce mai mult, atacatorii folosesc abordări noi prin crearea de malware, care câştigă accesul în mod neobservat şi încearcă să rămână nedetectat în scopul de a-şi menţine accesul în timp. Pe măsură ce numărul de ameninţări creşte, apar noi tipuri de malware şi trebuie să ne asumăm faptul că o compromitere este inevitabilă.

Arhitectura de securitate tradiţională a organizaţiilor s-a bazat în mare măsură pe controalele preventive realizate prin firewall-uri situate în perimetrul reţelei. Cu toate acestea, obiectivul principal s-a mutat către a permite accesul controlat la o gamă mai largă de utilizatori şi dispozitive, în loc de simpla prevenirea accesului. În plus, continua schimbare a peisajului ameninţărilor face necesar să se presupună că va apare o compromitere. Odată ce un atacator a obţinut acces la mediu, controale preventive care au fost ocolite devin lipsite de valoare. Deşi aceste controalele vor continua să aibă valoare, avem nevoie să punem accentul pe instrumente care să ne crească abilitatea de a supravieţui şi a ne recupera, odată ce atacatorii au căpătat accesul la mediu.

Necesitatea unui noi arhitecturi

Pe măsură ce nevoile de securitate continua să evolueze şi să se extindă, strategiile tradiţionale de securitate ale organizaţiilor nu mai sunt adecvate. Este nevoie de o arhitectura mai flexibilă şi dinamica pentru a permite adoptarea rapidă de noi dispozitive, modele de utilizare, noi capabilităţi, pentru a oferi securitate din cadrul unui mediu din ce în ce mai complex.

În consecinţă, Intel a format o echipă, care a inclus membri din întreaga organizaţie, să elaboreze o nouă abordare a securităţii organizaţiilor, o arhitectură plecând de la zero, pentru a sprijini noile cerinţe şi se determine apoi cum să se pună în aplicare această nouă arhitectură în mediul IT existent.

Arhitectura de securitate

S-a dezvoltat un plan radical de cinci ani, pentru reproiectarea arhitecturii de securitate a lui Intel. Intel consideră ca planul reprezintă o abordare nouă a securităţii organizaţiilor.

Scopul pentru Intel a fost să dezvolte o arhitectură care să permită o mai mare flexibilitate şi să fie productivă în sprijinirea noilor cerinţele ale afacerilor şi ultimelor tendinţele tehnologice, inclusiv consumerizarea IT, cloud computing, precum şi accesul de către o gamă mai largă de utilizatori. În acelaşi timp, arhitectura este proiectată pentru a reduce căile de atac şi de a îmbunătăţi supravieţuirea, chiar dacă peisajul ameninţărilor creşte în complexitate şi maliţiozitate.

S-a stabilit un calendar cinci ani pentru adoptare, deoarece punerea în aplicare necesită un efort amplu pe zona de IT şi pentru că nu toate tehnologiile necesare există astăzi.

Arhitectura se îndepărtează de modelul tradiţional de încredere, care este binar şi static. Cu acest model tradiţional, unui utilizator îi este, în general, fie acordat sau refuzat accesul la toate resursele; o dată acordat, nivelul de acces rămâne constant. Noua arhitectură înlocuieşte acest lucru cu un model de încredere dinamic, multinivel, care să exercite un control mai fin al accesului la resurse. Aceasta înseamnă că pentru un utilizator, nivelul de acces furnizat

poate varia dinamic în timp, în funcţie de o varietate de factori, cum ar fi cazul când utilizatorul realizează accesarea dintr-o reţea de PC administrate, de încredere sau de la un smartphone personal, neadministrat.

Cinci legi de necontestat privind securitatea informaţiilor

Noul model presupune că o compromitere este inevitabilă, mai devreme sau mai târziu; prin urmare, cheia este capacitatea de a supravieţui şi de recupera după o compromitere. Aceste cinci legi de securitate a informaţiilor, concepute de Malcolm Harkins, CISO (Chief Information Security Officer) la Intel şi Director General explica de ce o compromitere este obligatoriu să apară.

1. Informaţia vrea să fie liberă. *Oamenii vor să vorbească, să facă schimb de informaţii, şi ei fac să crească riscul făcând aşa.*

2. Codul vrea să fie greşit. *Niciodată nu vom avea software 100% fără erori.*

3.Serviciile vor să fie funcţionale. *Unele procese trebuie să fie de funcţionale întotdeauna în background şi deci pot fi exploatate de atacatori.*

4.Utilizatorii vor să facă clic. *Oameni în mod natural tind să faceţi clic când văd link-uri web, butoane, sau prompt-uri. Creatorii de malware ştiu acest lucru şi profită.*

5. Chiar şi o facilitate de securitate poate fi folosită pentru a face rău. *Instrumentele de securitate pot fi exploatate de către atacatori, la fel ca alte software-uri. Aceasta înseamnă că legile 2, 3, şi 4 sunt, de asemenea, valabile şi pentru capabilităţile de securitate.*

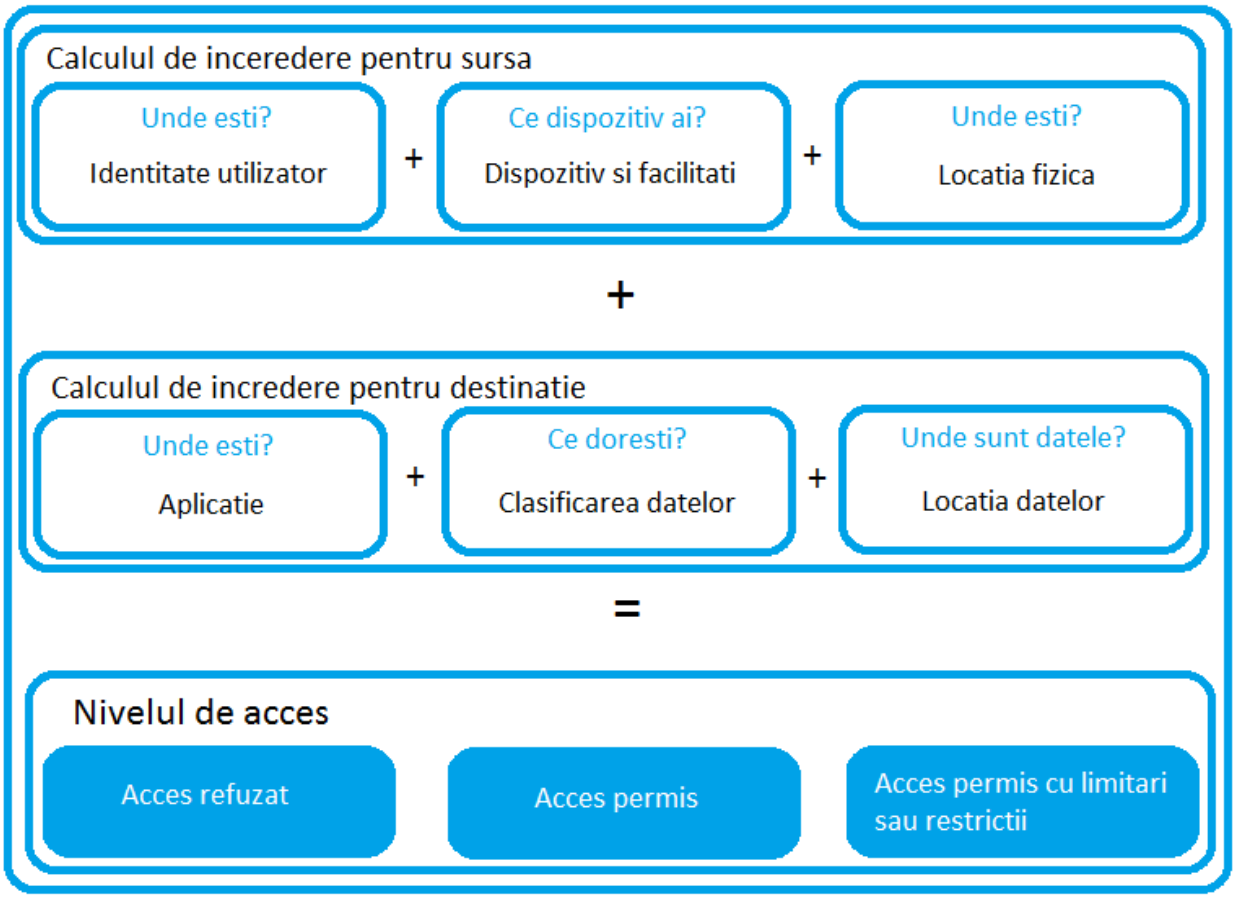


Figura 2. Calculul încredere ia în considerare cine, ce, şi unde, atât pentru sursă cât şi pentru destinaţie

Arhitectura de securitate se bazează pe patru piloni:

Calculul de încredere. Acest unic element de arhitectura este folosit pentru a determina dinamic dacă unui utilizator ar trebui să i se acorde accesul la anumite resurse specifice şi, dacă da, ce tip de acces ar trebui să-i fie acordat. Calculul se bazează pe factori cum ar fi

localizarea şi dispozitivul client al utilizatorului de resurse solicitate, şi controale de securitate care sunt disponibile.

Zonele de securitate. Mediul este împărţit în mai multe zone de securitate. Acestea variază de la zonele de încredere care conţin date critice, cu acces controlat strict, până la zone de încredere cu nivel scăzut, care conţin date mai puţin valoroase şi la care se acceptă un acces mai larg. Comunicarea între zone este controlată şi monitorizată. Acest lucru contribuie la asigurarea faptului că utilizatorii pot accesa numai resurse pentru care au fost autorizaţi şi previne compromiterea prin accesul la mai multe zone.

Controale echilibrate. Pentru a creşte flexibilitatea şi capacitatea de a reveni după un atac cu succes, modelul subliniază necesitatea unui echilibru al controalelor de detectare şi corective în plus controalelor preventive, cum ar fi firewall-urile.

Perimetre de utilizator şi date. Recunoscând că protejarea limitelor retelei organizaţiei nu mai este adecvată, se impune nevoia de a trata utilizatorii şi datele prin perimetre de securitate suplimentare şi a le proteja în consecinţă.

Cei patru piloni sunt descrişi în detaliu mai jos.

CALCUL DE ÎNCREDERE

Calculul de încredere joacă un rol esenţial în furnizarea flexibilităţii necesare pentru a sprijini o expansiune rapidă a numărului de dispozitive şi a modelelor de utilizare. Calculul permite reglarea dinamică a nivelului de acces furnizat, ca şi nivelul de monitorizare, în funcţie de factori, cum ar fi dispozitivul client al utilizatorului curent şi reţeaua pe care o foloseşte.

Se calculează încredere în interacţiunea solicitant (sursă) şi solicitare (destinaţie). Calculul constă dintr-un scor pentru sursă şi un scor pentru destinaţie şi de asemenea, se iau în considerare controale disponibile pentru reducerea riscului. Aşa cum se arată în Figura 2, rezultatul acestui calcul determină dacă utilizatorului i se permite accesul şi tipul de acces oferit.

De asemenea, calculul ia în considerare încrederea pe care o avem în fiecare element de scor, pentru că nu fi întotdeauna avem încredere în datele la dispoziţia noastră. Nu toate tehnologiei necesare pentru calculul de încredere există astăzi; se încurajează în mod activ dezvoltarea acestei tehnologii în cadrul industriei de securitate a informaţiilor.

SCORUL SURSEI

Încredere în sursă, sau solicitant, se calculează bazat pe următorii factori:

Cine. Identitatea utilizatorului sau a serviciului solicitant şi nivelul nostru de încredere în mecanismul de autentificare folosit - câtă încredere avem că utilizatorii sunt cei care pretind că sunt?

Ce. Tipul de dispozitiv, capacităţile sale de control şi capacitatea noastră de a valida aceste controale, şi măsura în care se administrează dispozitivul. De exemplu, un PC-ul de afaceri administrat este mai de încredere decât un smartphone neadministrat al clientului.

Unde. Locaţia utilizatorului sau serviciului. Pentru exemplu, un utilizator care se află în interiorul reţelei organizaţiei este mai de încredere decât acelaşi utilizator conectat printr-o reţea publică. Pot fi şi alte considerente cum ar fi localizarea geografică a utilizatorului.

SCORUL DESTINAŢIEI

Acesta se calculează pe baza aceleaşi trei factori, dar aceştia sunt consideraţi din perspectiva destinaţiei - informaţia pe care sursa încearcă să o acceseze.

Cine. Aplicaţie care stochează datele solicitate. Unele aplicaţii pot pune în aplicare controale mai puternice, cum ar fi managementul drepturilor organizaţiei (Enterprise Rights Management (ERM)) şi, prin urmare, se obţine un nivel mai ridicat de încredere.

Ce. Sensibilitatea informaţiei solicitate şi alte considerente, cum ar fi capacitatea de a le recupera în cazul în care sunt compromise.

Unde. Zona de securitate, în care se află datele.

CONTROALE DISPONIBILE

Calculul încredere, de asemenea, ia în considerare controale de securitate disponibile pentru zona respectivă. În cazul în care sunt disponibile doar controalele care doar blochează sau permit accesul, s-ar putea bloca accesul în lipsa altor opţiuni. Cu toate acestea, dacă avem controale preventive extinse, cu niveluri ridicate de granularitate pentru acces, log-uri detaliate, şi controale eficiente de detectare, ca şi capacitatea de a recupera sau de a corecta problemele - atunci ne putem permite accesul fără crearea de riscuri suplimentare.

CALCULAREA ÎNCREDERII

Calculul de încredere ia în calcul scorul sursei şi scorul destinaţiei pentru a ajunge la un nivel de încredere iniţială. Controalele disponibile sunt apoi luate în considerare pentru a lua o decizie finală dacă accesul este permis şi, dacă da, cum. Acest calcul este efectuat de un punct de decizie de politică (PDP) (policy decision point (PDP)), o entitate logică ce face parte dintr-o infrastructură de autentificare şi ia deciziile de control al accesului pe baza unui set de politici.

Pe baza rezultatelor acestui calcul, PDP poate lua una din următoarele decizii:

- Permite accesul.
- Interzice accesul.
- Permite accesul cu limitări sau restricţii.

Calculul de încredere permite aplicarea dinamică a unui control granular al accesului la anumite resurse ale organizaţiei.

De exemplu, angajaţiilor ce folosesc PC-uri de afaceri mobile administrate cu procesoare Intel ® Core ™ vPro ™ şi facilităţi hardware suplimentare, cum ar fi un TPM (Trusted Platform Module), un card de comunicaţie de date celular cu GPS (globale positioning system) şi criptare completă a discului, li se va permite accesul la mai multe resurse decât atunci când se utilizează smartphone-uri personale. Mai departe, angajaţii vor avea un acces mai larg decât de la kiosk-urile publice.

Angajaţii conectaţi direct la reţeaua organizaţiei li se va oferi un acces mai mare decât folosind o reţea publică. Dacă nu se poate verifica locaţia unui dispozitiv securizat, cum ar fi un PC administrat, acesta va avea un acces restrâns.

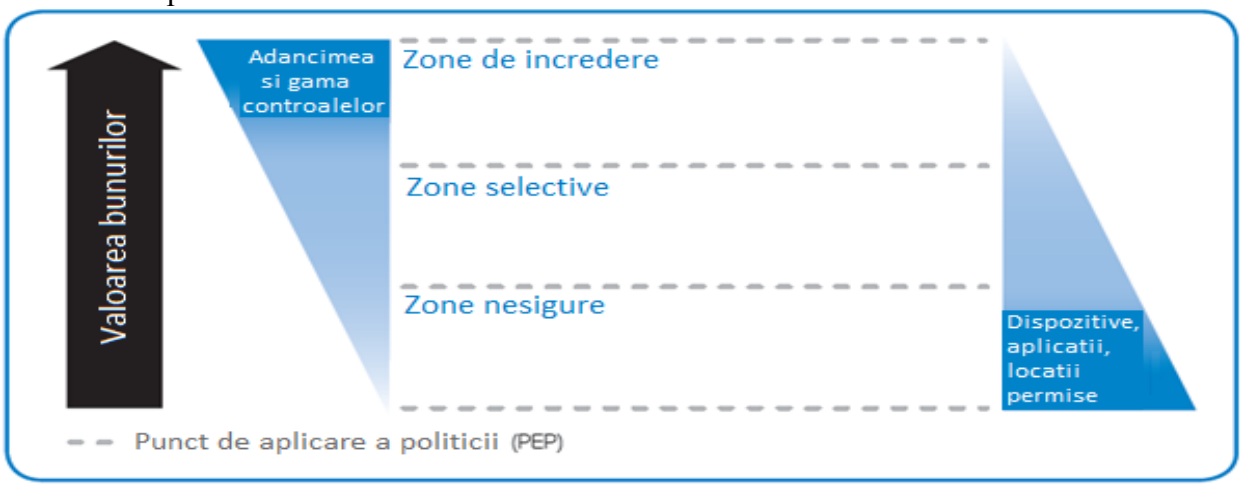


Figura 3. Pe măsură ce valoarea unui bun creşte, profunzimea şi gama controalelor creşte, în timp ce numărul de dispozitive, aplicaţii, şi locaţii permise scade.

Introducere

Calculul de încredere, de asemenea, poate fi folosit pentru a diferenţia modelele de smartphone-uri; s-ar putea oferi diferite niveluri de acces pe baza caracteristicilor de administrare, autentificare şi aplicaţiilor instalate.

S-ar anticipa situaţii în care nivelul de încredere nu este adecvat pentru a permite orice acces, dar poate exista cerinţa de a permite ca o conexiune sau tranzacţie să aibă loc. În aceste condiţii, rezultatul calculului de încredere poate favoriza o decizie care să permită accesul cu limitări, sau cu controale compensatoare care să minimizeze riscul. De exemplu, unui utilizator ar putea să i se permită un acces numai de citire, sau ar putea să i se permită accesul numai în cazul în care sunt disponibile controale suplimentare. O metodă ar fi să utilizeze un sistem care să afişeze informaţiile solicitate de utilizator, dar să nu transmită informaţiile la dispozitivul utilizatorului.

ZONE DE SECURITATE

S-a segment mediului în mai multe zonele de securitate. Acestea variază de la zone de nesigure, care oferă acces la mai puţine date valoroase şi la sisteme mai puţin importante, până la zone care conţin date şi resurse critice.

Deoarece zonele care necesită un nivel mai ridicat de încredere conţin informaţii mai valoroase, acestea trebuie protejate cu o gamă de controale cu o profunzime mai mare şi mai variate, şi trebuie permis accesul la mai puţine tipuri de dispozitive şi aplicaţii, aşa cum se arată în Figura 3. Cu toate acestea, dispozitivele cărora li se permite accesul în zonele cu nivel de încredere mai mare au mai multă putere – li se permite să realizeze acţiuni care nu sunt permise din zone cu nivel de încredere mai scăzut, cum ar fi crearea sau modificarea datelor organizaţiei.

Alinierea infrastructurii la acestă filozofie asigură o modalitate de a dimensiona în mod corect controalele de securitate, astfel încât resursele de securitate să fie utilizate eficient. Îmbunătăţeşte experienţa utilizatorului permiţându-i să aleagă dintr-o gamă variată de dispozitive, ca smartphone-uri pentru activităţi cu risc scăzut.

Accesul la diverse zone este determinată de rezultatele calculului de încredere şi este controlat de puncte de aplicare a politicilor (Policy enforcement points (PEP)). PEP poate include o serie de controale, inclusiv firewall-uri, aplicaţii proxy, sisteme de prevenire şi detectare a intruziunilor, sisteme de autentificare, sisteme de creare a log-urilor.

Comunicarea dintre zone este atent restricţionată, monitorizată şi controlată. Zonele sunt separate prin localizarea lor pe diferite LAN-urile fizice sau VLAN; PEP-urile controlează comunicarea între zone. Aceasta înseamnă că dacă o zonă este compromisă, se poate preveni răspândirea problemei către alte zone sau se cresc şansele de detectare în cazul în care totuşi s-a răspândit problema. În plus, putem utiliza controalele PEP, cum ar fi aplicaţii proxy pentru a furniza acces limitat dispozitivelor şi aplicaţiilor din zone mai puţin sigure, prin controlul accesul la anumite resurse în zone mai sigure, când este necesar.

Se consideră trei categorii principale de zone de securitate: nesigure, selective, şi de încredere. În fiecare zonă, pot exista mai multe subzone.

ZONE NESIGURE

Aceste zone găzduiesc date şi de servicii (sau interfeţele către ele) care pot fi expuse entităţilor care nu prezintă încredere. Acest lucru permite să se ofere acces larg la un set limitat de resurse de la dispozitive neadministrate, cum ar fi smartphone-uri, fără a creşte riscul accesării resurselor cu valoare ridicată, situate în alte zone. Zonele nesigure ar putea oferi acces limitat la resursele organizaţiei, cum ar fi e-mail şi calendare ale organizaţiei sau s-ar putea oferi pur şi simplu acces la Internet.

Se are în vedere că aceste zone au un risc ridicat de a fi atacate şi compromise. În consecinţă, trebuie pus accentul pe controalele de detectare şi corectare, pentru a atenua acest risc, ar putea include un nivel ridicat de monitorizare pentru a detecta activitatea suspectă şi capabilităţi de corecţie, cum ar fi un sistem de reţea - bazat pe îndepărtarea dinamică a privilegiilor utilizator.

Se anticipează nevoia de a oferi accesul controlat din aceste zone la resurse aflate în zone cu nivel de încredere mai mare. De exemplu, un angajat, folosind un smartphone, ar putea avea permis accesul limitat, doar acces de citire, la datele clienţilor situate într-o zonă de încredere, sau, smartphone-ul ar putea avea nevoie de a accesa directorul unui server într-o zonă cu nivel mai ridicat de încredere pentru a trimite un e-mail. Pentru a furniza acest acces într-o manieră controlată se pot folosi proxy-uri. Aceste controale PEP acţionează ca intermediari siguri - evaluând cererile de la dispozitiv, colectând informaţiile solicitate din zona cu nivel ridicat de încredere, şi trimiţându-le la aparat.

ZONE SELECTIVE

Zonele selective asigură o protecţie mai bună faţă de zonele nesigure. Exemple de servicii ce pot fi în aceste zone sunt aplicaţiile şi datele, accesate de către contractori, parteneri de afaceri, şi angajaţii, care utilizează dispozitive client administrate sau altfel spus, asigură un anumit nivel de încredere. Zonele selective nu conţin date critice sau de o valoare cu proprietate intelectuală mare. Câteva subzone pot oferi accesul la servicii sau utilizatori diferiţi. Ca şi în cazul zonelor nesigure, aplicaţii proxy se pot folosi pentru a accesa resurse în diferitele subzone, când e necesar.

ZONE DE ÎNCREDERE

Zonele de încredere găzduiesc servicii, date şi infrastructură critice pentru organizaţie.

Ele sunt extrem de securizate şi asigurate. Exemple de servicii în cadrul acestor zone includ accesul administrativ la serverele centrului de date şi la infrastructura de reţea, reţele şi dispozitive de producţie, aplicaţii ERP (Enterprise Resource Planning), sisteme de proiectare care conţin proprietate intelectuală. În consecinţă, se poate permite accesul direct la aceste resurse doar de la sisteme sigure, localizate în reţeaua organizaţiei şi toate accesele vor fi monitorizate strict, pentru a detecta comportamentele anormale.

CONTROALE ECHILIBRATE

În ultimul deceniu, securitatea organizaţiei s-a concentrat în mod deosebit pe controalele preventive, cum ar fi firewall-uri şi sistemele de detectare a intruziunilor.

Această abordare oferă beneficii clare: este mai puţin costisitoare pentru a preveni un atac decât pentru a corecta problemele după ce unul a avut loc, şi este uşor să se vadă când firewall-ul are succes în a împiedica o încercare de compromitere.

Cu toate acestea, noul model de securitate impune realizarea unui echilibru al controalelor preventive (monitorizare) cu cele corective, din mai multe motive.

În primul rând, punctul central al noului model este de a permite şi a controla accesul unei game mai largi de utilizatori şi dispozitive. În al doilea rând, schimbările continue ale peisajului de ameninţări face necesar să se presupună, că mai devreme sau mai târziu, se va produce o compromitere şi toate controalele preventive, în cele din urmă, vor eşua. După ce atacatorii au obţinut acces la mediu, controale preventive, care au fost ocolite, sunt lipsite de valoare.

Prin creşterea gradului de utilizare a controalelor de detectare şi prin implementarea unor controale corective mai agresive, putem reduce riscul unui acces larg. Aceste controale cresc, de asemenea, capacitatea de a supravieţui şi de a se recupera după un atac reuşit.

Se pot folosi informaţii de securitate – obţinute prin analiza şi corelarea datelor colectate prin monitorizare, pentru a detecta

şi contracara posibile atacuri. De exemplu, se pot detecta şi preveni situaţii anormale, cum ar fi cazul unui utilizator aparent conectat din locaţii diferite în acelaşi timp.

Echilibrul între controalele de detectare, preventive şi corective va diferi în funcţie de zona de securitate. De exemplu, în zone nesigure, se permite un acces larg la foarte puţine resurse şi se vor reduce riscurile prin utilizarea extensivă a controalelor corective şi de detectare. Redundanţa oferită de fiecare tip de control poate fi utilizată pentru a oferi protecţie suplimentară.

Posibile exemple de utilizare a controalelor de detectare şi prevenire pot include:

• un angajat încearcă să trimită printr-un e-mail un document clasificat la o adresă de e-mail care nu aparţine organizaţiei. Software-ul de monitorizare detectează încercarea, şi previne ca documentul să ajungă dincolo de firewall, apoi solicită angajatului să confirme dacă chiar doreşte să facă acel lucru. Dacă angajatul confirmă că doreşte trimiterea e-mail-ului, documentul va putea să fie transmis, sau dacă documentul este extrem de sensibil, o versiune redusă poate fi trimisă;

• utilizarea necorespunzătoare a unor informaţii ERM (enterprise rights management) incluse în document, conduce la revocarea accesului la document;

• sistemul permite accesul la anumite documente, dar urmăreşte activitatea. Un utilizator poate descărca câteva documente fără a cauza probleme. Cu toate acestea, în cazul în care utilizatorul încearcă să descarce sute de documente, sistemul încetineşte viteza de livrare (de exemplu, permiţînd ca doar 10 să fie expediate la un moment de timp) şi se alertează managerul de utilizatori. În cazul în care managerul aprobă, utilizatorul obţine un acces mai rapid.;

• detectarea unui sistem infectat determină plasarea acestuia într-o stare de remediere, izolând sistemul şi restricţionând accesul la informaţiile şi aplicaţiile organizaţiei. Sistemul poate păstra unele capacităţi de acces la informaţiile organizaţiei, dar întreaga activitate este atent memorată (sunt create loguri detaliate), pentru a permite reacţii la incidente, dacă este necesar.

• atunci când un sistem se dovedeşte a fi compromis, se vor examina toate activităţile recente şi interacţiunile cu alte sisteme. În plus, se activează automat monitorizarea acestor alte sisteme.

UTILIZATORI ŞI DATE: NOI PERIMETRE

Cu proliferarea de noi dispozitive, şi aşteptările utilizatorilor au evoluat spre posibilitatea de a accesa informaţii de oriunde, în orice moment, determinând ca graniţele de securitate pentru reţelele organizaţiei să devină mult mai poroase.

Acest lucru înseamnă că apărarea perimetrului reţelei devine din ce în ce mai puţin eficientă. Se va continua să se protejeze perimetrul reţelei, atunci când acest lucru are sens, dar va trebui concentrată atenţia pe protecţia bunurilor primare: proprietatea intelectuală, infrastructură, alte sisteme şi date critice.

Pentru a proteja aceste active, noua arhitectură extinde apărarea spre alte două perimetre: datele în sine şi utilizatorii care au acces la aceste date.

PERIMETRUL PENTRU DATE

Datele importante trebuie protejate permanent - atunci când sunt create, stocate, şi transmise. În acest scop, se pot implementa tehnologii cum ar fi managementul drepturilor organizaţiei (ERM) şi prevenţia scurgerilor de date (DLP-data leak prevention) sau marcarea datelor şi protecţia integrată a lor. De exemplu, cu ERM, creatorul unui document poate defini exact cine are drepturi de acces pe toată durata de existenţă a documentului şi poate revoca accesul oricând.

Arhitectura de securitate în acţiune: O zi din viaţă al unui angajat

Acest exemplu (a se vedea figura 4) descrie modul în care noua arhitectura de securitate permite Intel, diviziei de vânzări, să acceseze informaţiile de care au nevoie în cursul unei zile. În acelaşi timp, arhitectura de securitate protejează Intel prin ajustarea dinamică a nivelului de acces furnizat, bazat pe utilizator, dispozitiv şi locaţie, şi prin monitorizare pentru un comportament anormal.

*1. **Angajatul se deplasează la un site al clientului**. Angajatul foloseşte un smartphone personal şi îi este permis accesul doar la servicii accesibile din zone nesigure. De aici, angajatul poate vizualiza informaţii limitate despre clienţi, inclusiv comenzi recente, extrase dintr-un sistem de planificare a resurselor organizaţiei (ERP) aflat într-o zonă sigură, dar accesibile numai prin intermediul unui proxy server, care protejează zona de încredere şi care acţionează ca un intermediar, ce evaluează cererile de informaţii, accesează sistemul ERP, şi retransmite informaţiile la utilizator.*

În cazul în care smartphone-ul face un număr anormal de cereri de înregistrări ale clienţilor este o indicaţie că smartphone-ul poate să fi fost furat, accesul ulterior de la smartphone fiind blocat. Pentru a ajuta la înţelegerea motivului accesului considerat anormal, se vor monitoriza tentativele angajatului de a accesa sistemul de la orice dispozitiv.

*2. **Angajatul ajunge la site-ul clientului** şi se conectează în reţeaua Intel de la un PC mobil al organizaţiei. Deoarece acest dispozitiv este mult mai de încredere, angajatul are acum acces la capabilităţi suplimentare, disponibile în zone selective, cum ar fi capabilitatea de a vizualiza preţuri şi de a crea comenzi care sunt transmise printr-un proxy ca cereri la sistemul ERP aflat într-o zonă de încredere.*

*3. **Angajatul revine la un birou Intel şi se conectează la reţeaua organizaţiei**. Acum angajatul utilizează un dispozitiv de încredere, într-o locaţie de încredere şi are acces direct la sistemul ERP aflat într-o zonă de încredere.*

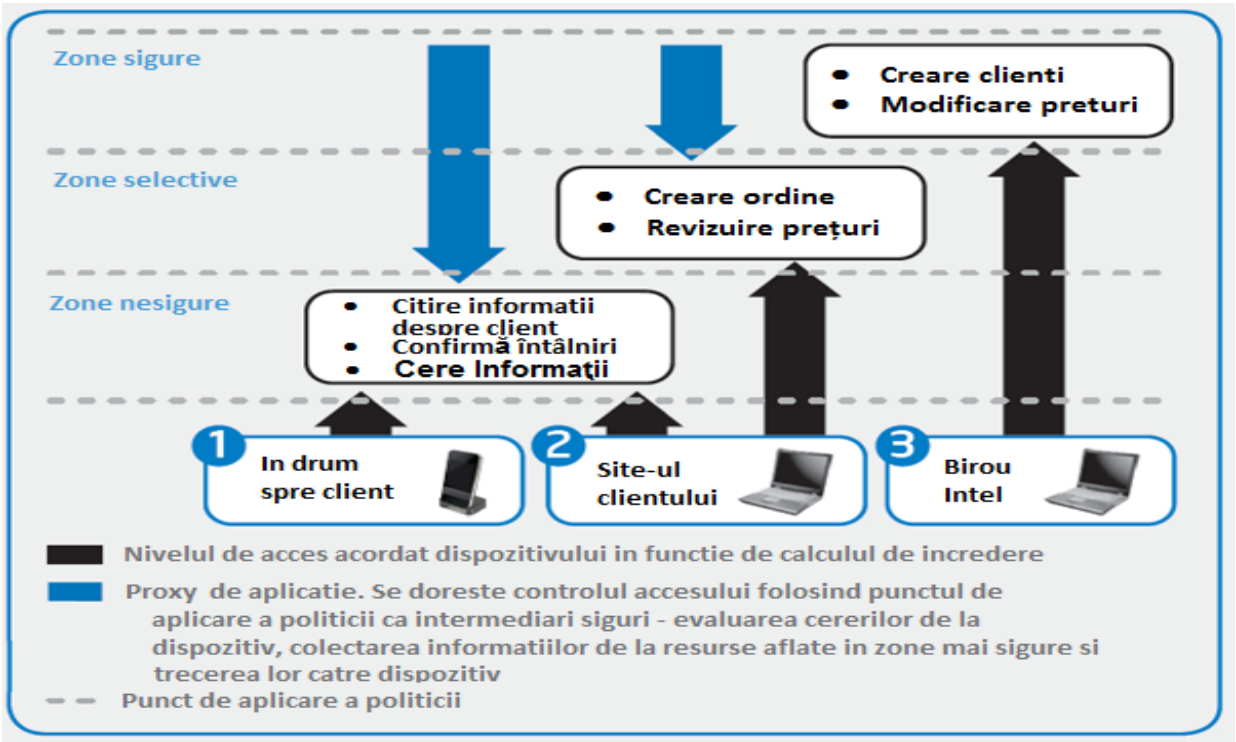


Figura 4. Noua arhitectura de securitate oferă angajaţilor informaţiile de care au nevoie, protejând în acelaşi timp bunurile informaţionale ale Intel.

PERIMETRU PENTRU UTILIZATORI

Utilizatorii însuşi pot deveni riscuri de securitate dintr-o varietate de motive. Ei sunt frecvent ţinte în atacurile de inginerie socială, şi sunt mult mai vulnerabili la aceste atacuri deoarece informaţiile lor personale sunt adesea disponibile pe site-urile de socializare. Aceştia pot, de asemenea, face clic pe link-uri cu malware primite în e-mail, să descarce malware, sau să stocheze date pe dispozitive portabile, pe care apoi le pierd.

Controalele de detectare pot fi folosite pentru a încuraja un comportament mai sigur; de exemplu, alertând utilizatorii atunci când încearcă să trimită documente clasificate în afara firewall-ul, şi îi poate face mai conştienţi de aspectele de securitate în viitor. Astfel, s-a descoperit că o combinaţie de instruire, recompense, şi alte activităţi, pot ajuta să se dezvolte o cultura corporativă de securitate şi protecţie a informaţiilor şi asigurare a confidenţialităţii, şi se încurajează cu succes angajaţii să devină responsabili în protejarea informaţiilor personale şi ale organizaţiei.

CONCLUZIE

Arhitectura de securitate este concepută pentru a satisface o gamă largă de cerinţe în evoluţie, inclusiv noi modele de utilizare şi ameninţări. Scopul este de a permite adoptarea mai rapidă de noi servicii şi capabilităţi, simultan cu îmbunătăţirea capacităţii de supravieţuire. S-a început punerea în aplicare a acestei arhitecturi aproximativ un an în urmă şi se prevede adoptarea de către Intel, în aproximativ cinci ani. S-au înregistrat deja unele succese. Utilizarea acestei abordări a permis să se ofere soluţii în situaţii provocatoare reducând în acelaşi timp efectiv riscurile. De exemplu, s-au implementat controale echilibrate şi zone de încredere pentru a permite accesul la reţea de la dispozitivele proprietate a angajatului. În unele cazuri, s-a constatat o scădere a problemelor de securitate la adoptarea acestui model.

Se anticipează că arhitectura îşi va dovedi valoarea în rezolvarea provocărilor de securitate din cloud computing. Într-un nor virtualizat, este dificil de a restricţiona eficient accesul utilizând controalele tradiţionale de securitate, cum ar fi firewall-uri, care presupun că locaţiile sistemelor şi datelor pe care le conţin sunt statice. În noua arhitectură, folosind instrumente, cum ar fi calculul încredere, se oferă un control mult mai dinamic şi granular asupra accesului la anumite resurse. În plus, prin creşterea utilizării controalelor de detectare şi corectare, se vor reduce vulnerabilităţile controalelor preventive disponibile în prezent.

Deşi nu toate tehnologiile de securitate necesare pentru implementarea completă a acestui model există astăzi, se consideră că ele sunt realizabile. Se încurajează activ cercetarea şi dezvoltarea tehnologiilor pentru a oferi toate capabilităţile necesare, cum ar fi calculul de încredere.

Bibliografie

IT @ Intel Cartea albă, Intel IT Best Practices Information Security, Ianuarie 2011

DESPRE TETRA

Căpitan ing. Viorel ADETU
Centrul 48 comunicaţii şi informatică strategice

TETRA (TErrestrial Trunked RAdio) este un standard dezvoltat de European Telecommunications Standards Institute (ETSI). Este o platformă comună de radiocomunicaţii utilizată de S.T.S., M.A.I., M.Ap.N. în asigurarea telecomunicaţiilor guvernamentale şi ale altor organisme statale.

Beneficiile tehnologiei tetra

Tehnologiile de bază utilizate în standard TETRA, cum ar fi Digital, Trunking şi Time Division Multiple Access (TDMA) oferă o serie de avantaje după cum urmează:

Digital

În prezent, practic tot ceea ce este electronic foloseşte tehnologia digitală iar comunicaţiile fără fir nu fac excepţie. Comunicaţiile radio digitale oferă următoarele avantaje:

- Calitatea convorbirii;
- Aria de acoperire;
- Servicii de date;
- Securitate;
- Cost.

Trunking

Tehnica de trunking a fost folosită de mulţi ani în reţele de telefonie comutate. Primele sisteme trunking de comunicaţii mobile radio au fost implementate la începutul anilor 70 în America de Nord cu protocoale diferite de semnalizare şi la scurt timp după aceea în Europa utilizând tehnologia analogică MPT1327. Principalul beneficiu al trunking-ului este randamentul spectral sau utilizarea unui canal RF de către mai mulţi utilizatori radio, comparativ cu un post de radio convenţional, datorită atribuirii automate şi dinamice a unui număr mic de canale de comunicare partajate între un număr relativ mare de utilizatori.

Deoarece sistemele Trunking suportă mai mulţi utilizatori decât sistemele convenţionale radio, administraţiile naţionale sprijină în mod activ dezvoltarea acestor sisteme deoarece acest lucru ajută la reducerea utilizării spectrului de frecvenţe. Totuşi, din punctul de vedere operaţional al utilizatorului radio, eficienţa spectrului radio nu înseamnă nimic. Ceea ce utilizatorii doresc este rezolvarea tuturor problemelor operaţionale asociate cu reţelele mobile private convenţionale, dar să păstreze încă simplitatea folosirii canalului de comunicaţii. Elementul fundamental, care rezolvă aceste probleme convenţionale este utilizarea unui canal de control.

Tabelul de mai jos enumeră problemele operaţionale ale reţelei mobile private convenţionale şi, de asemenea, modul de utilizare al canalului de control pentru rezolvarea acestor probleme.

Probleme convenţionale	Soluţia Trunking
Congestie	Toate cererile de apel sunt tratate pe canalul de control pentru preluarea apelurilor imediat sau în ordinea priorităţii din coada de aşteptare dacă sistemul este ocupat.
Comutarea manuală de canale	Comutarea automată elimină nevoia selectării manuale a canalului

Utilizarea ineficientă a canalelor	Atribuirea automată şi dinamică a unui număr mic de canale de comunicaţii comune, între un număr relativ mare de utilizatori, asigură un grad egal de servicii pentru toţi utilizatorii radio de pe sistem.
Lipsa de confidenţialitate	Alocarea dinamică şi aleatorie de canale face mai dificil pentru spărgătorii de coduri monitorizarea conversaţiilor.
Abuzul utilizatorilor radio	Abuzul este minimizat deoarece identitatea tuturor utilizatorilor radio, precum şi ora şi durata de convorbire sunt cunoscute şi prin urmare, agresorul poate fi uşor identificat.

Este important de reţinut că simplitatea operaţională a reţelelor mobile private convenţionale este încă menţinută prin implementarea pe terminale a funcţiei rapide "Push to Talk" (PTT).

Servicii şi facilităţi suplimentare

Canalul de control acţionează ca o legătură de semnalizare de comunicaţii între Controller Trunking şi toate terminalele mobile radio din sistem; Controller Trunking cunoaşte starea sistemului în orice moment de timp, precum şi istoricul utilizării, care este stocat în memoria lui. De exemplu, Controller Trunking ştie:

- Id-urile tuturor staţiilor radio şi ale grupurilor înregistrate în sistem;
- Id-ul, ora şi data când staţia radio se afiliază în sistem;
- Id-ul, ora şi data când staţia radio se dezafiliază din sistem;
- Timpul şi durata tuturor mesajelor radio transmise in sistem.

Time Division Multiple Access (TDMA)

Tehnologia TDMA a fost adoptată în TETRA deoarece a oferit soluţia optimă pentru a echilibra costurile de echipament, cu acela de a susţine serviciile şi facilităţile cerute de către utilizatori pentru o reţea de medie şi mare capacitate, oferind acoperire locală pentru un singur site sau pentru o zonă largă de acoperire prin interconectarea mai multor site-uri.

Un alt avantaj al tehnologiei TDMA este acela că permite noi servicii şi facilităţi să fie susţinute cu costuri minime. Unele exemple sunt:

Viteze mai mari pentru transmiterile de date

Legile fizicii limitează viteza maximă de date într-un anumit canal în funcţie de lăţimea de bandă. Presupunând că folosim aceeaşi modulaţie, cu cât lărgimea de bandă este mai mare cu atât viteza pentru transmiterile de date este mai mare. Deoarece TDMA foloseşte canale mai mari decât FDMA, viteza de transfer de date combinată pe un singur canal RF este mai mare.

Capacitate îmbunătăţită de date în condiţii precare de semnal RF

Viteza transmiterilor de date în TDMA este mai bună decât FDMA în condiţii precare de propagare. Acest lucru se datorează faptului că cereri automate de repetare (ARQ) sunt transmise atunci când datele primite au erori datorate perturbaţiilor RF. Deoarece terminalele TDMA funcţionează în full duplex cererile automate de repetare (ARQ) pot fi trimise eficient după transmiterea fiecărui interval de timp în loc să se aşteptare până la sfârşitul transmisiei de voce, aşa cum se întâmplă de obicei cu FDMA.

Lăţime de bandă la cerere

În TDMA orice număr de sloturi de timp, până la limita maximă a tehnologiei,

pot fi combinaţi pentru a spori viteza de transfer a datelor tranzitate, în funcţie de necesarul fiecărei aplicaţii.

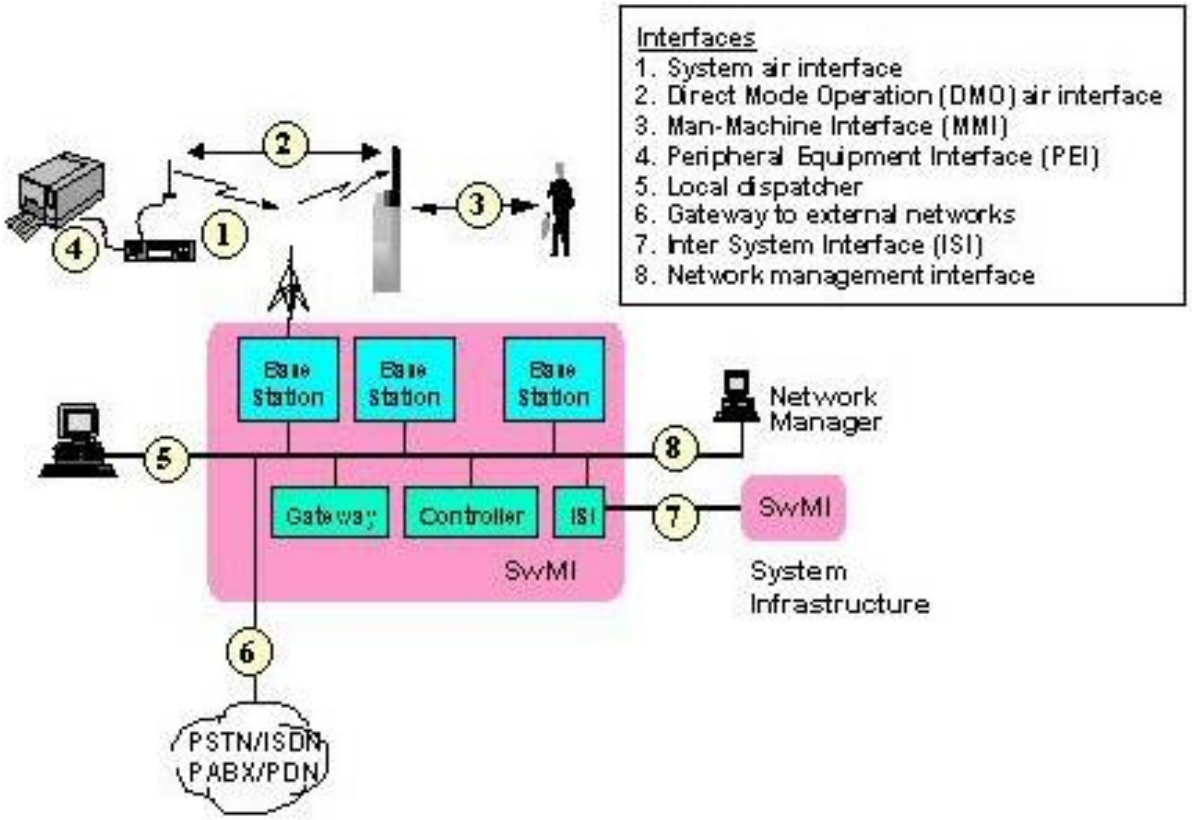
Concomitenţă voce şi date

Datorită structurii cu sloţi de timp în TDMA este posibilă folosorea unui slot de timp pentru a transmite voce şi următorul slot pentru a transmite date într-o transmisie pe doi sloţi între două terminale radio. Această capacitate efectiv permite unui singur terminal radio să transmită sau să primească voce şi date în acelaşi timp.

C*omunicaţii de voce full duplex*

Tehnologia TDMA suportă comunicare full duplex. Deşi comunicaţiile de voce duplex pot fi realizate şi pe sisteme FDMA, este nevoie de un duplexor şi o ecranare RF între emiţător şi receptor pentru a permite lucrul cu o singură antenă. Din acest motiv terminale radio care folosesc FDMA sunt de obicei mai costisitoare decât terminale TDMA.

O prezentare generală a elementelor de reţea acoperit în standard TETRA sunt prezentate în figura următoare:



Air Interface(1 & 2)

Cele mai importante (şi mai complexe) interfeţe sunt considerate a fi "air interface" între staţia de bază şi terminalele radio (1) şi interfaţa Direct Mode Operation (DMO) (2). DMO este o facilitate care permite terminalelor să opereze în reţele radio locale, independent de infrastructura principală a reţelei TETRA.

Interfeţele echipamentelor periferice (4)

Această interfaţă standardizează conectarea terminalului radio la un dispozitiv extern, şi suporta transmisii de date între aplicaţiile rezidente din aparat şi terminalul radio TETRA conectat. Serviciul PEI suportă, de asemenea, anumite elemente de control în cadrul terminalului radio de la dispozitivul extern şi / sau de la aplicaţie.

Interfaţa de control de la distanţă a dispecer-ului (5)

Această interfaţă a fost iniţial destinată pentru a permite conectarea la dispecer de la distanţă , cum ar fi cele situate în sălile de control majore . Din păcate, lucru pe această interfaţă a fost abandonat în ETSI TC TETRA deoarece complexitatea de a oferi o interfaţă universală fără a degrada performanţele a fost imposibilă. Acest lucru s-a întâmplat deoarece în industria reţelelor private mobile sunt constructori specializaţi în controlere care, în majoritatea lor, au metode diferite de conectare la interfaţa reţelei private mobile. În mod similar, structura producătorilor de reţele TETRA, este de asemenea diferită, aceasta contribuind la complexitatea de a oferi o interfaţă universală.

Din aceste motive numai specificaţiile producătorului TETRA sunt disponibile pentru a sprijini serviciul de voce, date şi aplicaţii care necesită acces la infrastructura TETRA.

PSTN / ISDN / PABX (6)

Această interfaţă standardizată permite conectarea TETRA la interfaţa cu PSTN, ISDN şi / sau PABX.

Interfaţa Inter-System (7)

Interfaţa Inter-System (ISI) standardizată permite infrastructurilor furnizate de diferiţi producători TETRA să interopereze una cu cealaltă, interoperabilitatea fiind permisă între două sau mai multe reţele. Există două metode de interconectare în standard, una acoperă transferul de informaţii folosind modul de circuite şi alta folosind pachete.

Interfaţa de management de reţea (8)

Ca şi interfaţa dispecer local, a fost recunoscut în timpul activităţilor de standardizare că o politică comună a interfeţei de management al reţelei nu este practică. Din fericire, această standardizare timpurie nu a fost irosită, deoarece mai târziu a fost transformată într-un ghid complet pentru a ajuta utilizatorii în definirea cerinţelor de management de reţea.

Pe lângă standardele acestor elemente de reţea, numeroasele servicii şi facilităţi disponibile în reţeaua TETRA sunt, de asemenea, standardizate. Cele mai importante dintre acestea fiind:

- Servicii de apel de grup avansate şi rapide - clare şi criptate;
- Apeluri individuale - clar şi criptate;
- Serviciul de mesaje scurte - clare şi criptate;
- Servicii de pachete de date - clare şi criptate;
- Voce + date (V + D).

Pentru a răspunde nevoilor organizaţiilor tradiţionale de utilizatori ai reţelei private mobile, o gamă largă de servicii de voce, date şi facilităţi au fost prevăzute în standard, dintre care cele mai importante sunt considerate a fi:

Servicii de voce şi facilităţi

- Apelul de grup;
- Apel prioritar (apeluri de urgenţă);
- Asignare dinamica a numărului de grup (DGNA);
- Ascultarea ambientală;
- Apel autorizat de dispecer;
- Aria de selecţie;
- Intrare târzie;
- Serviciul mesaje scurte;
- Pachete de date;
- Coada de aşteptare;
- Mod de operare directă (DMO);
- Criptarea vocii.

Servicii de voce

Apel de grup

Acesta este, probabil, cel mai de bază serviciul de voce în TETRA, dar si cel mai complex pentru a sprijini efectiv şi eficient. Acest lucru se datorează faptului că apelul de grup trebuie:

- să fie simplu de utilizat: "Push to Talk" furnizează rapid apelul de

comunicaţii în grup;

- să fie exploatate şi gestionate în mod special pentru a optimiza încărcarea reţelei;
- să opereze pe un site "preferat" pentru o încărcare optimă de reţea;
- să aibă definită o arie de funcţionare (aria de selecţie);
- să aibă un protocol de semnalizare al setărilor de apel fiabil, înfiinţat pentru a se asigura tuturor utilizatorilor dintr-un grup că sunt conectaţi împreună atunci când un apel este primul iniţiat (semnalul de recunoaştere al apelului nu este practic pentru apeluri de grup).
- să dispună de mecanisme de prioritate pentru a se asigura că utilizatorii specificaţi într-un apel de grup larg(site-uri care acoperă mai multe staţie de bază) sunt conectaţi împreună, atunci când o reţea este ocupată.

Această complexitate este necesară pentru a sprijini apelurile de grup, lucru care nu este posibil în reţelele celulare publice, pur şi simplu pentru că acestea au fost concepute iniţial pentru a sprijini apeluri de tip "unu la unu", spre deosebire de TETRA care a fost proiectat în principal pentru a sprijini apeluri de grup.

Apel prioritar

Aceste tipuri de apeluri, din care cea mai mare prioritate o are apelul de urgenţă, oferă cea mai mare prioritate pe uplink şi cea mai mare prioritate de acces la resursele reţelei. Dacă o reţea este ocupată, canalul convorbirii cu cea mai mică prioritate va fi ocupat de către apelul de urgenţă. Apel de urgenţă TETRA poate fi iniţiat cu ajutorul unui comutator dedicat situat pe terminal. Activarea apelului de urgenţă transmite alerte automate către sistemul de management, dispecer şi celelalte terminale care se afla in acelaşi talkgrup.

Asignare dinamică a numărului de grup (DGNA)

Acest serviciu permite crearea de grupuri unice de utilizatori pentru a gestiona diferitele nevoi de comunicare şi poate fi de asemenea utilizat pentru a grupa participanţii unei convorbiri aflate în desfăşurare. Acest serviciu este considerat de multe organizaţii de siguranţă publică a fie extrem de util deoarece permite înfiinţarea de grupuri de convorbire comune pentru anumite structuri. De exemplu, utilizatorii selectaţi din poliţie, pompieri şi serviciul de ambulanţă ar putea fi aduşi împreună într-un grup pentru a gestiona o situaţie de urgenţă majoră în cazul în care între cele trei servicii de urgenţă este necesară o strânsă coordonare.

Ascultarea ambientală

Un dispecerat poate seta un terminal radio în modul de ascultare ambientală, fără ca utilizatorul terminalului radio să primească vreo notificare. Această acţiune controlată de la distanţă permite dispecerului să asculte zgomotele de fundal şi conversaţiile din raza de acţiune a microfonului terminalului radio. Acesta este un serviciu important pentru utilizatorii care transportă materiale importante, valoroase sau sensibile, care ar putea fi deturnate. În mod similar, acesta este un serviciu util de a avea puse în aplicare în vehicule de serviciu public în cazul în care sănătatea unui mecanic de locomotivă şi de securitate ar putea fi la risc. Cu toate acestea, este important să se notă de faptul că mulţi utilizatori consideră că acest serviciu invadează intimitatea unei persoane şi pentru acest motiv numai acei utilizatori care au nevoie de serviciul de ascultare ambientală ca parte a îndatoririlor lor de muncă ar trebui să fie prevăzute cu acest serviciu.

Apel autorizat de dispecer

Acest serviciu permite expeditorului să verifice cererile de apel înainte ca apelurile să fie iniţiate. Acesta este un serviciu util atunci când se doreşte menţinerea disciplinei radio. Acest serviciu, de asemenea, reduce cantitatea de trafic radio pe o reţea, deoarece doar apelurile sunt permise. Totuşi, nevoia frecventă de a

comunica într-un grup de utilizatori şi intervalul de timp necesar pentru autorizarea apelurile pot face acest serviciu inacceptabil pentru unii utilizatori.

Aria de selecţie

Acest serviciu defineşte domeniile de operare pentru utilizatori. Acest serviciu simulează practic capacitatea unui dispecerat de a selecta diferite staţii de bază pentru a face un apel, aşa cum a fost posibil în reţelele convenţionale. Acest serviciu, de asemenea, ajută la îmbunătăţirea încărcării reţelei şi eficienţa spectrului prin limitarea zonelor de exploatare pentru toate apelurile selectate dintr-un grup.

Intrarea Târzie

Acest serviciu oferă actualizări continue ale apelului în curs, pentru a permite utilizatorilor sosiţi ulterior să adere la un canal de comunicare. Acest lucru nu este un serviciu, ci o interfaţă caracteristică care permite unui terminal radio trunked să se comporte într-un mod similar cu terminale radio mobile private convenţionale. De exemplu, dacă un utilizator porneşte terminalul său TETRA canalul de control va devia în mod automat terminalul utilizatorului pe un apel de grup, daca acesta este deja în curs.

Data Services

Short Data Service

Short Data Service poate oferi până la 256 de bytes de date, care pot fi utilizaţi pentru mesaje de stare ale staţiei de bază, informaţii privind localizarea acesteia şi gratuit aplicaţii pentru mesaje text, fie în formă "punct la punct" sau "punct la multipunct". Din cauza duratei relativ scurte a fiecărui mesaj de date, acest serviciu este acceptat de canalul de control TETRA în intervale orare TDMA.

Serviciul de pachete de date

Pachetele de servicii de date pot fi sprijinite pe un slot de timp TDMA cu o rată de biţi protejate brut de 4800 biţi / s sau mai multe sloturi de timp TDMA până la un maxim de patru sloturi de timp. Sloturile multiple de timp TDMA sunt adesea utilizate ca laţime de bandă la cerere şi poate fi folosită pentru a creşte rata datelor protejate de transfer de până la 19,2 kbits / s, crescând astfel numărul de aplicaţii non-voce, care pot fi suportate de TETRA.

Coada de aşteptare

TETRA este prevăzută cu canal de control, iar în timpul perioadelor când reţeaua este ocupată, sistemul poate stoca şi gestiona apelurile pe un First In First Out (FIFO), în baza de date, în ordinea de prioritate la nivel de utilizator. Avantajul este că un utilizator poate iniţia o cerere de apel o singură dată , deoarece în perioadele aglomerate apelul va fi stabilit în mod automat o dată ce canalul devine liber, reducând astfel neplăcerile cu care se confruntă utilizatorii, când reţeaua este ocupată.

Mod de operare directă (DMO)

Modul de operare directă (DMO) prevede posibilitatea terminalelor radio TETRA de a comunica direct, corespondent cu corespondent, independent de infrastructura de reţea TETRA.

DMO a fost concepută ca o reţea comună şi utilizată de către numeroase organizaţii tradiţionale PMR pe o perioadă lungă de timp. Cerinţa principală pentru DMO a fost determinată de necesitatea de a echilibra acoperirea de RF, gradul de utilizare (GOS) şi fiabilitate a unei reţele de comunicaţii cu cea a costurilor reţelei în ansamblu. Utilizarea DMO în reţele publice de telefonie mobilă nu este posibilă.

Criptare de voce

Standardul TETRA suportă un număr mare de algoritmi de criptare (TEA), diferenţele fiind tipurile de utilizatori care sunt autorizaţi să le utilizeze. Principalul beneficiu al criptării prin aer este că pot fi implementate soft-uri fără terminale radio şi echipamente ale staţiei de bază, în locul utilizării modulelor de criptare, care consumă spaţiu şi duce la creşterea costurilor. De asemenea standardul TETRA, suportă o varietate de algoritmi de criptare, considerate necesare de către organizaţiile de securitate naţională.

TETRA - securitate

Zona de securitate TETRA este extinsă, deoarece trebuie să furnizeze diferite nivele de securitate, de la ceea ce este acceptabil în reţelele comerciale la ceea ce este acceptabil pe o reţea naţională de siguranţă publică. Mecanismele de securitate în TETRA se realizează în standard, prin autentificare, criptare Air Interface (AIE) şi End to End encryption (E2E). Ameninţările la confidenţialitatea, autenticitatea, integritatea, disponibilitatea, precum şi responsabilizarea în sistemul TETRA sunt protejate cu ajutorul celor trei mecanisme de securitate.

Autentificarea reciprocă este un serviciu necesar pentru a se asigura că un sistem TETRA poate controla accesul la aceasta, şi pentru un terminal radio, pentru a verifica dacă într-o reţea se poate avea încredere. În TETRA, ca şi în cele mai multe alte sisteme sigure, autentificarea este baza pentru o mare parte a securităţii reţelelor globale şi pot fi de asemenea, utilizate pentru a asigura funcţionarea în sistemele de acces public, şi poate oferi baza pentru un canal de distribuţie sigur la informaţii sensibile, cum ar fi alte chei de criptare. Autentificarea mecanismelor comune de securitate protejează serviciile de voce cât şi cele de date. Standardul TETRA suportă patru Algoritmi de criptare TETRA (AIE), acestea fiind TEA1, TEA2, TEA3 şi TEA 4. Diferenţa constă în utilizarea şi exportarea echipamentelor care conţin aceşti algoritmi de criptare. De exemplu, TEA2 este destinat utilizării de către public, utilizatorii de siguranţă la Schengen şi mai ales în ţările europene, ceilalţi utilizatori folosind aplicaţiile pentru siguranţa publică în regiunile în care TEA2 nu este utilizat. Principalul beneficiu al criptării prin aer este acela de protecţie pentru toţi utilizatorii de semnalizare şi identitate, de voce şi date oferite de aceasta. Sistemul de criptare este strâns legat de TETRA, de semnalizare a protocoalelor şi algoritmi care pot fi puşi în aplicare în termen, la soft-urile terminalelor radio şi echipamentele staţiilor de bază, în locul modulelor de criptare, fără a consuma spaţiu şi a duce la creşterea costurilor.

Standardul TETRA suportă, de asemenea criptarea E2E folosind o varietate de algoritmi de criptare consideraţi necesari de către organizaţiile de securitate naţională. Asociaţia de Securitate TETRA şi Grupul de prevenire a fraudei, a extins activitatea în standardul TETRA, pentru a defini un cadru general în implementarea criptării E2E. Soluţiile simple recomandate au fost distribuite de International Data Encryption Algorithm (IDEA) algoritmul (DPI deţinute de Ascom) şi mai nou Advanced Encryption Standard (AES) algoritmul (DPI gratuit), care beneficiază de un algoritm criptografic mai mare ca dimensiune. Utilizarea algoritmilor locali este posibilă cu criptarea E2E, deşi acestea nu sunt recomandate pentru criptarea prin aer (AIE) din cauza nevoii de integrare în protocoale de semnalizare şi disponibilitatea de terminale standard.

Pe lângă capabilităţile de securitate, TETRA de asemenea poate suporta o gamă largă de capabilităţi de management de securitate, cum ar fi cele utilizate pentru a controla, gestiona şi a opera mecanismele de securitate individuale într-o reţea. Cel mai important dintre acestea este managementul cheilor de criptare, care este pe deplin integrat în funcţiile standard de criptare TETRA. Chiar dacă funcţiile de securitate sunt integrate într-o reţea acest lucru nu implică în mod automat că o reţea este pe deplin sigură. Cu toate acestea, este normal faptul că riscurile de securitate sunt condensate, chiar dacă elemente specifice concentrate în reţea poate fi controlate în mod adecvat.

Bibliografie: http://www.tetramou.com

COMUNICAŢIILE CUANTICE – COMUNICAŢIILE VIITORULUI

Maior Vasile MÎRZEA
Centrul 42 comunicaţii şi informatică de sprijin

În vara anului trecut o ştire de domeniul Star Trek ţinea prima pagină a ziarelor: „In iunie 2010, oamenii de ştiinţa chinezi de la University of Science and Technology of China, împreună cu colegii lor de la Tsinghua University din Beijing, au publicat in revista de specialitate Nature Photonics rezultatele unei cercetări, care arata ca "teleportarea prin entanglement cuantic" este cheia viitorului. Aceasta ar putea duce la dezvoltarea unor computere cuantice, dar si a unor comunicaţii cuantice, ce nu vor putea fi interceptate, ei reuşind teleportarea unor informaţii la 16 kilometri distanta" [1].

Aceasta este ştirea, dar să vedem cum s-a ajuns la aceste descoperiri de domeniul ficţiunii şi care este mecanismul acestei „teleportări".

Istoria acestui experiment [2] începe cu Einstein, Podolosky si Rosen care au încercat să realizeze un experiment (botezat EPR, după iniţialele lor) prin care să demonstreze că teoria cuantică era incompleta. Apărătorii teoriei au atacat argumentul lui Einstein, fără a produce însă date concrete in sprijinul acesteia. Eventualitatea tranşării disputei a apărut în momentul în care irlandezul John Bell a dovedit că, dacă particulele ar avea proprietăţi permanente (cum afirma Einstein), atunci ar exista o limită a similitudinii lor, dată de viteza finită a luminii.

In 1982, Alan Aspect şi colegii lui au reuşit în sfârşit sa realizeze Experimentul EPR folosind fotoni de lumină. Ei au descoperit că inegalitatea lui Bell nu se confirmă: doi fotoni separaţi prin distanţe mari păreau capabili sa „comunice" instantaneu, cu un nivel al corelaţiei depăşind cu mult inegalitatea respectiva. Implicaţiile erau majore: cum inegalitatea lui Bell căzuse, cel puţin una dintre presupunerile ei – aceea făcută de Einstein – era greşită. Concluzia: fie particulele nu au proprietăţi definite până ce nu sunt observate, fie sunt capabile sa comunice cu viteze mai mari decât viteza luminii. Sau si una, si alta. Pentru mulţi fizicieni, mesajul devenea clar: teoria cuantica era corecta. Mai rămânea de aflat cum comunica particulele inseparate. Experimentul lui Aspect părea să se dovedească însă un fenomen fără nici o valoare practica.

Au urmat alţi oameni de ştiinţă, care, încet-încet, au reuşit sa dea anumite aplicaţii inseparării. In 1985, David Deutsch a conceput un model de calcul capabil sa rezolve probleme extrem de complexe; in 2002, o echipa de la Universitatea Leiden (Olanda) a arătat ca efectul inseparării poate trece prin metal, iar in 2003, la Viena, profesorul Anton Zeilinger si colegii lui au transmis fotoni inseparaţi peste Dunăre. Acest experiment a constat in scanarea unui obiect si in folosirea unor perechi de particule inseparate pentru a le capta proprietăţile. Informaţiile astfel obţinute puteau fi folosite pentru a recrea obiectul oriunde ar fi fost trimise perechile inseparate ale primelor particule.

In 1997, Zeilinger si colegii reuşiseră „teleportarea" unui singur foton pe distanta de un metru utilizând insepararea cuantica.

Anul 2007 aduce un nou record în transmiterea de informaţii cu ajutorul teleportării cuantice: profesorul Ursula Gerber si colegii ei de la Universitatea din Viena au transmis date pe o distanta de 144 de kilometri, intre insulele La Palma si Tenerife [3]

Fizicienii au reuşit sa teleporteze date intre 2 telescoape situate pe 2 dintre Insulele Canare, La Palma si Tenerife, aflate la distanta de 144 km unul de altul, de 10 ori mai mult decât recordul anterior de teleportare in aer liber. Oamenii de ştiinţă au realizat acest lucru folosind fenomenul de

"corelaţie cuantica" ("quantum entanglement"),

Corelaţia cuantica, numita de către Einstein "acţiune ciudata [spooky] la distanta", se bazează pe faptul ca doi fotoni pot fi creaţi intr-un mod in care se comporta ca un singur obiect, chiar daca sunt separaţi de distante foarte mari. Comportându-se in acest mod, ei acţionează ca o maşina de teleportare, deoarece orice schimbare intr-unul dintre ei cauzează o schimbare similara in celalalt.

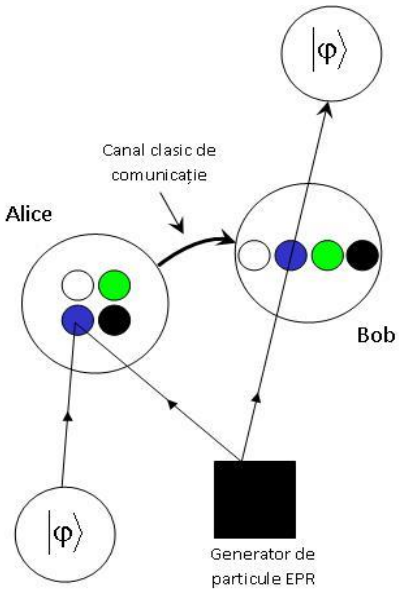


Figura 1-Schema clasică de funcţionare a comunicaţiei cuantice

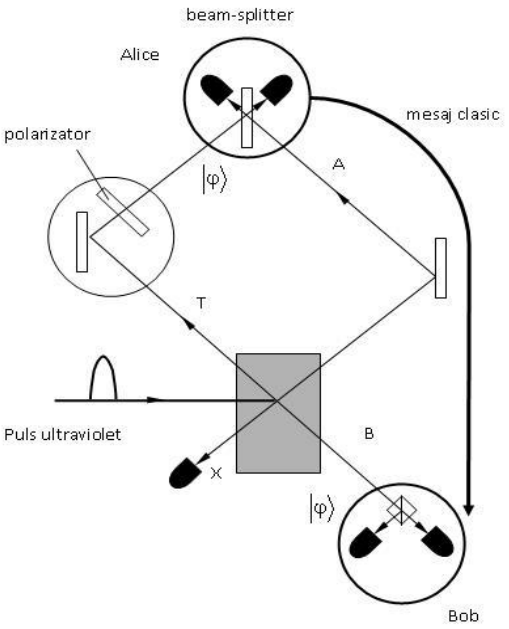


Figura 2-Schema simplificată a experimentului

Aceasta se realizează printr-un al treilea foton, care este teleportat intre cei doi fotoni. În acest proces, al treilea foton devine "corelat" cu fotonul transmiţător şi poartă astfel informaţia cuantica către fotonul receptor. Acesta interacţionează cu fotonul purtător intr-un mod care ii face identici pe cei doi, obţinându-se astfel transmiterea cu succes a informaţiei. Schema clasică de funcţionare a unei astfel de comunicaţii a fost propusă de Charles H. Bennett, Gilles Brassard, Claude Crepeau, Richard Jozsa, Asher Peres şi William K. Wooters şi funcţionează în felul următor:

Fie $|\varphi\rangle$ - starea particulei care trebuie teleportată (figura 1). Vom numi două personaje fictive ale experimentului, Alice – care posedă informaţia ce trebuie teleportată – şi Bob – care trebuie să intre în posesia lui $|\varphi\rangle$. Presupunem că Alice şi Bob au împărţit deja pe din două o pereche de particule EPR. Acum Alice nu mai are nimic de făcut decât să efectueze o măsurătoare Bell asupra sistemului format din $|\varphi\rangle$ şi propria sa particulă EPR. În urma acestei măsurători, Alice va obţine patru rezultate posibile, corespunzând celor patru stări ortogonale numite stări Bell. Stabilindu-şi anterior un cod prin care fiecărui rezultat îi era asociată o singură transformare locală, Alice îi poate transmite lui Bob un semnal constând din doi biţi de informaţie, printr-un canal de comunicaţie clasic. Astfel Bob va afla că propriei sale particule EPR i s-a întâmplat "ceva" şi că, aplicându-i transformarea corespunzătoare codului

primit de la Alice, îl va obţine tocmai pe $|\varphi\rangle$.

Spre exemplificare voi descrie schema simplificată a unui experiment.

Un puls ultraviolet străbate de 2 ori un cristal (al cărui indice de refracţie are un comportament nelinear), generând o pereche de fotoni cuplaţi deplasându-se către stânga (T, X) şi o alta - către dreapta - care va fi folosită drept pereche Alice-Bob. Fotonul de teleportat este preparat prin modificarea polarizării lui T şi apoi combinat cu fotonul lui Alice - A - într-un beam-splitter. Când ambele detectoare sunt declanşate simultan, s-a "măsurat".

Aceste descoperiri şi experimente ar putea duce la evoluţii noi in distribuţia de energie, precum şi la o mai bună înţelegere a relaţiei dintre informaţia cuantica şi de energia cuantica. Oamenii de ştiinţă afirmă însă că fenomenul poate fi folosit doar pentru transmiterea celor mai simple forme de materie, şi că pentru a teleporta oameni sau obiecte este nevoie de o cu totul altă metodă, necunoscută deocamdată. Tehnologia poate fi folosită pentru a transfera informaţie folosind criptare cuantică, care ar permite trimiterea de coduri de securitate ce nu pot fi sparte şi realizarea de calculatoare superrapide.

Referinţe:

1.http://www.realitatea.net/teleportare-cuantica-reusita-pe-o-distanta-record-de-16-kilometri_717464.html;
2.http://www.descopera.ro/stiinta/929144-atentie-urmeaza-teleportarea;
3.http://www.blitztech.ro/tehnologie/stiinta/nou-record-de-teleportare-cuantica/;
4.Alexander V. Sergienko: Quantum Communications a Cryptography, ed. Taylor & Francis, 2006.

MANAGEMENTUL FRECVENŢELOR RADIO – FACTOR ESENŢIAL PENTRU ASIGURAREA SUPERIORITĂŢII INFORMAŢIONALE

Maior Busuioc MUNTEAN
Locotenent Dorin CHIRCA
Centrul 346 comunicaţii RMNC

Începând cu secolul al nouăsprezecelea, când fenomenul fizic de unde radio a fost descoperit, spectrul de radiofrecvenţă a devenit un element decisiv din punct de vedere economic, industrial, social şi cu influenţe chiar şi în viaţa privată. Disponibilitatea lui este indispensabilă pentru radio, televiziune şi transmisiile multimedia în era nouă a societăţii globale informaţionale.

Frecvenţele au o valoare economică; ele pot sta la baza comerţului şi formează o bază importantă pentru creşterea economică şi competiţia industrială. O naţiune care-şi maximizează eficienţa privind managementul frecvenţelor, are capacitatea de a genera evoluţie tehnică, inovaţii şi de a reuni în mod constructiv provocările economice, sociale şi chiar politice. Este necesar ca această resursă rară să fie distribuită şi coordonată între naţiuni. În acelaşi timp naţiunile doresc să-şi exercite suveranitatea totală în ceea ce priveşte alocarea frecvenţelor. Pentru a face accesibilă folosirea spectrului în aceste circumstanţe este necesar ca toate naţiunile să se pună de acord şi să stabilească norme şi standarde comune pe care să le respecte.

Cu privire la comunicaţiile prin satelit şi navigaţie, la fel ca şi diseminarea tv şi fenomenul radio global, repartizarea frecvenţei trebuie să fie coordonată mondial.

La nivel mondial, spectrul de radiofrecvenţă a devenit din ce în ce mai important pentru dezvoltarea economiei. Cererea pentru spectrul radio sporeşte constant ca urmare a progresului tehnologic, a pieţei globale şi a dezvoltărilor regulate. Aceasta nu este contrabalansată de spectrul radio adiţional devenit disponibil prin introducerea de tehnologii noi şi eficiente. Consecinţa acestui fapt este dată de lipsa accentuată a spectrului radio. Acolo unde spectrul radio este aglomerat sunt necesare anumite decizii pentru a se echilibra cererea şi alocarea de spectru radio.

Responsabilitatea de a coordona şi a conduce a devenit mult mai complexă comparată cu anii trecuţi şi mediul pentru politica spectrului radio s-a schimbat semnificativ. În acest moment se dezvoltă servicii şi echipamente ce se implementează mai degrabă la nivel mondial decât naţional. Utilizatorii tradiţionali de spectru radio ce furnizează serviciile publice la nivel naţional sunt acum în competiţie pentru folosirea spectrului radio, prin creşterea numărului jucătorilor comerciali globali, în special în aria de telecomunicaţii şi de radiofuziune[8].

Disponibilitatea spectrului radio reiese ca urmare a soluţiilor găsite în urma tratativelor comerciale. În consecinţă, problema spectrului de radiofrecvenţă a fost dezbătută ca un subiect de importanţă majoră în negocierile internaţionale privind liberalizarea pieţei telecomunicaţiilor.

Toate acestea subliniază necesitatea unei cooperări internaţionale în ceea ce priveşte politicile de spectru radio pentru a înlesni promovarea şi furnizarea la nivel internaţional de servicii şi echipamente. De aceea este necesar să se asigure că interesele Alianţei şi a statelor membre sunt luate în considerare când vine vorba de disponibilitatea spectrului radio. Într-un mediu cu o piaţă liberalizată de telecomunicaţii, evoluţiile controlate conduc la emergenţa jucătorilor mondiali - o sarcină suplimentară pentru managementul frecvenţelor in mediul militar. Tot mai adesea cooperarea şi alinierea NATO cu partenerii în domeniul managementului

[8]Mr. Eberhard, Trautmann, *Spectrum Management Branch*, Presentation to the CEPT/ECC Civil/Military Meeting 1999,Revised 2004.

spectrului de radiofercvenţă trebuie să fie recunoscute ca obiectiv de importanţă strategică.

Spectrul electromagnetic este definit ca un număr nelimitat de frecvenţe de energie electromagnetică transmisă şi cuprinde undele radio, radiaţiile infraroşii, radiaţiile ultraviolete, razele X, lumina vizibilă şi multe altele.Undele radio sunt definite ca fiind undele electromagnetice cu frecvenţe sub 3000 GHz cu benzi internaţionale definite.

Inventatorul italian Marconi a realizat prima transmisie fără fir (wireless) în urmă cu un secol în 1895, într-un spectru neutilizat „curat". De atunci dezvoltarea tehnologică a condus la nenumărate descoperiri şi noi utilizări ale spectrului. În zilele noastre, viaţa modernă este de neconceput fără serviciile numeroase care cer folosirea acestei părţi a spectrului[9].

Spectrul de frecvenţe radio - este o resursă naturală epuizabilă şi se alocă cu respectarea principiilor noninterferenţei şi al asigurării compatibilităţii lucrului mijloacelor radioelectronice. Este, totodată o resursă administrată de fiecare naţiune în parte şi nu ţine cont de graniţele naţionale. Din moment ce majoritatea spectrului util, în special undele radio, este supus congestiei şi interferenţei între utilizatori, încă de la începutul folosirii spectrului radio, s-a recunoscut nevoia de a administra frecvenţele pentru a evita interferenţele dintre utilizatori.

În general porţiuni ale spectrului şi în particular porţiunea frecvenţelor radio sunt neutilizabile. Porţiuni ale spectrului, datorită propagării sau a altor caracteristici fizice sunt teoretic nelimitate.

În prezent se pare că nu este nevoie de o coordonare internaţională a frecvenţelor pentru aceste porţiuni de spectru. Ca exemple sunt mijloacele infraroşii şi aplicaţiile laser pentru o vastă varietate de sisteme de arme. Nevoia de a administra frecvenţe s-a accentuat ca urmare a evoluţiei folosirii spectrului de frecvenţe radio din ultimii 100 de ani. De când tehnologia s-a dezvoltat şi a devenit profitabilă din punct e vedere comercial, cu alte cuvinte când oamenii au început să facă bani folosind tehnologia, spectrul a devenit din ce în ce mai utilizat determinând aglomerarea şi interferenţa utilizatorilor.

Spectrul de radiofrecvenţă este o resursă naturală cu limite actuale. Nu putem divide la infinit fără ca frecvenţele alocate să nu se suprapună sau să interfereze şi în acelaşi timp nu putem continua urcând sau coborând în spectru pentru un spaţiu de frecvenţe adiţional.

Scopul managementului frecvenţei, indiferent de nivelul la care se exercită, naţional sau internaţional, este de a reglementa şi standardiza cât mai mult folosirea spectrului de frecvenţe şi de a

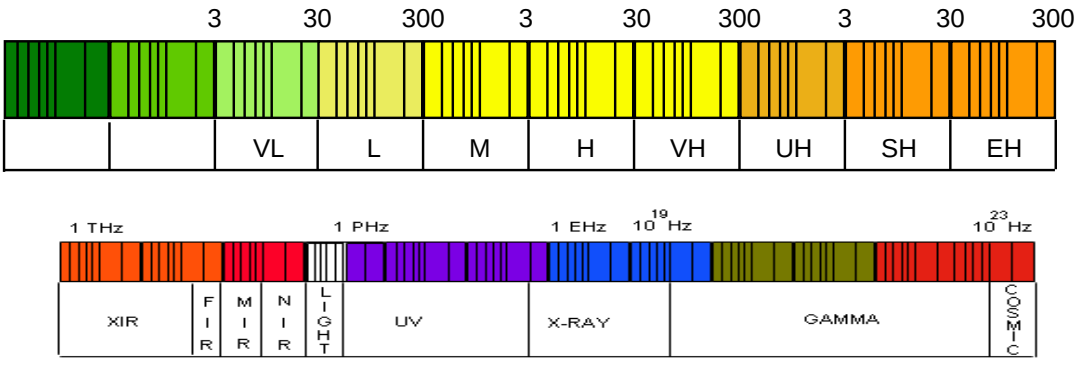
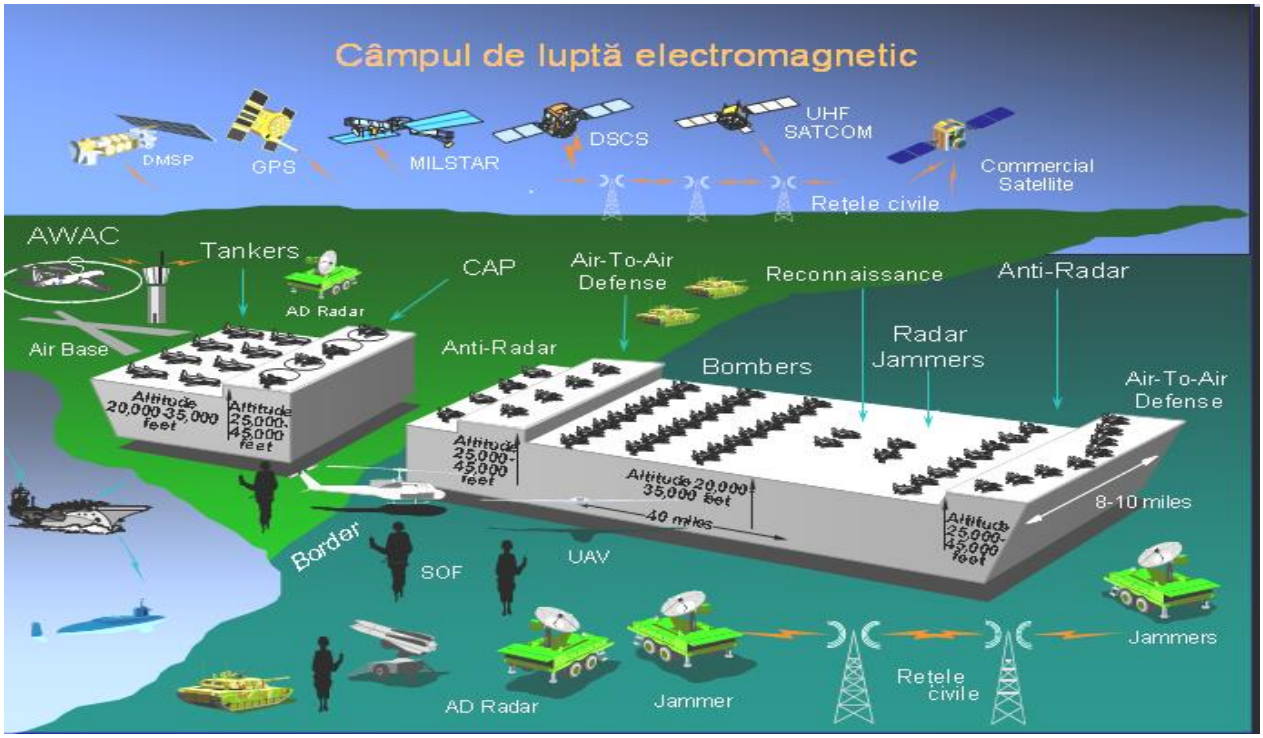


Figura 1: *Spectrul de radiofrecvenţă*

[9] AC/322-D (2006)0020, *NATO CONSULTATION, COMMAND & CONTROL BOARD (NC3B)*, 28 Apr 2006.

furniza mijloace de a coordona folosirea planificată a spectrului ceea ce nu va determina interferenţa cu alţi utilizatori. Un alt scop este de a rezolva problema interferării frecvenţelor atunci când ea apare. De când undele de radiofrecvenţă definite de I.T.U (International Telecommunication Union cu locaţia la Geneva, Elveţia), au ca limită superioară valoarea de 3000 de GHz, spectrul de radiofrecvenţă este o parte a spectrului electromagnetic care include lumina, razele x şi razele cosmice emise de corpurile cereşti în tot universul[10].

în mod firesc la o creştere majoră a cererilor de frecvenţă în sectorul civil. Din acest motiv, asigurarea eficienţei accesului militar la spectrul de radiofrecvenţă este o provocare care a crescut şi care are nevoie de un acord la cel mai înalt nivel diplomatic NATO, Consiliul Atlantic de Nord (NAC). Pentru motive operaţionale, necesităţile de spectru militar sunt extrem de variate şi importante (radare, telecomunicaţii, mijloace ajutătoare de navigaţie, rachete etc.). De aceea situaţia este foarte tensionată tratând alocarea spectrului ca o resursă. În ultimele două decenii s-au constituit



Expresia "managementul spectrului electromagnetic pe câmpul de luptă" se referă la gestionarea resurselor spectrului electromagnetic pentru sprijinirea cerinţelor de telecomunicaţii (inclusiv ale sistemelor de armă) şi de război electronic.

În ultimele două decenii, tehnologia s-a dezvoltat rapid şi a determinat o diversitate de servicii accesibile utilizatorilor. Succesul unor aplicaţii (telefonia mobilă, dispozitive de putere joasă, mijloace digitale, etc.) conduc

nenumărate organisme cu responsabilităţi la nivel naţional şi internaţional atât în domeniul civil cât şi cel militar.

În cadrul managementului internaţional al frecvenţelor radio militare, cel mai reprezentativ este ACP-190. Acesta este unul din principalele documente NATO de reglementare a activităţii în acest domeniu , fiind un ghid pentru managementul frecvenţelor radio pe timp de pace, în situaţii de criză sau la război.

Ghidul ACP-190 are un dublu scop. În primul rând, documentul este destinat informării comandanţilor de la structurile operaţionale ale NATO asupra rolului

[10] The NATO frequency management handbook (2006).

managementului spectrului radio, asigurându-le acestora informaţiile necesare desfăşurării activităţii.

Al doilea scop al acestui document este de a asigura instrucţiunile, directivele şi informaţiile tehnice planificatorilor militari şi managerilor de frecvenţe din cadrul ţărilor care îşi desfăşoară activitatea în structuri angajate în planificarea, coordonarea şi managementul spectrului în operaţii militare. Acest ghid este destinat optimizării utilizării spectrului electromagnetic disponibil de către forţele proprii în sprijinul asigurării superiorităţii informaţionale.

Politicile de planificare a frecvenţelor cu impact asupra operaţiilor sunt descrise în Manualul NATO pentru managementul frecvenţelor (NATO FM Handbook), manual editat de FMSC. Acest document (ACP-190) se află, de asemenea, în responsabilitatea FMSC, care are destinat un grup de lucru ce se ocupă de revizuirea/actualizarea şi îmbunătăţirea periodică a conţinutului acestui document.

Pentru a înţelege pe deplin termenii utilizaţi, este important de reţinut că în contextul NATO termenul C3 reprezintă CONSULTARE, COMANDĂ şi CONTROL (şi nu comandă, control, comunicaţii). Acest lucru este esenţial, deoarece consultarea între statele membre NATO trebuie să aibă întotdeauna loc înainte de exercitarea comenzii şi controlului în sprijinul procesului decizional. Totuşi, în cadrul comunităţii de management al spectrului, locul cel mai important lucru îl reprezintă COORDONAREA. SMO trebuie să se coordoneze cu autorităţile corespunzătoare din domeniu, în scopul obţinerii frecvenţelor necesare pentru a fi utilizate de ţara membră NATO respectivă sau de structura militară pe care o reprezintă[11].

SMO este denumirea generică a structurii care asigură managementul spectrului radio. Prin SMO, conform ACP-190, se înţelege "personalul, procedurile şi activitatea organizaţiilor responsabile cu managementul spectrului radio în cadrul NATO". Atunci când o forţă militară este dislocată în teatrul de operaţii aceste organizaţii care asigură managementul frecvenţelor radio pot fi întâlnite sub diferite denumiri, în funcţie de nivelul la care îşi desfăşoară activitatea.

[11] AC/322(SC/3)WP/38, 26 Aug 2002.

INSTRUIREA ASISTATĂ DE CALCULATOR

Locotenent Dorin-Horia ILIEŞ
Centrul 54 comunicaţii R.M.N.C.

O direcţie importantă de acţiune, pentru realizarea militarului secolului XXI (luptătorului modern), o reprezintă modernizarea instrucţiei, vizând atât conducerea cât şi desfăşurarea propriu-zisă a acesteia.

Concomitent cu stabilirea orientărilor strategice în instruirea forţelor, trebuie să se urmărească asigurarea valorificării tuturor resurselor şi posibilităţilor existente pentru adaptarea cu rapiditate a instrucţiei la cerinţele impuse de realizarea interoperabilităţii cu structurile similare din armatele moderne, iar managerii structurilor să deţină toate atributele şi să dispună de toate pârghiile necesare desfăşurării procesului de instrucţie pentru racordarea acestuia la principiul obţinerii calităţii în instruirea forţelor, în conformitate cu evoluţiile previzibile ale luptei armate.

În domeniul instruirii forţelor trebuie avută în vedere realizarea unui înalt nivel de perfecţionare acţională prin specializare şi pregătire temeinică. În prezent s-a trecut deja la pregătirea profesionistă, în baze de instrucţie centralizată, care presupune organizarea şi conducerea acesteia de către instructori strict specializaţi, pe bază de norme, principii, metode profesioniste şi standarde de performanţă.

Instrucţia trebuie să se execute în condiţii cât mai apropiate de solicitările câmpului de luptă modern, atât pentru tipurile clasice de conflict armat şi acţiuni militare, cât şi pentru acţiunile asimetrice de orice natură la care structurile militare pot fi chemate să facă dovada pregătirii şi capacităţii combative.

Proiectarea şi desfăşurarea propriu-zisă a instrucţiei profesionalizată impune organizarea acesteia pe tipuri de activităţi, în formă modular-secvenţională. Prin strategia de instruire, se va urmări, de asemenea, valorificarea eficientă a timpului avut la dispoziţie şi programarea formării luptătorului în raport cu etapele temporare de parcurs.

Efortul pentru formarea militarului modern este complex şi trebuie făcut atât în domeniul formării cadrelor la nivele ierarhice mici, adică al comandantului de grupă şi pluton, cât şi în domeniul pregătirii (instruirii) luptătorului. În acest sens, calculatorul şi tehnologiile asimilate acestuia trebuie considerate ca mijloace didactice (integrate în predarea diferitelor discipline) cu rol important în îmbunătăţirea calităţii instruirii şi ameliorarea procesului instructiv-educativ.

Conceptul educaţional şi contextul de instruire a fost transformat de la încorporarea noilor tehnologii informaţionale şi de comunicare nu numai în domeniul instrucţiei, ci şi în toate activităţile cotidiene. Societatea informaţională este mai mult decât o simplă revoluţie. Reţeaua telematică, multimedia, realitatea virtuală sunt noile decoruri în care acţionează oamenii.

Utilizarea calculatorului în procesul de instrucţie devine o necesitate în condiţiile dezvoltării accelerate a tehnologiei informaţiei. Pentru noile generaţii de militari, deja obişnuiţi cu avalanşa de informaţii multimedia, conceptul de asistare a procesului de instrucţie cu calculatorul este o cerinţă intrinsecă. A intrat deja în obişnuinţa zilnică utilizarea calculatorului pentru comunicare, informare, instruire.

Aplicaţiile informaticii în domeniul educaţional, utilizând ca mijloc tehnic de predare-învăţare calculatorul electronic, se reunesc sub titulatura: „instruire asistată de calculator”. Prin aceasta se înţelege utilizarea calculatorului ca instrument de organizare a mediului de instruire dirijat de către instructor.

Conceptul de asistare a procesului de instruire cu calculatorul include: predarea unor lecţii de comunicare de cunoştinţe, aplicarea, consolidarea, sistematizarea noilor cunoştinţe, verificarea automată a unei activităţi sau a unui grup de activităţi.

Numită de unii ca „inovaţia tehnologică cea mai importantă a pedagogiei moderne", instruirea asistată de calculator contribuie la eficienţa instruirii, este un rezultat al introducerii treptate a informatizării în instruire.

Interacţiunea militar-calculator permite diversificarea strategiei didactice, facilitând accesul militarului la informaţii mai ample, mai logic organizate, structurate variat, prezentate în modalităţi diferite de vizualizare.

O precizare consider că trebuie făcută: nu calculatorul în sine ca obiect fizic, înglobând chiar configuraţie multimedia, produce efecte pedagogice imediate, ci calitatea programelor create şi vehiculate corespunzător, a produselor informatice, integrate după criterii de eficienţă metodică în activităţile de instruire.

Armata trebuie să ţină pasul cu tehnologia, să înţeleagă şi să anticipeze impactul asupra modului de instruire. În armatele moderne calculatoarele au fost încorporate în programele de instruire oferindu-le celor ce se instruiesc o libertate şi flexibilitate mai mare, dar şi individualitate în sala de specialitate.

Utilizarea computerului, ca mijloc în predarea categoriilor de pregătire, duce la dezvoltarea capacităţii de a gândi critic, permiţând militarilor să se manifeste spontan, fără îngrădire ori de câte ori se creează o nouă situaţie de instruire. Satisfacţia noastră, a instructorilor, constă în a-i pune în evidenţă „talentul" de a realiza propria creaţie (algoritm de rezolvare a unei situaţii, de rezolvare a unei probleme). În cadrul acesta, militarul nu mai este un spectator, ca în instruirea tradiţională, ci „un începător în ştiinţă, un novice, dar activat după regulile cunoaşterii stiinţifice, dacă sunt adaptate specific, antrenate patru elemente: conţinutul, metodele, secvenţele şi contextul social"[1].

Având libertatea de a căuta, a alege şi folosi metodele cele mai adecvate, activitatea de instruire nu trebuie să aibă nimic cu şablonismul, cu schematismul, ea trebuie să aibă mereu un caracter creator.

Dacă vom şti să împletim în fiecare activitate de instruit în mod firesc tradiţionalul cu modernul, dacă vom reuşi sa-i facem pe militari să participe la propria instruire, dacă militarii pe care îi instruim vor şti să descopere anumite adevăruri, dovedeşte că metodele folosite de noi în procesul instructiv-educativ au fost cele mai potrivite, am ales calea cea mai bună.

[1] *„Metodele cognitive ale învăţării",* Prof. Univ. Dr. Elena Joiţa, Învăţământul nr. 4 /2003, pag. 9

CYBER AMENINŢĂRI LA ADRESA TELEFONIEI MOBILE BIOMETRIA ŞI SECURITATEA

Locotenent-colonel Iulian CIAUŞU
Locotenent Cornel ANTOCHE
Centrul 115 comunicaţii RMNC

Revoluţia în domeniul comunicaţiilor şi tehnologiilor informaţionale a dat naştere lumii virtuale. În viaţa reală depindem zi de zi de spaţiul cibernetic. Echipamentele electronice, calculatoarele, telefoanele mobile sunt adânc infiltrate în fiecare aspect al vieţii noastre sociale. Spaţiul cibernetic este real, prin urmare şi riscurile sunt reale.

Astăzi dispozitivele mobile avansate sunt bine intergrate în Internet şi au o funcţionalitate mult mai mare decât a telefoanelor mobile clasice. Ele sunt folosite în acelaşi mod ca şi calculatoarele personale, potenţial care le face susceptibile la ameninţări similare PC-urilor conectate la Internet.

Deoarece dispozitivele mobile pot conţine mari cantităţi de informaţii sensibile şi personale, acestea sunt ţinte atractive care oferă oportunităţi unice pentru cei ce intenţionează să le exploateze în folosul lor.

Pe măsură ce tehnologia dispozitivelor mobile evoluează, consumatorii o vor folosi la niveluri fără precedent. Tehnologia telefoanelor mobile a fost cea mai rapidă tehnologie adoptată în istorie, cu o valoare actuală estimată de peste 4,5 miliarde de utilizatori la nivel mondial.

Mai mult, progresele tehnologice au alimentat o capacitate de calcul portabil fără precedent, crescând dependenţa utilizatorilor pentru dispozitivele mobile şi pentru abonamentele de telefonie mobilă în bandă largă. Dispozitivele mobile au devenit o parte integrantă a societăţii şi pentru unii, un instrument esenţial. Cu toate acestea, design-ul complex şi funcţionalitatea sporită a acestor dispozitive introduce vulnerabilităţi suplimentare. Aceste vulnerabilităţi, împreună cu cota de piaţă în expansiune, face tehnologia mobilă o ţintă atractivă şi viabilă pentru cei interesaţi în exploatarea acesteia.

În trecut, activitatea maliţioasă având ca ţintă telefonia mobilă a fost relativ limitată în comparaţie cu cea a PC-urilor. Dispozitivele mobile actuale au o funcţionalitate mult mai mare şi arhitecturi mult mai accesibile, ducând la o creştere a activităţii malware împotriva lor. Acestea includ smartphone-uri Apple iPhone, Google Android, Blackberry, Symbian, dispozitivele bazate pe Windows Mobile ş.a.

Datorită funcţionalităţii similare între dispozitivele mobile şi Pc-uri, distincţia între cele două a devenit neclară. Dispozitivele mobile au devenit la fel de sensibile la cyber-ameninţări şi vor fi probabil afectate de multe din ameninţările care există pe Internet pentru PC-uri.Varietatea de informaţii sensibile disponibile pe un dispozitiv mobil prezintă, de asemenea, un potenţial mai mare şi mai ispititor decât cea a unui telefon mobil tradiţional sau a unui computer.

Utilizatorii vor profita de portabilitatea şi comoditatea dispozitivelor mobile pentru activităţi bancare, e-mail, accesul în reţelele sociale, menţinerea de contacte şi calendare. Caracteristicile dispozitivelor mobile introduc tipuri suplimentare de informaţii, care de obicei nu

sunt disponibile la un PC, cum ar fi informaţiile legate de sistemul de poziţionare globală (GPS), funcţionalitate şi mesagerie text.

O multitudine de ameninţări există pentru dispozitivele mobile, iar lista va continua să crească mai ales în sfera ingineriei sociale, exploatarea reţelelor de socializare, mobile botnets, exploatarea aplicaţiilor mobile şi de comerţ electronic.

Actori rău intenţionaţi au creeat şi utilizat malware orientat spre dispozitivele mobile. Numărul total de malware a crescut semnificativ după 2004, cu lansarea publică a code-ului sursă Cabir. Cabir este un vierme bluetooth şi primul răspândit pe scară largă pentru dispozitivele mobile. Rulează pe telefoane mobile care folosesc platforma Symbian şi se răspândeşte în rândul dispozitivelor compatibile bluetooth care sunt descoperite. Viermele provoacă telefonul să încerce permanent o conexiune bluetooth ducând la descărcarea bateriei.

Un alt exemplu recent şi mai abject de malware mobil este Ikee.B, vierme iPhone creat cu motivaţie financiară. Caută informaţii financiare sensibile stocate pe dispozitivele iPhone şi încearcă să comande iPhone-ul infectat prin intermediul unui server botnet. De exemplu un iPhone victimă în România poate fi accesat de la un alt iPhone situat în Asustralia şi forţat să extragă date la comanda unui server botnet din Rusia.

FlexiSpy este un spyware comercial vândut cu 349 dolari şi oferă capacităţi ca:

- monitorizează apelurile, citeşte SMS-urile, jurnalele de apel şi e-mailurile,
- identifică localiţia GPS a telefonului
- ascultă convorbirile din împrejurimile telefonului
- controlează toate funcţiile telefonului prin SMS.

FlexiSpy pretinde că este creeat pentru a ajuta şi proteja copiii şi familiile, dar implicaţiile acestui tip de software sunt mult mai mari. Imaginaţi-vă un străin care ascultă fiecare conversaţie, vizualizează fiecare SMS şi e-mail trimis şi primit sau ne urmăreşte fiecare mişcare fără ştirea noastră.

Una din cele mai comune metode de răspândire a malware este prin ingineria socială. Exploatarea acestui segment este extrem de profitabilă şi probabil va creşte semnificativ în piaţa de telefonie mobilă.

Site-urile de reţele sociale, cum ar fi Facebook, Twitter sau hi5, au devenit piloni în schimbul de mesaje electronice. Informaţiile schimbate apar adesea ca fiind de încredere iar utilizatorii acceptă mesaje de la utilizatori necunoscuţi. Deoarece în reţelele mobile URELE-ul este redus la 17 caractere utilizatorul nu poate cunoaşte destinaţia link-ului fără a face clik pe el. URL-urile legitime sunt imposibil de distins de cele care sunt rău intenţionate. Această tactică ar putea atrage o victimă care, în necunoştinţă de cauză, să descarce un malware sau să viziteze un site fraudulos.

Peste 70% din utilizatorii de smartphone accesează reţele sociale folosind un browser mobil, făcând ca reţelele sociale să devină un loc natural „dulce” pentru actori rău intenţionaţi.

M-comerţul (comerţul electronic prin telefonia mobilă) este o altă ameninţare la adresa dispozitivelor mobile. Consumatorii pot utiliza dispozitivele mobile din orice locaţie pentru a obţine informaţii despre produse, pentru a compara preţurile, pentru a face achiziţii sau pentru a comunica cu diverşi clienţi. Smarphone-urile pot fi folosite pentru furtul de informaţii despre card, furturi de informaţii bancare sau comerciale.

Ce puteţi face pentru a va proteja telefoanele mobile şi PDA împotriva atacurilor?

- **Urmaţi orientările generale pentru protejarea dispozitivelor portabile**. Luaţi măsuri de precauţie pentru asigurarea dispozitivelor mobile în acelaşi mod în care ar trebui să le luaţi pentru un computer.
- **Fii atent la postarea numărului tău de telefon şi adresei e-mail**. Atacatorii folosesc adesea software care citesc adresele de e-mail. Aceste adrese pot deveni ţinte pentru atacuri şi spam. Prin limitarea numărului de persoane care au acces la informaţiile dumneavoastră limitaţi riscurile de a deveni o victimă.
- **Nu urmaţi link-urile trimise în mesaje e-mail sau text**. Fiţi suspicioşi cu URL-urile nesolicitate.
- **Fiţi prudenţi la descărcarea de software.** Există multe site-uri care oferă jocuri sau aplicaţii ce se pot descărca gratis pe telefonul mobil. Acest soft ar putea include un cod maliţios. Evitaţi descărcarea fişierelor de site-uri în care nu aveţi încredere. Dacă se descarcă un fişier de pe un site web, luaţi în considerare salvarea în calculator şi scanarea manuală de viruşi înainte de al utiliza.
- **Evaluaţi setările de securitate.** Asiguraţi-vă că profitaţi de caracteristicile de securitate oferite de dispozitivul mobil. Atacatorii pot profita de conexiuni bluetooth sau wireless pentru a accesa sau descărca informaţii. Dezactivaţi bluetooth şi wireless-ul când nu le folosiţi pentru a evita accesul neautorizat.

Ce puteţi face pentru a vă proteja datele?

- **Utilizaţi parole.** În procesul de obţinere a informaţiilor de pe dispozitivele portabile aţi întâlnit, probabil mai multe solicitări pentru parole. Profitaţi de această oportunitate. Nu alegeţi opţiuni care să permită memorarea parolelor, nu alegeţi parole care se pot ghici cu uşurinţă, utilizaţi parole diferite pentru diferite programe şi profitaţi de metodele suplimentare de autentificare.
- **Luaţi în considerare stocarea separată a datelor importante**. Există multe forme de medii de stocare a informaţiilor (CD, DVD, flash), pe care se pot salva datele de pe dispozitivele mobile.
- **Criptarea fişierelor.** Prin criptarea fişierelor vă asiguraţi că persoane neautorizate nu pot viziualiza datele chiar dacă acestea au acces fizic la dispozitivul mobil.
- **Instalaţi şi actualizaţi periodic antivirusul.**
- **Instalaţi şi menţineţi un firewall.**

Este esenţial să se înţeleagă că un dispozitiv mobil nu mai este doar un telefon şi nu poate fi tratat ca atare. Spre deosebire de generaţia anterioară de telefoane mobile dispozitivele mobile moderne sunt similare cu PC-urile şi supuse aceloraşi ameninţări.

Imaginaţi-vă că sunteţi James Bond şi trebuie să intraţi într-un laborator secret pentru a dezarma o armă mortală biologică şi de a salva lumea. Dar mai întâi, trebuie să treceţi de sistemul de securitate. Este nevoie de mai mult decât o cheie sau o parolă - trebuie să aveţi structura irisului lui, vocea lui şi forma mâinii lui pentru a intra.

S-ar putea întâlni, de asemenea, acest scenariu, mai puţin arma mortală biologică, în decursul unei zile normale la locul de muncă. Aeroporturi, spitale, hoteluri, magazine alimentare şi chiar parcuri

tematice precum Disney care utilizează din ce în ce mai mut **biometria** - "constă în metode de recunoaştere a unui individ bazate pe una sau mai multe trăsături **fizice** sau **comportamentale**. În informatică, în special, biometria este folosită ca *o formă de gestionare a identităţii* şi *de control al accesului*. De asemenea, este utilizată pentru a identifica persoane în grupuri, care sunt sub supraveghere "- pentru mai multă siguranţă.

În fiecare zi luaţi măsuri de precauţie, folosiţi o cheie pentru a intra în propria casa şi log on pe computer cu un nume de utilizator şi parola. Probabil aţi experimentat, de asemenea, panica care vine când încurcaţi cheia sau uitaţi parola. Nu e o problemă doar că nu poţi obţine ceea ce aveţi nevoie, dar dacă vă pierdeţi cheile sau bucata de hârtie pe care aveţi notate parolele, atunci altcineva le poate găsi şi să le folosească ca şi cum aţi fi dumneavoastră.

În loc să folosiţi ceva ce aveţi (o cheie) sau ceva ce ştiţi (cum ar fi o parolă), elementele biometrice integrate folosesc **trăsăturile dumneavoastră** pentru a vă identifica. Elementele biometrice integrate pot folosi **caracteristicile fizice**, cum ar fi faţa dumneavoastră, amprentele digitale, irişi sau structura venelor precum şi **caracteristici comportamentale** ca vocea dumneavoastră, modul de scriere de mână sau ritmul dactilografierii. Spre deosebire de chei şi parole, trăsăturile personale sunt extrem de dificil de a fi pierdute sau uitate. Ele sunt, de asemenea, foarte dificil de copiat. Din acest motiv, mulţi oameni le consideră ca fiind mult mai sigure decât cheile sau parolele.

Sistemele biometrice pot părea complicate, dar ele folosesc aceleaşi etape:

• **Înregistrarea**: Prima dată când utilizaţi un sistem biometric, acesta înregistrează informaţiile de bază despre dumneavoastră, cum ar fi numele dumneavoastră sau un număr de identificare. Elementele biometrice surprind apoi o imagine cu toate trăsăturile dumneavoastră specifice.

• **Depozitarea**: Contrar a ceea ce puteţi vedea în filme, cele mai multe sisteme nu au stocată imaginea completă a înregistrării dumneavoastră. Ele analizează în schimb trăsăturile dumneavoastră şi le traduce într-un cod sau un grafic. Unele sisteme, înregistrează aceste date pe un card inteligent pe care îl aveţi mereu la dumneavoastră.

• **Compararea**: data viitoare când utilizaţi sistemul, acesta compară trasatura dumneavoastră şi vă prezintă informaţii cu privire la dosar. Apoi, fie acceptă sau respinge că sunteţi cine pretindeţi a fi.

Sistemele folosesc, de asemenea, aceleaşi trei componente:

- Un **senzor** care detectează caracteristicile fiind utilizat pentru identificare
- Un **computer** care citeşte şi stochează informaţiile
- **Software-ul** care analizează caracteristicile, le traduce într-un grafic sau cod şi efectuează comparaţii în timp real.

1.1. Scrisul de mână

La prima vedere, utilizarea scrierii de mână pentru a identifica persoanele nu ar părea o idee bună. La urma urmei, mulţi oameni pot învăţa să copie scrisul altor

oameni cu un pic de timp şi practică. Se pare că ar fi uşor pentru cineva să obţină o copie a semnăturii cuiva sau parola necesară şi să le înveţe.

Dar sistemele biometrice nu se uită doar la modul în care arată fiecare formă a

literei; ele analizează actul de a scrie în sine. Acestea examinează presiunea care este utilizată, viteza şi ritmul cu care scrieţi. Ele înregistrează, de asemenea, secvenţial modul în care scrieţi literele, cum ar fi dacă adăugaţi puncte sau cruci după ce aţi terminat cuvântul.

Spre deosebire de formele simple de litere, aceste trăsături sunt foarte dificil de a fi create. Chiar daca cineva are o copie a semnăturii dumneavoastră, sistemul, probabil, nu ar accepta-o.

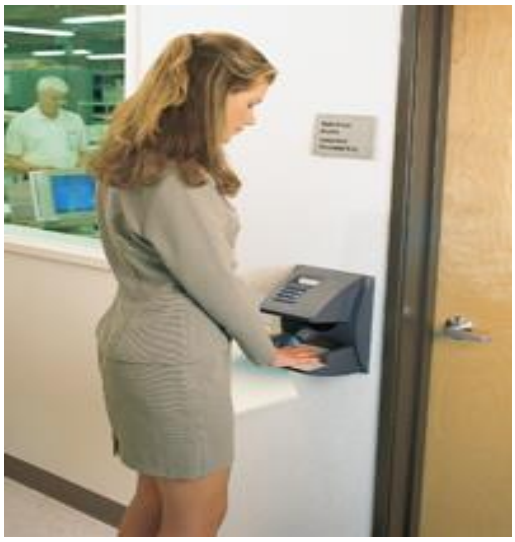
Senzorii unui sistem de recunoaştere a scrierii de mână poate include o suprafaţă de scriere sensibilă la atingere sau un stilou care conţine senzori care detectează unghiul, presiunea si direcţia. Software-ul traduce scrisul de mână într-un grafic şi recunoaşte micile modificări în scrisul unei persoane de la o zi la alta şi de-a lungul timpului.

1.2 Geometria mâinii şi a degetelor

Mâinile oamenilor şi degetele sunt unice, dar nu la fel de unice ca alte caracteristici, cum ar fi amprentele digitale sau irişii. De aceea, întreprinderile şi şcolile, folosesc de obicei geometria mâinilor şi a degetelor pentru **autentificarea** utilizatorilor, pentru a le **identifica** identitatea. Parcurile tematice ca Disney, de exemplu, utilizează geometria degetelor pentru a acorda bilete la diferite părţi ale parcului. Unele companii utilizează cititoare de mână în loc de fişele de pontaj.

Sistemele care măsoară geometria mâinii şi a degetelor folosesc un aparat de fotografiat digital şi lumina. Pentru a o utiliza, vă plasaţi pur şi simplu mâna pe o suprafaţă plană, aliniind degetele pentru a asigura o citire destul de precisă. Apoi, un aparat de fotografiat are una sau mai multe poze cu mâna şi-i aruncă umbra. Se utilizează aceste informaţii pentru a determina lungimea, lăţimea, grosimea şi curbura mânii sau degetele. Aceste informaţii se vor traduce într-un şablon numeric.

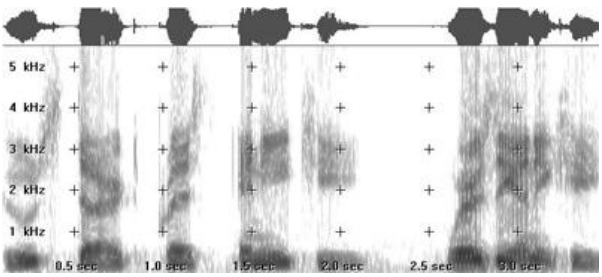
Geometria mâinii şi a degetelor au puncte forte şi puncte slabe. Deoarece mâinile şi degetele sunt mai distinctive decât amprentele digitale sau irişii, unii oameni simt mai puţin că sistemul le invadează intimitatea lor. Cu toate acestea, mâinile multor oameni se modifică în timp din cauza unor accidentări, modificări în greutate sau artrita. Unele sisteme se actualizează zilnic pentru a reflecta modificările minore de la o zi la alta.



1.3 Amprenta vocală

Pentru o mai mare securitate, sistemele biometrice utilizează mult mai multe caracteristici unice, cum ar fi vocile. Vocea dumneavoastră este unică din cauza formei cavităţii vocale şi modul în care vă deplasaţi gura când vorbiţi. Pentru a utiliza un sistem de amprentă vocală, trebuie să rostiţi exact cuvintele sau frazele pe care le cere software-ul, sau vă dă un eşantion extins de discurs, astfel încât computerul să poată identifica, cuvintele pe care le rostiţi.

Când oamenii se gândesc la amprente vocale, ei cred că tiparul vocii ar fi un osciloscop. Dar datele folosite într-o amprentă vocală este **spectrograma**, nu o formă de val. O spectrogramă este de fapt un grafic care prezintă un sunet de frecvenţă pe axa verticală şi timpul pe axa orizontală. Sunetele diferite creează forme diferite în grafic. Spectrogramele sunt folosite, de asemenea, colorate sau în nuanţe de gri pentru a reprezenta calităţile acustice ale sunetului.



Unele companii folosesc recunoaşterea amprentei vocale, astfel încât oamenii să poată avea acces la informaţii sau să dea autorizaţie fără a fi prezenţi fizic. În loc de geometria degetelor, a mâinii sau de un scanator de retină, cineva poate da autorizaţie de efectuarea a unui ordin printr-un simplu apel telefonic. Din păcate, oamenii pot ocoli unele sisteme, în special cele care funcţionează prin telefon, cu o simplă înregistrare a parolei unei persoane autorizate. Acesta e motivul pentru care unele sisteme folosesc mai multe parole aleator alese în loc de anumite cuvinte. Altele folosesc tehnologia care detectează artefacte create la înregistrare şi redare.

1.4. IRIS SCANNING

Scanarea irisului poate părea futurist, dar în inima sistemului este un simplu aparat de fotografiat digital CCD. Se foloseşte atât lumina vizibilă cât şi infraroşu pentru a face o imagine mai clară, cu un contrast ridicat al irisului unei persoane. Cu lumina infraroşu, irisul unei persoane devine foarte negru şi este mai uşor pentru computer să izoleze pupila de iris.

Când te uiţi într-un dispozitiv de scanare a irisului, camera focalizează automat sau va folosi o oglindă sau stimuli sonori de la sistem pentru a vă asigura că sunteţi poziţionat corect. De obicei, ochiul este de 10 centimetri şi la o distanţă de un metru faţă de aparatul de fotografiat. Când aparatul foto are o imagine, computerul localizează:

- Centrul pupilei
- Marginea pupilei
- Marginea irisului
- Pleoapele şi genele

Se analizează apoi modele de iris care sunt traduse într-un cod.

Influenţa tehnologiei biometrice asupra societăţii, potenţialele riscuri la viaţa privată şi ameninţările la adresa identităţii, vor solicita medierea prin intermediul legislaţiei. Examinarea atentă a importanţei datelor biometrice, precum şi modul în care acestea ar trebui protejate de lege, trebuie sa se facă acum la o scară mai largă.

PROVOCĂRI ŞI INSTRUCŢIE

Căpitan Gabriel IANCU
Batalionul instrucţie comunicaţii şi informatică „Fraţii Buzeşti”

În Batalionul instrucţie comunicaţii şi informatică „Fraţii Buzeşti”, soldaţii şi gradaţii voluntari se instruiesc în cadrul următoarelor module de pregătire şi cursuri:

1. Modulul instruirii individuale;
2. Modulul perfecţionării instruirii de specialitate;
3. Curs avansat de instruire pentru gradaţi voluntari;
4. Curs de specializare în arma comunicaţii şi informatică pentru soldaţii de alte arme;
5. Curs de rezervişti voluntari care nu au îndeplinit stagiul militar.

Standardizarea instrucţiei, conturarea clară a conceptelor, obiectivelor şi standardelor specifice modelelor luptătorului şi specialistului au făcut din pregătirea soldaţilor şi gradaţilor voluntari în arma comunicaţii şi informatică un proces definit, continuu, flexibil şi suplu ceea ce conduce către concluzia că provocările specifice noilor conflicte nu ne este străină.

Experienţa consistentă în instrucţia individului şi grupei/echipajului, lecţiile învăţate, metodele noi şi de actualitate implementate în instruire, pregătirea instructorilor, baza materială avută la dispoziţie, funcţie de cursurile urmate de către soldaţi/gradaţi voluntari, au facilitat structurii posibilitatea de a fi suplă şi flexibilă, centrată pe misiune, deschisă noilor provocări şi conectată la noile realităţi ale spaţiului luptei.

Cifrele de şcolarizare din 2010-2011, normale şi fireşti, în concordanţă cu numărul de instructori, au adus structurii o capacitate maximă de dozare a eforturilor educat-educator astfel încât putem afirma că soldatul/gradatul voluntar instruit astăzi deţine pregătirea necesară îndeplinirii cu succes a funcţiilor pe care le va încadra.

Împlinirea în anul 2010 a 30 de ani de la înfiinţare a adus Batalionul Instrucţie Comunicaţii şi Informatică „Fraţii Buzeşti” la pragul maturităţii. Examenele de foc concretizate în atâtea şi-atâtea promoţii de soldaţi/gradaţi, rezultatele remarcabile avute de-a lungul timpului, constatările comisiilor de control, au adus structurii sentimentul lucrului bine făcut şi personalului propriu încredere şi mândrie.

Munca cu omul, insuflarea dorinţei de a fi cel mai bun, formarea deprinderilor, formarea competenţelor de luptător, specialist, uneori educator, conducător de microstructuri, închegarea şi formarea competenţei de cetăţean responsabil, formarea deprinderilor necesare pregătirii şi conducerii activităţilor instructiv-educative, menţinerea capacităţilor de rezistenţă la efort fizic şi psihic prelungit, creşterea încrederii în forţele proprii şi formarea spiritului de echipă şi de autodisciplină,

cultivarea spiritului de luptător şi a virtuţilor militare, a abilităţilor militarului de a acţiona eficient în situaţii critice sunt numai câteva din activităţile noastre cotidiene desfăşurate cu energie şi sudoare.

Anul 2011 ne-a adus o nouă provocare - primul *Curs de specializare în arma comunicaţii şi informatică* destinat militarilor de alte arme. Acesta a debutat în martie cu un plan de pregătire punctual, bazat pe formarea şi dezvoltarea deprinderilor în lucrul cu mijloacele de comunicaţii şi informatică moderne. În cadrul acestui curs metodele de instruire s-au îmbunătăţit permanent punându-ne în posibilitatea nu numai de-a forma deprinderi ci şi de a le perfecţiona, având la dispoziţie un fond bun datorat pregătirii anterioare a soldaţilor şi actelor pe care aceştia le-au demonstrat: voinţă şi conştiinţă. Trecând de la metodele de învăţământ de comunicare (explicaţia, descrierea, prelegerea, instructajul, etc.), cele de explorare (observaţia, demonstraţia etc.), cele de acţiune (exerciţii, jocul de rol, etc.), am implementat şi câteva metode de raţionalizare cum ar fi instruirea asistată de calculator.

Drumul de la „ştiu" la „vreau să ştiu" şi până la „am învăţat" a fost extrem de laborios, iar tehnicile de predare/ învăţare/instruire sunt perfecţionate prin dezvoltarea acestor capacităţi ţinând cont atât de gradul de instruire anterioară al soldaţilor voluntari cât şi de vârsta acestora. Din practică, un individ cu vârsta între 18-26 ani, cu un grad de instruire mediu, provenit dintr-o societate unde sursa principală de informare/educare nu mai este biblioteca ci internetul, este foarte atras de mijloacele de instruire simulativ-intuitive. Instruirea programată, asistată de calculator, trebuie să devină realitate, fiindcă ea poate ajuta individul mult mai uşor în capacitatea acestuia de analiză şi sinteză.

După principiul „o imagine face cât o mie de cuvinte" instrucţia în *Batalionul Instrucţie Comunicaţii şi Informatică „Fraţii Buzeşti"* , în anul 2011, are la bază deopotrivă, atât un pronunţat caracter practic-aplicativ cât şi *imaginea*.

Şi sigur nu vom greşi!

ASPECTE DE NOUTATE ÎN STATUTUL CADRELOR MILITARE DIN MINISTERUL APĂRĂRII NAŢIONALE

Colonel drd. Silviu PREDA
Comandamentul comunicaţiilor şi informaticii

La data de 29 aprilie 2011 a intrat în vigoare Legea nr. 53/2011 pentru modificarea şi completarea Legii nr. 80/1995 privind statutul cadrelor militare. În acest sens, prezint în continuare cele mai importante reglementări aduse de noul act normativ, statutului cadrelor militare din Ministerul Apărării Naţionale. Aşadar, noul act normativ introduce *obligativitatea cadrelor militare în activitate de a participa la misiuni în afara teritoriului statului român,* reglementare care vizează în mod special cadrele militare care fac parte din structurile desemnate să participe la astfel de misiuni, în sensul că până acum acestea puteau refuza participarea, chiar şi comandant de pluton fiind, la un pluton care pleaca în teatrul de operaţii din afara teritoriului naţional. Totodată, noul act normativ reglementează faptul că acele cadre militare în activitate care participă la misiuni în afara teritoriului statului român nu pot fi trecute în rezervă ca urmare a prezentării demisiei pe timpul executării misiunii.

O nouă reglementare este *dreptul la concedii fără plată,* care poate fi acordat în următoarele condiţii:

a) atunci când cadrele militare doresc să-şi însoţească soţia sau soţul trimis în străinătate pentru a reprezenta interesele statului român, pentru o perioadă mai mare de 6 luni sau ele însuşi au fost selecţionate pentru a încadra posturi de expert cu statut de angajat temporar în structurile organizaţiilor internaţionale din care România face parte, situaţii în care durata concediului poate fi de cel mult 4 ani, cu posibilitatea prelungirii acestuia cu cel mult un an de către ministrul apărării naţionale;

b) pentru alte cazuri, temeinic motivate, ca de exemplu: însoţirea în străinătate a unui membru de familie care necesită a fi operat sau tratat de o anume afecţiune, precum şi altele, durata concediului poate fi de cel mult un an, cu posibilitatea prelungirii acestuia cu cel mult un an de către ministrul apărării naţionale.

În perioada concediului fără plată, cadrele militare sunt suspendate din funcţie şi nu beneficiază din partea Ministerului Apărării Naţionale de niciun drept, cu excepţia celui de folosire a locuinţei de serviciu, dacă dispun de aceasta la data solicitării concediului. Totodată, la încetarea concediului fără plată, Ministerul Apărării Naţionale are obligaţia de a numi cadrul militar pe o funcţie vacantă s-au să-l pună la dispoziţie în vederea încadrării, ceea ce înseamnă că funcţia în care va fi numit pote fi sub nivelul celei deţinute înaintea suspendării.

Revenirea la *înaintările în grad înainte de termen sau în mod excepţional* este, de asemenea, o reglementare de noutate pentru statutul cadrelor militare din Ministerul Apărării Naţionale. Aşadar, conform Legeii nr. 53/2011 cadrele militare din armată, pe parcursul întregii cariere militare, de la gradul de sergent până la cel de colonel, pot beneficia fie de două înaintări în grad înainte de termen sau de două înaintări în grad la excepţional, fie de o înaintare în grad înainte de termen şi una la excepţional. Prin aceste noi reglementări nu înseamnă că toate cadrele militare din armată, beneficiază în mod obligatoriu de acest drept. Asemenea înaintări în grad sunt de fapt excepţii de la regulă, care în opinia mea, ar trebui publicate, în mod obigatoriu, în Buletinul Informativ al Armatei spre informarea întregului personal al armatei, ca exemple, şi care va trebui, tot în opinia mea, să aibă la bază fie rezultate profesionale de excepţie, fie fapte de eroism.

Un alt aspect de noutate este cel al *modificării limitelor de vârstă în grad* până la care cadrele militare pot fi menţinute în activitate, limite care potrivit prevederilor noului act normativ au devenit egale cu vârstele standard de pensionare stipulate în Legea nr. 263/2010 privind sistemul unitar de pensii publice. Ca urmare, limitele de vârstă în grad pentru cadrele

militare născute înainte de 01 ianuarie 1970 sunt raportate la anul şi luna naşterii fiecărei persoane şi sunt prevăzute în anexa nr. 6 din Legea nr. 263/2010, cu excepţia generalilor, a căror limită de vârstă în grad este de 60 de ani, iar pentru cadrele militare născute după 01 ianuarie 1970 limita de vârstă în grad este de 60 de ani indiferent de grad. Totodată, noul act normativ reglementează faptul că acele cadre militare născute înainte de 01 ianuarie 1970 pot solicita, prin raport personal înaintat ierarhic spre aprobare ministrului apărării naţionale, anual până la împlinirea vârstei de 60 de ani, menţinerea în activitate peste limita vârstei standard de pensionare prevăzută de Legea nr. 263/2010.

Alte noi reglementări introduse de Legea nr. 53/2011 în statutul cadrelor militare din Ministerul Apărării Naţionale vizează trecerea în rezervă sau direct în retragere a acestora în cazul *neavizării în vederea acordării autorizaţiei de acces la informaţii clasificate sau certificatului de securitate, la retragerea acestor documente sau atunci când acestea nu mai sunt revalidate*, din motive imputabile lor, precum şi în cazul în care acestea sunt puse la dispoziţie ca urmare a *limitării nivelului de acces la informaţii clasificate* iar până la expirarea perioadei legale de punere la dispoziţie nu s-a identificat o funcţie corespunzătoare gradului deţinut cu o prevedere de acces la informaţii clasificate înscrisă în fişa postului, la nivelul acordat după limitare. De asemenea, tot ca o noutate, cadrele militare în activitate *condamnate prin hotărâre judecătorească rămasă definitivă la pedeapsa închisorii cu executarea acesteia* se trec în rezervă sau direct în retragere din oficiu. În situaţia *condamnării pentru infracţiuni săvârşite cu intenţie la pedeapsa amenzii penale sau cu închisoare, cu suspendarea executării ori graţiere înainte de începerea executării pedepsei*, cadrele militare în activitate aflate în această situaţie pot fi trecute în rezervă sau direct în retragere ori menţinute în activitate, pe baza propunerilor înaintate ierarhic comandanţilor/şefilor care au competenţe în acest sens, mai concret pentru ofiţeri competenţa aparţine ministrului apărării naţionale iar pentru maiştrii militari şi subofiţerii din Comandamentul Comunicaţiilor şi Informaticii şi unităţile militare subordonate competenţa aparţine comandantului comandamentului.

Printre noile modificări aduse statutul cadrelor militare din Ministerul Apărării Naţionale se numără şi *eliminarea punerii la dispoziţie a cadrelor militare în activitate în cazul cercetării penale pentru fapte care nu au legătură cu exercitarea atribuţiilor funcţiilor în care sunt încadrat*e. De asemenea, Legea nr. 53/2011 elimină obligativitatea încadrării cadrelor militare în activitate din Ministerul Apărării Naţionale în fucţii cu grade egale celor deţinute, acestea putând fi numite în funcţii prevăzute în statele de organizare cu grad superior celui pe care îl au.

Ultimul aspect de noutate pe care doresc să-l prezint în acest articol şi pe care îl consider foarte important pentru corpul maiştrilor militari şi subofiţerlor este dreptul acestora de a purta uniforma militară după trecerea în rezervă sau direct în retragere. Obţinerea acestui drept este condiţionată de o vechime în serviciu militar de cel puţin 20 de ani şi de rezultatele obţinute în activitatea desfăşurată. Totodată, pot obţine acest drept, chiar dacă nu au o vechime în serviciu militar de 20 de ani, acele cadre militare care au adus patriei servicii deosebite.

EVOLUŢIA COMUNICAŢIILOR MOBILE

Căpitan Ovidiu DOBOŞ
Centrul 115 comunicaţii RMNC

Evoluţia comunicaţiilor mobile se confundă, în mare măsură cu evoluţia radiocomunicaţiilor. Astfel, transmisiile de mesaje între nave şi uscat sau între nave reprezentau o practică obişnuită chiar şi înaintea primului razboi mondial. Legăturile mobile terestre apar între cele două războaie mondiale ca, de exemplu comunicaţiile mobile ale poliţiei din Detroit (1921) în banda de 2 MHz şi sistemul de comunicaţie mobil din New York (1932). După cel de al doilea razboi mondial şi pâna la apariţia sistemelor mobile celulare, se pot cita câteva realizări importante ca sistemul B (Germania 1971), sistemul Loran (destinat navigaţiei maritime, cu începere din 1958), sistemul Shinkansen (Japonia 1964, pentru trenul de mare viteză), sistemul IMTS (SUA, 1969) şi altele. Totuşi, dezvoltarea intensa a comunicaţiilor mobile se realizează doar după apariţia circuitelor integrate şi miniaturizarea realizată în domeniul componentelor, deci după crearea condiţiilor de miniaturizare a echipamentelor şi după realizarea unor surse de alimentare fiabile si cu dimensiuni relativ reduse. Pentru realizarea unor reţele de dimensiuni mari, cu mulţi utilizatori, având la dispoziţie o bandă de frecvenţe limitată, s-a trecut la folosirea acoperirii celulare.

Sistemele celulare de comunicaţii mobile celulare au fost dezvoltate, pâna în prezent, în trei generaţii distincte:

- Generatia 1 (1G), destinată să ofere un singur serviciu, cel vocal, cuprinde sisteme ca NMT, AMPS, TACS etc. şi a apărut cu începere din 1980. Erau sisteme cu prelucrarea analogică a semnalului, funcţionând în benzile de 450 MHz sau de 800-900 MHz.În prezent sistemele de generaţia 1 sunt la finalul „carierei”, fiind scoase din exploatare în multe dintre ţările în care au funcţionat.
- Generatia 2 (2G), a fost iniţial destinată să ofere servicii vocale, având în acelaşi timp şi o capacitate limitată pentru serviciile de transmisii de date, cu viteză relativ redusă. Sunt sisteme cu prelucrare digitală a semnalului, cu funcţionare în benzile de 900 MHz şi 1800 MHz. Ca exemple de astfel de sisteme sunt GSM, D-AMPS etc. Primele sisteme GSM au fost introduse în exploatare în 1991. Sistemele 2G sunt în prezent la „apogeul” dezvoltării lor. În evolutia 2G se pot pune în evidenţă trei faze de dezvoltare: 1, 2 si 2+. În faza 2+, GSM oferă posibilitatea sporirii vitezei de transmisie a datelor prin introducerea unor procedee speciale ca HSCSD şi GPRS. Astfel, prin folosirea transmisiei cu pachete de date, prin procedeul GPRS, viteza de transmisie a datelor poate fi de pâna la 172 kbit/s (prin comparaţie cu viteza de 14,4 kbit/s oferită în faza 1 de dezvoltare). Devine astfel posibilă realizarea unor transmisii de tip multimedia.
- Generatia 3 (3G) oferă viteze de transmisie sporită, de pâna la 2 Mbit/s (în unele variante pâna la 8 Mbit/s) şi prezintă posibilităţti multiple pentru servicii multimedia de calitate şi pentru operare în medii diferite. Sunt sisteme cu prelucrarea digitală a semnalului, ce funcţionează în banda de 2 GHz. Exemple de asemenea sisteme sunt WCDMA şi TD/CDMA, ambele în varianta europeană pentru interfaţa UTRA, WCDMA în varianta japoneză, CDMA2000 (S.U.A) etc. La nivel mondial, 3G este desemnat şi ca IMT-2000. iar varianta dezvoltată în Europa este denumită UMTS. Introducerea în exploatarea a primelor sisteme 3G a fost realizată în 2001-2002, fiind deci la începutul evoluţiei. La baza dezvoltării 3G se află sistemele 2G. Astfel, GSM în variantele 2 si 2+ vor fi treptat integrate în 3G, dezvoltarea UTRA fiind realizată tocmai pornind de la interfaţa GSM.

Între diferitele sisteme 3G se încearcă, în prezent, realizarea unei compatibilităţi cât mai bune.

Sintetic, evoluţia tehnică în concepţia sistemelor celulare pâna în prezent, este expusă în fig. 1. iar cea în timp în fig. 2

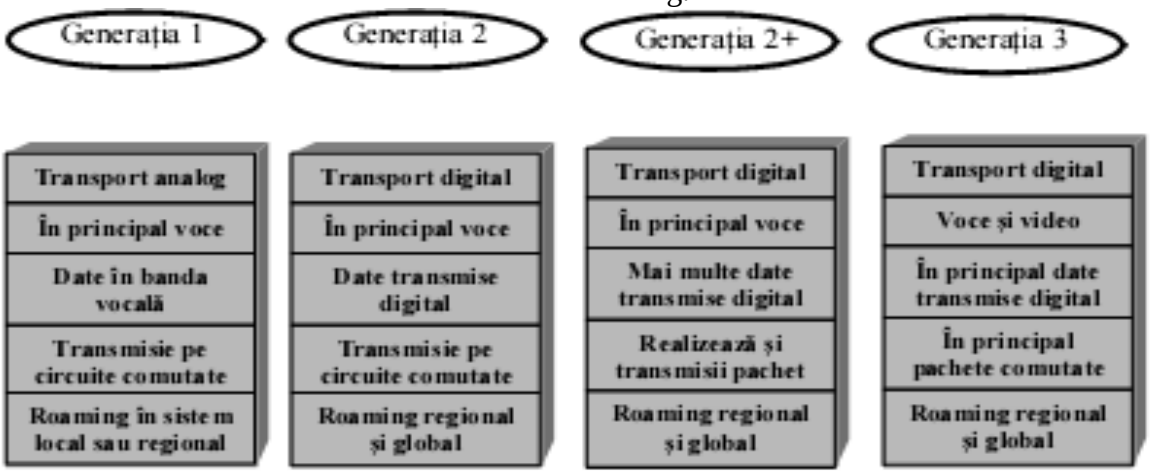


Fig. 1 Evoluţia sistemelor de comunicaţii mobile celulare

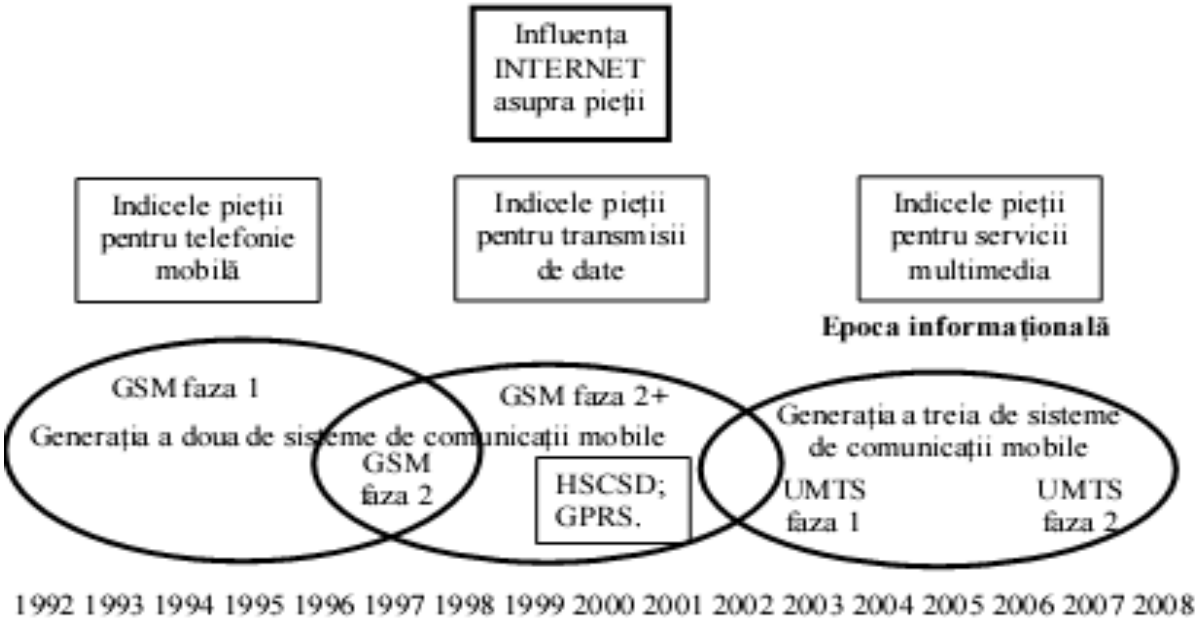


Fig.2 Evoluţia sistemelor de comunicaţii mobile

În prezent, pe lângă preocupările pentru introducerea sistemelor 3G în funcţiune, au început lucrări experimentale pentru o nouă generaţie de sisteme de comunicaţii mobile digitale, 4G, pentru care se prevede realizarea unor viteze de transmisie de utilizator de până la 100 Mbit/s. Caracteristica principală a 4G va fi reprezentată de controlul exercitat de utilizator asupra serviciilor, pe care le va gestiona în funcţie de pachetul de servicii la care s-a abonat. Deci utilizatorul va avea libertatea de a selecta serviciul dorit, cu un indice de calitate dorit, la un preţ acceptabil, oriunde si oricând.

CERINŢE MINIME DE CALIFICARE REFERITOARE LA CAPACITATEA TEHNICĂ = PRODUSUL MUNCII COLECTIVE A SPECIALISTULUI TEHNIC ŞI SPECIALISTULUI ÎN ACHIZIŢII

Locotenent-colonel Marian ŢOPA
Comandamentul comunicaţiilor şi informaticii

După ce am stabilit ce, când şi cum dorin să achiziţionăm, evident se pune şi intrebarea: de la cine? Chiar dacă nu recunoaştem, se pune acestă întrebare mai ales de către beneficiarii achiziţiei. .

Punându-ne în situaţia beneficiarului şi încercând să gândim achiziţia ca şi cum s-ar face din banii proprii constatăm că atenţionările sunt foarte întemeiate . Ca achizitor care utilizez fonduri publice trebuie să aplic legislaţia în vigoare şi aici aş face trimitere in special la principiile enumerate la art. 2 din OuG34/2006, cu modificările şi completările ulterioare(nediscriminarea,tratamentulegal,recunoaşterea reciprocă,transparenţa, proporţionalitatea,eficienţa utilizării fondurilor publice,asumarea răspunderii).

Prezentăm în cele ce urmează o varianta optimă între a filtra ofertanţii astfel încât să asigurbeneficiarului garanţia unui contract fără probleme cauzate de furnizor/prestator/executant şi restricţionarea nejustificată a participanţilor la procedură.

Plecând de la modelul Fişei de date a achiziţiei încercăm să supunem analizei fiecare posibil criteriu de calificare.

1. In ceea ce priveşte **capacitatea economico-financiară** a ofertanţilor, există posibilitatea solicitării indeplinirii mai multor cerinţe de calificare.

   Una dintre ele se referă la o cifră medie de afaceri pe ultimii 3 ani de maxim dublu valoarea contractului suspus achiziţiei (a celui mai mare contract subsecvent în cazul unui acord cadru). În practică am observat foarte frecvent că se solicită depunerea de bilanţuri dar fără a se solicita ca din acestea să rezulte îndeplinirea vreunei cerinţe (cifră medie de afaceri peste o anumită valoare). Din discuţii cu unii colegi din domeniul achiziţiilor publice am înţeles că se solictă bilanţurile sau se pun condiţii pe cifra de afaceri din simplul motiv de a cere ceva. Am intâlnit remarci de genul „ e prea mare achiziţia ca să nu cerem ceva, măcar cifra de afaceri şi experienţă similară". În majoritatea cazurilor cerinţele referitoare la trecutul economico-financiar al operatorilor economici este irelevant având in vedere că atribuim un contract care se va desfăşura în viitor. Am observat că această idee este susţinută de mulţi colegi cu experienţă în domeniu şi trebuie să precizez că atunci când ne referim la trecutul economic-financiar nufacem referire la ofesionalismul şi seriozitatea operatorului economic in executarea contractelor (aceste aspecte reies din experienţa similară).

   Alte cerinţe referitoare la capacitatea economico-financiară a ofertanţilor sunt cele la solvabilitatea şi lichiditatea acestora. Pentru stabilirea acestori indicatori sunt necesare bilanţurile. La fel ca şi la cifra de afaceri, consider că în marea majoritate a achiziţiilor nu se justifică impunerea unor cerinţe referitoare la acesţi indicatori. Politica de investiţii a unui operator economic poate determine o lichiditate sau solvabilitate sub pragurile minime pentru calificare însă în realitate acel operator

economic este pe un trend de dezvoltare şi ulterior foarte probabil va avea o capacitate economică sporită. Astfel, nu se justifică cerinţe de calificare referitoare la aceşti indicatori economici. .Se impune concluzia că în general nu este relevant să impunem cerinţe minime de calificare pe partea economico-financiară. Impunerea acestor cerinţe nu ne asigură că vom selecta doar ofertanţi care dau garanţia beneficiarului că vor executa contractul în condiţii optime;

2. Dacă in majoritatea achiziţiilor nu este foarte relevant indeplinirea unor cerinţe de calificare referitoare la cifra de afaceri sau alţi indicatori economici, în ceea ce priveşte **capacitatea tehnică sau profesională** a ofertantului este necesar şi totodată relevant să stabilim unele plafoane in vederea calificarii (mai ales la contractele de servicii mai complexe sau de lucrări). Astfel, putem accepta doar ofertanţi de un anumit profesionalism şi de o anumită potenţa în a executa contractul, insă, aşa cum rezultă din cele prezentate în continuare, pentru stabilirea corectă a acestor cerinţe, este necesară o strânsă colaborare cu personalul beneficiarului achiziţiei specializat în omeniul din care face parte achiziţia.

O cerinţă privind capacitatea tehnică este cea referitoare la experienţa similară. Putem impune un cumul de contracte similare cu o valoare de maxim egală cu cea a contractului supusă analizei. Este de menţionat că dacă impunem cerinţă de calificare referitoare la experienţa similară neapărat trebuie să specificăm în documentaţie valoarea minimă a cumulului contractelor este necasara pentru a fi calificat ofertantul. Totodată aceste contracte trebuie însoţite de dovada executării lor în bune condiţii, iar în cazul în care beneficiarii sunt autorităţi contractante aşa cum acestea sunt definite de OuG34/2006, dovada consta în certificatul constator emis conform OuG 34/2006. cu modoficările şi completările ulterioare. Totodată este de menţionat că este discriminatoriu să impunem ca indeplinirea contractelor care atestă experienţa similară să fie către anumiţi beneficiari. Nici impunerea unui anumit numar de contracte nu este corectă. Singurul element corect constă în valoarea activităţilor de acelaşi gen cu cel din achiziţia în cauză efectuate de ofertant. Acest element ne dă o imagine asupra profesionalismului şi seriozităţii ofertantului în executarea contractelor, însă nu ne certifică capacitatea acestuia de a executa contractul care face obiectul achiziţiei respective.

Referitor la cerinţa privind dotările cu echipamente tehnice, etc. de care poate dispune operatorul economic pentru îndeplinirea contractului, apreciez că se poate marja foarte mult pe această cerinţă. Dacă ofertantul face dovada unei dotări corespunzătoare pentru executarea contractului atunci există o minimă garanţie privind reuşita achiziţiei. Este important de ştiut că trebuie să acceptăm orice fel de dovadă privind posibilitatea ofertantului de a utiliza echipamentele, soft-urile etc necesare (dotare proprie, leasing, inchiriere, susţinerea unui terţ etc). Nu putem impune anumite mărci de echipamente, tehnologii referitoare la dotări, putem solicita doar generic ceea ce are legătură directă cu îdeplinirea contractului suspus achiziţiei.

Pentru a califica ofertanţi care au capacitatea profesională de a executa contractul, în funcţie de specificul acestuia putem impune cerinţe minime privind personalul de specialitate. Nu se justifică să impunem cerinţe de calificare

privind personalul de conducere, administrativ al ofertantului. Fac această precizare deoarece pe SEAP se găsesc documentaţii prin care se cere ca ofertantul să aibă un anumit număr de directori sau managerul ofertantului să aibă o anumită specializare. Totodată trebuie avut în vedere faptul că ofertantul trebuie să facă dovada specializării persoanelor respective prin prezentarea de copii după diplome/certificate care atestă pregătirea persoanelor respective şi copii după documentele care atestă că intre persoanele respective şi ofertant există raporturi juridice (cărţi de muncă, contracte de colaborare, contracte de prestări servicii etc). Personal, consider că putem impune anumite condiţii privind experienţa personalului de specialitate doar in situaţiile în care pe parcursul evoluţiei în specialitatea respectivă se pot obţine anumite trepte/grade de specializare. În aceste cazuri putem impune anumite grade/trepte doar dacă acest lucru este relevant pentru execuţia contractului în cauză.

3. În principal pentru contractele de servicii sau de lucrări se pot impune cerinţe minime de calificare referitoare la **sistemul de management al calităţii sau al mediului** conform unor standarde ISO. După menţionarea fiecărui tip de standard se menţionează "sau echivalent" şi trebuie avut în vedere că în cazul sistemului de management al mediului trebuie acceptat orice dovadă a ofertanţilor care atestă implementarea unor astfel de standarde OuG 34 art. 191. În anumite tipuri de contracte indeplinirea acestor cerinţe poate da o imagine asupra ofertantului, trebuie avut învedere că sunt operatori economici care chiar dacă au un sistem de management al calitaţii sau al mediului nu au fost interesaţi de obţinerea unor certificări. Nu putem merge pe principiul dacă nu au certificări e problema lor privind obţinerea de contracte, deoarece chiar unii dintre cei mai buni operatori economici în domeniu lor de activitate nu au aceste certificări. Spre exemplu, la momentul scrierii acestui articol unul dintre cei mai mari operatori de servicii de telecomunicaţii din România nu are certificare privind implementarea unui sistem de management al mediului. Foarte important in cadrul unor contracte de servicii şi lucrări este să impunem cerinţe minime de calificare referitoare la autorizările specifice domeniilor respective. Această certificare este foarte importantă, deoarece pe langă faptul că este obligatorie, cel ce deţine acestă certificare indeplineşte anumite condiţii privind protecţia mediului şi privind sistemul calitaţii. Din aceste exemple se deduce că inainte de toate trebuie cunoscut bine domeniul serviciilor sau lucrarilor din care face parte contractul, care sunt certificările specifice acestui domneniu şi ce aspecte reglementează aceste certificări.

Subiectul cerinţelor minime de calificare poate fi mult mai amplu dezbătut, însă din succinta descriere de mai sus se poate deduce o concluzie:

Pentru a crea garanţia că necesitatea beneficiarului achiziţiei va fi satisfăcută corepunzător de ofertantul declarat căştigător, dacă pentru partea de livrare este decisivă descrierea din caietul de sarcini, pentru partea de servicii şi lucrări este foarte importantă calificarea ofertanţilor. În ambele situaţii trebuie impuse anumite cerinţe şi praguri dar fără a restricţiona în mod nejustificat participarea la procedura. Acest lucru se poate face doar printr-o muncă de echipă între personalul tehnic al beneficiarului şi achizitor a cărui rezultat să fie o armonizare între cerinţele tehnice asupra produsului, serviciilor, lucrării (prestatorului şi executantului) şi prevederile legale privind utilizarea eficientă a fondurilor publice.

CAPABILITĂŢI ACTUALE ALE SUBSISTEMULUI RADIO HF AL FORŢELOR NAVALE

Maior Tiberiu STOICA
Statul Major al Forţelor Navale

Având în vedere particularităţile şi limitările în domeniul asigurării comunicaţiilor pentru forţele navale, subsistemul radio şi, în particular cel în gama HF sunt de o importanţă deosebită.

Atenţia deosebită acordată acestui subsistem a fost reliefată permanent şi de volumul şi complexitatea testelor planificate în domeniul radio monocanal de către Forţele Navale în cadrul exerciţiilor CETATEA.

În acest context, cunoscând termenul de livrare al primelor hub-uri tactice RF-6010 TNAU achiziţionate de Forţele Navale, am solicitat în cadrul conferinţelor de planificare ale acestui exerciţiu, în anii 2005 şi 2006, autostaţii Falcon care ne-au fost puse la dispoziţie prin amabilitatea Statului Major al Forţelor Terestre. Experienţa acumulată şi abilităţile dobândite în planificarea infrastructurii, a reţelelor radio şi realizarea fişierelor de programare ne-au permis ca începând cu luna mai 2007, imediat după terminarea exerciţiului CETATEA (în cadrul căruia a fost testată viabilitatea infrastructurii proiectate) şi la numai 2 luni de la recepţionarea hub-urilor, reconfigurând toată tehnica implicată la nivelul categoriei de forţe să dăm în exploatare şi să menţinem în regim 24/7 până în prezent infrastructura detaliată în figurile alăturate, care asigură următoarele tipuri de servicii:

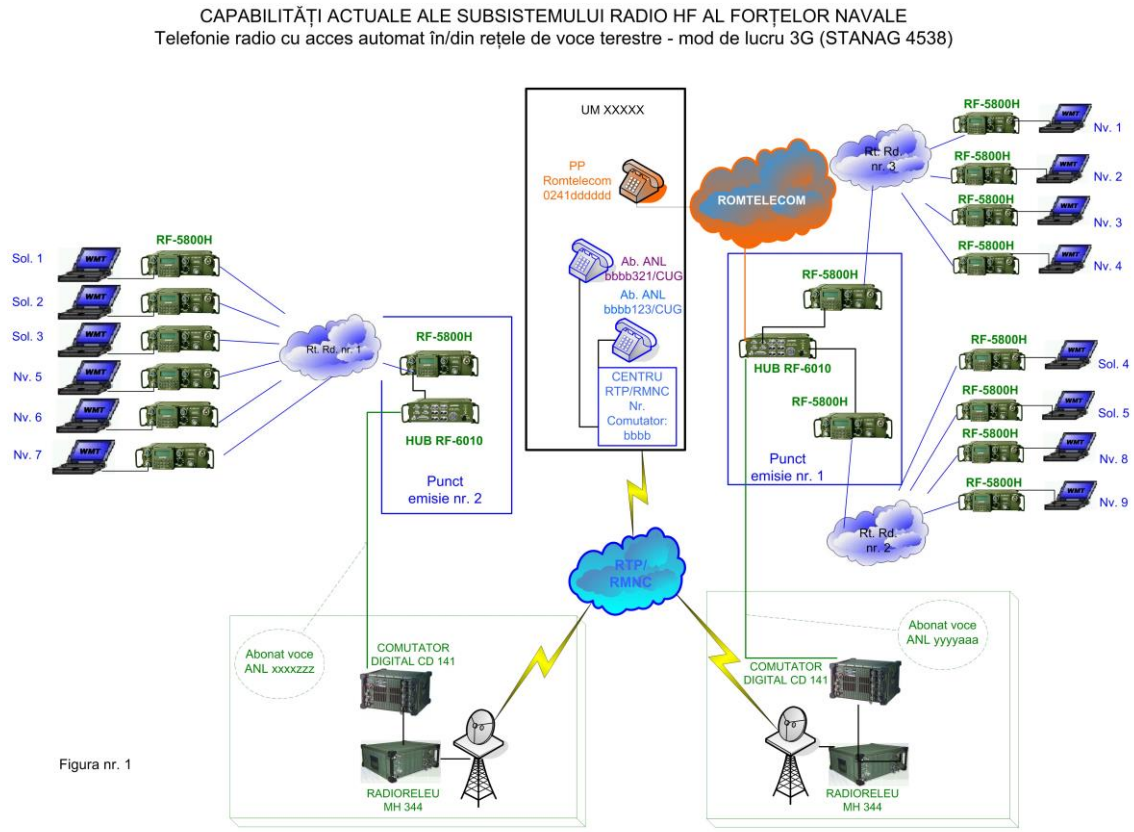


Figura nr. 1

Servicii de voce (figura nr. 1):

a) comunicaţii radio în gama HF, acoperite în timp real, între staţiile radio din reţelele configurate;

b) acces automat din/în reţele de telefonie terestre către/dinspre abonaţi radio HF staţionari sau mobili, cu acoperirea în timp real a comunicaţiilor radio.

Abonaţii de voce din grupul configurat în Reţeaua de Transmisiuni Permanentă/Reţeaua Militară Naţională de Comunicaţii (Closed User Group - CUG) pot efectua convorbiri cu corespondenţi radio şi viceversa, fără intervenţia vreunui operator. Prin interconectarea la hub şi a unei linii telefonice aparţinând operatorului ROMTELECOM, această facilitate este extinsă şi pentru apelurile dinspre/spre abonaţi ai reţelelor de telefonie. Definirea CUG rezolvă şi securizarea accesului la huburi numai pentru numerele de abonat solicitate prin cerinţele operaţionale.

Această capabilitate poate fi folosită, la nevoie, şi în situaţii de urgenţă, când volumul de încărcare al infrastructurii reţelelelor de telefonie terestră este prea mare sau acestea sunt indisponibile.

Menţionez că toate cele 8 linii de interconectare cu reţele de telefonie terestre sunt interoperabile cu comutatoarele digitale ale operatorilor existenţi, iar începând cu versiunea de firmware 4.0 pentru hub, corespondenţii radio pot selecta numărul liniei către care doresc să iniţieze apelul telefonic (la versiunile anterioare, selectarea liniei de către abonatul radio nu era posibilă iar hub-ul translata apelul telefonic dinspre abonatul radio, secvenţial pe liniile conectate, funcţie de disponibilitatea acestora, începând cu linia nr. 1).

O altă facilitate a hub-ului este funcţia de centrală telefonică pentru un număr de maxim 4 abonaţi telefonici locali; aceştia pot accesa şi ei oricare din vectorii radio conectaţi la hub. O soluţie tehnică interesantă identificată pentru rezolvarea unei cerinţe operaţionale reale este faptul că

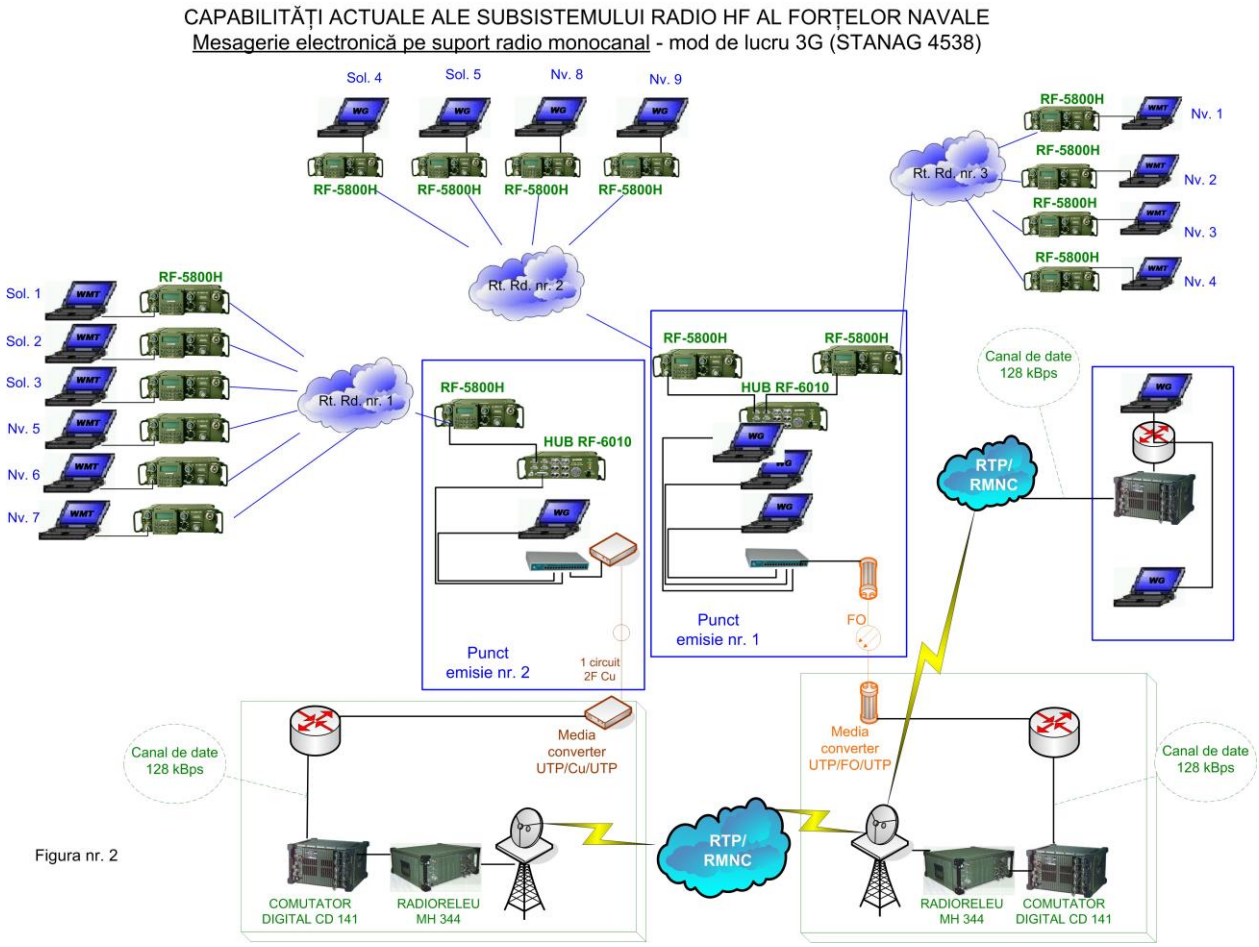


Figura nr. 2

prin combinarea facilităţilor de HOT LINE respectiv CENTRAL OFFICE ale comutatorului digital CD141 s-a reuşit

emularea unui abonat al hubului peste 2 comutatoare.

Servicii de transmiteri de date (figura nr. 2):

a) mesagerie electronică pe suportradiomonocanal HF, acoperită, întreterminalele de date locale ale staţiilor radio;

b) mesagerie electronică pe suportradiomonocanal HF, acoperită, pentreterminale de date distante, interconectate

cu staţiile radio prin canale de date configurate pe suport R.T.P./R.M.N.C.

Privind asigurarea acestui tip de serviciu, de remarcat este faptul că prin interconectarea celor 2 huburi existente în cele 2 puncte de emisie devine posibilă rutarea automată a mesajelor între corespondenţi din reţele „abonate" la huburi diferite.Capabilităţile hubului tactic RF-6010NW001, elementul cheie al infrastructurii care permite asigurarea capabilităţilor menţionate, sunt evidenţiate în figura nr. 3.

STAŢIA RADIO SOFTWARE – ELEMENT AL CÂMPULUI DE LUPTĂ DIGITAL

Locotenent ing. Marian UDROIU
Statul Major al Forţelor Aeriene

Asigurarea suportului informaţional pentru operaţiile multi-naţionale sau de coaliţie, compatibilizarea cu sistemele autorităţilor civile şi guvernamentale, reducerea efortului financiar şi logistic pentru realizarea comunicaţiilor între diferitele categorii de forţe armate, volumul şi viteza mari de transmitere a informaţiei sunt cerinţe care au determinat realizarea unui nou tip de sistem radio, în tehnologie digitală, configurabil atât la nivel hardware cât şi software, care să asigure un grad mare de interoperabilitate, flexibilitate şi adaptabilitate, garantându-se astfel răspunsul adecvat la toate cerinţele impuse de natura misiunilor pe câmpul de luptă, în prezent şi în viitor, eliminând astfel deficienţele staţiilor radio actuale.

Astfel apare, ca necesitate obiectivă pentru abordarea complet nouă şi unitară a problemei, **staţia radio software,** concept cunoscut şi sub denumirea de *staţie radio definită software* SDR(software defined radio). Aceasta trebuie să fie uşor de utilizat, să aibă redundanţă, determinând astfel siguranţa în funcţionare, cu un nivel ridicat de supravieţuire. Este o staţie multi-mod, multi-bandă, cu arhitectura deschisă, prevăzută cu interfeţe şi comenzi digitale, asigurând comunicaţii de voce, date şi video. Este reprogramabilă software, modulară atât hardware cât şi software, cu posibilităţi de criptare etc.. Se poate integra în reţele prin interfeţe şi protocoale standard, se adaptează unei mari varietăţi de medii de lucru şi tipuri de misiuni, putând asigura comunicaţii terestre, aeriene, navale şi satelitare, la viteze mari de transmisie.

Staţia radio software utilizează dispozitive digitale programabile pentru a emite şi recepţiona informaţii în banda de bază prin intermediul frecvenţelor radio. Dispozitivele ca procesoarele digitale de semnal(DSP) şi ariile logice programabile(FPGA) sunt configurate software pentru a oferi cerinţele mai sus menţionate prin funcţionalitatea procesării semnalului. Această tehnologie oferă o flexibilitate mai mare şi o potenţială durată de viaţă mai lungă, din moment ce staţia poate fi upgradată software, variantă ce impune un cost mult mai redus.

Figura 1. Staţia radio software HMS – staţie cu capabilităţi de interconectare la platforma reţea (Network-Centic) a sistemelor C4I2

Primul sistem radio software a fost iniţiat în proiectul **SPEAKeasy** al guvernului SUA. Proiectul şi-a propus dezvoltarea unor arhitecturi şi tehnologii care să răspundă cerinţelor viitoare ale armatei (servicii multimedia în reţea). A fost implementat în două faze şi a fost prima mare investiţie în domeniul militar cu scopul de a integra numeroasele tipuri de staţii radio într-o singură familie, cu capabilităţi multi-bandă, multi-mod, proiectată cu componente comerciale (COTS-commercial off-the-shelf), care putea lucra în domeniul de frecvenţe 2 MHz-2GHz (comunicaţii terestre, aeriene, maritime şi satelitare), cu performanţe excelente în mediile multi-cale, cu măsuri anti-bruiaj şi eliminare a interferenţelor. Prima fază a proiectului (1992-1995) a produs un radio sub forma de module ce se introduc pe magistrala VME(Versa Module Eurocad) a unei staţii de lucru SUN. Domeniul de frecvenţe radio foarte larg de la intrarea receptorului nu a putu fi prelucrat cu tehnologia existentă în acel moment şi a fost împărţit în trei game (2-30MHz, 30-400MHz, 400MHz-2GHz). Procesarea numerică a semnalelor a fost realizată cu un modul bazat pe procesorul TMS320C40 pe 16 biţi. Au fost implementate scheme de modulaţie de bandă îngustă şi largă, printre care şi saltul de frecvenţă. A doua fază a proiectului (1995-1999) a produs un sistem prevăzut cu magistrala PCI. Procesarea semnalelor a fost realizată cu DSP-uri şi, pentru prima oară în sistemele radio, FPGA-uri. Un microprocesor separat a fost utilizat pentru criptarea datelor.

Joint Tactical Radio System (JTRS) este programul DoD al SUA, început în 1999, fiind o continuare a proiectului SPEAKeasy. A fost iniţiat pentru a asigura interoperabilitatea între toate sistemele radio ale armatei americane pentru introducerea reprogramării software, validând suportul pentru utilizarea numeroaselor protocoale de comunicaţii existente. Ca o continuare a acestui proiect a fost dezvoltat un concept nou denumit SDR(Software Define Radio) care a reuşit să capteze atenţia atât a mediului civil, cât şi a celui militar, stimulând apariţia unor noi standarde care conduc industria de profil dincolo de generaţia a treia de sisteme de comunicaţii, având potenţialul necesar accesării următorului stadiu al tehnologiilor wireless.

În ideea promovării unei înţelegeri mai bune a tehnologiei SDR, au fost stabilite 5 niveluri care cuprind diferitele categorii de sisteme radio definite software.

Nivelul 0 descrie staţiile radio bazate pe tehnologii hardware şi în fapt nu este considerat un nivel din domeniul SDR. Cea mai simplă tehnologie SDR începe cu ***nivelul 1*** care cuprinde *staţiile radio controlate software* în care doar funcţiile de control sunt procesate software. Cel mai simplu exemplu de staţie care aparţine acestei categorii este telefonul celular dual mode care constă în două staţii radio hardware pentru două standarde diferite. Softul controlează doar care dintre cele două va fi utilizat. La acest nivel, upgradările ulterioare pentru un nou standard nu mai sunt posibile.

Nivelul 2 este reprezentat de *staţiile radio reconfigurabile software.* După cum se deduce şi din nume, aceste sisteme SDR realizează reconfigurări software prin controlul care se poate exercita asupra tehnicilor de modulaţie, funcţiilor de securitate (cum ar fi saltul în frecvenţă) şi cerinţelor formelor de undă, într-o gamă largă de frecvenţe. SDR din nivelul 2 includ module şi aplicaţii asociate de procesare, cum ar fi circuite integrate pentru aplicaţii specifice (ASIC), unităţi poartă de câmp programabil (Field-Programmable Gate Arrays – FPGA) şi procesoare de semnal digital (Digital Signal Processors – DSP). Deşi SDR reconfigurabile sunt sisteme utilizate în mod comun, în prezent, în special în aplicaţiile militare, datorită sofisticării rapide a tehnologiilor SDR, aceste sisteme tind să devină demodate. Un exemplu de sistem de nivel 2 îl reprezintă staţiile radio Harris din generaţia Falcon II.

Nivelul 3 de staţii definite software, denumit şi staţii software ideale (ideal

software radios – ISR), va fi probabil cel mai implementat tip de sistem radio în viitorul apropiat. Bazat pe extinderea posibilităţilor de programabilitate asupra întregului sistem, conversia analogică rămâne să fie realizată doar de antenă, microfon şi difuzoare. Componentele de heterodinare care servesc funcţiunilor de convertire a frecvenţelor radio în frecvenţe intermediare sunt de asemenea eliminate în staţiile radio software ideale, ca şi componentele pentru amplificarea analogică.

Nivelul 4, ultim, reprezintă însă doar o viziune despre SDR. Aceste staţii (USR – ultimate software radios) sunt definite doar în scopuri de realizare a comparaţiilor. În teorie, aceste staţii se presupune a fi capabile să suporte un domeniu extrem de larg de frecvenţe de lucru, aplicaţii şi tipuri de interfeţe cu mediul de transmisie, să permită comutări între diferitele formate de interfaţare cu mediul de transmisie şi diferitele aplicaţii în doar câteva milisecunde.

Schema bloc a unui radio software ideal este prezentată în fig. 1: circuite de intrare RF(Radio Frecvenţă), convertor analog-digital şi partea de procesare numerică a semnalelor. În această arhitectură simplă, limita analog/digital (hardware/software) este mutată foarte aproape de antenă.

Ideea fundamentală a unei staţii radio software este de a înlocui cât mai multe din dispozitivele hardware utilizate pentru anumite funcţii particulare ale staţiei, cu circuite numerice programabile de tip DSP şi FPGA.

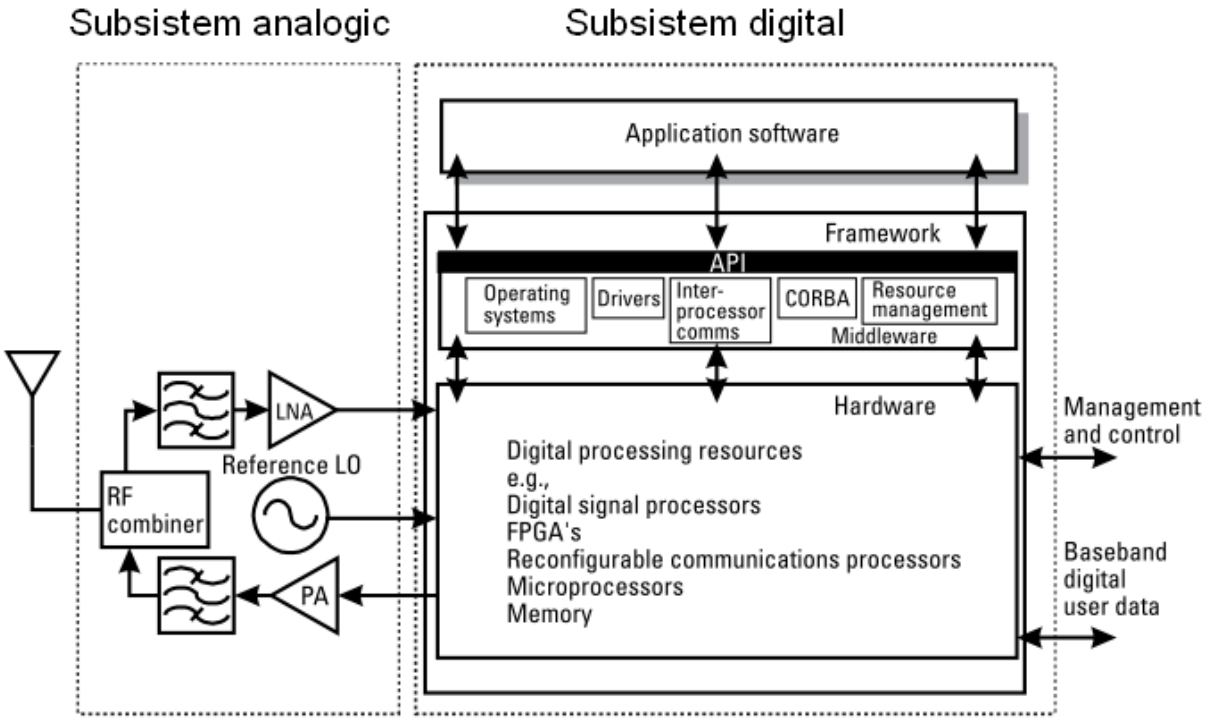


Fig. 1 Schema bloc receptor radio-software ideal

Dacă banda de frecvenţă a semnalului de radiofrecvenţă recepţionat este de câteva sute de MHz, cerinţele pentru CAD(Convertor Analog-Digital) şi DSP sunt foarte mari, iar convertoarele A/D şi procesoarele actuale nu pot satisface deocamdată aceste cerinţe.

O variantă apropiată de ce ideală (realizabilă practic) este cea a unui receptor **radio software pe frecvenţa intermediară (FI)**. Acesta constă dintr-o parte analogică pentru conversia semnalelor RF în domeniul IF(Intermediary Frequency), un CAD şi componente procesoare de semnal pentru prelucrarea semnalului de frecvenţă

intermediară. Tehnica numită sub-eşantionare poate fi utilizată pentru eşantionarea frecvenţei relativ înaltă din traseul intermediar, determinând utilizarea unor convertoare A/D de viteză mică.

M3TR (Multiband Multimode Tactical Radio) – R&S

M3TR asigură o flexibilitate maximă atât în ceea ce priveşte utilizarea benzilor de frecvenţă cât şi a celor mai diferite tipuri de semnale, pentru practic orice tip de misiune, categorie de forţe armate sau varianta de ambarcare.

Multi-bandă

Se acoperă benzile:

- HF: 1,5 – 30MHz pentru legăturile la mare distanţă (operative sau strategice)
- VHF-FM: 30 – 88MHz (extensie 108MHz) pentru legăturile tactice ale forţelor terestre
- VHF: 118 – 137MHz pentru legăturile sol-aer cu aviaţia civilă
- UHF: 225 – 400MHz pentru legăturile sol-aer cu aviaţia militară

Benzi continue:

- HF/VHF-FM: 1,5 – 108MHz (staţia MR3000H)
- VHF-FM/VHF/UHF: 25 – 512MHz (staţia MR3000U)

(ambele staţii cu extindere de bandă în viitor)

Existenţa benzii continue permite legături cu sisteme radio celulare civile şi militare, legături cu reţele de radio-telefoane şi legături prin satelit (GPS, UHF-DAMA).

Multi-mod

Staţiile R&S operează cu o multitudine de moduri, asigurând legături la cele mai diverse eşaloane şi interoperabilitatea cu alte reţele de comunicaţii. Permite transmisia simultană date/voce pe acelaşi canal. Are capabilităţi COMSEC prin criptarea informaţiei (voce/date) şi TRANSEC prin salt de frecvenţă şi ALE.

a) Forme de undă militare:

- ECCM: SECOM, SECOS, SATURN, HQ, STANAG 4444;
- Deschisă pentru implementarea altor metode ECCM (la cerere);
- ALE: MIL-STD-188-141, ALIS.

b) Forme de undă clasice:

- AM, FM, SSB, FSK, etc.

c) Transmisii de date de mare viteză:

- 5,4 Kb/s pentru HF;
- 64Kb/s pentru VHF/UHF;
- Deschisă pentru viitoare extinderi.

d) Securitatea informaţiei:

- COMSEC intern;
- Compatibilă cu modulele externe standard COMSEC.

e) Voce digitizată

- 16Kb/s CVSD (Continously Variable Slope Delta Modulation);
- 2400b/s – 16Kb/s – Vocoder adaptabil la modul de lucru şi bandă.

Multi-rol (Multi-misiune)

Staţiile se pot utiliza la nivel tactic (pluton, companie) şi nivel operativ-strategic (în centrele de comandă şi control).

a) operare ca terminal în reţeaua radio proprie:

- CNR (Combat Net Radio);
- PRN (Packet Radio Network);
- SCRA (Single Channel Radio Acces).

b) operare ca staţie de retranslaţie:

- REN (Range Extension Node)

c) operare ca nod de acces în reţelele fixe de comunicaţii (ISDN/PSTN/LAN):

- RAP (Radio Acces Point)

d) operare ca nod de acces în reţelele de trunking:

- TETRA – interoperabilitate cu reţelele civile şi guvernamentale;
- Alte reţele de radio-telefonie mobilă.

e) operare ca staţie de legătură prin satelit:

- GPS;
- UHF-DAMA, SATCOM.

f) operare ca Gateway/Interfaţă:

- către WAN/LAN;

- între reţele HF/VHF/UHF;
- EUROCOM.

BIBLIOGRAFIE

1. C. Bălan, „Receptoare radio cu prelucrare digitală a semnalelor”, Academia Tehnică Militară, Bucureşti 2003;
2. Paul Burns, „Software defined radio for 3G”, Artech House, Boston 2002;
3. C. Bălan, „Studii avansate pentru dezvoltarea sistemelor de comunicaţii militare”, Editura Academiei Tehnice Militare, Bucureşti 2005.

SUPORTUL PLATFORMELOR DE COMUNICAŢII DE TIP „FORCE XXI BATTLE COMMAND BRIGADE AND BELOW” PENTRU ÎMBUNĂTĂŢIREA SPRIJINULUI LOGISTIC INTEGRAT

Colonel dr.ing. Alexandru ALEXANDROAIA
Locotenent Benedictos IORGA
Comandamentul logistic întrunit

Realitatea conflictelor militare din prezent cat şi dezvoltarea exponenţială a tehnicii militare, cu preponderenţă a celei de comunicaţii, ne demonstrează faptul că, indiferent de tipologia acţiunii de luptă, reţeta succesului este generată de trei factori esenţiali:

1. calitatea operaţională a forţelor;
2. sprijinul logistic;
3. sprijinul de comunicaţii.

Analizând în ansamblu realitatea din teatrele de operaţii la care România a participat şi participă în mod activ, observăm că aceşti 3 factori sunt într-o relaţie de interdependenţă, generându-se reciproc. Acest articol îşi propune să analizeze raportul existent între sprijinul de comunicaţii şi suportul logistic, prin prisma utilizării sistemelor de comandă control de tipul FBCB2 cu care sunt echipate maşinile de luptă tip MRAP (Mine Resistant Ambush Protected) intrate în utilizarea forţelor româneşti dislocate în T.O. Afganistan.

Denumirea **FBCB2** provine de a abrevierea denumirii în limba engleză a sistemului de monitorizare a forţelor proprii (Blue Force Tracking) utilizat de către armata americană în cadrul tuturor acţiunilor militare la care este parte - **„Force XXI Battle Command Brigade and Below”.** Sistemele B.F.T. ce utilizează platforma FBCB2 se regăsesc pe aproape orice tip de vehicul destinat acţiunilor militare, indiferent că vorbim de maşină blindată destinată transportului de materiale şi echipamente (autocamioane, autocisterne etc.), elicoptere (de luptă, de transport, de tip MEDEVAC etc.) sau autospeciale şi maşini blindate de luptă. Eficacitatea sistemului este desigur relevantă şi fără echivoc având în vedere faptul că la nivel global vorbim de aproximativ 5 milioane de utilizatori ce populează platforma FBCB2.

Sistemul a plecat de la ideea asigurării unei nevoi de comunicare permanentă, bazată pe necesitatea comandanţilor de a urmări permanent forţele ostile concomitent cu acţiunile forţelor proprii şi aliate la nivelul unei singure platforme software. În acest sens s-a dorit conştientizarea permanentă de către factorii

decidenţi a situaţiei de pe câmpul de luptă, sub toate aspectele, prin colectarea şi actualizarea informaţiilor în timp real pe baza raportărilor cu privire la locaţia şi starea tuturor vehiculelor şi a personalului implicat în acţiunea militară, concomitent cu oferirea posibilităţii tuturor tipurilor de interogări şi schimburi reciproce de mesaje şi rapoarte. Informaţiile colectate sunt reprezentate grafic cu ajutorul unei platforme software de tip SOLARIS[12] şi interschimbate în timp real, fie sub forma unor mesaje text simple, formatate, fie sub forma unor rapoarte complexe.

Dezvoltarea sistemului este gestionată prin parteneriat de tip guvernamental de un manager de proiect reprezentat de o componentă specială a Armatei SUA, pe linie CIS, dispusă în locaţia Fort Monmouth, New Jersey, printr-un proiect special C3T (Tactical, Command Control and Communication).

Sistemul în faza incipientă a fost testat printr-un program special de către „Divizia I digitală din cadrul Diviziei a IV-a infanterie" cu sediul în Fort HOOD Texas, iar mai apoi, în anul 1997 a fost testat în cadrul Centrului Naţional de pregătire din Barstow, California. În anul 1998 Divizia I a coordonat şi desfăşurat teste pe un număr limitat de echipamente, ca mai apoi sistemul să fie declarat apt pentru a fi introdus în producţie. Din punct de vedere operaţional, sistemul a fost folosit pentru prima dată în cadrul conflictului din Iugoslavia în anul 1998, iar apoi, începând cu anul 2003, sub conceptul de Forţa XXI în cadrul operaţiunilor din Iraq şi Afganistan.

Sistemul este considerat încă din anul 2001 ca fiind unul din cele 5 cele mai bune platforme software gestionate şi utilizate de către guvernul SUA, în toată industria de apărare. În anul 2005 a fost declarat drept cea mai bună platformă integrată de comunicaţii în operaţii de sprijin de tip Joint Coalition Forces, iar momentan, sistemul numără aproximativ 5 milioane de utilizatori fiind indispensabil în toate zonele de conflict.

Dorinţa este de a realiza o platformă universală standard, la nivelul tuturor forţelor, de tipul unei platforme mixte sprijin-luptă – „Mixt Joint Battle Command Support Platform" care să acopere toate cerinţele unei acţiuni militare începând de la nevoia de comunicare şi finalizând cu nevoia de sprijin logistic al acţiunilor de luptă propriu-zise.

Funcţionabilitate, capacităţi şi facilităţii oferite.

La baza fiecărei platforme BFT indiferent de suportul vehicular sau static folosit (elicopter, auto blindat, navă, centru de operaţii tactic sau întrunit, personal militar) se află principiul asigurării unor servicii de comunicaţii satelitare în bandă KU combinate cu raportarea poziţiei GPS, toate acestea, integrate sub o platformă software comună, cu aplicaţii diverse în funcţie de nevoile misiunii.

Din compunerea sistemului fac parte următoarele elemente, astfel: **platforma software de tip FBCB2** ce utilizează aplicaţii predefinite şi software specializat sub forma unui sistem de informaţii geografice (GIS), reprezentate fie în imagini satelitare la scară sau în caroiaj rectangular de tip Mercator sau Gauss; **un terminal de date** folosit pentru procesarea şi rularea aplicaţiilor ce are înglobat o unitate de imagine (hard-disk), cu rol de stocare al

[12] Solaris-platformă software dezvoltată de Sun Microsystems încă din anul 1992. Este cunoscută în momentul actual sub denumirea de ORACLE SOLARIS ca urmare a preluării de către firma ORACLE a firmei Sun Microsystems.

aplicaţiilor şi informaţiilor procesate; **un echipament de recepţie a poziţiei GPS de tip „DAGGER”** cu rolul de a raporta şi de a recepţiona locaţia exactă a utilizatorului; **o unitate de afişare cu tuch-screen** (display unit) ce permite afişarea datelor şi informaţiilor cât şi introducerea acestora prin intermediul facilităţilor tuch-screen cu ajutorul unei tastaturi virtuale sau pe baza rapoartelor standard predefinite; **o tastatură** cu rol de dispozitiv de intrare şi **o antenă** de tip **„transceiver[13]”** ce permite realizarea conexiunii satelitare permanente în banda Ku.

Principiul de funcţionare se bazează pe interoperabilitate elementelor componente, astfel:

1. Platforma software FBCB2 se află instalată şi memorată împreună cu toate aplicaţiile şi facilităţile oferite unitatea de imagine (hard-disk);

2. Unitatea de imagine conlucrează şi recunoaşte permanent atât transciverul cât şi echipamentul GPS tip DAGER (in sistem „bound-unbount”), fapt ce nu permite schimbarea unui echipament de la o platformă la alta;

3.Echipamentul GPS oferă satelitului

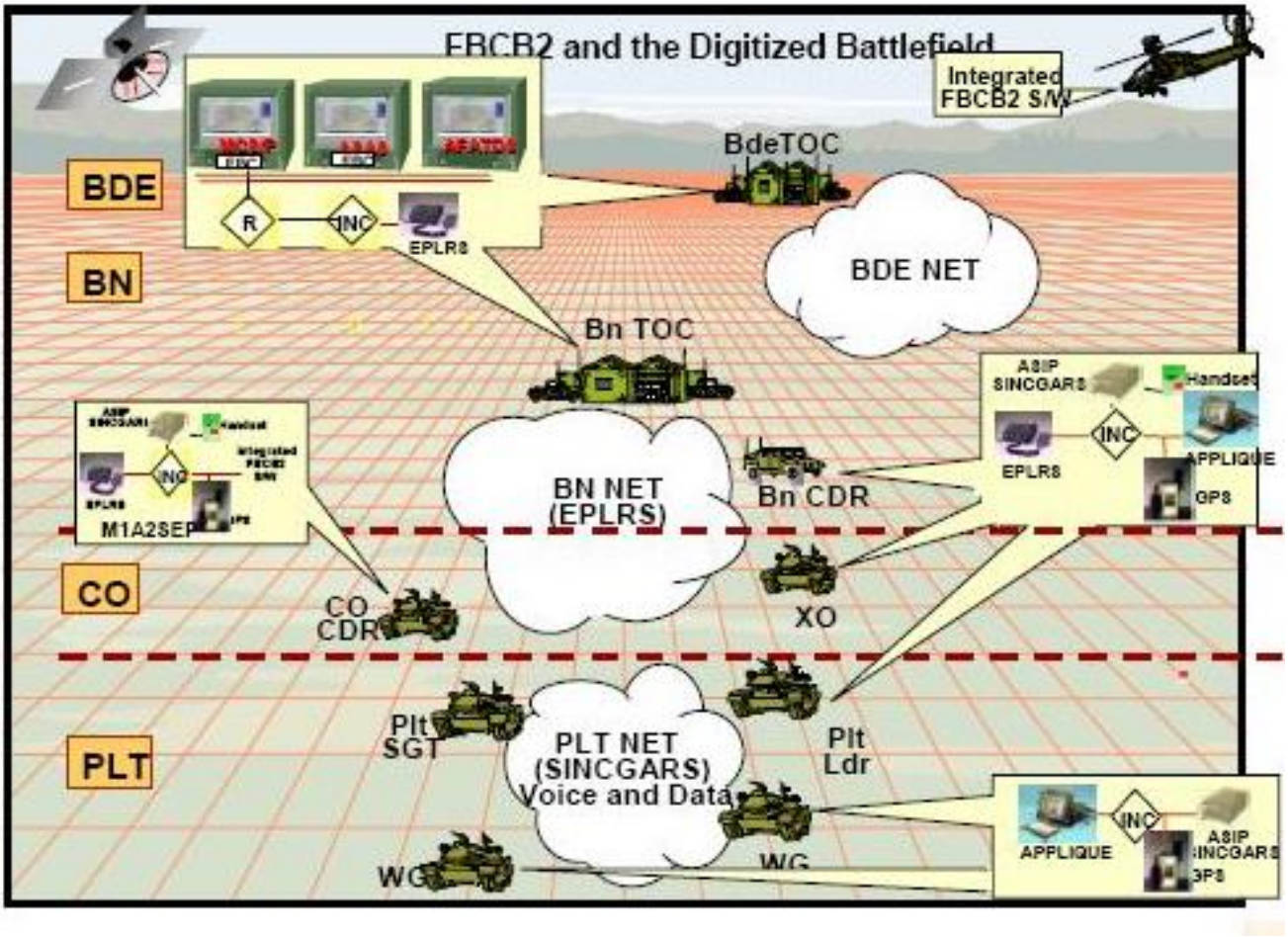


Figura nr. 4 - Schimbul de informaţii la nivel brigadă

poziţia GPS şi comunică prin intermediul platformei FBCB2 informaţii asupra locaţiei către utilizator. Poziţia GPS este transmisă şi recepţionată permanent la intervale de „referesh” ce variază între 10 m (5 minute) – 100 m (30 minute). Lipsa echipamentului GPS obligă utilizatorul la introducerea

13

Caracteristici: gama 40 to 60 GHz, putere 5 W, rate de transfer de date, variabile, susţinute cu capacitatea cuprinsă intre 512 Kbps to 0.6 Kbps, latenţă 1 secundă si cu o valoare a aperturii cuprinsă între 6 - 10 db.

manuală a poziţiei vehicolului sau platformei auto şi actualizarea acesteia la intervale de timp prestabilite.

4. Unitatea de afişare permite afişarea situaţiei tactice şi a întregii platforme FBCB2, precum şi utilizarea tuturor aplicaţiilor în vederea asigurării nevoilor de comunicaţii cu toţi corespondenţii şi cu celelalte forţe partenere. Totodată permite introducerea datelor cu ajutorul unei tastaturi virtuale.

Atunci când se doreşte realizarea unei transmisii sau a unei comunicări cu un alt utilizator al platformei FBCB 2 (corespondent) acesta poate fi identificat fie nominal prin cunoaşterea numelui de adresare (nick name/role) sau prin selectarea acestuia dacă se află în aria de acoperire a hărţii. Utilizatorii platformei pot comunica permanent, individual sau în grup, orice fel de informaţie de la simple mesaje text la rapoarte MEDEVAC, la rute de transport, profiluri de misiune, rapoarte logistice, şi chiar statusuri cu privire la situaţia consumului de carburant, muniţie, starea personalului sau elemente complexe precum imagini live din zona de acţiune, fotografii cu poziţionarea trupelor inamice, cu rutele de transport şi starea acestora sau de ce nu, transmisii video referitoare la incidentele din timpul misiunii.

Practic, platforma hardware şi software oferă posibilităţi limitate doar de timp şi de nivelul de bandă al comunicaţiei satelitare, în rest, sunt puse la dispoziţia combatantului suficiente mijloace de comunicaţii necesare atât structurilor ce oferă suportului logistic din zona de operaţii cât şi celorlalte elemente din actul decizional. Orice tip de comunicare nu se realizează direct utilizator la utilizator (“pear to pear”) ci prin intermediul unui centru de control denumit Centrul de Operaţii Întrunite al Armatei (US Army Joint Operation Center).

Utilizarea sistemului în realizarea sprijinului logistic.

Scopul principal al sistemelor BFT şi implicit al platformei FBCB2 este de creştere a gradului de operativitate a trupelor prin aplicarea tehnologiei de vârf din domeniul comunicaţiilor şi prin punerea la dispoziţia decidenţilor a informaţiior despre condiţiile existente pe câmpul de luptă. Pentru realizarea acestui deziderat nimic nu poate fi mai important decât relaţia suport de comunicaţii - suport logistic.

În condiţiile în care acţiunea militară a suferit modificări esenţiale, iar la baza oricărei manevre de forţe se află manevra de mijloace, logistica pare a fi câştigat întâietatea în ceea ce priveşte lupta cu celelalte arme de sprijin. În acţiunile militare de azi, iar conflictele din teatrele de operaţii nu pot decât să confirme acest lucru, logistica reprezintă nu numai cheia succesului unei operaţiuni, indiferent de natura ei, ci de multe ori poate fi chiar catalizatorul sau obstacolul declanşării unui conflict.

Realitatea cotidiană ne determină să afirmăm faptul că, pe lângă componenta logistică, un alt element ce susţine acţiunea militară, indiferent că vorbim de acţiuni tip combat sau de acţiuni de tip suport, este reprezentat de „serviciile de comunicaţii integrate”.

Comunicaţiile şi în special cele integrate din generaţia a III- a, sunt suportul pentru ceea ce înseamnă optimizarea oricărei acţiuni, iar din punct de vedere logistic pot fi privite atât ca element de sprijin cât şi ca element acţional în cadrul operaţiilor logistice.

Transportarea unor mijloace sau a unor materiale din locaţia A în locaţia B poate fi în zona de conflict o operaţiune logistică banală sau în funcţie de context, una care, desfăşurată cu succes, poate duce la obţinerea succesului faţă de forţele adverse. Indiferent de situaţie, platformele de comunicaţii integrate BFT, deşi gândite iniţial ca şi sisteme de tip „situation awarnes” oferă mijlocul cel mai vizibil prin care operaţia logistică poate fi desfăşurată cu succes, optimizată sau de ce nu încetinită. Dacă conflictele din fosta Iugoslavie, Iraq şi mai apoi Afganistan ne-au demonstrate că utilizarea platformelor nu aduce decât

beneficii, lipsa acestora din sistemul naţional de apărare nu face altceva decât să ne confirme faptul că tot ceea ce înseamnă suport, operativitate şi combat se desfăşoară anevoios cu un consum exagerat de timp şi cu o lipsă evidentă de eficienţă.

Dar ce pot face sistemele BFT şi platforma FBCB2 pentru sprijinul logistic în cadrul operaţiunilor şi conflictelor militare din prezent?

Sistemul, amplasat pe platforme specifice cerinţelor şi nevoilor de misiune, asigură atât sprijin de luptă (CS), cât şi servicii tip Combat service support (CSS), concomitent cu planificarea şi executarea operaţiunilor. FBCB2 reprezintă o schimbare de paradigmă importantă pentru acţiunea militară. Pentru prima dată, structurile militare ce acţionează într-o zonă de conflict sunt interconecate prin platforme şi organigrame software ce le oferă o imagine comună a câmpului de luptă, simultan cu facilitarea furnizării tuturor serviciilor de comunicaţii atât de necesare în sprijinul manevrei.

Pe lângă toate acestea, poate cel mai important este faptul că oferă personalului şi liderilor din domeniul logistic înţelegerea situaţiei acţionale din spaţiul de luptă. Sistemele BFT oferă, de asemenea, creşterea capacităţii de sincronizare între unităţile de sprijin şi unităţile de tip client. Funcţionalitatea sistemelor BFT şi implicit a platformei FBCB2 include punerea la dispoziţie a următoarele elemente: rapoartele de logistică situaţională (LOGSITREP), rapoarte cu privire la starea personalului (PERSITREP), punctele de aprovizionare cu bunuri şi materiale, locaţiile punctelor ce oferă servicii, rapoarte de stare a tehnicii, apel logistic pentru sprijin (logistics call for support - CFS), ordinele de sarcină logistică (logistics task orders - LTO), solicitări de sincronizare logistică (logistics task synchronization), management logistic (logistics task management) etc.

Adiţional, dar esenţial, este faptul că platforma FBCB2 pune la dispoziţia utilizatorului sub formă de rapoarte standard: rapoarte medicale (medical unit situation report), rapoarte referitoare la pierderi (mortuary affairs report), rapoarte logistice (LOGREP) ce asigură înţelegerea din punct de vedere logistic a situaţiei de luptă.

În prezent, FBCB2 permite transmiterea de date şi informaţii folosind text liber, comentariile, mesaje, rapoarte standard şi formatate, dar şi entităţi de date complexe cum ar fi: imagini live, hărţi, poziţionare de obstacole, rute de deplasare, topologia terenului şi rute de acces. În mod ideal, sistemele automatizate sunt concepute pentru a facilita transmiterea rapidă şi integrată a informaţiilor. În aceste cazuri, utilizatorul de sistem înţelege faptul că importanţa informaţiilor şi datelor face ca manipularea şi transmiterea acestora să fie realizată automat de sistem, către sediul central imediat superior în organigrama acţiunilor.

În acţiunile militare din zonele de conflict două elemente sunt vitale pentru un raport logistic de situaţie (LOGSITREP): acurateţea şi detalierea conţinutului acestuia, pe de o parte şi rapiditatea transmiterii acelui raport către factorii decidenţi din domeniu, pe de altă parte. În cadrul rapoartelor logistice "LOGSITREP" ce sunt înaintate cu ajutorul platformei FBCB2, utilizatorul are posibilitatea de a introduce în status, solicitări pentru toate clasele de aprovizionare clasa I, II, III (P), III (B), IV, V, VII, şi IX. Astfel elementele şi solicitările din raport trec automat prin fiecare eşalon de comandă ce are acces la platforma FBCB 2, folosind un element de tip „listă de urmărit" (command tracked item list update message). Platforma software a sistemului transmite automat rapoartele, în timp real, în primul rând către ordonatorul principal (primul element din lanţ care poate asigura solicitarea) apoi către lanţul de comandă la S4/S4 batalion/brigadă de manevră. Concomitent, aplicaţia realizează şi înaintează copii cu situaţia actualizată la cel mai înalt nivel de sprijin al operaţiei respective. Toate rapoartele vor urma lanţului de comandă aşa cum se

specifică în organizarea de sarcini a unităţii ce participă sau desfăşoară acţiunea de luptă. Astfel, toţi destinatarii LOGSITREP au capacitatea de a privi cu un nivel de comandă mai jos. Acest lucru oferă utilizatorului abilitatea de a vedea raportul prezentat la acest nivel pentru fiecare clasă de aprovizionare, precum şi orice observaţii care au fost făcute. Comentariile făcute cu LOGSITREP nu pot fi eliminate. Orice comentarii necesare pentru prelucrare ulterioară a solicitărilor conform lanţului de raportare, trebuie să fie reintroduse în următorul raport.

Deşi pare complex, toate activităţile necesare se realizează extrem de simplu şi sarcina transmiterii şi procesării informaţiilor revine aproape total aplicaţiei, fiind în mare parte rapoarte predefinite. Scopul esenţial este de a oferi unităţii de comandă vizibilitatea asupra echipamentelor, materialelor şi personalului, de fapt, starea reală de la ultima raportare logistică la nivel de unitatea/structură. Un scop secundar, pe lângă oferirea unei vizibilităţi asupra statusului unei unităţi din punct de vedere logistic, este anticiparea mult mai bine a cerinţelor pe linie logistica. În mod optim, utilizatorul nu va trebui să solicite în mod expres aprovizionare de mărfuri raportate prin intermediul acestui raport. Acest lucru se datorează faptului că eşalonul superior este conştient de cerinţele acestui şi poate începe acţiunea necesară aprovizionării, înainte ca materialele şi echipamente să devină vitale pentru acţiune.

În cazuri de extremă urgenţă este utilizat **„apelul de sprijin logistics" (logistics call for suppor - CFS)** cu scopul de a solicita asistenţă imediată de „tip combat service support". Orice platformă FBCB2 poate solicita sprijin prin funcţia mesajului predefinit de tip CFS. CFS este un mesaj predefinit şi poate fi trimis direct la prima structură logistica de sprijin, dar poate fi trimis automat la eşalonul imediat superior. Acest lucru permite măsuri de sprijin imediate pe câmpul de luptă, de tip multiplicator. Orice FBCB2 poate trimite sau primi un mesaj de CFS. În cazul în care solicitările de sprijin nu au fost asigurate prin LOGSITREP sau dacă unele cerinţe de sprijin nu au fost sau nu au putut fi anticipate, orice utilizator poate solicita expres sprijin prin această funcţie. Mesajele de tip CFS sunt de asemenea predefinite „de tip template" şi sunt trimise, pe procedura de operare standard (SOP), la structura logistica de sprijin, care va furniza serviciile logistice de sprijin.

Sistemul FBCB2 găzduieşte şase categorii de cereri CFS: întreţinere, transport, alimentare, medicale, religioase şi altele iar acţiunile de aprovizionare includ: clasa I, III, IV, VIII, IX, servicii de spălătorie şi mortuare, acţiuni de transport, informaţii, acţiunile de întreţinere, reparaţii, recuperarea, servicii, acţiunile medicale, evacuări, acţiuni religioase, servicii funerare şi servicii memoriale.

Structura logistică care a recepţionat CFS, are datoria prin structura de conducere de a identifica sursa de aprovizionare cea mai adecvată cererii pentru a executa misiunea.

Autoritatea pe linie logistică (comandantul) trimite un LTO (logistic task order) la sursa de aprovizionare. Acest mesaj este acelaşi şablon ca mesajul CFS primit, prin urmare, conţine în antet unitatea solicitant si locaţia acesteia. Odată ce sursa de aprovizionare primeşte mesajul, aplicaţia FBCB2 va cere automat să se întoarcă un mesaj de confirmare (mesaj de tip ACK), care să ateste dacă poate, nu poate, sau deja a executat misiunea (WILCO, CANTCO, HAVECO). Dacă sursa de aprovizionare răspunde cu un WILCO, aplicaţia va solicita, de asemenea, să trimită un mesaj de confirmare de IDLE sau ACTIVE. Această acţiune specifică, confirmă faptul că resursa este activă sau în caz contrar nu se poate realiza aprovizionarea momentan deoarece este în executare o altă misiune. Odată ce recunoaşterile au fost trimise, sursa de aprovizionare va efectua sincronizarea cu unitatea care solicita sprijin, prin trimiterea un mesaj text gratuit declarând că solicitarea este pe drum, va fi acolo, la un punct de întâlnire, la un anumit timp.

Sistemul gândit prin platforma FBCB2 a fost realizat în urma analizei situaţionale şi cazuistice din câmpul tactic actual. Operaţiuni care în mod curent durează una, două zile din punct de vedere birocratic, sunt realizate automat de către o platformă integrată de comunicaţii şi transmise simultan la toate structurile necesare a fi implicate în scopul atingerii unui deziderat unic – succesul acţiunii militare.

Pentru structurile de conducere dispuse în centrul de comandă, monitorizarea transporturilor şi a misiunilor de sprijin logistic devine un film, o transmisie live în care actorii principali sunt forţele proprii iar cursul acţiunii este stabilit precis şi controlat permanent, fiind modificat doar de acţiunile inamicului care şi acestea pot fi previzionate şi evitate cu mai multă uşurinţă. Totul se reduce astfel la oferirea de sprijin în timp real şi la cunoaşterea permanentă situaţiei. Oferirea de sprijin logistic în timp util, eficient, este mai critică în prezent. Armata trebuie să aibă suport logistic optim pentru a maximiza puterea de luptă. De sprijinul de luptă şi de serviciile logistice (servicii de sănătate, sprijin financiar, de personal, de aprovizionare, întreţinere, servicii de transport) depinde succesul şi implicit realizarea misiunii. Aşa cum tacticieni trebuie să concentreze puterea de luptă pentru îndeplinirea misiunii lor, la fel trebuie să se concentreze logisticienii activelor logistice pentru îndeplinirea misiunii proprii. Liderii trebuie să ştie totul despre resurse: tipul, cantitatea, locaţia, condiţii şi disponibilitatea. Ei trebuie să cunoască nivelul actual de utilizare şi să poată estima ratele viitoare de consum pe baza situaţiei tactice.

Legătura între ceea ce există în teren, ceea ce pot oferi logisticienii, ceea ce au nevoie forţele luptătoare şi lideri este realizată de sistemele de comunicaţii moderne, mai bine spus, de sistemele de comandă-control, iar în cazul de faţă platforma FBCB2.

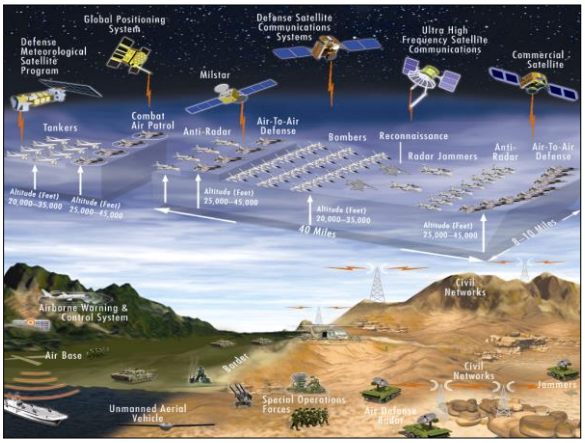
Se afirmă că „norocul ţine cu cei puternici” şi privind realitatea conflictelor din ultimul deceniu, putem spune că norocul a favorizat întotdeauna comandanţii care au informaţii mai bune şi mai multe în timp util cu privire la ceea ce se întâmplă pe câmpul de luptă. Acest lucru este cu siguranţă
adevărat pentru nu prea îndepărtatul IRAQ şi recentul Afganistan, cazuri în care realizările tehnologice militare au fost cu adevărat remarcabile. Mulţi factori, cum ar fi personalul de înaltă calitate, echipamente avansate, sistemele complexe de armament, formarea şi pregătirea exigentă şi inovatoare au ieşit în evidenţă, diferenţiind capabilităţile forţelor de coaliţie faţă de adversari.

Lupta este practic decisă de un element esenţial numit **superioritatea informaţiei** iar acest element are la bază fără echivoc sistemul Blue Force Tracking.

UNELE ASPECTE DE ACTUALITATE PRIVIND MANAGEMENTUL SPECTRULUI RADIO

Colonel Liviu BÎRSAN
Locotenent-colonel Sorin PARFENE
Agenţia Militară pentru Managementul frecvenţelor Radio

Influenţa covârşitoare a tehnologiei asupra calităţii vieţii este acceptată şi chiar dorită de cei mai mulţi dintre noi, ca un rezultat firesc al evoluţiei sociale. Utilizăm zilnic un număr impresionant de echipamente tehnice pentru a comunica, a călători, a munci, a găti, a ne distra şi chiar a ne odihni cât mai confortabil şi eficient. Câţi şi-ar fi putut imagina cu doar 10-15 ani în urmă că vom fi nedespărţiţi de telefoanele mobile, că vom folosi mai degrabă cuptorul cu microunde decât plita … cu inducţie, că ne vom deplasa oriunde în lume numai cu ajutorul GPS-ului sau că vom accesa Internet-ul indiferent de locul unde ne-am afla. Acestea prezentate mai sus, şi încă multe altele, care au devenit indispensabile zilelor noastre, sunt posibile utilizând frecvenţele radio sau aplicaţii ale acestora.



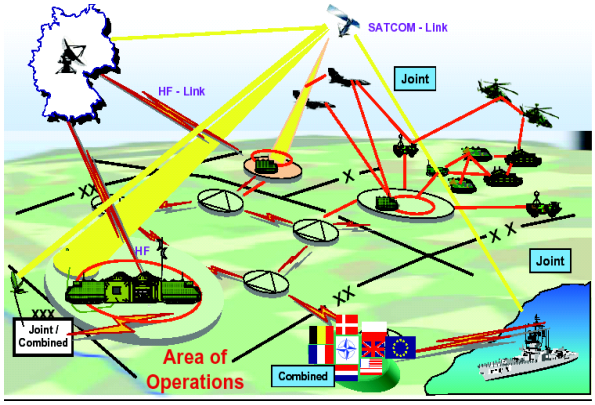
Ce este important de subliniat este faptul că, majoritatea acestor *gadget*-uri ne fac viaţa mai uşoară atât timp cât funcţionează corect şi în parametrii proiectaţi, devenind o adevărată pacoste în cazul defectării sau funcţionării necorespunzătoare. Şi cum o mare parte a echipamentelor sunt *wireless*, folosite cu precădere în benzi de frecvenţe cu un grad ridicat de congestie, cauzele perturbaţiilor sunt foarte des identificate în mediul electromagnetic al echipamentului perturbat.

Chiar dacă aceste echipamente pot fi utilizate de către oricine fără licenţă de emisie, este bine de ştiut că, pentru a ne proteja sănătatea, fiecare echipament *wireless* trebuie să fie însoţit de o declaraţie de conformitate, din partea producătorului sau importatorului, privind respectarea cerinţelor esenţiale de compatibilitate electromagnetică. Acest certificat vă asigură că aparatul corespunde standardelor de compatibilitate şi biocompatibilitate electromagnetică şi poate fi utilizat în siguranţă pe teritoriul ţării unde se comercializează. De exemplu, utilizarea în România a unui aparat telefonic *cordless* produs pentru Australia, în banda de frecvenţe de 450 MHz, poate crea perturbaţii electromagnetice în reţelele de telefonie mobilă CDMA.

Standardele de compatibilitate electromagnetică valabile în România şi la care trebuie să se raporteze orice echipament radioelectric comercializat pe teritoriul ţării noastre

sunt grupate în *Lista standardelor armonizate*, actualizată periodic de Ministerul Comunicaţiilor şi Tehnologiei Informaţiei, fiind publicată în Monitorul Oficial al României, Partea I.

Aşa cum probabil se intuieşte, aceste standarde armonizate se referă, în principal, la echipamente comerciale - COTS (Commercial off-the-shelf) şi doar în mică măsură se pot aplica echipamentelor cu destinaţie specială, utilizate în domeniul militar, al cercetării sau explorării spaţiale etc. Specificaţiile tehnice ale acestor echipamente cu destinaţie specială conţin referiri la standarde tehnice armonizate, care permit atât atingerea unui grad ridicat de interoperabilitate, cât şi respectarea cerinţelor esenţiale de compatibilitate electromagnetică.



Interoperabilitatea este asigurată prin standardele deja foarte cunoscute în mediul militar sub denumirile de STANAG (Acord de Standardizare), SM (Standard Militar) sau MIL-STD (Standard Militar SUA) etc. Rămâne însă în discuţie modul în care se poate verifica respectarea cerinţelor esenţiale de compatibilitate electromagnetică a echipamentelor cu destinaţie specială, în condiţiile în care apar perturbaţii prejudiciabile în mediul electromagnetic al echipamentului, în ciuda declaraţiei de conformitate a producătorului/importatorului.

Perturbaţii electromagnetice pot fi produse atât prin intermediul unor cuplaje galvanice, inductive sau capacitive, cât şi prin radiaţie electromagnetică. Această din urmă cauză poate fi analizată prin raportarea unor valori de câmp electromagnetic la valorile etalon, precizate în normele sau recomandările Uniunii Internaţionale de Telecomunicaţii (UIT) privind monitorizarea spectrului (ex. ITU-R SM.1541-3), standarde tehnice ale ETSI *(European Telecommunications Standards Institute)* sau ale IEEE-SA *(Institute of Electrica land Electronics Engineers Standards Association).* Consultarea acestor standarde însă se face contra cost şi, din această cauză, cunoaşterea şi aplicarea lor este rezervată unui număr redus de specialişti.

Apare aşadar nevoia unei cooperări între cei care pot accesa şi gestiona standarde de compatibilitate electromagnetică şi cei care trebuie să aplice aceste standarde în activitatea lor zilnică. Noul ordin al ministrului apărării naţionale M. 31 din 19.04.2011, intrat în vigoare la data de 02.05.2011 o dată cu publicarea în Monitorul Oficial la României nr. 300, Partea I, rezolvă această problemă de coordonare între structurile cu responsabilităţi pe linia asigurării compatibilităţii electromagnetice în Ministerul Apărării Naţionale.

Odată cu intrarea în vigoare a ordinului menţionat mai sus, atribuţiile Agenţiei Militare pentru Managementul Frecvenţelor Radio pe linia compatibilităţii electromagnetice şi avizării obiectivelor de radiocomunicaţii cresc în complexitate, fiind absolut necesare anumite ajustări de ordin organizatoric şi de înzestrare, care să permită coordonarea eficientă a domeniului, atât de sensibil, al compatibilităţii electromagnetice (CEM).

În conformitate cu recomandarea nr. 1.7.2. din cadrul Acordului Vilnius-2005, metoda de calcul armonizată (HCM) acceptată prin Acord pentru realizarea analizei de compatibilitate electromagnetică în serviciile fix şi mobil, va fi implementată în noua aplicaţie şi va permite determinarea mult mai rapidă a nivelurilor maxime admisibile ale câmpurilor perturbatoare, a distanţelor transfrontaliere maxime în cazul coordonării cu ţările vecine, a factorului de corecţie pentru nivelul admisibil de câmp perturbator în cazul lucrului pe frecvenţe fixe etc. Toate aceste analize pot fi realizate corect cu ajutorul aplicaţiilor informatice numai în măsura în care informaţiile introduse în programul de simulare a condiţiilor de propagare în mediul electromagnetic sunt corecte şi complete. Realitatea ne-a arătat că cel mai sigur mod de determinare a condiţiilor de propagare şi a valorilor de câmp electromagnetic, în special în situaţia apariţiei unei perturbaţii prejudiciabile, este folosirea în teren a echipamentelor de monitorizare.

În cele ce urmează prezentăm, informativ, unele situaţii cu care unitatea s-a confruntat în soluţionarea de interferenţe prejudiciabile produse de echipamente militare ori pe timpul avizării obiectivelor de radiocomunicaţii aparţinând altor utilizatori, cu scopul protejării lucrului mijloacelor radioelectrice proprii.

AGREEMENT

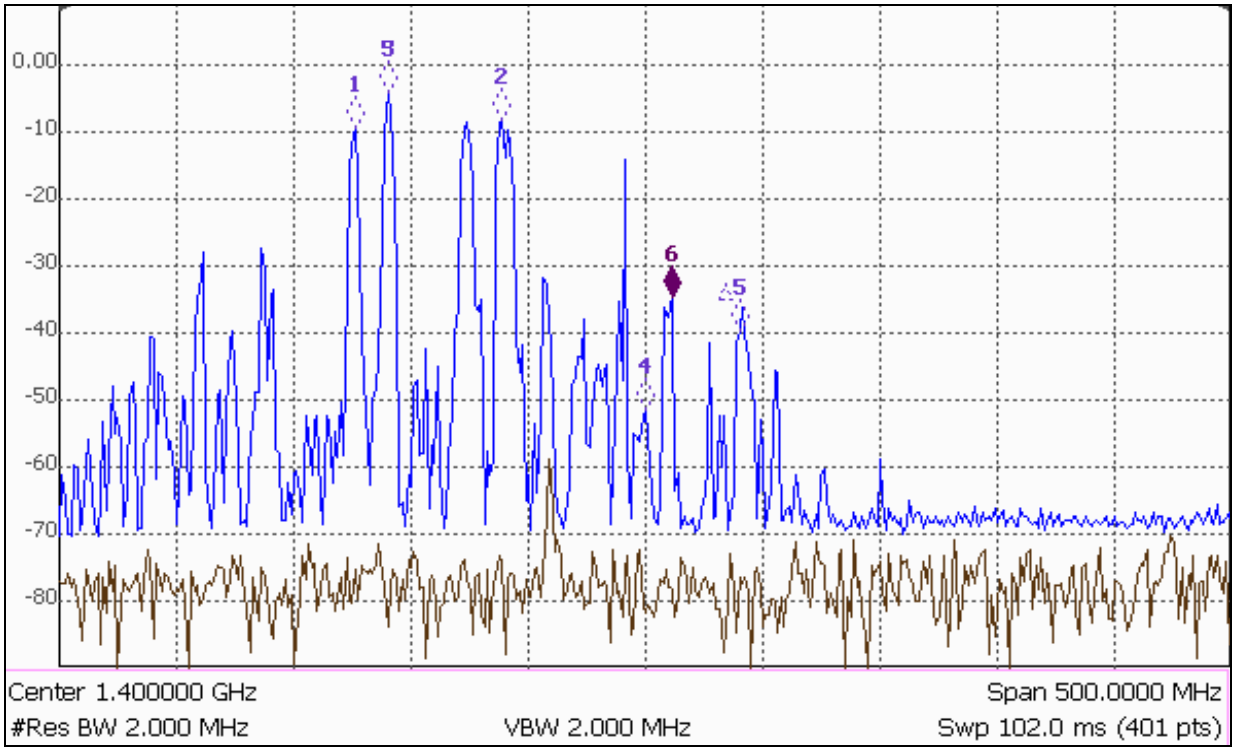
between the Administrations of
Austria,
Belgium,
The Czech Republic,
Germany,
France,
Hungary,
The Netherlands,
Croatia,
Italy,
Liechtenstein,
Lithuania,
Luxembourg,
Poland,
Romania,
The Slovak Republic,
Slovenia
and
Switzerland

on the co-ordination of frequencies between
29.7 MHz and 39.5 GHz
for the fixed service and the land mobile service.

(HCM Agreement)
Vilnius, 12 October 2005

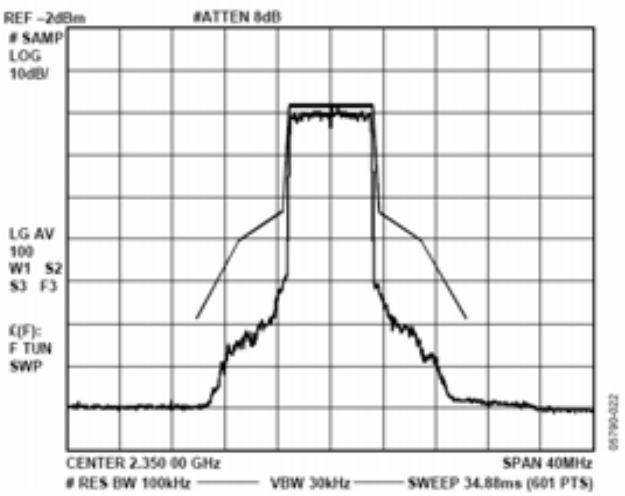
În figura de mai jos este prezentată, pe baza unui caz real, achiziţia semnalului de emisie a unui echipament radar exploatat într-o bandă de frecvenţe adiacentă serviciului pasiv de exploatare a Pământului prin satelit. Nerespectarea cerinţelor esenţiale de compatibilitate electromagnetică, precizate în detaliu pentru aceste tipuri de echipamente în regulamentele, rezoluţiile şi recomandările UIT sau în standardul ETSI EN 301 783, au condus la depăşirea nivelului admis al semnalului în afara benzii de emisie şi, implicit, au creat perturbaţii

prejudiciabile altor echipamente radioelectrice, cu repercusiuni asupra disponibilităţii serviciilor acestora.



Experienţa specialiştilor şi calitatea echipamentului de monitorizare sunt esenţiale în determinarea cauzelor unei perturbaţii electromagnetice şi în luarea măsurilor tehnice sau organizatorice cele mai potrivite pentru eliminarea perturbaţiei.

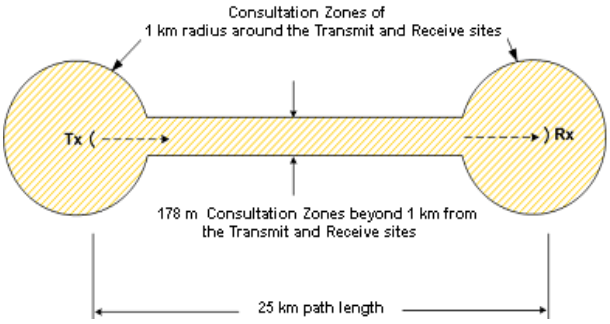
În imaginile de la jos, se demonstrează practic, prin măsurători şi din analiza măştii semnalului, că identificarea unui nivel ridicat al semnalului în banda de gardă, atât pentru staţii WiMax (IEEE 802.16), cât şi pentru echipamente radar, conduce la restricţii de instalare în funcţie de frecvenţele de lucru utilizate şi caracteristicile de propagare din mediu. Se stabileşte astfel instalarea unei antene tip WiMax la o distanţă de cel puţin 1 Km faţă de un radar care emite pe o frecvenţă mai mare de 3,4GHz şi al cărui nivel al semnalului de emisie la borna de antenă are o valoare de -76 dBc PEP. Asignarea unei frecvenţe radio mai mari de 3,4 GHz determină



o creştere logaritmică a distanţei minime necesare lucrului fără perturbaţii a unei staţii WiMax, ajungând ca la 3,405 GHz, distanţa de protecţie să fie de 11 Km.

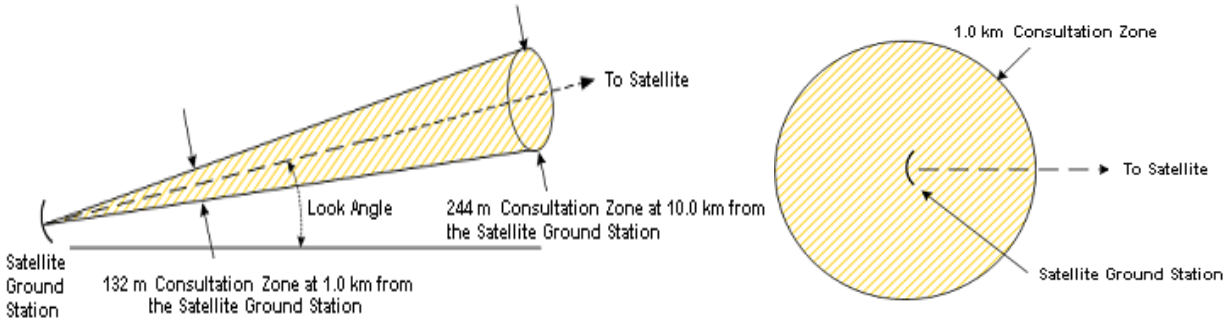
Protejarea lucrului echipamentelor radioelectrice proprii este una din responsabilităţile de bază ale AMMFR. Analiza de compatibilitate electromagnetică stă la baza acordării de către AMMFR a avizelor CEM de instalare a unor echipamente în mediul electromagnetic al unui echipament radioelectric militar. Importanţa efectuării unei analize profesioniste, bazate pe informaţii pertinente şi un nivel ridicat de expertiză a specialiştilor, este evidentă, cel puţin din punct de vedere al consecinţelor, în cazul în care, din eroare, este avizată favorabil construirea unei instalaţii fixe (turn, centrală eoliană etc) pe direcţia de legătură sau în zona de supraveghere a unui echipament militar.

Protejarea lucrului staţiilor de sol sau a terminalelor de comunicaţii



Zona de protecţie a echipamentelor radioelectrice de tip punct la punct

prin satelit pe teritoriul României devine astfel o obligaţie pentru ANCOM şi implicit pentru AMMFR, în cazul exploatării echipamentelor prin satelit în benzi de frecvenţe partajate sau dedicate exclusiv aplicaţiilor militare.



Zona de protecţie pentru un echipament de comunivcaţii prin satelit

Doar din această trecere rapidă în revistă a unor domenii în care Agenţia Militară pentru Managementul Frecvenţelor Radio este implicată în asigurarea compatibilităţii electromagnetice pentru echipamentele radioelectrice din dotarea MApN, se poate contura o imagine realistă despre importanţa crescândă a domeniului CEM şi despre implicaţiile pe care nerespectarea standardelor şi măsurilor de asigurare a CEM le poate avea atât asupra bunei funcţionări a echipamentelor proprii, cât şi asupra sănătăţii personalului aflat într-un mediu electromagnetic perturbat.

SECURITATEA EUROATLANTICĂ ŞI MANAGEMENTUL CRIZELOR

General maior (r) dr.Constantin MINCU

Evoluţiile în planurile politic, militar, economic, financiar, demografic, tehnologic şi de mediu manifestate la nivel global, regional, zonal, şi statal solicită în mod imperios o reanalizare continuă şi multidisciplinară a mediului de securitate internaţional, în structurile multinaţionale existente, dar şi în fiecare stat în parte.

România, în calitate de membru presupus responsabil al comunităţii internaţionale, membru NATO (aprilie 2004) şi membru al Uniunii Europene (ianuarie 2007) este obligată prin tratate şi înţelegeri multilaterale şi bilaterale să aplice, cu bună credinţă şi eficienţă, în legislaţia şi practica interne, inclusiv în domeniul managementului crizelor:

- **Reglementările şi rezoluţiilor ONU** şi a altor organisme la care România este parte;
- **Prevederile Tratatului Atlanticului de Nord** (The North Atlantic Treaty, Washington, 04 Aprilie, 1949);
- **Principiile şi obiectivele** menţionate în **Conceptul Strategic al NATO**, aprobat de către şefii de stat şi de guvern la **Lisabona în noiembrie 2010;**
- **Atribuţiile şi obiectivele** organismelor şi comandamentelor NATO, între care: Consiliul Nord-Atlantic (Nord Atlantic Council); Comitetul de Planificare a Apărării (Defence Planning Comitee); Comitetul Politic (The Political Comitee); Comitetul Militar (The Military Comitee); Comitetul de Planificare a Urgenţelor Civile (The Civil Emergency Planning Comitee); Comandamentele strategice şi operaţionale ale NATO din Europa; alte agenţii şi comitete NATO; Centrul de situaţie al NATO, cu funcţionare permanentă (The NATO Situation Centre);
- Obligaţiile ce revin din reglementările Uniunii Europene pentru fiecare stat membru (în context menţionez documentele şi planurile EDA/EU[14] precum şi reglementările specifice managementului crizelor şi protecţiei infrastructurilor critice – Directiva 2008/114/08 Decembrie);
- Obligaţiile ce revin României din tratatele multilaterale şi bilaterale la care este parte;
- Reglementările şi acţiunile pentru protecţia mediului;
- Reglementările şi obligaţiile ce revin României pentru protecţia drepturilor fundamentale ale omului.

Problematica complexă, dinamică, fluidă şi de multe ori cu dezvoltări imprevizibile şi contradictorii a securităţii globale, în general, a făcut şi face obiectul analizelor şi studiilor organismelor menţionate, dar şi a autorităţilor şi think-tank-urilor din ţara noastră, îndeosebi în ultimii zece ani. Menţionez aici structuri de cercetare din domeniul academic (Academia Română, Academia Oamenilor de Ştiinţă din România, Universitatea Naţională de Apărare „Carol I", Universitatea Politehnică Bucureşti, Universitatea Creştină „Dimitrie Cantemir", prin Institutul de Studii de Securitate etc.), precum şi fundaţii (Eurisc) şi asociaţii (de exemplu Asociaţia de Geopolitică „Ion Conea") etc.

Pentru cei interesaţi este necesară o inventariere şi o cunoaştere aprofundată a numeroaselor studii, articole şi materiale documentare publicate sau comunicate în cărţi de specialitate, reviste, simpozioane, mese rotunde etc[15]. Efortul ar merita să fie

[14] European Defence Agency (EDA/EU)

[15] Revista de Ştiinţe Militare, editată de Secţia de Ştiinţe Militare a AOS-R, cu apariţie trimestrială; Revista Impact Strategic, editată de Centrul de Studii Strategice de Apărare şi Securitate – U.N.Ap „Carol I", cu apariţie trimestrială; Revista „Univers Strategic", editată de Universitatea Creştină „Dimitrie Cantemir" - Institutul de Studii de Securitate, cu apariţie trimestrială (a se vedea nr. 2, iunie

făcut, în mod deosebit, de către reprezentanţii structurilor executive ale statului, cu obligaţii directe stabilite prin legi şi alte acte normative în domeniul securităţii şi al managementului crizelor.

1. Abordări NATO în „Conceptul Strategic - Lisabona 2010"

Pentru că în recentul document al NATO **„Conceptul Strategic"** adoptat la Lisabona în noiembrie 2010 se face o evaluare a Conceptului Strategic, apreciată ca fiind corectă şi acceptată de statele membre, consider necesar să subliniez acele pasaje care au un impact direct asupra securităţii colective, cât şi asupra sistemelor de management a crizelor din toate statele membre, inclusiv România, astfel:

- „Deşi în zona euroatlantică este pace, iar ameninţarea unui atac convenţional împotriva teritoriului NATO este redusă, riscul există":
  - ✓ multe ţări din diferite regiuni deţin capabilităţi militare moderne;
  - ✓ proliferarea rachetelor balistice, precum şi proliferarea armelor nucleare şi a altor arme de distrugere în masă, constituie ameninţări reale la adresa securităţii;
  - ✓ terorismul constituie o ameninţare directă la adresa securităţii cetăţenilor ţărilor Alianţei precum şi la stabilitatea şi prosperitatea internaţională. Tehnologia modernă duce la creşterea potenţialului teroriştilor de a produce distrugeri;
  - ✓ dependenţa de reţelele de calculatoare face ca guvernele şi economiile să fie vulnerabile în cazul unor atacuri cibernetice, fapt ce devine tot mai frecvent;
  - ✓ ţările depind tot mai mult de rutele de comunicaţii, de transport şi de tranzit pe care se desfăşoară comerţul, inclusiv furnizarea energiei; acest fapt sporeşte vulnerabilităţile pentru ţările membre NATO;
  - ✓ dezvoltarea tehnologiei, inclusiv în spectrul electronic, folosirea laserelor şi posibila limitare a accesului în spaţiu cosmic pot afecta, de asemenea, planificarea militară şi operaţiile NATO;
  - ✓ instabilitatea sau conflictul dincolo de frontierele Alianţei pot ameninţa securitatea naţiunilor NATO, iar factorii globali precum competiţia crescută pentru resurse, schimbările climatice şi influenţa factorilor de sănătate pot afecta negativ mediul de securitate.

Riscurile prezentate în **„Conceptul Strategic NATO"** afectează direct sau indirect şi România, fapt pentru care analiza realităţilor globale, zonale şi regionale trebuie să facă obiectul atenţiei factorilor responsabili care, prin legislaţie şi acţiuni practice să pună în valoare resurse umane, materiale şi financiare, pentru protejarea vieţii cetăţenilor şi bunurilor acestora. Constituirea şi consolidarea unui **„Sistem Naţional de Management al Situaţiilor de Urgenţă" (S.N.M.S.U)** este elementul principal, fără de care, în aceste vremuri, statul român poate avea probleme grave (despre acest subiect vom încerca să prezentăm unele plusuri dar şi minusuri la nivelul anului 2011).

În continuare nu vom insista asupra capabilităţilor militare ale Alianţei, prezentate în **„Conceptul Strategic",** dar vom sublinia acele prevederi care au

2010); Revista Geopolitica, editată de Asociaţia de Geopolitică „Ion Conea" (www.geopolitic.ro).

relevanţă în managementul crizelor, în principal în aspecte nonmilitare, care trebuie avute în vedere, din punct de vedere organizaţional, uman şi financiar de către fiecare stat membru în parte:

- Alianţa va trebui să răspundă la apariţia oricăror ameninţări şi provocări;
- Alianţa va trebui să fie pregătită să acţioneze o gamă de instrumente şi să coopereze cu alţi actori pentru a contribui la o abordare comprehensivă ce va combina eficient elemente politice, civile şi militare pentru o realizare deplină a obiectivelor sale de securitate.
- Sprijinul eforturilor de reformă în sectoarele de securitate şi apărare; acesta poate include şi angajamente de sprijin al contractorilor;
- Este posibil ca eforturile de stabilizare şi reconstrucţie să fie necesare în toate fazele crizei. Prin urmare, Alianţa trebuie să aibă capacitatea de a planifica, pregăti şi desfăşura activităţi de reconstrucţie şi dezvoltare.
- Capacităţile C3 sunt facilităţi cheie (pivotal enablers) pentru îndeplinirea flexibilă şi eficientă a obiectivelor de securitate ale Alianţei. Acest fapt necesită definirea şi implementarea unei strategii C3 clare ce va asigura o consultare consistentă şi funcţii de comandă, robuste, flexibile şi măsurabile. Sistemele C3 ar trebui să beneficieze de cele mai recente tehnologii, precum şi de cele prevăzute a fi dezvoltate în viitor. Totuşi, astfel de aranjamente vor fi eficiente doar dacă vor fi adoptate la scară largă de aliaţi, folosind aceeaşi filosofie de bază, în special în ceea ce priveşte gradul în care ei sunt pregătiţi să împartă informaţii sensibile sau să permită accesul la acestea prin mecanisme care depind de accesul tehnologic între federaţii de reţele. Este vorba, în final, de disponibilitatea naţiunilor de a face posibilă o capabilitate facilitată de reţea NATO (Network Enabled Capability).
- Planificarea NATO, dar şi a naţiunilor, ar trebui să ţină cont şi de efectele potenţiale ale accesului aliaţilor la rutele de comunicaţii, tranzit şi transport vitale, furnizarea energiei, probabilitatea atacurilor cibernetice asupra sistemelor informatice sau altor sisteme vitale ale naţiunilor Alianţei; probabilitatea ca teroriştii să fie capabili să folosească mijloace tot mai sofisticate în îndeplinirea scopurilor lor în viitor.
- NATO va avea drept scop reducerea impactului strategic al ameninţărilor asimetrice cu mijloace explozive improvizate (IED).
- Interoperabilitatea este un factor de multiplicare care va permite Alianţei dezvoltarea în parteneriat a unui pachet de capabilităţi/forţe, capabile să desfăşoare acţiuni de luptă în orice mediu.
- NATO va monitoriza sistematic accesul restricţionat şi deficitul de resurse energetice, naturale, de apă / hrană, de informaţii şi umane.
- Alianţa trebuie să aibă o capabilitate proprie pentru evaluarea şi controlul impactului tehnologiilor, expertizei comunităţii tehnice şi ştiinţifice, a provocărilor şi a capabilităţilor de informaţii ale comunităţii internaţionale în domeniul securităţii, cu referire la: evaluarea mediului operaţional, potenţialul distructiv al tehnologiilor emergente, a influenţei asupra capabilităţilor de apărare şi descurajare ale Alianţei.
- Calitatea de membru al Alianţei, atrage după sine şi distribuţia echitabilă a rolurilor, riscurilor şi responsabilităţilor. În acest context, bugetul alocat apărării din cadrul PIB-ului naţional, precum şi procentajul alocat din acest buget cheltuielilor cu înzestrarea sunt indicatori ai efortului unui stat membru în domeniul apărării. În principiu se recomandă ca statele membre să aloce în mod constant 2 % din PIB sau mai mult pentru apărare (n.a. - oare cum stă România la acest capitol?!!).

Ţărilor membre care în mod frecvent alocă resurse sub acest procent, li se recomandă să stopeze acest lucru şi să crească nivelul alocaţiilor bugetare, conform angajamentelor asumate.

- Eficienţa costurilor va continua să fie un factor de o importanţă

deosebită. Acest lucru impune (şi pentru România) o prioritizare a investiţiilor, creşterea eficienţei din punct de vedere al costurilor în operaţii şi pentru mentenanţă, precum şi redirecţionarea resurselor alocate structurilor şi programelor învechite către alte priorităţi.

- Pentru creşterea eficienţei din punct de vedere al costurilor, se recomandă, de asemenea, folosirea pârghiilor cooperării multinaţionale în folosirea fondurilor alocate şi pentru realizarea unora care sunt imposibil de realizat de către un singur membru. Se vor încuraja abordările şi cooperarea multinaţională în domeniul înzestrării, instruirii şi educaţiei, a sprijinului logistic, crearea de mari unităţi multinaţionale, precum şi de dezvoltare a unor capabilităţi civile, care să determine creşterea interoperabilităţii şi a planificării şi execuţiei operaţiilor, chiar dacă în acest context există o serie de obstacole tehnice şi legale în acest sens (cerinţe legislative, prevederi diferite referitoare la offsetul industrial, existenţa unor acorduri şi termeni diferiţi în privinţa cooperării dintre forţele armate aparţinând altor ţări, precum şi dintre forţele armate şi societatea civilă a aceleiaşi ţări), pentru dezvoltarea de capabilităţi la costuri reduse.
- Folosirea eficientă a resurselor critice impun ca statele NATO şi ale UE să identifice / dezvolte capabilităţi comune ambelor organizaţii.

2. Starea instituţională, operaţională şi tehnică din România, în domeniul managementului crizelor:

a. România, aflată în plin proces de tranziţie, nu s-a putut concentra cu suficientă atenţie asupra construirii unui sistem închegat, coerent şi eficient de management al crizelor. La această realitate s-a adăugat lipsa cronică de resurse şi unele dispute interinstituţionale pornite de la considerarea locului şi rolului instituţiilor cu atribuţii în domeniu.

Totuşi s-au făcut studii şi analize privind factorii de risc la adresa securităţii naţionale (militari, nonmilitari, economici etc.) şi s-a dezvoltat limitat infrastructura de lucrări civile, comunicaţii şi informatică, mijloace speciale de intervenţie la Ministerul Administraţiei şi Internelor, Ministerul Apărării Naţionale, Serviciul Român de Informaţii, Serviciul de Telecomunicaţii Speciale (fără a avea încă un caracter coerent şi unitar).

Se poate sublinia progresul remarcabil în domeniul reţelelor de comunicaţii fixe şi mobile aflate sub autoritatea de reglementare a Ministerului Comunicaţiilor şi Tehnologiei Informaţiilor. Astfel, au apărut după anul 1995 reţelele de telefonie mobilă Connex, Orange, Zapp, Cosmorom, iar în anul 1997 a fost privatizată Societatea Naţională de Telecomunicaţii Romtelecom S.A., cu efecte pozitive asupra modernizării reţelelor.

Capacităţile reţelelor de comunicaţii şi informatică de stat (M.A.I, M.Ap.N, S.T.S) şi ale reţelelor comerciale, permit deja, cu puţine eforturi financiare, realizarea suportului tehnic necesar conducerii, cooperării şi înştiinţării în cadrul "Sistemului Naţional de Management al Situaţiilor de Urgenţă" (în condiţiile în care aceste instituţii sunt obligate să coopereze).

b. În unele documente elaborate după anul 2003 autorităţile române, precum şi unii analişti politico-militari au identificat principalii factori de risc la adresa securităţii şi stabilităţii României, astfel:

- existenţa în plan regional sau subregional a unor tensiuni şi conflicte militare ce se pot extinde, precum şi a unor acumulări necontrolate şi destabilizatoare de forţe şi tehnică de luptă în spaţiul de interes strategic al României;
- proliferarea şi diseminarea necontrolată a tehnologiilor şi materialelor nucleare, a mijloacelor de distrugere în masă, a armamentelor şi altor mijloace letale neconvenţionale;
- prelungirea unor dificultăţi interne de natură economică, financiară şi socială care afectează critic şi vital funcţionarea societăţii româneşti (în special datorate amatorismului deciziilor economice majore);
- expansiunea reţelelor şi

activităţilor teroriste şi a crimei organizate transnaţionale (terorism politic, terorism pe baze etnice, criminalitate economico-financiară, trafic transfrontalier ilegal de persoane, trafic de droguri, de materiale radioactive şi strategice, de armament şi muniţii etc.);

- deteriorarea mediului ambiant, prin nerespectarea normelor ecologice, precum şi existenţa în proximitatea frontierelor naţionale a unor obiective cu grad ridicat de risc;
- catastrofele naturale de proporţii (cutremure, inundaţii, incendii etc.);
- limitarea accesului statului român la unele resurse vitale pentru populaţie şi economie (în special resurse energetice);
- acţiuni ce pot aduce atingere statului român şi instituţiilor democratice, care conduc la separatism, xenofobie, intoleranţă şi conflicte etnice şi religioase.

Desigur că evoluţiile politice, economice şi sociale din ultima perioadă, între care menţionăm integrarea României în NATO (aprilie 2004) şi integrarea în Uniunea Europeană (ianuarie 2007) impun o reanalizare a factorilor de risc, în noul context. Se observă că importanţa unora scade, a altora creşte şi apar noi factori de risc şi noi ameninţări, de genul atacurilor teroriste de amploare. De fapt, aceste schimbări se reflectă parţial şi în O.U. nr. 21/15.04.2004 (Legea nr. 15/2005).

c. În România, la data de 14.04.2004 (anterior adoptării O.U. nr. 21/ 15.04.2004) următoarele instituţii aveau atribuţii privind managementul crizelor:

- ✓ Preşedinţia României;
- ✓ Consiliul Suprem de Apărare al Ţării;
- ✓ Guvernul României;
- ✓ Ministerul Administraţiei şi Internelor, cu structurile subordonate:
  - Inspectoratul General al Poliţiei;
  - Inspectoratul General al Poliţiei de Frontieră;
  - Comandamentul Naţional al Jandarmeriei;
  - Comandamentul Protecţiei Civile;
  - Comandamentul Naţional al Pompierilor;
  - Serviciile publice comunitare pentru situaţii de urgenţă.
- ✓ Ministerul Apărării Naţionale, cu marile unităţi şi unităţile din subordine, din Forţele Terestre, Forţele Aeriene şi Forţele Navale, precum şi forţele şi mijloacele destinate realizării şi exploatării sistemului de comunicaţii şi informatic strategic (STAR);
- ✓ Ministerul Afacerilor Externe;
- ✓ Ministerul Transporturilor, Construcţiilor şi Turismului;
- ✓ Ministerul Economiei şi Comerţului;
- ✓ Ministerul Agriculturii, Pădurilor şi Dezvoltării Rurale;
- ✓ Ministerul Mediului şi Gospodăririi Apelor;
- ✓ Ministerul Sănătăţii;
- ✓ Ministerul Comunicaţiilor şi Tehnologiei Informaţiei;
- ✓ Serviciul Român de Informaţii;
- ✓ Serviciul de Telecomunicaţii Speciale;
- ✓ Serviciul de Protecţie şi Pază;
- ✓ Oficiul Central de Stat pentru Probleme Speciale.

d. Responsabilităţile instituţiilor menţionate la punctul 3 în domeniul managementului situaţiilor de urgenţă au fost şi sunt încă reglementate în legi, Ordonanţe de Urgenţă şi Hotărâri de Guvern (care în termen de 180 de zile de la publicarea O.U. nr. 21/15.04.2004, respectiv la data de 26.10.2004, ar fi trebuit modificat, abrogate sau completate). Acest proces nu a fost încheiat încă nici în 2011. Este vorba de aproximativ 20 de acte normative necesar a fi armonizate.

e. Din analiza comparativă a legilor şi altor acte normative menţionate la punctul d, precum şi a legilor care reglementează organizarea şi funcţionarea instituţiilor menţionate la punctul c se desprind o serie de concluzii:

- există un număr excesiv de mare de reglementări (de ordinul zecilor), adesea confuze şi contradictorii;
- se referă doar la o parte din situaţiile de urgenţă ce pot apare (catastrofe naturale, incendii, accidente diverse);
- instituie o serie de comisii care nu au activitate permanentă, cu o mică putere de decizie şi fără resurse specifice;
- sistemul legislativ în vigoare dispersează prea mult responsabilităţile instituţiilor, astfel că în situaţii de urgenţă fie că se acţionează greşit, fie nu se cooperează, fie că se calcă pe picioare;
- sunt slab definite relaţiile instituţionale, sistemele de comunicaţii şi informatică, organizarea şi desfăşurarea acţiunilor de prevenire. Nu există încă echipamente specifice unei game largi de intervenţii;
- de fapt nu putem vorbi, sub nici o formă de un sistem instituţional închegat, cu responsabilităţi bine definite, chiar dacă Legea 15 / 2005 ar trebui să îşi facă efectul.

f. Din punct de vedere operaţional şi tehnic unele ministere şi organe centrale dispun de lucrări civile (clădiri şi amenajări specifice), centre de comandă, sisteme de comunicaţii şi informatică digitale de voce, date şi videoconferinţă, care, printr-un efort conjugat, pot fi utilizate pentru a asigura resursele tehnice necesare conducerii, cooperării şi înştiinţării în cadrul "Sistemului Naţional de Management al Situaţiilor de Urgenţă".

g. Realităţile interne prezentate pe scurt la punctul 2, precum şi elementele prezentate în expunerea de motive la Ordonanţa de Urgenţă 21/15.04.2004 (Legea 15/2005) se constituie în argumente pertinente pentru consolidarea organizatorică şi tehnică a noului „Sistem Naţional de Management al Situaţiilor de Urgenţă". Acţiunea a început în anul 2005 şi este încă în desfăşurare, cu resurse materiale şi financiare limitate (procesul, în elementele sale principale, este departe de a fi încheiat).

În acest proces de consolidare trebuie să aibă în vedere şi:

- apariţia unor noi factori de risc şi ameninţări care pot afecta România, între care se evidenţiază acţiunile teroriste de amploare;
- modificarea ponderii şi posibilităţii producerii unor evenimente grave din cadrul paletei de factori de risc analizaţi;
- existenţa unui cadru legislativ stufos şi confuz, care, pe baza experienţei proprii şi a celei europene, trebuie modificat (operaţiune foarte dificilă);
- existenţa unui cadru instituţional stabilizat (ministere, organe centrale, servicii publice, administraţie locală) care pot primi, prin lege, atribuţii specifice în cadrul unui "Sistem Naţional de Management al Situaţiilor de Urgenţă" unitar şi care pot fi obligate să coopereze, în scopul îndeplinirii obiectivelor stabilite (chiar dacă acestea nu doresc);
- persistenţa, până la această dată, a unui sistem instituţional neînchegat, în domeniul managementului, prevenirii şi gestionării situaţiilor de urgenţă (se referă doar la unele instituţii şi acţiuni);
- condiţii materiale favorabile datorate în principal existenţei:
  - ✓ lucrărilor civile la ministere şi organe centrale (clădiri, locuri pentru centre operative);
  - ✓ sistemelor şi reţelelor de comunicaţii şi informatică moderne guvernamentale, militare şi ale operatorilor comerciali;
  - ✓ echipamentelor specifice diferitelor intervenţii (vechi şi limitate calitativ);
- capacităţii manageriale şi tehnice pentru captarea corectă a cerinţelor sistemului, stabilirea fluxurilor informaţionale şi elaborarea aplicaţiilor software specifice pentru gestionarea bazelor de date şi elaborarea planurilor de intervenţie (aflate la această dată în dezvoltare).

3. Definirea obiectivelor pentru consolidarea „Sistemului Naţional de Management al Situaţiilor de Urgenţă”

a. Ţinând seama de complexitatea “Sistemului Naţional de Management al Situaţiilor de Urgenţă”, de numărul mare de instituţii, forţe şi mijloace implicate, de reglementările internaţionale în materie la care România este parte (ONU, NATO, UE, tratate), de realităţile interne (legislative, instituţionale, operaţionale şi tehnice) şi resursele disponibile, în termen scurt şi mediu pot fi avute în vedere următoarele obiective principale:

- studierea şi evaluarea legislaţiei în materie din ţările membre NATO şi ale Uniunii Europene;
- reevaluarea legislaţiei interne în vederea modificării, completării sau, după caz, al abrogării unor prevederi (în regim de urgenţă);
- studierea experienţei autohtone în situaţii de intervenţii în caz de calamităţi naturale, accidente grave, alte situaţii (lecţiile învăţate);
- inventarierea resurselor umane, materiale şi financiare ale instituţiilor cu atribuţii în domeniul managementului crizelor, în scopul evitării unor cheltuieli inutile (am arătat deja că există multe resurse de luat în seamă);
- proiectarea şi realizarea lucrărilor de interoperabilitate a sistemelor şi reţelelor de comunicaţii şi informatică existente, şi, acolo unde este cazul, completarea cantitativă şi calitativă a acestora. Echiparea corespunzătoare a centrelor operaţionale şi operative şi realizarea unor aplicaţii software performante;
- definirea relaţiilor dintre instituţii, a fluxurilor informaţionale şi a conţinutului principalelor documente care vor trebui elaborate şi care vor circula în sistem (necesită o muncă de analiză şi coordonare foarte dificilă);
- analiza, realizarea şi implementarea bazelor de date necesare funcţionării sistemului:
  - ✓ zonele de inundaţii şi barajele;
  - ✓ zonele seismice;
  - ✓ instalaţiile industriale periculoase;
  - ✓ instalaţiile nucleare din România şi din ţările vecine cu potenţial de pericol;
  - ✓ forţele şi mijloacele de intervenţie pe scenarii şi situaţii de urgenţă posibile, inclusiv necesarul de echipamente specifice;
  - ✓ date obligatorii pentru funcţionarea sistemelor de comunicaţii şi informatică (capacitate, dispunere, datele de lucru, cărţi de telefon, cărţi de adrese e-mail, alte documente);
  - ✓ orice alte date care se cristalizează pe parcursul anilor (lecţiile învăţate);
- elaborarea, într-o primă formă a unor regulamente, planuri, programe, documente operative, memoratoare, instrucţiuni de lucru pentru personalul de intervenţie (supuse analizei şi propunerilor structurilor parte la „Sistem...”);
- consolidarea instituţională, operaţională şi tehnică reală a “Sistemului Naţional de Management al Situaţiilor de Urgenţă” integrat, stabilirea relaţiilor de lucru şi desfăşurarea unor exerciţii

pentru pregătirea personalului şi învăţarea corectă a instrucţiunilor. (prin aplicaţii anuale);

- reevaluarea funcţionării sistemului după şase luni de la punerea în funcţiune a elementelor principale, în vederea aducerii corecturilor necesare;
- adaptarea permanentă la realităţile internaţionale şi interne în domeniul managementului crizelor.

b. În concluzie, obiectivele menţionate, dar şi altele care pot fi identificate pe timpul proiectării **"Sistemului Naţional de Management al Situaţiilor de Urgenţă"** (în special în definirea interrelaţiilor instituţionale şi a platformei de comunicaţii şi informatică, a bazelor de date şi a aplicaţiilor software specifice) pot şi trebuie să fie abordate în contextul internaţional în care România activează (ONU, NATO, UE), în scopul realizării obiectivelor de eficienţă şi interoperabilitate necesare.

4. Definirea domeniilor de risc

a. Considerăm că înainte de a defini domeniile de risc, specifice în această perioadă în România, să definim termenii utilizaţi, conform Ordonanţei de Urgenţă nr. 21/2004 (Legea 15/2005), astfel:

- ✓ "Sistemul Naţional de Management al Situaţiilor de Urgenţă" se înfiinţează, se organizează şi funcţionează pentru prevenirea şi gestionarea situaţiilor de urgenţă, asigurarea şi coordonarea resurselor umane, materiale, financiare şi de altă natură necesare stabilirii stării de normalitate;
- ✓ "Sistemul Naţional de Management al Situaţiilor de Urgenţă" este organizat de autorităţile administraţiei publice şi se compune dintr-o reţea de organisme, organe şi structuri abilitate în managementul situaţiilor de urgenţă, constituite pe niveluri sau domenii de competenţă, care dispune de infrastructură şi resursele necesare pentru îndeplinirea atribuţiilor prevăzute în lege;
- ✓ Situaţie de urgenţă – eveniment excepţional, cu caracter nonmilitar, care prin amploare şi intensitate ameninţă viaţa şi sănătatea populaţiei, mediul înconjurător, valorile materiale şi culturale importante, iar pentru restabilirea stării de normalitate sunt necesare adoptarea unor măsuri şi acţiuni urgente, alocarea de resurse suplimentare şi managementul unitar al forţelor şi mijloacelor implicate;
- ✓ Amploarea stării de urgenţă – mărimea ariei de manifestare a efectelor distructive ale acesteia în care sunt ameninţate sau afectate viaţa persoanelor, funcţionarea instituţiilor statului democratic, valorile şi interesele comunităţii;
- ✓ Intensitatea situaţiei de urgenţă – viteza de evoluţie a fenomenelor distructive şi gradul de perturbare a stării de normalitate;
- ✓ Starea potenţial generatoare de situaţii de urgenţă – complex de factori de risc care prin evoluţia lor necontrolată şi iminenţa ameninţării ar putea aduce atingere vieţii şi populaţiei, valorilor materiale şi culturale importante şi factorilor de mediu;
- ✓ Iminenţa ameninţării – parametrii de stare şi timp care determină declanşarea inevitabilă a unei situaţii de urgenţă;
- ✓ Starea de alertă – se declară potrivit legii şi se referă la punerea de îndată în aplicare a planurilor de acţiuni şi măsuri de prevenire, avertizare a populaţiei, limitare şi înlăturare a consecinţelor situaţiei de

urgenţă;

- ✓ Managementul situaţiei de criză – ansamblul activităţilor desfăşurate şi procedurile utilizate de factorii de decizie, instituţiile şi serviciile publice abilitate pentru identificarea şi monitorizarea surselor de risc, evaluarea informaţiilor şi analiza situaţiei, elaborarea de prognoze, stabilirea variantelor de acţiune şi implementarea acestora în scopul restabilirii situaţiei de normalitate;
- ✓ Monitorizarea situaţiei de urgenţă – proces de supraveghere necesar evaluării sistematice a dinamicii parametrilor situaţiei create, cunoaşterii tipului, amploarei şi intensificării evenimentului, evoluţiei şi implicaţiilor sociale ale acestuia, precum şi a modului de îndeplinire a măsurilor dispuse pentru gestionarea situaţiei de urgenţă;
- ✓ Factor de risc – fenomen, complex sau proces de împrejurări congruente, în acelaşi timp şi spaţiu, care pot determina sau favoriza producerea unor tipuri de risc;
- ✓ Gestionarea situaţiilor de urgenţă – identificarea, înregistrarea şi evaluarea tipurilor de risc şi a factorilor determinanţi ai acestora, înştiinţarea factorilor interesaţi, avertizarea populaţiei, limitarea, înlăturarea sau contracararea factorilor de risc, precum şi a efectelor negative şi a impactului produs de evenimentele excepţionale respective;
- ✓ Intervenţia operativă – acţiunile desfăşurate, în timp oportun, de către structurile specializate în scopul prevenirii agravării situaţiei de urgenţă, limitării şi înlăturării, după caz, a consecinţelor acesteia;
- ✓ Evacuarea – măsură de protecţie luată în cazul ameninţării iminente, stării de alertă, ori producerii unei stări de urgenţă şi care constă în scoaterea din zonele afectate sau potenţial a fi afectate, în mod organizat, a unor instituţii publice, agenţi economici, categorii sau grupuri de populaţie ori bunuri şi dispunerea acestora în zone şi localităţi care asigură condiţii de protecţie a persoanelor, bunurilor şi valorilor, de funcţionare a instituţiilor publice şi agenţilor economici;

b. Domeniile (factorii) de risc în accepţiunea legii sunt:

- ✓ incendii, cu referire la cele de proporţii în zone împădurite, unităţi industriale, localităţi etc.;
- ✓ cutremure, cu referire la cele cu potenţial distructiv, în zonele seismice identificate pe teritoriul României (curbura Arcului Carpatic – Vrancea, Banat). Aceste mişcări seismice au efecte grave în estul şi sudul ţării, aşa cum au demonstrat evenimentele din 1940 şi 1977;
- ✓ inundaţii de mare amploare în bazinele hidrografice a unor cursuri de apă fără amenajări hidrotehnice sau cu lucrări nesatisfăcătoare (Mureş, Olt, cele trei râuri Someş, Prutul, Siretul, Bistriţa şi uneori chiar Dunărea);
- ✓ accidente diferite, de amploare;
- ✓ explozii accidentale sau provocate în unităţi industriale sau pe timpul transportului unor substanţe periculoase;
- ✓ avarii la instalaţii industriale, lucrări hidrotehnice, lucrări civile etc.;
- ✓ alunecări sau prăbuşiri de teren datorate unor inundaţii sau cutremure;
- ✓ îmbolnăviri în masă datorate

unor cauze externe sau a unor fenomene interne ce ţin de condiţiile de mediu şi de viaţă;
- ✓ prăbuşiri ale unor construcţii, instalaţii sau amenajări, ca efect al unor greşeli de construcţie sau a calamităţilor naturale sau acţiunilor teroriste;
- ✓ eşuarea sau scufundarea unor nave, în spaţiul maritim sau pe fluviul Dunărea, ca urmare a unor evenimente diverse;
- ✓ căderi de obiecte din atmosferă ori din cosmos;
- ✓ tornade;
- ✓ avalanşe;
- ✓ eşecuri de amploare a serviciilor de utilităţi publice;
- ✓ alte calamităţi naturale;
- ✓ sinistre grave sau evenimente publice de amploare determinate ori favorizate de factori de risc specifici;
- ✓ acţiuni teroriste care vizează obiective pe teritoriul românesc, inclusiv luarea de ostatici, în ţară sau în străinătate;
- ✓ accidente nucleare la obiective din ţară sau din ţările vecine (în special Ucraina şi Bulgaria);
- ✓ alte evenimente care nu pot fi prevăzute la această dată.

c. În concluzie se poate afirma că Legea nr. 15/2005 defineşte domeniile (factorii) de risc pe baza experienţei dobândite până acum şi a realităţilor prezente din lume, din Europa şi din România. Factorii de risc îşi schimbă, în timp, ponderea şi probabilitatea de a deveni ameninţări reale, iminente.

5. Realizarea şi adoptarea deciziei privind responsabilităţile principale pentru fiecare domeniu de risc definit

a. În România, în perioada 1990-2009 au existat mai multe încercări pentru a legifera şi realiza un sistem unitar pentru managementul crizelor. Aceste demersuri nu s-au finalizat din mai multe cauze:

- Parlamentul şi Guvernul nu au considerat problema ca fiind o prioritate;
- diverse grupări politice şi partide au avut puncte de vedere opuse în privinţa unor principii şi reguli;
- ministere şi organe centrale au dorit (şi din păcate doresc încă) să-şi sporească, consolideze şi perpetueze atribuţii specifice şi în acest domeniu, fără a ţine seama de realităţi şi experienţa internaţională în domeniu (lipseşte încă dorinţa de cooperare deschisă în interesul ţării şi al cetăţenilor ei);
- ministerele şi organele centrale nu au făcut (şi nu fac încă) schimb de informaţii pentru a pune "în coşul comun" resursele necesare realizării cu costuri minime a "Sistemului Naţional de Management al Situaţiilor de Urgenţă";
- experienţa din ţările NATO a fost studiată superficial sau deloc şi nu au fost trase concluzii pertinente cu aplicabilitate într-un sistem autoritar;
- numeroase modificări instituţionale, mai ales în aria de responsabilitate a Ministerului Administraţiei şi Internelor, nu au creat climatul de stabilitate necesar şi nu au permis unor specialişti români să propună un "Sistem Naţional de Management al Situaţiilor de Urgenţă" valabil;
- mijloacele materiale şi financiare disponibile au fost insuficiente.

b. În primăvara anului 2004, ca urmare a evoluţiilor politice internaţionale şi pe plan intern, precum şi a cerinţelor NATO şi UE, guvernul României a solicitat ministerelor şi organelor centrale să ajungă la un consens asupra principiilor, obiectivelor şi acţiunilor ce trebuie adoptate pentru a pune în operă un "Sistem Naţional

de Management al Situaţiilor de Urgenţă" integrat, eficient.

Rezultatul efortului a fost elaborarea şi adoptarea Ordonanţei de Urgenţă nr. 21/2004, privind "Sistemul Naţional de Management al Situaţiilor de Urgenţă", care, la această dată reprezintă actul normativ de bază, în domeniu. Cu toate că O.U.G 21/2004 stabileşte termene pentru modificări legislative şi acţiuni practice, acestea nu au fost respectate până acum.

c. În privinţa realizării consensului şi adoptarea unor decizii corecte şi unanim acceptate referitor la responsabilităţile principale pentru fiecare domeniu (factor) de risc definit, sunt de presupus eforturi şi acţiuni în perioada următoare, concretizate prin elaborarea de regulamente, planuri, programe, instrucţiuni etc. În acest demers experienţa occidentală este foarte importantă, atât în abordarea fondului problemelor, cât şi în forma reprezentării documentelor.

- ✓ **ROŞU** – de coordonare generală – Primul-ministru;
- ✓ VERDE – de conducere operaţională la nivelul ţării – Comitetul Naţional pentru Situaţii de Urgenţă, sub conducerea ministrului administraţiei şi internelor;
- ✓ **ALBASTRU** – de conducere la nivel departamental şi local – comitetele ministeriale, municipale, orăşeneşti, comunale;
- ✓ **GALBEN** – de execuţie, cu rol principal – ministerul (organizaţia) care dispune de forţe şi mijloace adecvate evenimentului produs;
- ✓ **MARO** – de execuţie, cu rol secundar – ministerele (organizaţiile) care acordă sprijinul uman şi logistic factorului de execuţie secundar.

MINISTERUL (ORGANIZAȚIA)		FACTORUL DE RISC	INCENDII	CUTREMURE	ACCIDENTE	IMBOLNAVIRI IN MASĂ	AVARII INDUSTRIALE	SCUFUNDARI (EŞUĂRI) DE NAVE	ATENTAT TERORIST	EŞECUL SERVICIILOR DE UTILITĂȚI
Comitetul Național pentru Situații de Urgență										
M.A.I.	Inspectoratul General									
	Servicii publice									
M.Ap.N										
M.A.E			-		-					
M.T.T.C										
M.E.C					-					
M.A.P.D.R					-					
M.M.G.A					-					
M.S.										
M.C.T.I										
S.R.I										
S.T.S										
S.P.P					-	-	-	-		-
O.C.S.P.S					-					
Alte organizații (de la caz la caz)										

d. În funcţie de natura, amploarea şi efectele situaţiilor de urgenţă, instituţiile şi structurile definite de lege ca parte integrantă a "Sistemului Naţional de Management al Situaţiilor de Urgenţă" îndeplinesc următoarele funcţii:

e. Un exemplu pentru unele situaţii de urgenţă, care generează evenimente grave şi care impun cooperarea interinstituţională potrivit legii, poate fi:

i. Analiza privind rolul şi locul instituţiilor, precum şi a forţelor special destinate pentru intervenţii, în funcţie de caracterul evenimentului produs, poate fi extinsă la întreaga gamă de factori de risc şi ameninţări posibile la un anumit moment. Un element de sprijin poate fi şi experienţa din unele ţări occidentale care au sisteme de management al crizelor bine puse la punct (SUA, CANADA, FRANŢA, GERMANIA, BELGIA etc.).

f. O prezentare schematică a compunerii S.N.M.S.U şi interrelaţiilor dintre acestea se prezintă în anexa nr.1.

Ca o concluzie finală analiza şi evaluarea periodică a problematicii complexe a Managementului crizelor (de orice natură) trebuie să rămână în atenţia autorităţilor desemnate de lege, dar şi în preocuparea specialiştilor din mediul ştiinţific, capabili şi dornici să-şi aducă o contribuţie reală în folosul comunităţii.

Totodată, respectarea cu bună credinţă a angajamentelor României ca membru ONU, NATO şi UE în domeniul securităţii şi managementului crizelor, reprezintă o condiţie esenţială a prestigiului unei ţări democratice moderne.

BIBLIOGRAFIE

***Noul „Concept Strategic al NATO", Lisabona, Noiembrie 2010.

***Ordonanţa de Urgenţă Nr. 21 din 15 aprilie 2004 privind „Sistemul Naţional de Management al Situaţiilor de Urgenţă" (devenită Legea nr. 15/2005).

***Materialele publicate în Revista Geopolitică, Anul VI, nr. 27 (3/2008), editată de Asociaţia Geopolitică „ION CONEA".

***Revista „Univers Strategic", nr. 2/2010, editată de Universitatea Creştină „Dimitrie Cantemir" - Institutul de Studii de Securitate.

Dr. Gheorghe Văduva, *Frontierele, securitatea şi efectul de falie.*

Drd. Cristina Vasile Mardale, *Criminalitatea organizată transfrontalieră – o ameninţare în expansiune.*

Comisar Şef Marius Balaban, *Terorismul de stat – o ameninţare la adresa securităţii.*

Drd. Cristian Rădulescu, *Factori de risc la adresa securităţii medicale a populaţiei în situaţii de crize, calamităţi şi dezastre. Gestionarea riscului.*

Prof. univ. dr. Eugen Siteanu, *Conceptul securităţii infrastructurii critice.*

Dumitru Cristea, *Ciberterorismul şi protecţia reţelelor de calculatoare, surse de instabilitate la nivel global şi regional. Implicaţii pentru România.* Ed. U.N.Ap, Bucureşti, 2004.

Constantin Mincu, *Studiu preliminar – versiunea 2.0, „Sistemul Naţional de Management al Situaţiilor de Urgenţă" (SNMSU),* 01.07.2005, comunicat unor autorităţi ale statului român (I.G.S.U. M.Ap.N).

Dr. Teodor Frunzeti, Dr. Vladimir Zodian, *LUMEA 2009, Enciclopedie Politică şi Militară (Studii Strategice şi de Securitate),* AOS-R – Secţia de Ştiinţe Militare, Ed-CTIA, Bucureşti 2009.

Marian Rizea, Daniela Enăchescu, Cristiana Neamţu-Rizea, *Infrastrucuri Critice,* Ed. U.N.Ap, Bucureşti 2010.

James F. Dunnigan, *Noua ameninţare mondială: Cyber-terorismul,* Ed. Curtea Veche, Bucureşti, 2010.

Radu Dan Septimiu Popa, *Războiul Informaţional şi Securitatea Naţională,* Ed. Militară, Bucureşti 2009.

Eugen Bădălan, Mircea Udrescu, Constantin Mincu, *Condiţionări Logistice în Epoca Globalizării,* Ed. A.O.S-R, Bucureşti, 2010.

SERVERELE MAGUAY

Andreea POPESCU

Maguay a început activitatea în domeniul Tehnologiei Informaţiei în 1997, în Bucureşti.

Activitatea principală a companiei se centrează pe integrarea propriilor linii de servere, sisteme desktop şi notebook-uri**.** Sistemele, notebook-urile şi serverele **Maguay** sunt mărci înregistrate şi se adresează utilizatorilor care doresc echipamente performante, fiabile şi stabile precum şi o competentă consultanţă tehnică .

Maguay garantează calitatea produselor sale prin recunoaşterea venită de la două nume mari ale IT-ului mondial: **Intel** şi **Microsoft** şi deţine cele mai importante certificari: **Intel Technology Provider Platinum Partner** şi **Microsoft Partner.**

Sistemele Maguay: servere, PC–uri sau notebook–uri, se remarca print-o serie de avantaje:

1. Sunt construite întotdeauna pe cele mai noi tehnologii; componentele folosite sunt standardizate, non-proprietare;
2. Sunt **configurabile** în funcție de necesitățile clienților. Din acest motiv, pot fi oricând upgradate, pe parcursul exploatarii lor;
3. Sunt echipamente uşor identificabile, testate, validate și certificate Intel și Microsoft*;* desigur, alături de procedurile interne de validare și certificare;
4. Sunt construite în vederea minimizării **costului total** achiziţie + operare 3 ani de zile
5. Garantie pana la 36 de luni sau chiar mai mult prin extensie; service rapid si prompt executat de oameni bine pregatiti!

De-a lungul timpului am primit o multitudine de premii si recunoasteri din partea celor mai importante redactii media de specialitate.

Maguay este prima companie romaneasca din domeniul IT care a obtinut eticheta ecologica europeana pentru sisteme desktop si laptop.

Sistemele de tip server reprezintă focalizarea principală a activităţii Maguay. Serverele Maguay sunt mărci înregistrate şi nume consacrate pe piaţa românească. În anul 2009, am obtinut statutul de Intel Server Local Leader, fiind o recunoastre pe care Intel o acorda celor mai importanti parteneri. Tot ca o recunoaştere a statutului de integrator de servere este şi premiul oferit de Intel pentru cea mai mare creştere a vânzărilor de servere în 2008, din zona CEE (Europa Centrală şi de Est), acordat în cadrul evenimentului Intel Solution Summit.

În toamnă vom lansa noua linie de servere Maguay **eXpertSERVER**, cu procesoare bazate pe arhitectura Sandy Bridge.

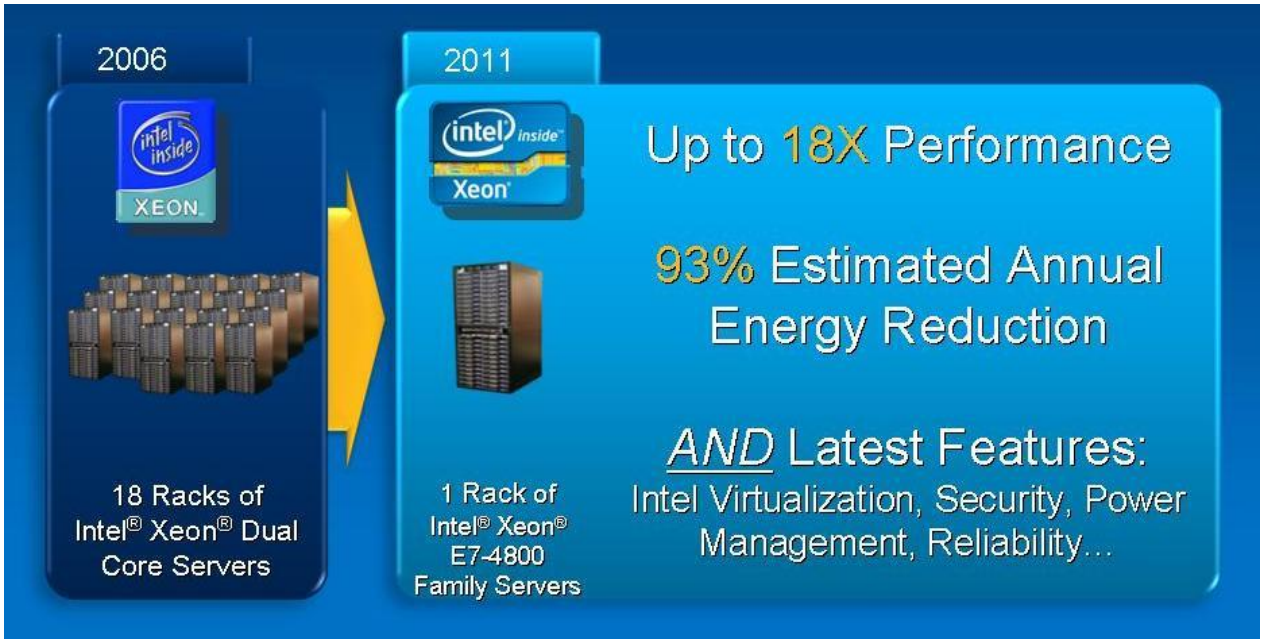
Noile Intel® Xeon® E7-8800/4800/2800 sunt bazate pe tehnologia de productie de 32 nm, detin până la 10 nuclee si Hyper-Threading, 30MB Smart Cache, tehnologii: Turbo-Boost, AES-ni, VT-x, Intel 64, EIST, Execute Disable Bit, Intel TXT, Thermal Monitoring.

Aceste caracteristici asigura o performanta dovedita de benchmark-uri cu 40% mai mare comparativ cu generatia anterioară, ceea ce implica o putere de procesare deosebita si eficienta crescuta in aplicaţiile de computing de înaltă performanţă. De asemenea, ele imbunatatesc multitasking-ul si pot determina analiza unor volume mai mari de date, responsivitate in timp real – astfel incat creeaza premisele mai multor decizii corect informate.

Tehnologiile de virtualizare VT-x incluse in serverele Maguay vor creşte viteza cu 25% comparativ cu generaţia anterioară in mediile virtuale, permitand consolidarea mai multor servere si aplicatii precum si un management imbunatatit. Practic, 18 servere cu procesoare Intel Core vor putea fi inlocuite cu un singur Maguay eXpertSERVER cu procesor Intel Xeon E7, scazand in acelasi timp semnificativ costurile cu consumul de energie.

Noile instrucţiuni de securitate: Intel® Advanced Encryption Standard (AES-NI) permit serverelor să cripteze şi să decripteze rapid date pentru schimbul de informatii confidentiale, în timp ce tehnologia Intel® Trusted Execution (Intel TXT) creează o platformă securizată de boot care protejează aplicaţiile instalate impotriva atacurilor malitioase asigurând astfel integritatea datelor.

EIST, Thermal Monitoring permit reducerea consumului procesorului devenind astfel foarte eficiente din punct de vedere energetic.



Serverele Maguay vor fi lansate in 3 categorii, acoperind toate optiunile posibile:

- Entry-level - monoprocesor, se vor lansa inclusiv in formate Small Form Factor miniITX si procesoare Xeon E3.
- Mainstream - dual-procesor, bazate pe platforme Intel Romley cu 24 sloturi de memorie si 80 magistrale PCI-E generatia 3.0, procesoare Xeon E5.
- High-End - quad-procesor cu procesoare Intel Xeon E7

Cateva tehnologii comune utilizate in noile servere Maguay eXpertSERVER vor fi:

- eUSB SSD – dispozitiv SSD (Solid State Disk) pentru mici sisteme de operare de boot de tip hypervisor
- chip TPM (Trusted Platform Module) cu suport TXT – modul detasabil cu chip STMicro
- Control panel comun pentru toate platformele cu porturi I/O separate, LCP (Local Control Panel) cu display ce afiseaza in mod text pe o linie erorile critice

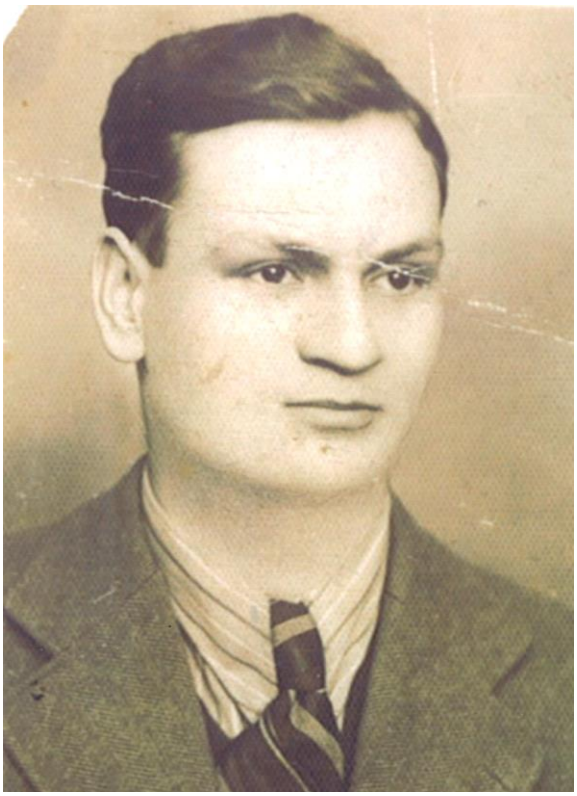
Toate aceste tehnologii reprezinta un nou punct de referinta in dezvoltarea serverelor mission-critical.

RESTITUIRI ISTORICE
O invenţie românească necunoscută – telefonul robot

Ing. Traian BALABAN

Încerc prin această relatare să fac cunoscut armatei române şi transmisioniştilor în mod deosebit că în istoria comunicaţiilor şi perfecţionărilor tehnice a existat o minte de român iscoditoare, în persoana tatălui meu Traian BALABAN, care la vârsta de 21 de ani, în anul 1938, în vremea aceea student la Politehnica din Bucureşti, secţia telecomunicaţii, a conceput şi realizat primul robot telefonic.

Tatăl meu, Traian BALABAN, născut la 24.08.1917 la Focşani, a fost cel mai mic din cei cinci băieţi ai familiei Petre şi Safta Balaban. Primii trei băieţi au



Traian BALABAN

îmbrăţişat cariera militară (Constantin, Dumitru şi Nicolae, respectiv medic militar, armurier şi artilerist terestru), al patrulea Gheorghe Balaban a fost inginer de mine şi petrol, iar tatăl meu a absolvit liceul Unirea din Focşani şi Politehnica din Bucureşti.

În perioada 25.02.1941 - 06.05.1941 a fost concentrat. Pe data de 13.02.1942 a fost trimis pe front ca sergent TR la Comandamentul trupelor de geniu, iar pe 01.11.1942 a căzut prizonier la Cotul Donului. În perioada de prizonierat în URSS 1942-11.06.1948, în lupta pentru supravieţuire în lagărul de la Oranki, a început şi realizat mai multe invenţii şi inovaţii cum ar fi vehicule individuale, dispozitive, tehnică militară. Astfel, dintr-un motor de drujbă a realizat schiuri de stepă cu motor, dublarea periscopului de tanc cu vizor direct cu protecţie mecanică, pistol mitralieră cu 450 cartuşe şi altele. Aceasta i-a adus mutarea din lagărele siberiene (OMSC, Novosibirsk) timp de doi ani în lagărul central de ofiţeri de lângă Moscova, unde datorită aptitudinilor şi meritelor sale a avut libertatea de a-şi organiza o echipă de nemţi, francezi şi austrieci foarte buni specialişti cu care a conceput şi realizat multe proteze mecanice pentru invalizi.

După terminarea războiului datorită preocupărilor avute, a mai fost reţinut o perioadă în lagărul de la Oranki până în 1948 când a revenit în ţară.

Tatăl meu a urmărit în special punerea în practică a ideilor sale, de multe ori cu sacrificii deosebite pentru a-şi realiza concepţiile tehnice, neurmărind obţinerea de brevete sau foloase materiale.

Revenind la conceperea şi realizarea robotului telefonic, acesta prezintă multe asemănări cu roboţii existenţi astăzi, inclusiv numele. Această realizare de excepţie a fost publicată în „Ziarul ştiinţelor şi călătoriilor” nr. 12/1938, colecţia Reviste vechi – Biblioteca naţională drept o invenţie românească graţie căreia orice convorbire telefonică se poate înregistra la domiciliu şi reda apoi în întregime, articol pe care îl redăm integral mai jos.

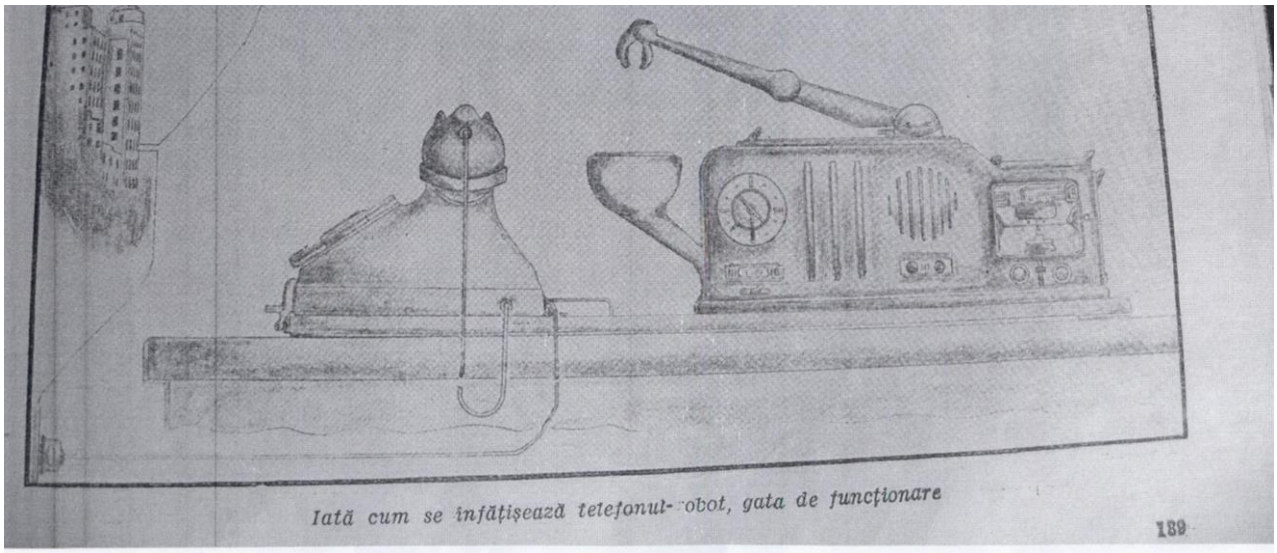
„Dispozitivul acesta, anexat la aparatul telefonic, vine să-l întregească complectamente. Simplu ca închipuire, el este pe atât de uşor de realizat, fiind compus din două părţi: prima electromotrice şi a doua cuprinzând un sistem de înregistrare.

Partea electromotrice se compune dintr'un mic electromotor ce acţionează un sistem de pârghii (robotul propriu zis) cu contacte şi descontacte automate pentru aducerea receptorului în cupele sistemului de înregistrare. În momentul acesta, în „Parlocupă" se stabileşte un contact ce pune în funcţie un gong armonios, caracteristic, anunţând astfel că robotul ascultă. Din acest moment intră în funcţiune partea a doua a dispozitivului. Sunetele primite de „cupa microfon" sunt înregistrate printr'un sistem „Mnemofon Stiehlle" pe un fir de oţel, dispozitiv ce până azi nu avea o întrebuinţare specifică.

Principiul acestui aparat, aşa precum se vede din schema alăturată, constă dintr'un fir de oţel foarte fin, ce înregistrează convorbirea în trecerea lui printre polii unui electro-magnet pus în legătură cu sursa electrică şi microfonul.

Pentru redarea convorbirii e acelaşi sistem, numai că în circuitul de pe firul magnetului se află acum, prin tăierea contactului, numai difuzorul. Se înţelege că pentru aceasta va trebui ca firul să fie luat dela capăt pentru a avea convorbirile în ordinea avută.

Modul de manipulare e extrem de simplu: un indicator ne arată prezenţa convorbirilor înregistrate de aparat, pe care le putem ori când asculta prin punerea în funcţie a difuzorului. Ele se pot păstra oricât timp voim, fără a se uza cu nimic; ceva mai mult, acest fir poate fi întrebuinţat de mii de ori, căci o suprapunere a unei convorbiri noui peste cea anterioară o anulează, fără a şterbi cu nimic din claritatea acesteia din urmă.



Iată cum se înfăţişează telefonul-robot, gata de funcţionare

189

Mărimea lui fiind aproximativ de 15/30 cm, nu-l face incomod atât pe biroul unui ministru supra încărcat, cât şi în budoarul unei doamne elegante."

ACORDAREA DISTINCŢIEI MILITARE CU DENUMIREA ONORIFICĂ „OMUL ANULUI 2010” ÎN COMANDAMENTUL COMUNICAŢIILOR ŞI INFORMATICII

Comandamentul comunicaţiilor şi informaticii

Locotenentul Adrian STAN s-a născut la data de 20.12 1980, în localitatea Sighetu Marmaţiei, judeţul Maramureş, este căsătorit din anul 2007, iar în luna iunie anul acesta va deveni tătic.

Încă din copilărie a fost fascinat de cariera armelor, mai ales după nenumăratele povestiri şi întâmplări relatate de bunicul lui despre luptele celui de-al Doilea Război Mondial unde acesta participase în mod direct, fapt ce l-a determinat ca la sfârşitul cursurilor gimnaziale să urmeze cursurile Liceului Militar din Alba-Iulia.

Datorită calităţilor şi spiritului combativ de care dă dovadă, începând cu anul 2006 a fost implicat şi a participat la toate exerciţiile şi activităţile desfăşurate în cadrul Comandamentului Comunicaţiilor şi Informaticii. Dintre acestea amintim: Exerciţiul „Cetatea 2006”, Exerciţiul „Cetatea 2007”, Summitul NATO (2008), Exerciţiul „Getica 2008”, Exerciţiul „Cetatea 2008”, Exerciţiul „ROUEX 2009”.

Pe lângă activităţile executate în ţară, începând cu anul 2009 a executat un număr de peste 7 misiuni de instalare, mentenanţă şi reconfigurare a sistemului de comunicaţii şi informatică din teatrele de operaţii.

Pentru modul exemplar şi profesionist în care şi-a îndeplinit sarcinile şi misiunile încredinţate în anul 2010, a fost recompensat cu distincţia militară „Omul anului 2010” – Etapa pe Comandamentul Comunicaţiilor şi Informaticii (Locul 1) şi distincţia militară „Omul anului 2010” – la nivelul Statului Major General (Locul 3).

Dintre misiunile executate în anul 2010, amintim câteva:

- a condus şi executat prima misiune de dezinstalare, mutare şi instalare a unui Modul de Comunicaţii şi Informatică Desfăşurabil (MCID) în TO Afganistan cu o echipă formată numai din specialişti militari de comunicaţii;
- a condus 4 misiuni de reconfigurare a sistemului de comunicaţii şi informatic în TO Afganistan, planificând şi organizând într-un mod profesionist aceste misiuni;
- a reprezentat CCI la Exerciţiul multinaţional cu forţe speciale „ROUSOFEX 10”, participând efectiv la planificarea, organizarea şi desfăşurarea acestuia; pentru activitatea desfăşurată a primit aprecieri scrise din partea conducerii exerciţiului şi a şefului Direcţiei operaţii /SMG;
- a îndeplinit responsabilităţi majore în cadrul CCI (managementul TETRA, SCVTC, RCSat, CIS din TO);
- a fost evidenţiat pentru activitatea desfăşurată în TO Afganistan în publicaţia militară „Observatorul militar” nr. 49/2010.

Studii:

- 1996 – 2000 – Liceul Militar "Mihai Viteazul"– Alba Iulia;
- 2000 – 2004 – Academia Forţelor Terestre "Nicolae Bălcescu"– Sibiu;

Cursuri de formare profesională:

- 2004 - 2005 – Curs de bază în arma comunicaţii şi informatică – Şcoala de aplicaţie pentru Transmisiuni, informatică şi război electronic Sibiu;
- 2008 – Curs echipamente videoteleconferinţă – ASSIM;
- 2010 – Curs Echipamente satelitare;
- STANAG limba engleză: 2,2,2,2.

Funcţii:

1. Comandant pluton servicii şi sisteme informatice la Regimentul 47 Transmisiuni al Comandamentului 2 Operaţional Întrunit Buzău - 01.08 2005 – 01.05 2006;
2. Comandant pluton 1 comutaţie în compania 1 centre comunicaţii şi informatică ale punctelor de comandă la Batalionul 47 Comunicaţii şi Informatică al Comandamentului 2 Operaţional Întrunit Buzău – 01.05 - 01.11 2006;
3. Comandant Centru 1 Comunicaţii de sprijin în compania 3 centre comunicaţii de sprijin din Batalionul 3 al Centrului 48 comunicaţii şi informatice strategice – 01.11 2006 – 31.03 2007;
4. Ofiţer 4 la Comenduirea de comunicaţii a municipiului Bucureşti – 31.07 2007 – 01.08 2008;
5. Ofiţer 4 şi 3 în Biroul RMNC /G6 la Comandamentul Comunicaţiilor şi Informaticii, începând cu 01.08 2008.

Comandamentul comunicaţiilor şi informaticii

În urma desfăşurării concursului „OMUL ANULUI 2010" organizat în cadrul Statului Major General, faza pe Comandamentul Comunicaţiilor şi Informaticii, la secţiunea **„Credinţă şi altruism"**, candidatul Comandamentului Comunicaţiilor şi Informaticii, plutonierul adjutant (Com.Infm.) Budulică *Constantin* Marius a obţinut locul I.

Născut la data de 13 octombrie 1971 în Municipiul Roşiori de Vede, Judeţul Teleorman, plutonierul adjutant Budulică Marius este căsătorit din anul 1996 şi are o fiică în vârstă de 11 ani.

După absolvirea Institutului Militar de Transmisiuni "Decebal" din Sibiu, în anul 1992, a fost numit în funcţia de telegrafist în staţia pentru legături internaţionale din Centrul 89 Principal de Transmisiuni. În acelaşi an a fost numit în funcţia de şef autospecială (şi şofer) la autospeciala P-222 nr.1 a plutonului telegraf, cros şi electroalimentare din

compania telefon, telegraf, radioreleu si construcţii linii cablu greu.

După numai doi ani de la formarea ca subofiţer, la data de 01 ianuarie 1994, sergentul major Budulică Marius, datorită competenţei profesionale manifestată prin rezultate foarte bune în procesul de instrucţie, a fost promovat în funcţia de comandant pluton telegraf, cros şi electroalimentare, funcţie prevăzută cu gradul de căpitan.

În funcţia de comandant de pluton, subofiţerul şi-a îndeplinit în condiţii foarte bune atribuţiile funcţiei, acţionând ferm şi cu exigenţă. Pe timpul taberelor de instrucţie, exerciţiilor tehnico-tactice, aplicaţiilor, precum şi în procesul de instruire s-a remarcat prin experienţa de a comunica cu subordonaţii şi prin calitatea informaţiilor oferite acestora.

Fiind un bun organizator şi conducător al procesului de instrucţie, întreaga activitate şi-a desfăşurat-o pentru ridicarea nivelului de pregătire a militarilor. În tot acest timp, subofiţerul a fost un exemplu pentru cadrele din unitate şi un factor de mobilizare pentru subordonaţi şi colegi.

În perioada 01.07.1997÷31.05.2002, a îndeplinit atribuţiile funcţiei de şef autospecială (şi şofer) la autospeciala F-2016 din batalionul de transmisiuni la Centrul 89 Principal de Transmisiuni. Totodată, a îndeplinit şi atribuţiile funcţiei de comandant pluton şi comandant pluton – şcoală de gradaţi, obţinând în permanenţă rezultate foarte bune atât în procesul de instrucţie, cât şi în cadrul exerciţiilor şi aplicaţiilor de specialitate la care a luat parte.

La data de 01 iunie 2002, prin ordin al comandantului Comandamentului Transmisiunilor a fost promovat în funcţia de subofiţer de stat major în biroul personal din Secţia personal şi mobilizare la Comandamentul Transmisiunilor. S-a adaptat cu rapiditate şi eficienţă cerintelor noii funcţii, făcând faţă cu succes specificului activităţilor de subofiţer de stat major în comandament. Subofiţerul a acţionat cu responsabilitate şi competenţă profesională pentru a asigura îndeplinirea atribuţiilor funcţiei în care a fost încadrat.

În prezent, subofiţerul încadrează funcţia de subofiţer de stat major nivel 1 în biroul management personal din G.1 – Personal la Comandamentul Comunicaţiilor şi Informaticii.

În tot acest timp, subofiţerul şi-a îndeplinit foarte bine atribuţiile funcţionale. Permanent a acţionat cu competenţă şi responsabilitate îndeplinind în totalitate obiectivele de performanţă stabilite, având în acelaşi timp o preocupare deosebită pentru perfecţionarea pregătirii profesionale. Datorită schimbului de generaţii şi promovării în carieră a personalului militar, a devenit cadrul militar cu cea mai mare vechime şi experienţă în domeniul resurselor umane la nivelul comandamentului.

Subofiţerul îşi îndrumă şi ajuta colegii în rezolvarea sarcinilor de serviciu din cadrul biroului şi coordonează personalul care încadrează modulele de personal ale unităţilor militare subordonate, conform competenţelor asigurate atât de îndeplinirea atribuţiilor funcţiei pe care o încadrează, cât şi în totalitate a atribuţilor funcţiei de ofiţer 3 în biroul management personal, prin ordin de zi al comandantului Comandamentului Comunicaţiilor şi Informaticii, până la încadrarea acesteia;

De-a lungul carierei şi-a dezvoltat pregătirea profesională militară şi civilă superioară, prin absolvirea următoareleor forme de pregătire:

- Curs de comandant de pluton – Şcoala de Aplicaţie pentru Transmisiuni, 2000;
- Curs birotică – iniţiere – Şcoala de Aplicaţie pentru Transmisiuni, Informatică şi Război Electronic, 2003;
- Curs intensiv de limba engleză – nivel intermediar, terminologie generală – Centrul Secundar de Limbi Străine al Statului Major General, 2006;
- Curs de plutonier adjutant în domeniul gestionării resurselor

umane – Colegiul de Management al Resurselor Apărării, Educaţional şi al Achiziţiilor al Universităţii Naţionale de Apărare "Carol I", 2007;

- Curs gestionarea informaţiei utilizând baze de date Microsoft Office Professional: SQL, Excel, Acces, VBA – Agenţia pentru Sisteme şi Servicii Informatice Militare, 2007;
- Curs de reîmprospătare a cunoştinţelor de limba engleză – Departamentul de Limbi Străine al Universităţii Naţionale de Apărare "Carol I", 2008;
- Licenţiat în ştiinţe administrative, iulie 2009, la Facultatea de Ştiinţe Juridice şi Administrative, Braşov (şef de promoţie) – Universitatea Spiru Haret; absolvent al Facultăţii de Drept si Administraţie Publică, Bucureşti cu *Bursă de merit* pentru rezultatele deosebite în anul universitar 2007-2008.

Realizările din cariera militară i-au fost recunoscute prin conferirea unor ordine şi medalii:

- Medalia "Virtutea Militară" în clasa a III-a cu însemne pentru militari – 2004;
- Semnul onorific "În Serviciul Patriei" pentru XV ani de activitatate – 2007;
- Emblema de Onoare a Statului Major General – 2008;
- Medalia "Virtutea Militară" în clasa a II-a cu însemne pentru militari – 2010;
- Distincţia militară "OMUL ANULUI 2010", premiul I la secţiunea "Credinţă şi altruism", etapa pe Comandamentul Comunicaţiilor şi Informaticii.

Centrul de instruire pentru comunicaţii şi informatică „Decebal"

În pofida dificultăţilor pe care le traversează întreg mapamondul în această perioadă, implicit ţara noastră, soldatul român reprezintă un exemplu de profesionalism, spirit de sacrificiu şi seriozitate pentru partenerii Coaliţie.

Cu mândrie putem spune, că un asemenea brav soldat, om trecut prin focurile misiunilor din teatrul de operaţii din Afganistan, există şi la Sibiu, în Centrul de Instruire pentru Comunicaţii şi Informatică „Decebal". Este **caporalul Vergu Georginel**, fiul lui Gheorghe şi al Domnicăi, născut la data de 03.08.1971, în localitatea Perişani, judeţul Vâlcea, căsătorit, tatăl a doi copii. Este gradat voluntar al centrului încă din 1992, în prezent fiind încadrat pe funcţia de mecanic în cadrul grupei de întreţinere tehnică auto.

În anul 2009, impulsionat şi în aceeaşi măsură sfătuit de către fratele său, căpitan Vergu Nicolaie Leonard, militar cu experienţă în teatrele de operaţii, caporalul participă la prima misiune în cadrul ENS (Elementului Naţional de Sprijin), în teatrul de operaţii Afganistan, în perioada 18.10.2009-06.05.2010.

Lipsa emoţiilor şi încrederea în şansele de reuşită ale misiunii (articolul „Credinţă în reuşită", Observatorul Militar nr. 42/2009), au fost demonstrate de către gradatul voluntar pe toată perioada desfăşurării misiunii, dar în special în data de 20.11.2009, când în urma unui atac cu rachete asupra campusului românesc din Baza Kandahar acesta a reuşit să îi salveze viaţa sg. maj. TAIFAS Marius Bertoni, scoţându-l de sub dărâmături.

În urma acestui act de curaj cap. VERGU Georginel a fost decorat de către preşedintele României cu medalia „Bărbăţie şi Credinţă, clasa a II-a, cu însemn pentru

militari, de război" (Decretul 220/15.02.2010), iar mai apoi de către secretarul general al NATO, Anders Fogh Rasmussen cu medalia „Non Article 5 NATO Medal", fapte relatate în articolul „Când ajutorul este reciproc", din Observatorul Militar nr. 20/2010.

Toate aceste lucruri ne sunt povestite cu modestie, de către gradatul voluntar Vergu: „Am trecut prin multe momente grele dar astea m-au făcut mai puternic", şi le regăsim detaliate în articolul „Secundele eroului", din Observatorul Militar nr.21/2010.

La capătul acestei misiuni, caporalul a demonstrat încă o dată că este un adevărat profesionist, ce a reprezentat cu succes forţele de comunicaţii şi informatică în Afganistan şi speră la încă o misiune, care pentru cariera lui ar fi un impuls extraordinar.

Gradatul voluntar deţine cunoştinţe de specialitate excepţionale şi deprinderi practice deosebite. Este un exemplu pozitiv pentru ceilalţi militari, este demn de încredere în orice situaţie şi îşi păstrează calmul în condiţii de stres. Este flexibil în gândire, sesizează corect neajunsurile care apar în cadrul subunităţii şi se implică pentru rezolvarea acestora. Este capabil să îndeplinească funcţii superioare celei pe care este încadrat, iar potenţialul acestuia îl recomandă pentru trecerea în corpul subofiţerilor.

Este un simbol şi un exemplu pentru toţi gradaţii voluntari, fiind apreciat şi de celelalte cadre ale centrului, iar activitatea lui ar putea fi descrisă în trei cuvinte: ***competenţă, profesionalism şi seriozitate.***

Ca o recunoaştere a meritelor sale în aprecierea de serviciu pe anul 2010 a obţinut calificativul „***excepţional***", iar la concursul „***Omul Anului - 2010***", secţiunea „***Soldatul Universal***" etapa pe Comandamentul Comunicaţiilor şi Informaticii a fost clasat pe „***locul I***".

Dar el, omul Vergu, ştie să renunţe uşor la toate laudele pe care le merită, desfăşurându-şi în continuare activitatea în atelierul auto, în subunitate ca şi când nimic nu s-ar fi întâmplat.

Centrul 48 comunicaţii şi informatică strategice

Plutonierul adjutant Titi PIPOŞ s-a născut la 27 noiembrie 1960 in Tecuci. A absolvit Liceul Industrial nr. 2 Bacău şi Şcoala militară de maiştri militari şi subofiţeri ,,Gheorghe Lazar''(1980-1982).

De-a lungul carierei militare a absolvit următoarele cursuri:

- Curs de Comunicaţii Teritoriale la Centru de Perfecţionare a Personalului din Poşta şi Telecomunicaţii, în anul 1991;
- Curs de instruire pentru centrele de transmisiuni numerice din R.T.P./S.T.A.R., în anul 2001;
- Curs de plutonieri adjutanţi in arma comunicaţii şi informatică la Centrul de pregătire pentru comunicaţii şi informatică ,, Decebal'', în anul 2006;
- Curs de consilier al comandantului la Şcoala militară de maiştri militari şi subofiţeri a forţelor terestre ,,Basarab I'' în anul 2008.

A indeplinit următoarele funcţii:
- Şef staţie frecvenţă P-229 în perioada 1982 - 1990;
- Şef staţie legături la mare distanta P-255A în perioada 1990 - 1993;
- Şef staţie legături la mare distanta P-255 A M în perioada 1993 - 1997;
- Şef staţie satelit în perioada 1997 - 1999;
- Comandant pluton frecvenţă în perioada 1999 - 2001;
- Subofiţer de stat major la S 6 comunicaţii în perioada 2001 - 2005;
- Subofiţer de stat major la S 3 operaţii şi instrucţie în perioada 2005 – 2008;
- Consilierul comandantului pentru probleme ale maiştrilor militari şi subofiţerilor din 2008 până în present.

Începînd cu anul 2000 s-a ocupat, prin cumul şi de buna funcţionare şi gestionare a muzeului unităţii devenit pe parcurs Muzeul comunicaţiilor şi informaticii filială a Muzeului Militar Naţional ,,Ferdinand I''. Subofiţerul şi-a desfăşurat întreaga sa activitate de peste 29 ani în Regimentul 48 Transmisiuni actual Centrul 48 Comunicaţii şi Informatică Strategice. Menţionez că în toată această perioadă a obţinut numai calificative de "Foarte bun" si "Excepţional".

Centrul 42 comunicaţii şi informatică de sprijin

Domnul plutonier adjutant Sauciuc Gelu, născut la data 26.03.1969, în satul Hlipiceni, jud. Botoşani, a intrat în rândurile colectivului Comandamentului Comunicaţiilor şi Informaticii şi implicit al Unităţi Militare 01751 Râşnov, la data de 21.01.2008 în funcţia de administrator de unitate.

Cariera militară a început-o în anul 1987 când a fost admis la Şcoala Militară de Ofiţeri, Maiştri militari şi Subofiţeri de Geniu, Construcţii şi Căi Ferate – arma "Construcţii" şi pe care a absolvit-o în anul 1989.

Din anul 1989, de la obţinerea primului grad de subofiţer şi până în ianuarie 2008, şi-a desfăşurat activitatea într-o unitate militară tot din garnizoana Râşnov. Vrând parcă să nu se despartă de toate realizările sale în acea cazarmă (apreciată în acele vremuri din punct de vedere administrativ şi gospodăresc la nivelul Ministerului Apărării Naţionale), în ianuarie 2008 a fost mutat în interesul serviciului în unitatea noastră situată la câteva sute de metri de unitatea în care a dobândit vasta experienţă din domeniul construcţiilor. Încă din prima zi de serviciu în unitatea noastră şi-a exprimat ideea că activitatea sa va avea două obiective principale: crearea unor condiţii la cele mai înalte standarde pentru lucru la birouri şi cazarea militarilor, condiţii realizate prin dotări, reparaţii, întreţinere şi chiar construcţii la locurile de muncă şi de instrucţie, precum şi menţinerea tuturor spaţiilor interioare şi exterioare ale cazărmii

în cele mai bune condiţiuni din punct de vedere gospodăresc. Astfel a reuşit să realizeze condiţiile unui climat de trai şi de lucru excelent. La această dată putem aprecia faptul că aceste obiective personale

le-a înfăptuit cu succes, primind aprecierile şi felicitările întregului personal al unităţii. Activitatea sa a fost şi este apreciată în continuare de orice comisie de control sosită în unitate şi chiar de personal din afara Ministerului Apărării Naţionale care a putut constata condiţiile de trai şi de lucru din unitatea noastră.

Faptul că activitatea colegului nostru este apreciată în mod constant, este susţinută şi de aspectul că în timpul liber desfăşoară atribuţii în calitate de preşedinte de asociaţie de locatari în zona unde locuieşte împreună cu soţia şi fiica sa, funcţie ce presupune un bogat spirit gospodăresc şi administrativ. Aşadar, nu numai armata are nevoie de experienţa lui, ci şi mediul social civil.

Desemnarea domnului plutonier adjutant Sauciuc Gelu, "Omul Anului" 2010 – Secţiunea Logistică şi Infrastructură, etapa pe Comandamentul Comunicaţiilor şi Informaticii este binemeritată şi oglindeşte în cel mai obiectiv mod, spiritul gospodăresc îmbinat cu calitatea factorului uman.

Batalionului Instrucţie Comunicaţii şi Informatică „Fraţii Buzeşti"

La secţiunea „Moral, bunăstare şi recreere", în cadrul concursului „OMUL ANULUI în 2010" – etapa pe Comandamentul Comunicaţiilor şi Informaticii, colegul nostru **plutonierul major George STOIAN** a obţinut locul I.

Plutonierul major STOIAN George s-a născut în Craiova la data de 29 septembrie 1970 şi este consilierul comandantului Batalionului instrucţie comunicaţii şi informatică "Fraţii Buzeşti" pentru problemele maiştrilor militari, subofiţeri, soldaţi şi gradaţi voluntari din anul 2008.

În această funcţie subofiţerul s-a impus printr-un comportament şi o ţinută morală ireproşabile, în cadrul colectivului este cunoscut ca un adevărat „mentor" şi în timpul scurs de la numirea sa în funcţie, atât în unitate cât şi în afara acesteia, s-a dovedit a fi un bun organizator şi conducător al unor

multitudini de activităţi de recreere, cultural-educative şi sportive.

A absolvit Şcoala militară maiştri militari şi subofiţeri a Forţelor terestre „Basarab I" – Piteşti ca şef de promoţie, Facultatea de ştiinţe economice specializarea management şi are un master în specializarea managementul şi dezvoltarea resurselor umane. Este casătorit şi are o fiică.

Baza 191 logistică pentru comunicaţii şi informatică

Domnul **Zaharia Minel** îşi desfăşoară activitatea în Baza 191 logistică pentru comunicaţii şi informatică de peste 20 ani, fiind un veteran al locului şi unul dintre cei mai buni specialişti în mentenanţa tehnicii de comunicaţii. Lucrând într-un domeniu de vârf, în care apare în permanenţă ceva nou, se preocupă permanent de pregătirea profesionala, cu atât mai mult cu cât electronica este combinată cu informatica într-o măsură tot mai mare. Absolvent de studii superioare în domeniul electronicii şi informaticii, îşi valorifică potenţialul profesional atât în unitate cât şi în numeroasele misiuni în ţară şi peste hotare, fiind apreciat pentru competenţa dovedită prin scrisori de apreciere din partea conducerii unităţilor unde a efectuat misiuni.

Jovial, cinstit şi onest, face plăcut lucrul în echipă, iar cunoştinţele sale tehnice şi experienţa duc la o rezolvare facilă şi rapidă a problemelor apărute în configurarea şi mentenanţa tehnicii de comunicaţii şi informatică. În acelaşi timp reprezintă o adevărată enciclopedie tehnică pentru alţi specialişti, un izvor permanent de cunoştinţe despre noutăţile apărute în domeniu, colaborarea lui fiind plăcută şi dorită de specialiştii din unitatea noastră.

Centrul 89 principal pentru comunicaţii şi informatică

O unitate militară de elită ca CENTRUL 89 PRINCIPAL PENTRU COMUNICAŢII --ŞI INFORMATICĂ, cu misiuni atât de importante şi vitale pentru existenţa Armatei României, nu poate fi încadrată decât cu oameni de elită. Orice misiune, oricât de complexă ar fi, este mult mai simplă decât aceea de a face departajarea între militari. Aici cu greu poţi să spui că un militar este mai competent

decât altul, pentru că activităţile desfăşurate în această unitate presupun existenţa unui cumul de calităţi exact ca verigile unui lanţ în care, de la soldat la comandant, fiecare persoană trebuie să fie atât de puternică încât să nu îl poată întrerupe nimic. De aceea, în alegerea unui singur om care să poată reprezenta toată măiestria necesară desfăşurării acestor activităţi, nominalizările ar fi putut cuprinde aproape tot statul unităţii.

Maior Medic MARINESCU MIRCEA însumează toate aceste calităţi, mai ales datorită faptului că el este un excelent profesionist, şi un subordonat model, calităţi pentru care în anul 2010 a fost desemnat *"OMUL ANULUI"*.

Născut la data de 19 ianuarie 1973 în muicipiul Bucureşti, Mr. Mircea Marinescu este căsătorit din anul 1999 şi are doi copii.

Studii:

- Şcoala generală 8 clase, Bucureşti;
- Liceul sanitar, 4ani, învăţământ de zi, Bucureşti;
- Institutul Medico-Militar de 6 ani, în perioada 1993 – 1999, clasificat al 27-lea din 76 de absolvenţi, cu media generală 9,16.

Cursuri de formare profesională:

- Curs de perfecţionare postuniversitară a pregătirii profesionale – ecografie generală – 2004;
- Cursul pentru medici şefi de unitate desfăşurat la Institutul Medico-Militar– 2001;
- Centrul de pregătire în informaticăal Agenţiei pentru Sisteme şi Servicii Informatice militare- Curs pentru gestionarea informaţiei utilizând baze de date Microsoft Office cu durată de 1 lună;
- Centrul Naţional de Perfecţionare în Domeniul Sanitar – Programul de educaţie medicală continuă "Actualităţi în managementul serviciilor de sănătate - 2005;
- Şcoala naţională de sănătate publică şi management sanitary - Curs "Management spitalicesc, 2006;
- Curs pentru medici şefi de mare unitate, durata o lună - 2009, cu media de absolvire 9,42.

Funcţii:

- Medic de medicină generală – stagiar în cadrul Institutului de Medicină Militară, 1999 - 2000;
- Medic de medicină generală – stagiar Spitalul Clinic de Urgenţă Militar Central, 2000 - 2001;
- Medic şef la Batalionul 536 Transmisiunial Comandamentului ? Operaţional, 2001 – 2002;
- Medic şef la Centrul 89 Principal pentru Comunicaţii şi Informatică, 2002 – până în prezent;
- Şef centru de comunicaţii nodal de acces cu management local, din 2008 şi până în prezent.

La capitolul realizări mai pot fi enumerate şi următoarele:

- pregătire prin rezidenţiat de medicină de familie în perioada 2006 – 2009;
- obţinerea titlului de specialist de medicină de familie în anul 2009;

- înscris în programul de pregătire în a doua specialitate – reumatologie;
- medic de familie cu o listă de aproximativ 800 înscrise asiguraţi ai casei OPSNAJ.
- a efectuat gărzi la Unitatea de Primiri Urgenţe a S.C.U.M.C.

În calitatea deloc uşoară de Medic şef a reuşit să se evidenţieze, prin calităţile sale de specialist şi bun diagnostician.

A câştigat încrederea şefilor şi subordonaţilor săi prin îndeplinirea cu responsabilitate şi seriozitate a sarcinilor dificile şi complexe primite, de multe ori situându-se peste cerinţele funcţiei sale.

Ştie să-şi valorifice la maximum calităţile profesionale reuşind să depăşească cu uşurinţă momentele dificilereprezentate de cazurile cu un grad sporit de dificultate. Prin exemplul său personal, maiorul MARINESCU MIRCEA menţine un standard ridicat privind calităţile de militar şi profesionist.

Centrul 89 principal pentru comunicaţii şi informatică

Orice unitate militară are exponenţii săi care o diferenţiază de toate celelalte unităţi din acelaşi domeniu şi care o ridică în rândul unităţilor de elită cu misiuni vitale pentru existenţa Armatei României.

Un etalon în ceea ce priveşte eficienţă şi professionalism în comunicaţii şi informatică este locotenentul Badea Gelu a cărui biografie poate fi o foarte bună sursă de inspiraţie pentru cei care vor o carieră lungă şi încununată de succes în domeniul militar. Calităţile care îl recomandă sunt înalta pregătire, seriozitate, punctualitate,

perseverenţă şi determinare. În toate împrejurările a dat dovadă de o uimitoare forţă mobilizatoare reuşind să treacă uşor peste obstacole care păreau de netrecut. Acestea sunt doar o parte din calităţile care-l fac pe **locotenentul Badea Gelu** un real exponent al colegilor.

Născut la data de 22 ianuarie 1981 în localitatea Craiova, Judeţul Dolj, Gelu Badea este căsătorit din anul 2005 şi are un copil.

Studii:

- 1996 – 1998 – Liceul Militar Tudor Vladimirescu – Craiova;
- 1998 – 2000 – Colegiul Naţional Elena Cuza – Craiova;
- 2000 – 2005 – Academia Tehnică Militară – Facultatea de Electronică şi Telecomunicaţii;
- 2005 – ESISAR – Franţa – realizarea proiectului de diplomă.

Cursuri de formare profesională:

- 2007 – Curs de perfecţionare "Proiectare parametrizată în Autodesk Inventor" – Academia Tehnică Militară;
- 2007 – Curs RTP/STAR – Academia Tehnică Militară;

- 2008 – Sisteme de videoteleconferinţă – Tandberg, Norvegia;
- 2008 – Curs echipamente videoteleconferinţă – ASSIM;
- 2009 – Curs intensiv de limbă engleză – Universitatea Naţională de Apărare;
- În prezent participă la "Cursul avansat de logistică pentru ofiţeri" – Academia Tehnică Militară.

Funcţii:

- Ofiţer 5 cu protecţie personal şi securitate industrială, cu management chei şi protecţia informaţiilor la S6 în perioada 19.08 2005 – 04.06 2006;
- Şef Centru de Comunicaţii Nodal cu Management Regional în perioada 04.06 2006 – 01.10 2008;
- Şef Compartiment Videoconferinţă în perioada 01.10 2008 – 15.12 2010;
- Şef Centru de Comunicaţii Nodal cu Management General de Bază din 15.12 2010.

De la absolvirea Academiei Tehnice Militare şi până în prezent a fost încadrat la Centrul 89 Principal pentru Comunicaţii şi Informatică.

În anul 2010 a participat la conferinţa initială de planificare a exerciţiului Combined Endeavor, desfăşurată la Yerevan – Armenia, apoi a făcut parte din echipa ce a reprezentat România la acest exerciţiu.

În cadrul exerciţiului de Specialitate Cetatea 2010 a avut un rol important în realizarea primei videoconferinţe între reţeaua criptată de VTC a Ministerului Apărării Naţionale şi o reţea criptată de VTC a Serviciului de Telecomunicaţii Speciale.

A câştigat încrederea şefilor şi subordonaţilor săi prin îndeplinirea cu responsabilitate şi seriozitate a sarcinilor dificile şi complexe primite, de multe ori situându-se peste cerinţele funcţiei sale. S-a remarcat ca un bun pedagog în instruirea personalului militar tânăr cu care lucrează.

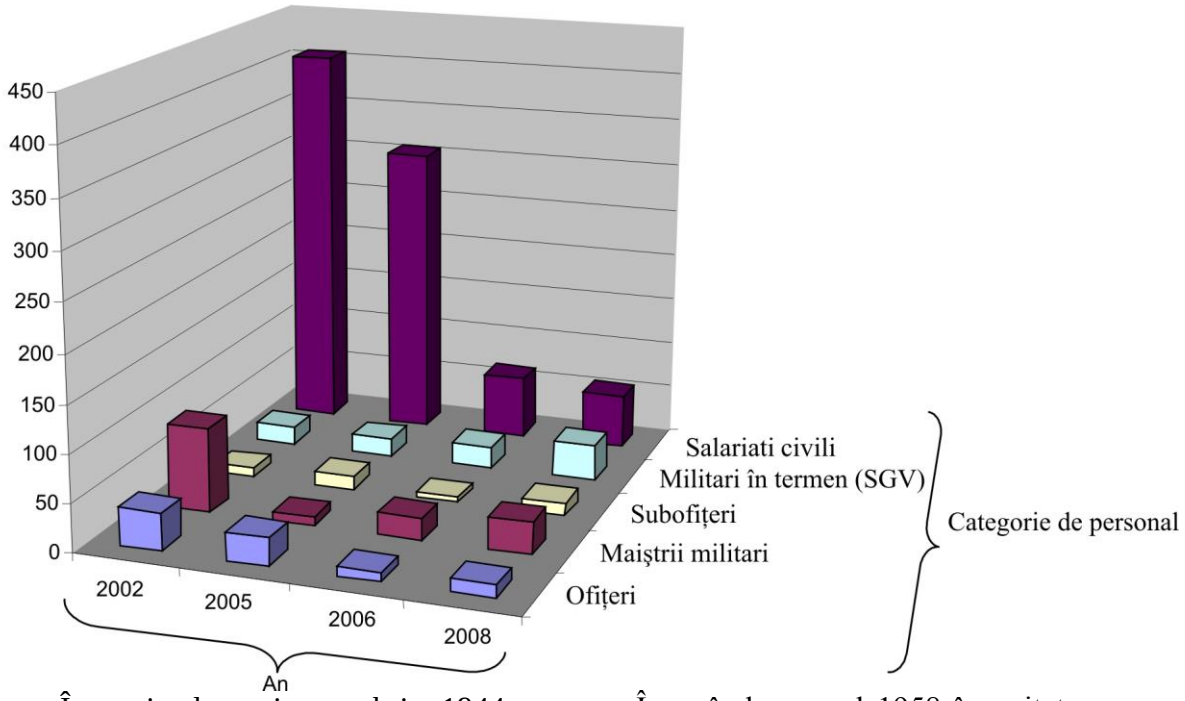
BAZA 191 LOGISTICĂ PENTRU COMUNICAŢII ŞI INFORMATICĂ - TRECUT, PREZENT ŞI PERSPECTIVĂ

Locotenent ing. Gabriel CIUCĂ
Baza 191 logistică pentru comunicaţii şi informatică

În conformitate cu ordinul *Ministerului de Război* nr. 519 din 01.06 1921 a luat fiinţă *Arsenalul Trupelor Tehnice*, executând repararea materialelor tehnice, printre care şi telefoane, activitate care până la acel moment intra în atribuţiile atelierelor de pe lângă regimentele de specialităţi şi corpurile de trupă. La data înfiinţării, *Arsenalul Trupelor Tehnice* era organizat pe 25 de ateliere, numărul acestora crescând la 33 în anul 1922.

În perioada mai-octombrie 1944 o parte din efectivele şi utilajele unităţii au fost mutate in localitatea Lipova, judeţul Arad unde s-au executat reparaţii de tehnică de transmisiuni. În anul 1948 denumirea unităţii devine *Arsenalul Transmisiunilor*. La data de 01.04 1952, unitatea devine atelier bugetar în întreprinderea economică socialistă, începând fabricarea de produse destinate pieţei (în principal baterii).

Din anul 1955 începe producţia de complete speciale pentru *Comandamentul Trupelor de Transmisiuni* precum şi realizarea de antene radio, piese de schimb pentru acumulatori, carosări autodube, echipamente pentru sălile de transmisiuni etc. În aceeaşi perioadă începe producţia de huse şi prelate şi se preia de la uzina *Electromagnetica* producţia de şlemafoane.



Începând cu anul 1958 în unitate se repară înregistratoare mecanice de tragere automată de pe navele marinei militare. În anul 1960, în colaborare cu întreprinderea *Frigocom* se începe producţia spaţiilor frigorifice, iar împreună cu întreprinderi ale *Ministerului Metalurgiei* se începe realizarea autoatelierelor M.F.A.

În baza H.C.M. nr. 1386-31.12 1962 unitatea îşi încetează activitatea ca unitate economică chibzuită şi se transformă în *Atelierul de Reparat Materiale de Transmisiuni,* unitate bugetară subordonată *Comandamentului Trupelor de Transmisiuni.* La aceeaşi dată, pe baza protocolului încheiat între *Ministerul Forţelor Armate* şi *Ministerul Metalurgiei* o parte din utilaje şi personal au fost preluate de uzina *Electromagnetica.*

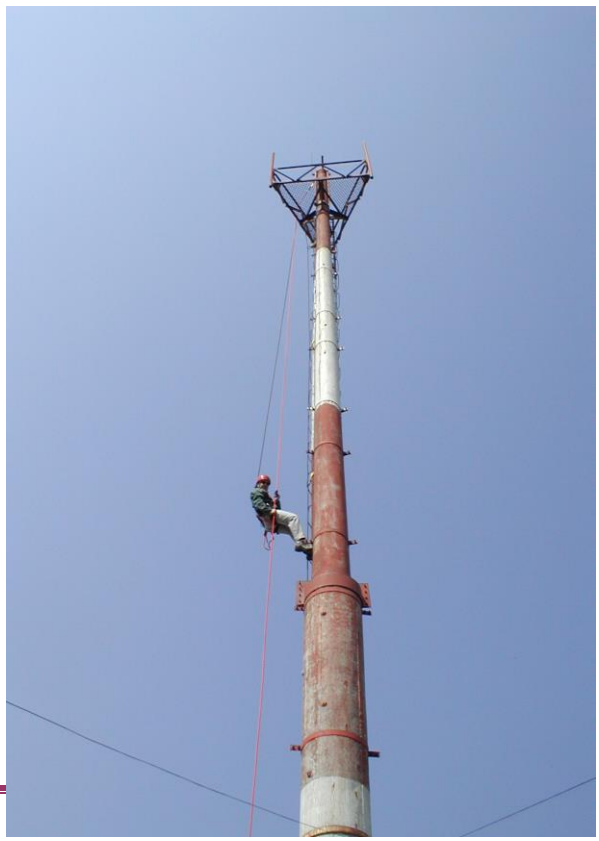
Conform ordinului *Comandamentului Trupelor de Transmisiuni* numărul 002990/1969, începând cu data de 01.07 1969 unitatea îşi schimbă denumirea în *Baza 191 pentru Reparat Tehnică de Transmisiuni.*

Având în vedere reforma din domeniul militar, în perioada 01.07 2002-31.03 2006, unitatea a trecut printr-o serie de transformări, culminând cu intrarea în vigoare la data de 01.04 2006 a noului stat de organizare, denumirea unităţii fiind transformată din *Centrul 191 Principal Construcţii Reţele de Transmisiuni şi Mentenanţă* (la data de 01.07 2002) în *Centrul 191 Mentenanţă şi Depozitare* (la data de 01.04 2006).

În acest moment, în unitate îşi desfăşoară activitatea un colectiv relativ tânăr, receptiv la tot ce înseamnă nou d.p.d.v. al dotării armatei cu tehnică de comunicaţii şi informatică. Activitatea de mentenanţă tehnică de comunicaţii şi I.T. este asigurată de cele trei secţii din compunerea unităţii.

Personalul specializat al unităţii asigură instalarea centrelor RTP/RMNC pe întreg teritoriul ţării. În acest moment există pregătită şi autorizată o echipă de pilonişti, care pe viitor vor putea asigura activităţi de instalare/aliniere antene precum şi mentenanţă piloni. Asistenţa tehnică preventivă sau la avarie a centrelor de comunicaţii din cadrul S.C.I.A.R. este asigurată de personalul unităţii, în colaborare cu agenţii economici. În unitate funcţionează şi depozitul de echipamente de tip MARCONI, putând asigura echipelor de instalare şi mentenanţă echipamentele şi subansamblele necesare desfăşurării misiunilor în timp cât mai scurt şi cu un înalt standard de calitate.

Mentenanţa staţiilor radio cu salt de frecvenţă tip „HARRIS" şi a echipamentelor aferente acestora se poate realiza în proporţie de 100% de către personalul ce încadrează atelierul de specialitate din unitate,special amenajat şi dotat (Staţia de



Testare Automată OM-100, pentru verificarea staţiilor radio pe U.S. şi U.U.S.este unică în ţară). Personalul a fost specializat la sediul firmei "HARRIS" din S.U.A. Mentenanţa staţiilor şi autostaţiilor radio cu salt de frecvenţă tip „PANTHER" (care în prezent asigură şi necesarul de legături radio pentru misiunile externe) se realizează în proporţie de 78% de către personalul ce încadrează atelierul de specialitate din unitate (în spaţiu special amenajat şi dotat). Mentenanţa echipamentelor ce compun Reţeaua Radio Operativă de Nivel Strategic este asigurată de specialiştii din unitate (piesele de schimb şi subansamblele de rezervă se găsesc în depozitele unităţii) în colaborare cu un agent economic.

În cadrul unităţii noastre funcţionează un laborator de metrologie, autorizat de Biroul Român de Metrologie Legală, unicat în cadrul Ministerului Apărării.

Structura şi organizarea unităţii permite rezolvarea problemelor de mentenanţă în timp operativ, prin echipe specializate, gata să se deplaseze în teren în cazuri de deranjamente, aplicaţii, exerciţii tehnice sau chiar în teatrele de operaţii.

La ora actuală, nu există unităţi militare sau agenţi economici care să dispună de personal specializat într-o gamă atât de variată de echipamente, de dotarea necesară şi nici de stocul de piese/module/subansamble de schimb necesare susţinerii unor astfel de activităţi cu costuri reduse şi timp de imobilizare minim, unitatea fiind unicat în Ministerul Apărării Naţionale.

De la *Arsenalul Trupelor Tehnice* la *Baza 191 logistică pentru comunicaţii şi informatică*, personalul unităţii se angajează să ducă mai departe tradiţiile istorice precum şi exigenţele impuse de tehnica modernă cu care a fost şi va fi înzestrată armata română.

ASISTENŢA RELIGIOASĂ ÎN ARMATA ROMÂNIEI-SIMBOL AL REFORMĂRII MODERNE A INSTITUŢIEI MILITARE

Rezumat al lucrării de absolvire a Colegiului Naţional de Apărare - 2002

Preot Ştefan STANCIU

Biserica şi Armata sunt cele două instituţii fundamentale ale unităţii şi continuităţii româneşti. Ele au însoţit şi sprijinit benefic starea şi evoluţia societăţii noastre, ele au fiinţat concomitent, s-au ajutat reciproc, au devenit trainice alcătuiri folositoare, şi-au constituit structuri, relaţii şi funcţii specifice, conferind poporului român puterea dăinuirii în faţa vrăjmaşilor şi a vitregiilor istorice. *"Biserica şi Armata sunt două instituţii înfrăţite care formează temelia fiinţării organizaţiei de stat"*, spunea episcopul general de brigadă - Partenie Ciopron, *"Armata a învăţat pe oşteanul român să-şi apere tărâmurile strămoşeşti de cotropitorii străini, Biserica a învăţat pe toţi fiii neamului acestuia să-şi apere sufletul şi credinţa strămoşilor, să se ferească de cotropitorii sufleteşti, de ispite si de relele altor neamuri"*, spunea P.F. Patriarh Teoctist într-o cuvântare.

Această relaţie este străveche, puternică şi viabilă. Spunem *străveche* ştiind că lângă regele geto-dac (care în antichitate era şi căpetenia oştirii) se afla marele preot Zamolxis, mai târziu Deceneu şi alţii. Prin anii 32 d.Hr. apostolul Andrei propovăduieşte în Scitia credinţa în Hristos strămoşilor noştri între care se află şi ostaşi. După cucerirea Daciei, coloniştii creştini, militarii aduşi din imperiu, veteranii stabiliţi aici, negustorii sosiţi din diferite ţări supuse de Roma au continuat să practice ritualurile creştine, intensificând creştinarea dacilor, civili şi soldaţi. Predicarea creştinismului necesită cler şi locaşuri de cult. Asistenţa religioasă în aceste biserici nu excludea, ci presupunea prezenţa militarilor care apărau comunitatea creştină. Deja la sfârşitul secolului VI, în părţile sud dunărene există o organizare bisericească temeinică, cu episcopii şi mitropolii, mai târziu extinzându-se şi consolidându-se în restul spaţiului intra şi extra carpatic. Creştinismul devine pentru români *"punctul de sprijin al existenţei lor morale şi fizice"*, cum spunea Mircea Eliade, iar ortodoxia *"parte importantă a civilizaţiei româneşti"* după Nicolae Iorga.

În Evul Mediu legătura preot-oştire a funcţionat relativ bine întrucât şi clerul şi militarul s-au identificat cu aspiraţiile neamului, cu interesele statului, fie ea Ţara Românească, Moldova sau Transilvania. Asistenţa religioasă în oştire s-a specializat întrucâtva exact în această perioadă; preoţii săvârşeau slujbe de sfinţire a steagurilor, de binecuvântare a oştilor înainte de luptă, de prohodire a oştenilor căzuţi etc. Preoţii şi călugării vor fi mereu sfetnici ai voievozilor şi mai târziu ai domnitorilor care sunt şi capi ai oştirii. Astfel, Nicodim de la Tismana era mâna dreptă a lui Vladislav Vodă (1364-1372), Alexandru cel Bun îi dăruieşte preotului Iuga din Baia în anul 1424 satul Buciumeni ca vrednic "preot de oaste". Ştefan cel Mare şi Sfânt are mulţi preoţi în oastea sa cu care luptă împotriva expansiunii otomane. Mihai Viteazu are de asemenea clerici în oaste. Sunt cunoscuţi preot Teodor de Sângeorz, Bistriţa şi preotul Stoica din Fărcaş, Dolj, despre a cărui vitejie poporul a scris în versuri următoarele:

"Popa Stoica din Fărcaş/ Care sare şapte paşi/ Şi iese din Liturghie/ Şi taie la turci o mie."

În perioadele următoare clerul ortodox s-a identificat întru totul cu aspiraţiile neamului de libertate şi unitate naţională pentru că *"ostaşii sunt poporenii lui, iar ţara este moşia tuturor"*. Andrei Mureşanu exprima sugestiv în Deşteaptă-te române: *"preoţi cu crucea-n frunte căci oastea e creştină"*.

Primele reglementări privind asistenţa religioasă în armată se fac abia după organizarea modernă a armatei române, începând cu anii 1830. Avem la 1834 un "confesor al capelei" în statul major al dorobanţilor, iar în 1837 un preot al oştirii pentru comandamentul superior. În 1850 şeful oştirii, marele spătar Nicolae Ghica cere Mitropoliei Ungro-Vlahiei a *"orândui câte un preot pe lângă fiecare polc de-al oştirii"* în garnizoanele Bucureşti, Craiova şi Brăila. În acelaşi an apare prima reglementare numită *"îndatoririle preoţilor de oştire"* care detaliază modul de organizare şi desfăşurare a asistenţei religioase în polcurile oştirii, rămânând în vigoare până în 1870, când a apărut Regulamentul clerului din armata permanentă. Acesta stabilea clar locul şi rolul preotului în oştire. Astfel se preciza că fiecare regiment sau batalion, dacă reprezenta o entitate (corp în parte), putea să includă în structura sa un preot care avea ca misiuni principale: serviciul divin, îngrijirea bolnavilor şi răspândirea ştiinţei de carte. Primul eveniment mare care a confirmat virtuţile cultivate prin această educaţie a fost Războiul pentru Independenţă, în timpul căruia alături de ostaşi au luptat cu arma în mână şi au murit nenumăraţi preoţi de oaste precum şi călugări şi călugăriţe care activau în spitalele de campanie. În al doilea război balcanic asistenţa religioasă se realiza prin varii forme: "unii din preoţi însoţesc ostaşii în mijlocul gloanţelor şi în tranşee, încurajându-i în luptă, alţii sunt la Crucea Roşie îngrijind de răniţi, iar alţii îmbracă haina militară intrând în rândurile ostaşilor combatanţi", spunea un martor al vremii.

În anul 1915 Sfântul Sinod întocmeşte *"Instrucţiunile asupra atribuţiunilor preoţilor la armată"* care prevedeau organizarea Serviciului Religios conform ierarhiei militare, asimilarea preoţilor militari cu ofiţeri în grad de locotenent, avansarea lor în grad, plata de la bugetul oştirii etc. Şeful Serviciului Religios a fost numit protopopul Constantin Nazarie.

În Primul Război Mondial arhivele militare nominalizează 207 preoţi militari, din care 15 au cunoscut ororile prizonieratului, 25 dispăruţi şi 5 morţi. Generalul Prezan elogiază prezenţa şi curajul preoţilor militari pe front care *"şi-au făcut mai mult decât datoria"*, iar ministrul de război, generalul Ioan Răşcanu îi apreciază ca fiind *"mai presus de orice laudă, ca adevăraţi apostoli, care n-au părăsit un moment postul lor sfânt şi de onoare, ajutând ofiţerimea spre a putea duce în glorie trupele"*, fapt pentru care *"armata nu se poate dispensa de serviciul sufletesc nepreţuit al preoţimii"*.

Anii 1921-1937 marchează adoptarea legislaţiei moderne în domeniu: Legea privitoare la organizarea clerului militar - 1921; Legea şi regulamentul cu privire la clerul militar - 1924; Legea pentru organizarea clerului militar - 1937. Aceste acte normative chemau la pastoraţie preoţi ortodocşi, catolici şi protestanţi, rabini şi imami, asigurând în armată cuvenita dimensiune ecumenică a asistenţei confesionale.

Un moment foarte important îl constituie anul 1921 când, prin Legea privitoare la organizarea clerului militar se înfiinţează Episcopia Armatei care va fi condusă de un episcop militar numit episcop de Alba-Iulia, cu grad de general şi membru al Sfântului Sinod.

Modelul românesc al Episcopiei militare se va dovedi viabil pe toate planurile. Episcopia Armatei va fi deosebit de activă la pace şi război, înscriind în istoria clerului militar perioada cea mai benefică. Din 1921 până în

1948, conexiunea Biserică-Armată şi-a demonstrat viabilitatea prin zidirea sufletească izbutită de cei 4 episcopi militari şi de preoţii care au fortificat psihic şi moral ostaşul român.

În perioada celui de-al Doilea Război Mondial, asistenţa religioasă în armată a fost asigurată de cei 110 preoţi militari activi cărora li s-au adăugat alte sute de preoţi mobilizaţi astfel încât toate structurile -mari unităţi, unităţi şi formaţiuni independente - aveau cel puţin un preot. Mulţi dintre ei au căzut prizonieri, au rămas invalizi sau au murit *"împreunând jertfa lor cu jertfa celor, pe care i-au dăscălit cu ceasuri în urmă",* cum spune un martor al vremii.

Din păcate, după 1945 zilele Episcopiei Armatei sunt numărate. Astfel, din 64 de preoţi militari activi nominalizaţi în 1944 şi din cei 92

mutaţi între diferite unităţi/puţini la număr ajung la enorii, multora înscenându-li-se procese, unii ajungând în aresturi, închisori, lagăre de muncă, aşa cum de altfel vor păţi foarte mulţi ostaşi şi ofiţeri. Curând clerul militar va trece de la subordonarea politică impusă de Moscova, la desfiinţare, care se va produce în august 1948, decretele 1519 şi 1532 din 30/31 august 1948, rupând Armata de Biserică, stipulând că cei 57 de preoţi militari „se şterg din controalele armatei de la categoria clerul militar", însuşi "episcopul Partenie Ciopron nemaifăcând parte din cadrele active ale armatei". Astfel, după sute de ani de existentă activă, asistenţa religioasă a fost înlăturată din structurile armatei române. Ateismul a înlocuit religia în cazărmi, şcoli şi spitale militare, garnizoane etc.

După 40 de ani Biserica şi Armata s-au regăsit, reluarea cooperării fiind un act reparatoriu faţă de nedreapta şi nejustificata întrerupere brutală din pricina unei ideologii atee, total străină poporului nostru, dar şi o necesitate pastorală şi un drept al soldaţilor la asistenţă spirituală. La 1 ianuarie 1994, în cadrul MApN a fost înfiinţat un Compartiment de Asistenţă Religioasă format dintr-un ofiţer si 2 preoţi (ambii cu jumătate de normă). La 11 octombrie 1995 a fost semnat *Protocolul privind organizarea şi desfăşurarea asistenţei religioase în armata română,* primul document care a creat un cadru, legal pentru această activitate în rândurile militarilor. Acum de jure şi de facto se revine la tradiţia multiseculară în care Armata şi Biserica lucrează laolaltă spre binele ţării.

La 1 aprilie 1996, prin OG 20 a Ministrului Apărării se constituie Secţia de asistenţă religioasă în cadrul MApN, iar la 23 aprilie în acelaşi an, un număr de 24 de preoţi sunt instalaţi în diverse structuri ale armatei române ca preoţi militari în urma absolvirii unui curs special în cadrul Academiei de Înalte Studii Militare.

Anul 2000 aduce Legea 195, privind constituirea şi organizarea clerului militar. Potrivit acestei legi, MApN, MI, M3-DG a Penitenciarelor, SRI, SIE, SPP, STS pot avea preoţi militari *„în scopul satisfacerii cerinţelor spiritual religioase ale militarilor, cultivării virtuţilor ostăşeşti, formarea răspunderii civice şi a sentimentelor patriotice în rândurile militarilor"*. Clerul militar se constituie în câte o Secţie de Asistenţă Religioasă în cadrul MApN, MI si MJ, iar în celelalte instituţii, ca structuri adecvate cerinţelor stabilite prin ordin al conducătorilor respectivelor instituţii.

Preoţii militari sunt asimilaţi, în funcţie de categoria garnizoanei, gradului de maior, locotenent-colonel sau colonel, iar şeful Secţiei Asistenţă Religioasă asimilat gradului de general de brigadă. Aceştia desfăşoară activitatea de la mare unitate până la nivel de unitate (batalion) şi în instituţiile militare de învăţământ.

Asistenţa religioasă prezentă în majoritatea structurilor militare ale României, are în principiu misiunea de a răspunde dreptului militarului de a dispune de un sprijin moral şi

religios ca drept fundamental al oricărei persoane la libertatea de exprimare. Mai are ca scop şi principiu, formarea permanentă în spiritul valorilor umane şi civile europene, acordând o atenţie deosebită eforturilor întregii societăţi româneşti de integrare în structurile euro-atlantice a armatei române. Relaţiile cu capelanatele armatelor membre NATO şi PfP sunt permanente şi de natură a aduce beneficiu-ambelor părţi.

Comuniunea dintre Cruce şi Scut atestă că asistăm la un reviriment spiritual şi moral al naţiunii române, la înscrierea în normalitate şi modernitate a instituţiei statului nostru şi neamului românesc.

Preot Ştefan STANCIU

Scurte consideraţii privind personalitatea şi activitatea autorului

Autorul articolului, preotul paroh Ştefan STANCIU, este o figură importantă ce reprezintă clerul în relaţia cu Armata Română şi cu deosebire cu Comandamentul comunicaţiilor şi informaticii.

Născut la data de 24.04.1956 în comuna Vulturu din judeţul Vrancea, a îmbrăcat de la vârsta de 15 ani veşmântul preoţesc, urmând treaptă cu treaptă, Seminarul Teologic Buzău şi Institutul Teologic de grad universitar Bucureşti, pe care l-a absolvit în anul 1981. Şi-a făcut ucenicia în parohiile Bragadiru şi Tintava, fiind promovat în anul 1986 în grupul de consilieri al PF Patriarh Teoctist, în Sectorul Tehnic.

Foarte bun cunoscător al limbilor franceză şi engleză, fin şi cultivat, cu o educaţie generală şi de specialitate ridicată şi cu mult har în a se apropia de oameni, s-a făcut imediat remarcat, fiind cooptat în "Instituţia Capelanatelor", participând la manifestările internaţionale din Europa şi SUA din perioada 1992-1996, la Roma, Budapesta, Washington, Stockholm, Florida.

De-a lungul anilor a trăit experienţe deosebite, fiind primit de preşedintele Italiei, Francesco Cossiga în anul 1992, de şeful Statului Major Întrunit al Armatei SUA, generalul Colin Powell în anul 1993, şi de regele Suediei în anul 1994.

Momentul cel mai înălţător pe domeniul clerical, l-a avut în anul 1992, când a fost primit în audienţă de Papa Ioan Paul al II-lea.

Din anul 1989 este Preot Paroh al Bisericii Sfinţii Arhangheli Mihail şi Gavriil şi Sfântul Spiridon din Parohia Parcul Ghencea Bucureşti.

Legătura cu Armata a fost făcută între anii 1976-1977 când şi-a satisfăcut stagiul militar de 9 luni. Dragostea sa foarte mare spre cele două instituţii fundamentale ale statului, Biserica şi Armata, a atins apogeul prin absolvirea în anul 2002 a Colegiului Naţional de Apărare.

Prezent permanent în rândul militarilor din unităţile Comandamentului comunicaţiilor şi informaticii, cu deosebire din garnizoana Bucureşti, Preotul Paroh Ştefan STANCIU poate fi meritat gratulat cu titlul de "Duhovnicul Transmisioniştilor".

SCURT ISTORIC PRIVIND LĂCAŞELE DE CULT DIN UNITĂŢILE MILITARE SUBORDONATE COMANDAMENTULUI COMUNICAŢIILOR ŞI INFORMATICII

„Religia transformă poporul într-o masă de oameni culţi”

PETRE ŢUŢEA

BISERICA MILITARĂ CU HRAMUL „ADORMIREA MAICII DOMNULUI” DIN GARNIZOANA TÂRGU JIU

În anul 1996 s-a iniţiat procesul de obţinere a avizelor necesare şi a autorizaţiei de construire, odată cu începerea activităţii de preot militar în Unitatea Militară nr. 01466 din garnizoana Târgu Jiu.

Piatra de temelie s-a pus pe 30.03 2002, cu aprobarea domnului general de brigadă dr. Neagoe Visarion comandantul garnizoanei Târgu Jiu, cu Înalta binecuvântare a Înalt Prea Sfinţiei Sale Teofan Arhiepiscop al Craiovei şi Mitropolit al Olteniei.

Lucrările de ctitorire au început cu o subunitate de deţinuţi de la penitenciarul Târgu Jiu, iar costurile au fost acoperite prin contribuţia financiară a cadrelor militare din unitate.

În anul 2004 şi apoi în anul 2005, unităţile militare din garnizoana Târgu Jiu au fost desfinţate, iar funcţia de preot militar precum si cazarma nr. 3475 care cuprinde biserica şi clopotniţa au fost preluate de Unitatea Militară nr. 01013 (Centrul 105 Comunicaţii R.M.N.C.) din garnizoana Târgu Cărbuneşti.

În tot acest timp preotul militar a continuat lucrările de construire a bisericii beneficiind de spijinul financiar şi material al mai multor agenţi economici din judeţ şi din ţară, precum şi de sprijinul autorităţilor locale şi centrale.

În anul 2009 s-a reuşit pictarea şi înzestrarea cu odoare şi inventarul liturghic a Sfintei biserici, amenajarea exterioară şi pregătirea pentru sfinţire.

O contribuţie însemnată, atât financiar cât şi material, a avut-o colectivul de militari al Unităţii Militare nr. 01013, dar şi unităţile militare subordonate Comandamentului Comunicaţiilor şi Informaticii.

În data de 23.08 2009 a avut loc sfinţirea bisericii militare, eveniment la care au participat personalităţi de prim rang al vieţii

politice româneşti şi Ministerului Apărării Naţionale.

Acest sfânt edificiu cuprinde în structura sa materială jertfa şi sudoarea tuturor iubitorilor de HRISTOS, atât militari cât şi civili, reprezintă locul de întâlnire spirituală a militarilor cu civilii, darul unora pentru ceilalţi.

În anul 2005, în incinta Centrului 105 Comunicaţii R.M.N.C., a fost amenajată o capelă înzestrată cu tot necesarul liturghic, pentru rugăciunea zilnică a personalului centrului.

Preot militar Constantin MĂGDOIU

BISERICA MILITARĂ „SFÂNTUL GHEORGHE ŞI EROII NEAMULUI" DIN GARNIZOANA BACĂU

Biserica Militară "Sfântul Gheorghe şi Eroii Neamului" din Garnizoana Bacău îşi are începuturile în visul primului preot militar al Bacăului după 1989 şi a credincioşilor în uniformă animaţi de dragostea de Dumnezeu şi de aproapele de a zidi lăcaş de închinare pentru militari. Astfel, acest vis capătă contur în data de 13 mai 1999, când se săvârşeşte de către Prea Sfinţitul Episcop Eftimie Luca cel Bun al Romanului slujba de sfinţire a locului viitoarei biserici.

În data de 1 septembrie 1999 se încep lucrările de zidire a bisericii cu toate etapele aferente. Transmisionişii băcăuani, împreună cu tot personalul din Sistemul Naţional de Apărare din Bacău, susţin şi participă activ la realizarea visului care se numeşte Biserica Militară din Bacău. Cu bucurii, realizări, împliniri dar şi piedici, greutăţi şi neajunsuri construcţia de zid iese din pământ şi se înalţă către cer. O dată cu această construcţie se zidesc şi sufletele militarilor cât mai aproape de Dumnezeu.

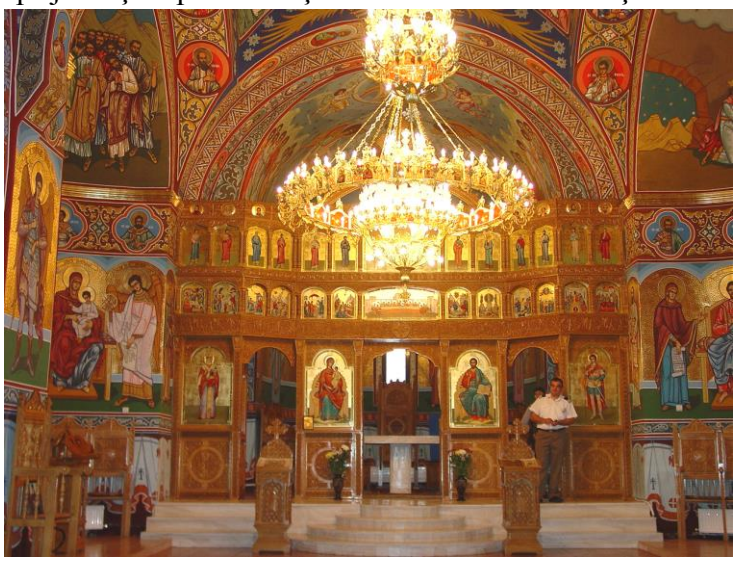
În anul 2000 biserica militarilor din Bacău primeşte vizita Mitropolitului Moldovei şi Bucovinei de atunci, actualul Patriarh al Bisericii Ortodoxe Române, Prea Fericitul Daniel. Deşi se plănuia sfinţirea pentru 2002, lipsa fondurilor a amânat-o pentru un an ulterior. Cu toate acestea, în anul 2002 s-au sfinţit crucile de pe turlele bisericii construite în stil ştefaniadă. Acoperişul a fost realizat de meşteri maramureşeni.

În anul 2004 biserica era zidită şi acoperită, iar pictura în tehnica fresco definitivată în Sf. Altar, dar tot în acest an, biserica îşi pierde ctitorul principal – preotul militar iconom stavrofor Iordache Pascariu, care pleacă la Dumnezeu la vârsta de doar 45 de ani. După pierderea camaradului lor, militarii se regrupează şi decid să continue visul părintelui Iordache. Se continuă pictura în stil neobizantin în toată biserica, se finalizează mobilierul bisericesc şi se termină finisajele începute.

După o muncă susţinută de 8 ani de zile, Biserica Militară "Sf. Gheorghe şi Eroii Neamului" primeşte Sfântul şi Marele Mir în data de 6 septembrie 2007. Finalizarea lucrărilor a fost coordonată de cel care a continuat plin de entuziasm şi dăruire visul conturat în 1999, preotul militar Lucian Butnaru. Sfinţirea bisericii a fost săvârşită de Preasfinţitul Episcop Vicar Ioachim Băcăuanul înconjurat de un impresionant sobor de preoţi şi diaconi alături de oficialităţi militare, reprezentanţi ai autorităţilor locale, invitaţi speciali şi mulţi credincioşi.

Este de menţionat faptul că atunci când construcţia bisericii a trecut prin momente dificile, personalul Centrului 115 Comunicaţii RMNC a fost cel care a intervenit prin ajutoare materiale dar şi pecuniare, susţinând definitivarea lăcaşului sufletelor lor.

Contribuţia personalului Centrului 115 Comunicaţii R.M.N.C. a fost una semnificativă atat din punct de vedere bănesc prin contribuţii benevole lunare dar mai ales prin sprijinul şi suportul susţinut de a vedea construcţia terminată.



S-au executat multe lucrări în cadrul construcţiei Bisericii Militare ctitorite de către personalul Unităţii Militare 01769 Bacău respectiv absida stângă a fost pictată din fondurile strânse de către ei precum şi o parte din străni şi pictura de pe spatele catapetesmei, lucruri evidenţiate şi în scris.

Acest sprijin al transmisioniştilor băcăuani a fost făcut din dragostea de Dumnezeu şi ca semn de mulţumire că sfântul lăcaş a poposit în această unitate de Dumnezeu păzită.

Preot militar Lucian Constantin BUTNARU

PARACLISUL BATALIONULUI INSTRUCŢIE COMUNICAŢII ŞI INFORMATICĂ „FRAŢII BUZEŞTI" DIN GARNIZOANA CRAIOVA

Paraclisul a apărut ca o completare a eforturilor comenzii unităţii de a asigura cele mai bune condiţii de trai, convieţuire şi instruire, atât pentru personalul propriu, dar mai ales pentru tinerii şi tinerele care îşi încep cariera militară în unitatea noastră prin parcurgerea modulelor de pregătire.

Având o dimensiune de 5,20 x 2,80 m, paraclisul se constituie într-un element de bază materială necesar procesului de instrucţie desfăşurat în unitatea noastră, facilitând asigurarea asistenţei religioase şi contribuind la îmbunătăţirea condiţiilor de recreere, de reculegere, de petrecere a timpului liber şi de recuperare a capacităţii de efort fizic.

Denumirea paraclisului a fost dată în cinstea Sfântului Mare Mucenic Gheorghe, Purtătorul de Biruinţă, patronul spiritual al Forţelor Terestre, fost general în armata română, care a sfârşit prin a fi decapitat pentru credinţa lui în Dumnezeu şi pentru faptul că a luat apărarea creştinilor, opunându-se distrugerii lăcaşelor de cult.

Desăvârşirea paraclisului a fost realizată de un colectiv de pictori condus de prof. Octavian Ciocşan în perioada mai – septembrie 2006, sub arhiereasca păstorire a Î.P.S. Teofan, pe atunci arhiepiscop al Craiovei şi Mitropolit al Olteniei.

Pentru amenajarea lăcaşului de cult, personalul unităţii a hotărât ca 2% din impozitul anual pe venit să fie direcţionat către construcţia bisericii de garnizoană, iar de aici, prin grija preotului de garnizoană Florin MIHALCEA şi cu sprijinul Î.P.S. dr Teofan Savu, au fost achiziţionate materialele necesare amenajării paraclisului şi a fost plătită contravaloarea picturii bisericeşti la interior.

Sfinţirea lăcaşului s-a săvârşit la data de 11.11.2006, de către un sobor de preoţi conduşi de P.S. Gurie Gorjeanu – episcop vicar al Mitropoliei Olteniei.

Activitatea de sfinţire a făcut parte din paleta de manifestări organizate cu prilejul depunerii jurământului militar de către ultima serie de militari în termen încorporaţi în vechiul sistem conscript.

Cu o cromatică aparte - ca de altfel orice pictură bisericească, reprezentând cele mai semnificative momente ale creştinătăţii, paraclisul simbolizează pe de o parte legătura străveche dintre armată şi biserică, dar şi exemplifică o dată în plus, dacă mai era nevoie, faptul că Armata României este una creştină, cu credinţă în Dumnezeu.

Poate că nu este întâmplător faptul că tinerii care se prezintă în unitate de bună voie, pentru a îmbrăţişa cariera militară, au ocazia de a se întâlni cu cealaltă instituţie aflată pe primul loc în topul încrederii populaţiei, alături de ARMATĂ – BISERICA.

Preot de garnizoană Florin MIHALCEA; preot Nicu LULĂ

BISERICA MILITARĂ A GARNIZOANEI ORADEA CU HRAMUL „SFÂNTUL MARE MUCENIC GHEORGHE”

Biserica militară din garnizoana Oradea, subordonată Centrului Militar Judeţean Bihor, poartă Hramul „Sfântul Mare Mucenic Gheorghe” – Purtătorul de biruinţă, sfânt ocrotitor al Trupelor Terestre. Acest sfânt locaş a fost înălţat pentru trebuinţele sufleteşti ale militarilor, cadrelor militare şi familiilor acestora, precum şi a tuturor credincioşilor care-i deschid uşile în duminici şi sărbători.

Biserica s-a construit în anul 2001, din contribuţia cadrelor militare din Oradea, atât cele ale

MApN, cât şi a altor structuri din municipiu, care şi-au manifestat dorinţa de a ajuta şi finaliza acest obiectiv.

Biserica a fost construită de firma S.C. RUSTIC S.R.L. – Baia Mare, societate condusă de ing. Cornel Cuşner, împreună cu echipa de lucru selecţionată în acest sens.

La data de 23 aprilie 2001, de Ziua Ocrotitorului Trupelor de Uscat „Sfântul Mare Mucenic Gheorghe", PS Sa dr. Ioan Mihălţan şi PS Sa dr. Petroniu Sălăjanul au târnosit Sfântul lăcaş al militarilor orădeni, de faţă fiind un număr mare de cadre militare şi credincioşi, preoţi şi reprezentanţi ai autorităţilor locale. Biserica a fost înzestrată cu toate cele necesare bunei desfăşurări ale rânduielilor bisericeşti, din donaţiile credincioşilor şi a cadrelor militare. De asemenea, preoţii din municipiu şi din Episcopia Ortodoxă a Oradiei au contribuit, după posibilităţi, la buna înzestrare a Bisericii.

Preot Mircea IONIŢĂ

SPAŢIUL SPIRITUAL DUHOVNICESC DIN CENTRUL 346 COMUNICAŢII RMNC – GARNIZOANA SEBEŞ

Pentru desfăşurarea asistenţei religioase în U.M. 01760 Sebeş, începând cu data de 01.07 2006, s-a amenajat un spaţiu spiritual duhovnicesc, cu sprijinul nemijlocit al comandantului şi aportul întregului personal în pavilionul „R" al unităţii, neexistând posibilitatea amenajării unei capele sau construirea unei biserici potrivit canoanelor şi rânduielilor bisericeşti.

Menţionez că este dotat cu toate cele necesare săvârşirii Sfintelor Taine şi Ierurgii, Sf. Evanghelie, Sf. Antimis, Sf. Vase (Potir şi Disc), Cruce cu picior şi alte obiecte liturgice care fac parte din altarul de campanie a preotului militar.

În acest spaţiu spiritual duhovnicesc militarii participă activ în sărbători la rugăciune şi Sfintele Taine a Spovedaniei, Împărtăşaniei şi la diferite rugăciuni necesare vieţii militarului, păstrând şi ducând mai departe frumoasele tradiţii şi obiceiuri ale Bisericii Ortodoxe Române.

Preot militar Ioan CĂRPINIŞAN

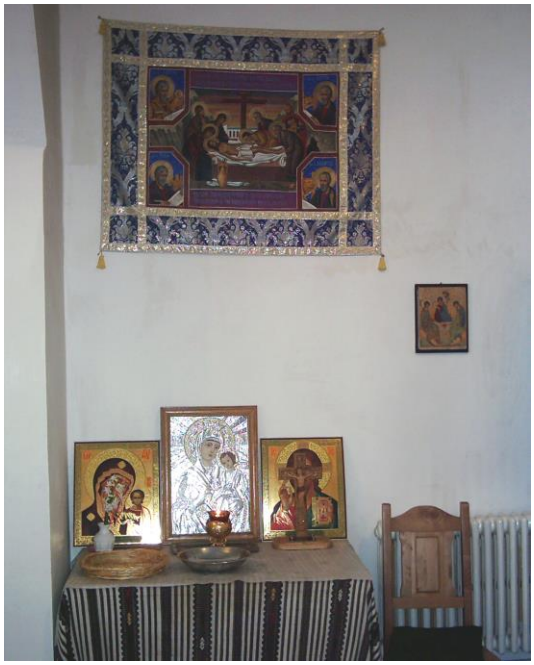
CAPELA CENTRULUI DE INSTRUIRE PENTRU COMUNICAŢII ŞI INFORMATICĂ – DECEBAL – SIBIU

În anul 2002, simţindu-se nevoia realizării unui spaţiu liturgic, care să vină în întâmpinarea personalului militar şi civil, a cursanţilor şi elevilor din centru, s-a hotărât realizarea unui proiect, al actualului col. (r) ing. Bădescu Constantin, ce viza amenajarea unui lăcaş de cult, de meditaţie şi rugăciune.

Prin bunăvoinţa comandantului unităţii, din acea perioadă, colonelul (r) Şerban Aurel şi a succesorului său, colonelul ing. (r) Crainic Dorin, dl. col. (r) Bădescu a coordonat întreaga activitate pentru realizarea capelei ortodoxe cu hramul Sf. Apostoli Petru şi Pavel.

Capela a fost sfinţită, la 12 decembrie 2002, de un sobor de preoţi format din PS Visarion Răşinăreanu, pe atunci episcop vicar al Sibiului, actual episcop al Tulcei, alături de preoţii Şpan

Gheorghe şi Şpan Mirel. De-a lungul anilor, au slujit Sfânta Liturghie în capela instituţiei noastre, PS Siluan actualul *episcop al Italiei* şi alţi preoţi, la loc de cinste în inimile credincioşilor, rămânând amintirea preotului Şpan Gheorghe.



Micul lăcaş de cult a contribuit decisiv la obţinerea de satisfacţii spirituale, linişte sufletească şi nu în ultimul rând, la motivarea personalului centrului în obţinerea de rezultate superioare în întreaga activitate.

Au fost luate măsuri specifice de a se permite accesul persoanelor din afara instituţiei care vor să participe la slujbele religioase şi care, conform tradiţiei creştine, vor să înalţe rugăciuni către Bunul Dumnezeu.

Din 2002 până în 2005 preotul unităţii a fost Şpan Mirel, în anul 2008, o dată cu restructurarea, funcţia de preot s-a desfiinţat.

Prin grija Arhiepiscopiei Sibiului, în momentul de faţă slujesc în capelă, benevol, preoţii: Iosif Toma, Damian Mircea, Marian Vlăduţ şi Vaida Cristian.

Capela s-a realizat cu sprijinul donatorilor din unitate, a sponsorizării de la SC Sibofarm SRL, cu contribuţia majoră a col. (r) ing. Bădescu Constantin, cu ajutorul substanţial al Mânăstirii Sf. Treime, din satul Strâmba - Jiu, jud. Gorj, de unde, s-au donat icoanele, prin intermediul Maicii Stareţe Marina. Iconostasul şi celelalte lucrări în lemn au fost realizate de dl. Drăghici Marcel, iar alte donaţii în icoane şi obiecte, pentru nevoile capelei, au avut loc şi după anul 2002.

În curtea centrului există un monument ridicat în memoria mr. p.m. Niţă Octavian, erou căzut la datorie în zilele revoluţiei din decembrie 1989, unde anual preoţii ce au slujit la capelă au săvârşit slujbe de pomenire.

Momentan, sub îndrumarea şi cu ajutorul nemijlocit a domnului comandant, colonel dr. Chirca Dorin, în curtea centrului de instruire se ridică o troiţă, cu efortul conjugat al personalului din instituţie şi cu aportul financiar al m.m. pr. Enescu Mihalache, consilier al comandantului pentru probleme de maiştri militari şi subofiţeri.

Să le ajute Dumnezeu tuturor celor care, de-a lungul timpului, au contribuit cu cât au putut, pentru a lăsa în urma lor ceva ... ceva care să încânte sufletul şi ochiul creştinului.

Mr. Hogea Ştefan

SEMNALE ŞI EVENIMENTE EDITORIALE

Colonel dr. Ionel CIOBANU
Comandamentul comunicaţiilor şi informaticii

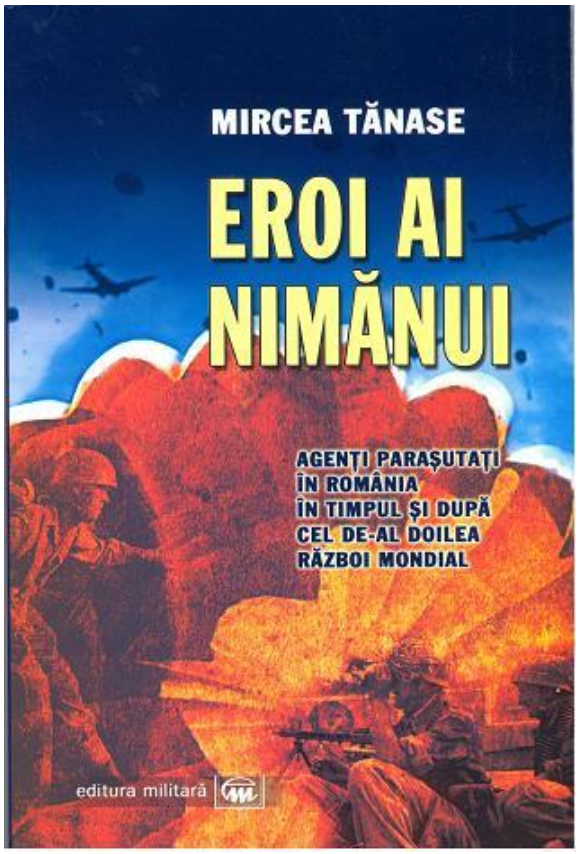
„EROI AI NIMĂNUI – Agenţi paraşutaţi în România în timpul şi după cel de-al doilea război mondial" – Mircea TĂNASE; Editura Militară, 2010.

După lecturarea lucrării, prima constatare pe care am făcut-o a fost aceea că autorul, distinsul nostru coleg, domnul col. dr. paraşutist transmisionist Mircea TĂNASE, Redactorul Şef al Revistei „Gândirea Militară Românească", şi-a continuat cu foarte mult succes frumoasa şi nobila misiune, de a reda pagini foarte bine scrise şi solid instrumentate istoric, principalele repere cunoscute sau am spune noi „cu osebire necunoscute" marelui public, din palpitanta istorie a trupelor de paraşutişti din Armata României, sau din cea a principalelor armate (germană şi sovietică), cu care ţara noastră a combătut în al Doilea război mondial.

Fin cunoscător al domeniului, „zburător" şi în acest moment, domnul colonel a studiat cu asiduitate în arhive, a avut discuţii cu foarte puţinii supravieţuitori ai vremurilor trecute şi a reuşit să ne aducă la lumină o reuşită lucrare, pe care o recomand cu căldură a fi citită şi ca o „carte de aventuri".

Structurată pe 6 capitole principale:

- Paraşutiştii – luptători pe frontul vizibil şi pe cel invizibil;
- Acţiuni ale paraşutiştilor militari inamici pe teritoriul României în perioada celui de-al doilea război mondial;
- Încercări de contracarare a actului de la 23 August 1944;
- Acţiunile grupurilor de paraşutişti în România după 23 August 1944;
- Cazul „ Schmidt – Stoicănescu/Operaţia „Miskolc";
- Paraşutaţi în România după încheierea



războiului.

Toate capitolele sunt interesante dar, pentru moment, doresc să vă stârnesc curiozitatea recomandându-vă „Operaţia Miskolc".

A reprezentat Grupul Etnic German, o alternativă pentru România ... Este Generalul Gheorghe Avramescu o victimă sau a complotat cu Guvernul de la Viena ... Cazul „Schimdt – Stoicănescu" – adevăr sau legendă ?

Cartea conţine 334 de pagini şi 4 anexe, este bine ancorată într-o bogată bibliografie şi se prezintă în condiţii grafice foarte bune.

Restituiri de suflet

Imi face o deosebita placere de a aduce in atentia cititorilor, nostalgici sau mai putin, cateva randuri primite de mine de la dl. actual colonel dr. Mircea TANASE ...dar scrise sub emotia primului grad , cel de locotenent.

LEGĂTURA RADIO

(tuturor celor care mai au nostalgia manipulatorului şi a legăturilor radio în cod Morse)

…undeva în dreapta, sus în dreapta, Carul Mare cu roţile împrăştiate în infinit. Noapte senină, undeva, mai în stânga, luna: mare, galbenă, trufaşă.

…somnul dulce, visele curmate dureros de mâna hotărâtă a plantonului: - *Scoală, e timpul, legătura…*

…umbra care se strecoară pe sub coroanele copacilor; luna, curioasă, îmi calcă înainte şi caută să-mi ghicească drumul spre staţia radio; ochii încă mi se mai închid spre a se deschide celuilalt tărâm, al viselor. Un clinchet de broască metalică ghicită în întuneric, deschisă printr-o rotire uşoară de cheie. Rând pe rând, unul după altul, trei becuri, apoi alte două, se înfig în întuneric. Roşii, galbene, verzi, se înfig în întunericul limpede al nopţii.

…mâna caută şi găseşte cu uşurinţa gestului reflex contacte, comutatoare, butoane. Clinchete seci de contacte metalice, arcuri eliberate de energie încătuşată, un zumzet care începe să toarcă egal, acele instrumentelor balansându-se spre stânga şi spre dreapta, mai mult spre dreapta, încă puţin, aşa, acum e bine, e maximum, manipulatorul apăsat, înalta tensiune cuplată, câteva mii de volţi încep să se zbată şi să lovească cu înverşunare grilele tuburilor electronice, după care se înghesuie spre antene, spre infinitul eter; aceleaşi ace ale instrumentelor se avântă de-acum hotărâte spre dreapta cadranelor luminate, mâna dreaptă apasă în continuare manipulatorul în timp ce stânga mângâie acordul fin, încă puţin înainte, ba nu, puţin înapoi – am spus că mâna doar mângâie acordul fin! – atât, emiţătorul e acordat, de-acum miile de kilohertzi călare pe caii putere ai staţiei fierb, dau în clocot la ieşirea spre antenă, o singură apăsare de buton şi vor trece prin spaţii cu viteza luminii, undele hertziene vor învălui pământul, căutându-şi perechea de antenă rezonantă, înălţată şi ea ca o dorinţă, aşteptând cu înfiorare să fie atinsă de această lumină nevăzută…

…receptorul staţiei în dreapta, comutatorul de subgame adună şi scade într-o matematică ameţitoare megahertzii, kilohertzii…, pocnete seci în căşti, fluieratul sacadat al telexurilor, frânturi de muzică, undeva la capătul benzii un clasament al hit-urilor de ultimă oră, poate Monte Carlo, poate Roma, la B.B.C. clopotele Big Ben-ului răsună în noaptea londoneză, la Moscova se transmit ştirile de dimineaţă, în câteva secunde toată Europa şi o parte din Asia trec prin căşti, cimpoaiele balcanice şi baiânele ruseşti se aud parcă cel mai bine, uite şi un radio-amator, ăştia n-au somn, domnule, la ora asta…, sau e vreunul din partea cu soare a globului…

…mâna învârte febril, înciudat, acordul brut, muzica şi radioamatorii rămân pentru altădată, acum în căşti doar pocnituri şi fluierături, se simte parcă intersectarea cu undele purtătoare din eter, cifrele se rotesc înnebunite pe cadran, încă puţin, da, acordul fin, mâna mângâie din nou acordul fin, deviaţia maximă a acelor… şi de-acum doar aşteptare, răbdare, auzul încordat până la durere, priviri rugătoare la ceas, zgomot uşor de file întoarse, data şi ora înscrise în jurnalul staţiei… şi din nou aşteptare,

privirea rotindu-se încă o dată jur-împrejurul panourilor pline cu becuri, scale, butoane, comutatoare, instrumente de măsură. În spatele lor o mulţime de tuburi electronice, diode, tranzistoare, relee, un vârf al electronicii în continuă evoluţie, toate evoluează pe lumea asta, rămân la fel sau aproape la fel – până când oare? – numai lucrurile mari şi aproape perfecte. De exemplu, alfabetul domnului Morse, americanul acela care – nu ştiu dacă şi-a dat seama atunci – a creat o limbă internaţională: linie-punct-linie… un *ESPERANTO* pentru cei iniţiaţi, pentru cei acordaţi pe aceeaşi frecvenţă, pentru toţi *corespondenţii* care acum, ca şi mine, aşteaptă încordaţi chemarea, apelul, legătura între staţiile risipite pe harta ţării, sub Carul Mare…

…tresărire la fiecare semnal în cască, nervi întinşi la maximum, un semnal imperceptibil aproape, parcă şoptit, volumul dat repede la maximum, nu, nu e el, e alt indicativ, pe cine-o căuta pe aici, uite că nu-i răspunde nimeni, sau poate că-i răspunde s-audă numai el, e şi aici o chestie… de tehnică a legăturii.

…ar fi trebuit să vină, e timpul, toţi ceilalţi din reţea îl aşteaptă. Tăcere, în continuare tăcere, ba nu, ce-a fost asta? …un sunet prelung, încă unul, în sfârşit! a venit, s-a acordat, îl simt de fiecare dată când vine, ştiu dacă e vesel sau supărat, asta se simte din fermitatea sau tremurul semnalului, parcă îl văd aplecat asupra manipulatorului, îl cunosc fără să-l fi văzut vreodată...

…apelul, o combinaţie de litere şi cifre, un fel de nume codificat, eu sunt AQ5H, tu eşti RN6Z, el este…ne chemăm pe rând şi răspundem tot pe rând, puncte şi linii prefăcute în comenzi pentru mâna care apasă manipulatorul sau care scrie în jurnalul staţiei…da, te aud foarte bine, parola mea este…şi aşa mai departe, până când totul e OK, da, chiar aşa se şi transmite, OK, în linii şi puncte, pentru că totul este o înlănţuire de linii şi puncte în limba aceasta a privilegiaţilor cunoscători ai alfabetului Morse şi ai codului de comunicări radio. Da, totul e OK, legătura funcţionează normal, ne *vedem* la următoarea, acum am făcut doar o verificare, dar dacă va fi nevoie… vom fi la legătură.

…becurile roşii, galbene, verzi se sting pe rând, staţia se opreşte din tors, receptorul închide şi el ochii şi îndeamnă la somn – la ce-a mai rămas din noapte – o uşoară părere de rău după topurile şi ritmurile de pe întreg mapamondul încătuşate în interiorul acestor panouri metalice, poate mâine seară…aceiaşi promisiune amânată de fiecare dată; lumina din plafonieră se topeşte încet, clinchet de broască închisă, în urechi locul liniilor şi punctelor lui Morse este luat de cântecul greierilor ieşiţi şi ei la *legătură* la ora asta, umbra neagră strecurată pe sub copaci, luna la fel de galbenă, dar parcă mai puţin trufaşă, tot acolo, deasupra, în stânga Carului Mare cu roţile împrăştiate în infinit…

Colonel dr. Mircea Tănase

(scrisă în 1986 când eram locotenent, comandant pluton radio la Regimentul 60 Paraşutişti Buzău)

„MAGNETICA – 80 de ani – Mii de vieţi într-o singură familie" – Adrian N. IONESCU şi Victor CHIRILĂ; Editura Economică, 2010

Carte document, prezintă în mod succint 80 de ani de istorie, de realizări şi momente decisive, ale uneia dintre cele mai reprezentative uzine din România – „Electromagnetica".

„Frumuseţea" lucrării este, în opinia mea, dată de folosirea cu înţelepciune a interviurilor cu oamenii ce au lucrat in intrepridere de la înfiinţare şi până în prezent,simultan sau mai bine spus, pas cu pas, cu prezentarea faptelor, cifrelor, realizărilor tehnice.

Foarte importantă mi se pare prezentarea încă de la început a unei „Cărţi de vizită seculară", a unei „Table de materii" cum inspirat au denumit-o autorii –

„a unui sinoptic cu ideile vii ale fiinţei vii pe nume Electromagnetica”.

Mărturisesc că studierea cu răbdare şi atenţie a acestuia, mi-a deschis curiozitatea de a citi ulterior cartea, capitol după capitol.

Îmi este foarte greu să enumăr toate capitolele datorită lipsei spaţiului editorial, dar totuşi doresc să emfazez enunţurile Secţiunilor:

- Secţiunea I. Anii 1990–2000: Viziunea dezvoltării durabile;
- Secţiunea a II-a. Anii 1930-1940: Începuturile strategice;
- Secţiunea a III-a. Anii 1950-1960: Electromagnetica în febra dezvoltării totale;
- Secţiunea a IV-a. Anii 1970: Apogeul. Anii 1980: Oamenii depăşesc limitele sistemului;
- Secţiunea a V-a. Producţia militară după 1950;
- Secţiunea a VI-a. Proprietăţi şi servicii imobiliare;
- Secţiunea a VII-a. Mărturiile oamenilor de la Magnetica.

Pe bună dreptate aş putea fi întrebat, ce caută recenzia unei cărţi ce face „apologia” unei firme private, în paginile unei reviste militare.

Sunt convins că răspunsul a fost dat prin prezentarea secţiunii: Producţia militară după 1950.

Acest capitol căruia i-au fost alocate 15 pagini, respectiv 15% din corpul principal al lucrării, necesită o studiere mai atentă.

Autorii prezintă argumentat ştiinţific începuturile, dezvoltarea cronologică, apogeul şi starea actuală (decăderea) Fabricii de Produse speciale a companiei.

Întrepătrunderea în cei peste 60 de ani, a producţiei de tehnică militară din domeniul transmisiunilor (comunicaţiilor) a fabricii, cu arma pe care o sărbătorim astăzi, apreciez eu, că aduce suficiente argumente pentru apariţia în revistă.

„PRODUCŢIA SPECIALĂ – 1930-2010 - ELECTROMAGNETICA”
Redactor şef: Gral.mr.(r) ing. Ionel DUMITRESCU; Editura Andromeda Company

Încă de la începutul recenziei acestei lucrări, vă mărturisesc că eram absolut convins, cunoscând stilul deosebit de vivace şi de nonconformist al redactorului şef, stimabilul nostru predecesor, dl.gral mr.(r) ing. Ionel DUMITRESCU, că lucrarea nu este ceea ce părea a fi: o simplă monografie a realizărilor uzinei ELECTROMAGNETICA în domeniul apărării naţionale, în cei 80 de ani de colaborare, un capitol mai detaliat al celeilalte lucrări aniversare „MAGNETICA – 80 de ani – Mii de vieti într-o singură familie” ..... Şi nu m-am înşelat !

Lucrarea se constituie într-o frumoasă elegie, de oameni, fapte şi relatări, a unor evenimente deosebit de importante în evoluţia dotării cu armament şi tehnică a Armatei României, cu emfazarea evidentă a domeniului comunicaţii şi informatică, specific „producţiei speciale” a Electromagenticii.

Cartea are vervă, consistenţă, prezintă documente, realizări şi pe oamenii care au stat la baza edificării industriei naţionale de armament.

Din paginile cărţii ne zâmbesc şi ne prezintă pe scurt etape foarte importante din cariera lor, cu aplecare spre domeniul analizat, foşti miniştri ai apărării şi ai industriilor, foşti şefi ai Statului Major General şi ai Departamentului de Înzestrare al Armatei, generali şi ofiţeri ce au activat ca reprezentanţi militari în ministerele şi uzinele de „producţie specială”, în cercetare şi în învăţământ, alături de cei care la trupe, au testat şi folosit tehnica produsă. Deosebit de interesante mi s-au părut şi articolele scrise de persoanele cu funcţii de conducere şi decizie din conducerea Electromagneticii (directori generali, directori pentru „producţia specială”, ingineri şi tehnicieni etc.), ce au prezentat în termeni elogioşi şi realişti, anii de frământări, de căutări, de adaptări şi de inovaţie, desfăşuraţi împreună cu specialiştii militari ce au făcut posibilă producerea în România a aparaturii de comunicaţii şi informatică, în condiţiile deosebit de grele ale Războiului Rece, de interzicere a importului de „know-how” din ţările puternic industrializate, toate pe fondul interzicerii folosirii unor fonduri financiare necesare, în special în deceniile opt şi nouă ale secolului trecut.

Ritmul şi periodicitatea prezentărilor, civil-militară şi invers, ne ţine atenţia trează şi ne face părtaşi fizic şi emoţional la această „odisee” a producţiei speciale. Îmi este foarte greu să remarc sau să pun într-o lumină mai bună o prezentare sau alta, fără a face o nedreptate.

Cartea este realizată în condiţii grafice foarte bune, conţine 360 de pagini, cu relatări, scheme şi albume foto, fiind structurată pe: Cuvânt înainte (ing. Eugen SCHEUŞAN – director general S.C. ELECTROMAGNETICA S.A.), Cuvântul redactorului şef, 42 de articole şi un Album Foto.

Special am lăsat la sfârşit câteva consideraţii pe care doresc să le fac la adresa domnului gral.mr.(r)ing. Ionel

DUMITRESCU, redactorul şef şi sufletul acestei lucrări.

Noutatea pe care o introduce acum constă în notele de subsol. Ori de câte ori apreciază că este necesar, intervine cu scurte prezentări ale autorilor sau nota bene cu păreri personale, care nevrând să altereze articolul scris de autor, face de cele mai multe ori să clarifice anumite evenimente sau fapte şi de ce nu, să pună în faţa cititorilor şi un alt gen de întrebări. Este evident că domnul general este consecvent cu sine însuşi în anumite probleme şi aserţiuni, pe care, din motive subiective, nu doresc să le nominalizez, dar vă mărturisesc că le-am verificat şi în alte cărţi ale domniei sale.

Felicitările noastre pentru frumosul produs literar întocmit de colectivul redacţional şi urăm mult succes dl. gral.mr.(r) ing. Ionel DUMITRESCU, în onoranta poziţiei de „Şef al rezerviştilor din arma comunicaţii, informatică şi război electronic".

TEZĂ DE DOCTORAT : CONTRIBUŢII PRIVIND STUDIUL ŞI IMPLEMENTAREA ARHITECTURII DE SECURITATE PENTRU SISTEMELE DE RADIOCOMUNICAŢII ÎN STANDARD TETRA. Autor col. Marian BURIC, Academia Tehnică Militară, 2011.

Obiectivul principal al lucrării îl reprezintă analiza detaliată a aspectelor de securitate pentru sistemul de radiocomunicaţii în standard TETRA şi propunerea de noi soluţii care fie să se constituie ca soluţii complementare la mecanismele de securitate existente fie să se constituie ca noi puncte de vedere în abordarea domeniului de securitate pentru acest sistem.

Teza este structurată în şase capitole. în primul capitol se prezintă în mod succint arhitectura şi componentele sistemului de radiocomunicaţii TETRA, în conformitate cu standardul ETSI. Prezentarea este realizată prin prisma primelor trei niveluri ale arhitecturii OSI (fizic, al legăturii de date şi reţea), niveluri ce sunt definitorii pentru descrierea standardului TETRA. în cadrul descrierii se accentuează pe nivelurile şi componentele din cadrul acestora care sunt determinante în implementarea şi derularea mecanismelor de securitate.

Capitolul al doilea are ca obiectiv prezentarea unei prime metodologii prin care se poate implementa o arhitectură de securitate, aplicabilă sistemelor de radiocomunicaţii în standard TETRA - cea oferită prin Recomandarea ITU-T X.805. Mai întâi se definesc termenii de ameninţare, atac, securitate şi vulnerabilitate. Se trec apoi succint în revistă tipologiile de ameninţări, consecinţele materializării acestora şi factorii care le determină.

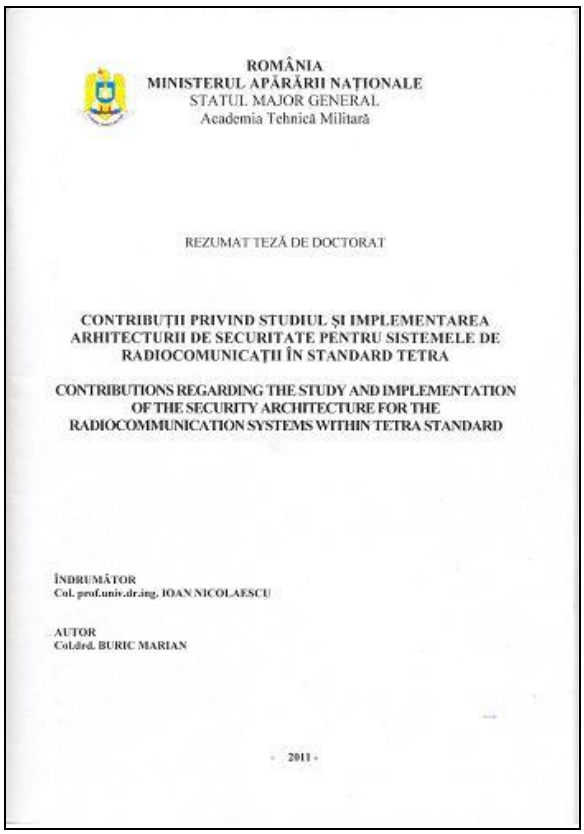
În capitolul al treilea sunt analizate mecanismele de securitate la nivelul interfeţei spaţiale: autentificarea, criptarea, managementul cheilor criptografice şi cel de activare/dezactivare a terminalelor şi utilizatorilor. Este pusă în evidenţă flexibilitatea sistemului din punct de vedere al securităţii evidenţiind posibilitatea de scalabilitate a mecanismelor de securitate în funcţie de profilurile de securitate ale utilizatorilor. Un aspect important al managementului cheilor de criptare, avut în vedere în cadrul acestui capitol, îl reprezintă criptoperioadele pentru cheile criptografice. S-a propus astfel, plecând de la analiza riscurilor, o variantă modificată în comparaţie cu cea prevăzută de standardul ETSI EN 300 392-7, pentru o categorie de utilizatori denumită generic „Public Safety".

Capitolul al patrulea abordează domeniul mecanismului de criptare „End-To-End" în sistemele de radiocomunicaţii în standard TETRA.

Sunt prezentate două categorii de soluţii de criptare:

- O primă categorie ce utilizează algoritmi şi chei simetrice.

- A doua, propusă şi verificată practic de autor, este o categorie hibridă, în care sunt utilizaţi algoritmi cu chei publice pentru stabilirea cheilor de criptare de sesiune şi autentificarea utilizatorilor şi apoi un algoritm simetric şi cheia de criptare de sesiune stabilită anterior, pentru criptarea comunicaţiilor dintre cei doi utilizatori. Un alt element de noutate al acestei soluţii îl reprezintă faptul că este destinată nu doar pentru criptarea comunicaţiilor între terminalele TETRA ci şi pe cele dintre un terminal TETRA şi un terminal GSM sau PSTN.



ROMÂNIA
MINISTERUL APĂRĂRII NAȚIONALE
STATUL MAJOR GENERAL
Academia Tehnică Militară

REZUMAT TEZĂ DE DOCTORAT

CONTRIBUȚII PRIVIND STUDIUL ȘI IMPLEMENTAREA ARHITECTURII DE SECURITATE PENTRU SISTEMELE DE RADIOCOMUNICAȚII ÎN STANDARD TETRA

CONTRIBUTIONS REGARDING THE STUDY AND IMPLEMENTATION OF THE SECURITY ARCHITECTURE FOR THE RADIOCOMMUNICATION SYSTEMS WITHIN TETRA STANDARD

ÎNDRUMĂTOR
Col. prof.univ.dr.ing. IOAN NICOLAESCU

AUTOR
Col.drd. BURIC MARIAN

- 2011 -

În capitolul al cincilea sunt analizate profilurile de securitate ale utilizatorilor din punct de vedere al mecanismului de criptare „End-To-End". Sunt definite trei categorii de utilizatori, pentru fiecare realizându-se o descriere generală, se schiţează modul în care sunt percepute ameninţările, cerinţele mecanismului de criptare „End-To-End", algoritmii de criptare utilizaţi şi cerinţele de implementare. Scopul acestui capitol este de a propune, în funcţie de profilul utilizatorilor, soluţii diferite pentru algoritmii criptografici utilizaţi, tipul şi lungimea cheilor de criptare, soluţiile de management a cheilor şi de implementare.

În capitolul al şaselea se porneşte de la ideea că un nivel corespunzător de securitate, pentru un sistem de radiocomunicaţii în standard TETRA, reprezintă mai mult decât mecanismele de securitate prezentate şi descrise în capitolele anterioare. Securitatea trebuie să aibă în vedere o abordare echilibrată a aspectelor tehnice, de personal, fizice şi procedurale. Plecând de la această idee se scoate în evidenţă necesitatea unei metode coerente şi comprehensive de analiză şi management a riscurilor pentru sistemul de radiocomunicaţii în standard TETRA. Se propune în acest scop metoda CRAMM. Metoda aleasă este apoi prezentată şi aplicată pentru un sistem de radiocomunicaţii în standard TETRA.

Ultimul capitol conţine concluziile care se desprind din acest studiu şi subliniază contribuţiile aduse de autor la studiul şi implementarea arhitecturii de securitate pentru sistemele de radiocomunicaţii în standard TETRA.


BASIC