

REVISTA COMUNICAȚIILOR ȘI INFORMATICII

- NUMĂR SPECIAL -



**A XXXV-a aniversare a
Batalionului Instrucție Comunicații și Informatică
"FRAȚII BUZEȘTI"**

Nr. 1/2015

**REVISTA
COMUNICAȚIILOR ȘI INFORMATICII**
fondată sub denumirea
BULETINUL TRANSMISIUNILOR

editată de
**Centrul de Instruire pentru Comunicații și Informatică
„Decebal“**

sub îndrumarea
Direcției Comunicații și Informatică
și a
Comandamentului Comunicațiilor și Informaticii

Coordonatori științifici:
Col. dr. Valentin BECHERU
Gl. bg. Radu-Marius POP
Col. dr. ing. Costică POSTOLACHE
Col. dr. Ionel CIOBANU

Redactor șef:
Col. dr. Dorin ALEXANDRESCU

Redactori:
Col. Octavian RAȚIU
Lt. col. dr. ing. Mircea BORA
Mr. Daniel-Gheorghe DURDUN

Procesare text și fotografii:
Plt.maj. Daniel SUCIU
P.c.c. Karin TIUCĂ-LEUTSCHAFT

ADRESA REDACȚIEI:

SIBIU, Bd. V. Milea, nr. 3-5, jud. Sibiu
Telefoane: 0269233930
int. 106, 241

**Răspunderea juridică pentru materialele publicate aparține autorilor,
în conformitate cu prevederile Legii nr. 206 din 27.05.2004.**

ISSN: 1841-0758

**Tiparul a fost executat
la Centrul Tehnic Editorial al Armatei
sub comanda.....**

CUPRINS

EVENIMENT

Mesajul șefului Direcției Comunicații și Informatică	3
- Colonel Dr. Valentin BECHERU	
Ordinul comandantului Comandamentului Comunicațiilor și Informaticii	4
- General de brigadă Radu-Marius POP	
Mesajul șefului Direcției Pregătirea Teritoriului pentru Apărare și Rechiziții	6
- General de brigadă Dr. Dorin CHIRCA	
Mesajul comandantului Brigăzii 2 Infanterie „Rovine”	7
- General de brigadă Dorin BLAIU	
Mesajul comandantului Centrului de Instruire pentru Comunicații și Informatică „Decebal”	8
- Colonel Dr. Dorin ALEXANDRESCU	
Batalionul Instrucție Comunicații și Informatică „Frații Buzești” – istorie, performanță și devenire	9
- Colonel Dr. Gheorghe DINCA	
Scurt istoric al Batalionului Instrucție Comunicații și Informatică „Frații Buzești”	12
- Maior Ionuț-Daniel ȘERBAN	
Batalionul Instrucție Comunicații și Informatică „Frații Buzești” – 35 de ani în slujba armii comunicații și informatică	15
- Locotenent-colonel Leonide CUNE	
Gânduri la ceas aniversar – o unitate cu statut de carte de vizită	18
- Colonel Marian APOSTOL	

INSTRUCTIE ȘI ÎNVĂȚĂMÂNT

Baza materială – rol determinant în procesul de instrucție din Batalionul Instrucție Comunicații și Informatică „Frații Buzești”	20
- Locotenent-colonel Ionel CRĂCIUN	
Unele opinii privind relația intrinsecă dintre educație și instrucție	22
- Locotenent-colonel Torino NUȚĂ	
Opinii privind interdependența/relaționarea procesului patrimonial cu procesul managerial în Batalionul Instrucție Comunicații și Informatică „Frații Buzești”	26
- Maior Cornel DRĂGHICI	
Batalionul de instrucție – particularități manageriale	28
- Maior Ionuț-Daniel ȘERBAN	
Instrucția individuală în domeniul apărării cibernetice - factor esențial în securitatea sistemelor informatice și de comunicații	30
- Maior Cătălin GHERGHEL	
Motivarea personalului pentru îndeplinirea obiectivelor	34
- Căpitan Daniel DACICA	
Concepția de elaborare a PAAP în vederea asigurării unor condiții optime de instruire pentru soldații și gradații profesioniști	37

- Căpitan Cezar MAICAN

Stilurile de leadership utilizate de către comandantul de pluton în instruirea soldaților profesioniști și eficiența acestora 39

- Locotenent Răducu OPREA

ACTUALITATE ȘI PERSPECTIVE/OPINII

Radiațiile electromagnetice și efectul lor asupra sănătății populației - un pericol pentru sănătate? 43

- Locotenent-colonel Dinu BUTALIU

Inițiativa forțe inter-conectate 46

- Locotenent-colonel dr. Gheorghe-Adrian GÎRTONEA

Criptografie bazată pe matematica curbelor eliptice 50

- Maior George ZAMĂ

Mentenanța echipamentelor militare..... 52

- Maior Silviu SĂPOI

Planificarea, organizarea și exercitarea controlului managementului logistic la nivelul unității..... 54

- Maior Cristian STATE

Analiză comparativă privind hrănirea personalului Armatei României 55

- Maior Marius CHIRIȚĂ

Securitatea cibernetică – necesitate a secolului al XXI-lea..... 60

- Căpitan Gabriel-Nicușor IANCU-IACOB

Unele opinii privind adaptarea instrucției de comunicații și informatică la mediul internațional actual 63

- Locotenent Iulian ACSINTE

Spațiul cibernetic - principala sursă de amenințări 68

- Locotenent Daniel CALCIU

Despre criptografie, criptanaliză și criptologie..... 70

- Locotenent Adrian VĂTAFU

Voice over IP – soluție unificată de comunicații ca premisă a comunicațiilor inteligente 73

- Sublocotenent Teodor MITREA

Războiul bazat pe rețea și importanța specialiștilor de comunicații și informatică 77

- Sublocotenent Alexandra-Cerasela AVRAM

Standardul IEEE 802.11 în rețelele de comunicații wireless 79

- Sublocotenent Daniel RISTEA

IN MEMORIAM

Radiorelee germane din cel de-al doilea război mondial 83

- Locotenent-colonel Cătălin DASCĂLU

DISTINCTII

Acordarea distincției militare cu denumirea onorifică „Omul anului 2014” în Comandamentul Comunicațiilor și Informaticii 87

M E S A J U L

ȘEFULUI DIRECȚIEI COMUNICAȚII ȘI INFORMATICĂ PRIVIND ANIVERSAREA A 35 DE ANI DE LA ÎNFIINȚAREA BATALIONULUI INSTRUCȚIE COMUNICAȚII ȘI INFORMATICĂ „FRAȚII BUZEȘTI”



01.06.2015 este o zi importantă în calendarul armei comunicații și informatică, este ziua în care BATALIONUL INSTRUCȚIE COMUNICAȚII ȘI INFORMATICĂ „FRAȚII BUZEȘTI” aniversează 35 de ani de existență puși în slujba armeei.

Continuator al tradițiilor de luptă ale Regimentului 46 Transmisiuni și Bazei 14 Instrucție Transmisiuni, batalionul se prezintă, la ceas aniversar, ca o unitate de elită a armei comunicații și informatică, care, an de an, și-a îndeplinit cu profesionalism misiunile încredințate, atât pe timpul exercițiilor și aplicațiilor, dar mai ales pe linia instruirii soldaților și gradaților profesioniști ai armeei.

BATALIONUL INSTRUCȚIE COMUNICAȚII ȘI INFORMATICĂ „FRAȚII BUZEȘTI” se află, astăzi, alături de întreaga armată, într-un continuu proces de modernizare a bazei materiale de instrucție necesar asigurării celor mai bune condiții de instruire a soldaților și gradaților profesioniști, astfel încât să fie în măsură să asigure formarea și perfecționarea unor specialiști de comunicații și informatică bine pregătiți și capabili să își îndeplinească misiunile în domeniul CIS, atât în țară, cât și în teatrele de operații.

Doamnelor și domnilor ofițeri, maiștri militari, subofițeri, soldați și gradați profesioniști, personal civil contractual,

Ați demonstrat, în cei 35 de ani de existență a unității, calități profesionale deosebite, implicare și determinare, hotărâre, devotament și pasiune în îndeplinirea misiunilor.

Pentru maniera profesionistă și comportamentul exemplar dovedite în îndeplinirea misiunilor, transmisioniștilor din unitatea dumneavoastră li s-au conferit distincții și medalii, iar Drapelul de luptă a fost decorat în numeroase rânduri.

Aționați și de acum înainte cu aceeași dăruire pentru dezvoltarea cunoștințelor teoretice și perfecționarea deprinderilor practice în lucrul cu tehnica de comunicații și informatică, iar scopul dumneavoastră să fie acela de creștere a prestigiului armeei pe care o reprezentați.

Deviza „ONOARE ȘI PATRIE”, înscrisă pe Drapelul de luptă, să vă motiveze ca unitatea dumneavoastră să devină „batalionul viitorului”, unitate-model pentru întreaga Armată a României.

În această zi de sărbătoare, gândurile noastre se îndreaptă, în egală măsură, spre efortul și dăruirea înaintașilor dumneavoastră, spre munca și eforturile tuturor aceluia care, prin dăruire, loialitate, curaj, altruism și responsabilitate, au transformat această unitate într-una de elită a armei comunicații și informatică și a Armatei României.

Cu prilejul sărbătoririi a 35 ani de la înființarea BATALIONULUI INSTRUCȚIE COMUNICAȚII ȘI INFORMATICĂ „FRAȚII BUZEȘTI”, vă transmit felicitările mele și ale personalului Direcției Comunicații și Informatică pentru modul ireproșabil în care vă desfășurați activitatea și vă urez noi succese în îndeplinirea misiunilor ce vă revin, realizări profesionale remarcabile, multă sănătate dumneavoastră și familiilor dumneavoastră.

LA MULȚI ANI!

ȘEFUL DIRECȚIEI COMUNICAȚII ȘI INFORMATICĂ

Colonel

Dr. Valentin BECHERU

ORDINUL COMANDANTULUI COMANDAMENTULUI COMUNICAȚIILOR ȘI INFORMATICII PRIVIND SĂRBĂTORIREA A 35 DE ANI DE LA ÎNFIINȚAREA BATALIONULUI INSTRUCȚIE COMUNICAȚII ȘI INFORMATICĂ „FRAȚII BUZEȘTI”



La 1 iunie 2015, sărbătorim 35 de ani de la înființarea Batalionului Instrucție Comunicații și Informatică „FRAȚII BUZEȘTI”, continuator al tradițiilor de luptă ale Regimentului 46 Transmișiuni.

În cele 3 decenii și jumătate de existență, unitatea a cunoscut o serie de transformări structurale și funcționale în acord cu misiunile și responsabilitățile primite.

Continuând frumoasele tradiții ale armeei comunicații și informatică, personalul unității a instruit și format numeroase contingente de militari, obținând an de an rezultate remarcabile pe timpul pregătirii și desfășurării instrucției individuale, a

exercițiilor și antrenamentelor.

În contextul procesului de modernizare și transformare a societății, în general, și a armatei, în mod special, Batalionului Instrucție Comunicații și Informatică „FRAȚII BUZEȘTI” îi revin misiuni și responsabilități extrem de importante și precise în formarea, specializarea și perfecționarea soldaților și gradaților profesioniști din arma comunicații și informatică și, împreună cu celelalte unități din subordinea Comandamentului Comunicațiilor și Informaticii, în participarea la realizarea și implementarea sistemelor C4I2SR.

În prezent, Batalionul Instrucție Comunicații și Informatică „FRAȚII BUZEȘTI” este angrenat, alături de întreaga armată, într-un amplu proces de modernizare a infrastructurii necesare creării condițiilor optime de instruire a personalului pentru îndeplinirea misiunilor la cele mai înalte standarde.

Doamnelor, domnișoarelor și domnilor ofițeri, maiștri militari și subofițeri, soldați și gradați profesioniști, personal civil contractual,

Reprezentați una dintre cele mai importante unități de comunicații și informatică ale armatei noastre.

Ați demonstrat până acum calități profesionale deosebite și o mare capacitate de adaptare la noile cerințe de compatibilitate și interoperabilitate cu structurile similare ale NATO, ceea ce ne conferă garanția că puteți continua cu succes să vă aduceți contribuția la continuarea procesului de profesionalizare a Armatei României și la obiectivul de aderare deplină a Armatei României la cadrul general în domeniul instrucției și exercițiilor stabilit la nivelul Alianței.

Decizia de decorare a Drapelului de luptă al Batalionului Instrucție Comunicații și Informatică „FRAȚII BUZEȘTI” cu „Emblema de Onoare a Armatei României” cu însemn de război cu ocazia festivității prilejuite de retragerea Armatei României din Teatrul de Operații din Afganistan – provincia Zabul, reprezintă recunoașterea, de către factorii de conducere ai Ministerului Apărării Naționale, a valorii intrinseci a unității.

Fiți demni de misiunea ce vi s-a încredințat! Formați specialiști din ce în ce mai bine pregătiți în arma comunicații și informatică! Acționați cu hotărâre pentru însușirea cunoștințelor militare generale și de specialitate, pregătiți-vă temeinic pentru a fi în măsură să lucrați cu echipamentele și sistemele de comunicații și informatice din dotarea unității, precum și cu cele care vor intra în înzestrare în perioada imediat următoare!

Muncați cu tenacitate și profesionalism pentru creșterea prestigiului armeei comunicații și informatică!

Dovediți un înalt spirit civic și patriotism în tot ceea ce întreprindeți sub deviza: „ONOARE ȘI PATRIE”, înscrisă pe Drapelul de luptă!

* * *

În această zi, când sărbătorim 35 de ani de la înființarea Batalionului Instrucție Comunicații și Informatică „FRAȚII BUZEȘTI”, aduc mulțumiri întregului personal activ, în rezervă și retragere, pentru rezultatele remarcabile obținute în întreaga perioadă.

Vă felicit și vă doresc succes în îndeplinirea misiunilor care v-au fost încredințate!

La mulți ani!

**COMANDANTUL COMANDAMENTULUI
COMUNICAȚILOR ȘI INFORMATICII
General de brigadă**

Radu-Marius POP

M E S A J U L
ȘEFULUI DIRECȚIEI
PREGĂTIREA TERITORIULUI PENTRU APĂRARE ȘI RECHIZIȚII
CU OCAZIA SĂRBĂTORIRII CELEI DE-A XXXV-A ANIVERSĂRI A
BATALIONULUI INSTRUCȚIE COMUNICAȚII ȘI INFORMATICĂ
„FRAȚII BUZEȘTI”



Aniversarea la data de 01.06.2015 a **BATALIONULUI INSTRUCȚIE COMUNICAȚII ȘI INFORMATICĂ „FRAȚII BUZEȘTI”**, continuator al Regimentului 46 Transmisiuni, înființat prin Ordinul General al Ministrului Apărării Naționale nr. 008 din 02 aprilie 1980, transformat ulterior în Bază de instrucție, iar acum, sub actuala structură și denumire, îmi oferă plăcutul prilej de a adresa un mesaj camaraderesc acestei unități de care mă leagă numai amintiri frumoase.

Fac acest lucru și pentru faptul că în perioada cât am exercitat funcția de **comandant al Centrului 346 Comunicații R.M.N.C.** am fost beneficiarul militarilor instruiți în baza de instrucție sau în batalionul de instrucție, dar mai ales prin prisma faptului că în perioada 2009-2013, fiind **Comandantul Centrului de Instruire pentru Comunicații și Informatică „DECEBAL”**, am conlucrat direct cu această unitate, am cunoscut preocupările, obiectivele propuse, realizările obținute și am fost convins de locul și importanța acestei unități de instrucție și învățământ din arma comunicații și informatică.

În cei 35 de ani, indiferent de situația în care s-a găsit, unitatea și-a îndeplinit de fiecare dată cu prisosință misiunile încredințate, între care, la loc de cinste, stă aceea de instruire a soldaților și gradaților profesioniști ai armei comunicații și informatică, din toate categoriile de forțe și comandamente de sprijin. Aprecierile comandanților unităților militare în care își desfășoară activitatea militarii instruiți în **BATALIONUL INSTRUCȚIE COMUNICAȚII ȘI INFORMATICĂ „FRAȚII BUZEȘTI”**, rezultatele obținute de militarii transmisioniști în țară și în teatrele de operații, îmi întăresc convingerea că, în această unitate, instruirea se desfășoară cu multă responsabilitate și cu un profesionalism desăvârșit.

În această zi aniversară vă rog să primiți din partea celor ce servesc ca și dumneavoastră patria cu cinste, onoare, devotament și demnitate, în cadrul unor structuri cu specific militar din cadrul Ministerului Afacerilor Interne, felicitări pentru consecvența cu care acționați și pentru tot ceea ce ați realizat în acești ani în cadrul Armatei României.

LA MULȚI ANI!
BATALIONULUI INSTRUCȚIE COMUNICAȚII ȘI INFORMATICĂ
„FRAȚII BUZEȘTI”

Cu cele mai alese sentimente,

ȘEFUL DIRECȚIEI
PREGĂTIREA TERITORIULUI PENTRU APĂRARE ȘI RECHIZIȚII
General de brigadă

Dr. Dorin CHIRCA

M E S A J U L
COMANDANTULUI BRIGĂZII 2 INFANTERIE „ROVINE”
CU OCAZIA SĂRBĂTORIRII CELEI DE-A XXXV-A ANIVERSĂRI A
BATALIONULUI INSTRUCȚIE COMUNICAȚII ȘI INFORMATICĂ „FRAȚII
BUZEȘTI”



Sărbătorirea a 35 de ani de existență a Batalionului Instrucție și Comunicații „Frații Buzești”, continuatorul tradițiilor de luptă ale Regimentului 46 Transmisiuni, înființat la 1 iunie 1980 în garnizoana Craiova, constituie pentru personalul Brigăzii 2 Infanterie „Rovine” un prilej deosebit de a vă felicita și a vă transmite cele mai sincere urări de bine. De-a lungul a peste trei decenii, structura dumneavoastră a cunoscut o serie de transformări, atât în ceea ce privește organizarea, cât și misiunile sau obiectivele de îndeplinit, ajungându-se ca la acest moment aniversar să se constituie într-o structură strict specializată în instruirea specialiștilor de comunicații și informatică. Datorită evoluției tehnologiei generale, coordonatele misiunii de bază pentru unitatea craioveană au fost în permanență adaptate realităților temporale, tehnicii și tehnologiilor existente, și, nu în ultimul rând, modalităților de pregătire pentru viitorii specialiști. Evoluția sistemelor de comunicații și informatică, precum și standardele impuse de nevoia atingerii depline interoperabilități cu structurile NATO, au impus noi exigențe în pregătirea personalului de specialitate, pentru care aparatura modernă și performantă de transmitere a datelor informatice constituie modul firesc al muncii dumneavoastră cotidiene. Realizările Batalionului Instrucție Comunicații și Informatică „Frații Buzești” în domeniul comunicațiilor și informaticii, concretizate în perfecționarea pregătirii a generații întregi de specialiști, este apreciată la cel mai înalt nivel. De altfel, foarte mulți militari români ce fac parte din această nobilă armă, comunicații și informatică, au participat alături de ceilalți militari români la toate misiunile Armatei României în teatrele de operații sau la exercițiile multinaționale desfășurate împreună cu aliații noștri din cadrul Alianței Nord-Atlantice, fiind apreciați pentru modul remarcabil în care și-au îndeplinit misiunile.

Apreciind modul exemplar în care instructorii militari craioveni își îndeplinesc misiunea principală de a pregăti specialiști din ce în ce mai buni, precum și imaginea excelentă pe care aceștia o au în rândul militarilor din garnizoana Craiova, sunt deosebit de onorat de posibilitatea oferită ca, în calitate de comandant al Brigăzii 2 Infanterie „ROVINE”, să adresez dumneavoastră și subordonaților dumneavoastră sincerele mele felicitări pentru rezultatele obținute, să le transmit mesajul de bine din partea scorpionilor craioveni și tuturor celor care au lucrat sau lucrează în instituția dumneavoastră să le urez tradiționalul

La mulți ani!

COMANDANTUL BRIGĂZII 2 INFANTERIE „ROVINE”

General de brigadă

Dorin BLAIU

M E S A J U L
COMANDANTULUI CENTRULUI DE INSTRUIRE PENTRU
COMUNICAȚII ȘI INFORMATICĂ „DECEBAL”
CU OCAZIA SĂRBĂTORIRII CELEI DE-A XXXV-A ANIVERSĂRI A
BATALIONULUI INSTRUCȚIE COMUNICAȚII ȘI INFORMATICĂ
„FRAȚII BUZEȘTI”



Sărbătorim astăzi, 1 iunie, a XXXV-a aniversare a înființării Batalionului Instrucție Comunicații și Informatică „Frații Buzești” din garnizoana Craiova, într-un moment în care toți cei care au îmbrățișat domeniul armei comunicații și informatică sunt chemați să facă față în activitatea lor profesională unor cerințe tot mai complexe, fiind gata să răspundă permanent provocărilor generate de noua eră informațională.

Cunosc îndeaproape eforturile care se fac în această unitate pentru a fi la nivelul cerințelor educaționale și de instruire solicitate în arma noastră. În câțiva ani, sub coordonarea Centrului de Instruire pentru Comunicații și Informatică „Decebal” din Sibiu, s-au schimbat radical condițiile de instrucție, baza materială a procesului instructiv-formativ, mentalitatea cu privire la profesionalismul în armă, atitudinea generală față de procesele ce se desfășoară aici, astfel încât batalionul instrucție să devină principala „poartă de intrare” a tinerilor care optează pentru cariera militară și care să le ofere o imagine reală, integratoare a cerințelor și realităților din armată, a perspectivelor de pregătire și promovare.

Experiența acumulată, precum și valoarea personalului unității, de la comandant până la soldatul instructor, ne îndreptățesc să fim optimiști în continuare și să-i asigurăm pe toți că vor primi serii de soldați/gradați profesioniști tot mai bine instruiți, încrezători în forțele proprii, căliți din punct de vedere fizic și psiho-moral, bine motivați, cu deprinderile de bază ale luptătorului și cu cerințele specifice formate pentru prima funcție pe care vor fi încadrați.

La ceas aniversar, Batalionul Instrucție Comunicații și Informatică „Frații Buzești” se prezintă ca o structură flexibilă, performantă, corect dimensionată pentru îndeplinirea misiunii, cu un corp de cadre și instructori foarte bine pregătiți profesional, cu o bază materială în conformitate cu cerințele instrucției moderne, cu programe analitice și de instrucție proiectate conform standardelor nord atlantice privind organizarea, desfășurarea și evaluarea procesului de instrucție. Pregătind cea mai importantă resursă a armei comunicații și informatică – soldatul profesionist – unitatea de instrucție a armei încearcă și, apreciem noi, și reușește să-și îndeplinească misiunea cu rezultate dintre cele mai bune.

Convins fiind că succesul deplin al acțiunilor noastre comune poate fi obținut doar prin intermediul unor strânse relații camaraderești, vă rog să primiți, dragi colegi, urările mele de sănătate, putere de muncă și succese depline în activitate.

La mulți ani!

COMANDANTUL CENTRULUI DE INSTRUIRE PENTRU
COMUNICAȚII ȘI INFORMATICĂ „DECEBAL”
COLONEL
DR. DORIN ALEXANDRESCU

BATALIONUL INSTRUCȚIE COMUNICAȚII ȘI INFORMATICĂ „FRAȚII BUZEȘTI” – ISTORIE, PERFORMANȚĂ ȘI DEVENIRE

Colonel Dr. Gheorghe DINCĂ

Batalionul Instrucție Comunicații și Informatică „Frații Buzești”



35 de ani de la înființarea **BATALIONULUI INSTRUCȚIE COMUNICAȚII ȘI INFORMATICĂ „FRAȚII BUZEȘTI”**. O fi mult? O fi puțin? Poate că nu este nici mult, dar nici puțin. Este însă important. Important pentru că **Regimentul 46 Transmisiuni** al Armatei a 3-a, în perioada 1980-

1995 și-a făcut, cu prisosință, datoria - aceea de a asigura nevoile de legătură necesare comandamentului armatei pentru conducerea forțelor. Cu eforturi, cu griji, cu frământări, cu sacrificii, dar și cu multă dăruire, abnegație și spirit de sacrificiu.

Important și pentru că **Regimentul 46 Transmisiuni** s-a instruit și a acționat în perioada 1995-2001 pentru instalarea unor centre de comunicații ale unor puncte de comandă ale Statului Major al Trupelor de Uscat. A arătat că poate îndeplini cu succes aceste misiuni cu ocazia unor exerciții și aplicații desfășurate în această perioadă (...) care s-au constituit în veritabile evaluări ale capacității acționale a regimentului privind operativitatea și capabilitățile, privind oportunitatea realizării unor legături, privind eficacitatea unor manevre de forțe și mijloace cu scopul asigurării continuității, stabilității, flexibilității și viabilității sistemului de comunicații realizat la nivel operativ-strategic. Aceleași sacrificii, griji, întrebări, încercări, verificări, antrenamente, evaluări, estimări, preocupări.

Mai important pentru că în perioada 2001-2005 **Regimentul 46 Transmisiuni** se reorganizează structural și se transformă în **Baza 14 Instrucție Transmisiuni**, conform planului de transformare a Armatei României și priorităților acelei perioade. A fost una dintre cele mai grele etape ale existenței unității. Misiunea de bază a

fost fundamental schimbată și a devenit, dintr-una de asigurare a unor relații informaționale și realizare a unor legături într-una de instruire centralizată a tuturor soldaților (deopotrivă militari în termen și militari cu termen redus) transmisioniști din toată Armata României. Au fost luni și ani de căutări, de frământări, de identificare a unor spații suplimentare de cazare și hrănire a efectivelor (cifrele de instruire depășeau 1100-1200 de oameni pe serie), de transformare a bazei tehnico-materiale. Unitatea a început să funcționeze în mai multe locații (trei la un moment dat) aspect ce a pus în fața comenzii noi provocări - delegare de competențe, intensificarea actului de control, planificare multi-nivel și execuție pe măsură, dislocări de tehnică, materiale, carburant cu toate implicațiile patrimoniale specifice. A fost una dintre perioadele foarte grele din existența unității, cu multiple și complexe probleme de rezolvat, cu frecvente activități de evaluare și apreciere privind modul de îndeplinire a noii misiuni.

În această perioadă s-au realizat foarte multe săli de specialitate, în mod special în cazarma actuală a unității, unde s-au făcut și re compartimentări și transformări ale destinațiilor unor spații, dar și în cazarma de la FĂCĂI, unde funcționa unul dintre batalioanele bazei.

Și mai important pentru că în anul 2005, **Baza 14 Instrucție Transmisiuni** s-a transformat în **Batalionul Instrucție Transmisiuni** care a funcționat până la 01.09.2008 când acesta s-a reorganizat în **BATALIONUL INSTRUCȚIE COMUNICAȚII ȘI INFORMATICĂ „FRAȚII BUZEȘTI”** (actuala denumire a unității). Apreciez că și această perioadă, începând cu anul 2005, a fost una dintre etapele grele ale existenței unității, pentru că, în acest interval de timp, unitatea și-a fundamentat și consolidat în fața propriei conștiințe, dar și a eșaloanelor superioare, posibilitatea de a îndeplini greua misiune - aceea de desfășurare a instruirii centralizate a soldaților transmisioniști din toată Armata României. Au fost baze de instrucție care s-au desființat - la Târgu Jiu, Piatra Neamț etc. Baza de la Craiova și-

a continuat menirea, asigurându-și continuitatea prin batalionul de instrucție rezultat în urma reorganizării. Această structură de batalion, mai mică, a fost în concordanță cu tendința națională a scăderii efectivelor și cu cerințele noi care stăteau în fața procesului de instrucție, odată cu intrarea Armatei României în Alianța Nord-Atlantică.

A fost, spuneam, tot o perioadă grea, ca de altfel întreaga existență de 35 de ani a unității. Un moment de cotitură în istoria unității l-a constituit anul 2007, când s-a renunțat la sistemul concript și s-a trecut la serviciul militar voluntar. A fost o schimbare majoră - de filosofie a instrucției, de mentalitate a instructorilor, dar și a soldaților voluntari, de sistem de instrucție cu toate determinările sale. A apărut modelul luptătorului și specialistului în arma comunicații și informatică. Au apărut cerințe noi, bareme noi, s-au schimbat instrucțiunile și regulamentele. A fost aproape un nou început. A fost greu, dar a fost și incitant, provocator, frumos.

În anul 2007, a intrat în înzestrarea unității prima autospecială PANTHER 2000 H pe șasiu de ARO 323 T.D. de 400 W, moment pe care și astăzi îl consider de referință în înzestrarea cu tehnică modernă a unității.

În perioada 2008-2012, s-au reorganizat total sălile de instrucție militară de specialitate (I.M.S.), dar și de instrucție militară generală (I.M.G.). Au fost realizate săli în concordanță cu specialitățile instruite și cu disciplinele de bază din programul de instrucție. S-a continuat dotarea unității cu mijloace digitale moderne radio, telefonice și radioreleu, cu containere radioreleu dislocabile, cu centre tip „C” pentru instrucția operatorilor R.M.N.C. A fost realizată sala RI-STI pentru pregătirea operatorilor tehnică de calcul, sala electroalimentare și sala de aparatură de mentenanță nivel 1.

De menționat este că și în domeniul instrucției militare generale s-au obținut realizări remarcabile. S-au realizat, astfel, sălile de educație militară și cabinet S.S.M., sala de instrucție tactică generală, sala pentru instrucție pe linia armelor, apărare C.B.R.N. și instrucție genistică, sala pentru I.T.A.I. și sala pentru instrucția pe linia armelor.

Realizări remarcabile în istoria recentă a unității sunt și cele legate de clarificarea situației patrimoniale a Poligonului de instrucție GHERCEȘTI, care a devenit, din anul 2014, a doua cazarmă a batalionului, fiind luat în evidența cantitativ-valorică și devenind, prin facilitățile

multiple de instruire (atât militară generală, cât și de specialitate) determinant pentru îndeplinirea misiunii de bază a batalionului, aceea de formare a luptătorului și inițiere a specialistului în arma comunicații și informatică.

Poligonul, în ansamblul lui, dar și unitatea au fost potențate din punct de vedere al bazei materiale pe linia E.F.M. prin realizarea și omologarea, în condiții de maximă siguranță și economicitate, a pistei cu obstacole tip CISM - pentru militarii din toate armele care este - în acest moment - cea mai modernă din garnizoana CRAIOVA.

Realizarea unei săli a tradițiilor unității, care să sintetizeze toți cei 35 de ani de existență prin tehnică, documente, echipamente militare, simboluri, insigne, registre istorice, albume și alte materiale intuitive - specifice, apreciem că a fost o realizare importantă a ultimei perioade de timp din existența batalionului.

Paraclisul realizat cu sprijinul MITROPOLIEI OLTENIEI, cu o pictură deosebit de expresivă, reprezintă un element inedit și important de bază materială, care, inaugurat în anul 2006, favorizează posibilitatea confesiunii religioase a personalului și facilitează asigurarea asistenței religioase a cursanților pe întreg parcursul procesului de pregătire desfășurat în unitatea noastră.

Continuând, la nivel calitativ superior, realizările din anii precedenți ale personalului unității, în anul 2010, s-a realizat și utilat un nou spațiu pentru biblioteca unității care are în evidență aproximativ 14.000 de volume de carte, a fost constituită o sală modernă de lectură și s-au modernizat și îmbunătățit continuu condițiile de trai, hrănire, recreere, petrecere a timpului liber și recuperare după efort ale cursanților veniți în unitate pentru pregătire.

Demn de remarcat, și în completare cu toate cele prezentate până în prezent, opinăm că este atenția specială acordată de management celei mai importante resurse a unității - personalul militar și civil. Astfel preocuparea pentru formarea continuă a acestuia, pentru autoperfecționare, dar și pentru perfecționare prin cursuri de carieră și de nivel, prin absolvirea diferitelor forme de pregătire militară și civilă a constituit o prioritate și un vector ascendent al stilului de conducere adoptat în ultimii ani de existență ai unității.

În ceea ce privește viitorul unității, opinăm că în atenția noastră, a tuturor, în perioada imediată vor sta următoarele priorități:

- implementarea, cu rezultate dintre cele mai bune, a modificărilor aduse programului de instrucție pentru cursul de formare începând cu seria aprilie 2015;

- creșterea eficienței actului educațional prin standardizarea procesului de instrucție și învățământ și prin folosirea unor metode și tehnici cât mai moderne, adaptate mediului educațional național și internațional;

- actualizarea permanentă a ofertei educaționale specifice prin fundamentarea de cursuri noi, determinate de înzestrarea cu tehnică CIS nouă, cursuri de schimbare de armă, cursuri de informatică;

- corelarea permanentă a bazei materiale de instrucție cu oferta educațională și continuarea actualizării permanente a nivelului de pregătire al instructorilor.

Această instituție de instrucție și învățământ, această unitate unică în armă și în Armata României, și-a dovedit necesitatea, utilitatea și eficiența și opinăm că, în contextul internațional actual, pe termen mediu și lung, având în vedere importanța domeniului CIS în relație cu comanda-controlul structurilor de forțe, devenirea acestei instituții nu poate fi decât una pe măsura trecutului și rezultatelor obținute - o structură modernă, eficientă, flexibilă și deschisă permanent către performanță.

Toate cele prezentate și altele care ar putea fi spuse dar, din lipsă de spațiu, pot fi lăsate pe

altă dată, se pot constitui în argumente privind ***DEVENIREA BATALIONULUI INSTRUCȚIE COMUNICAȚII ȘI INFORMATICĂ „FRAȚII BUZEȘTI” CA O UNITATE DE INSTRUCȚIE A VIITORULUI ÎN DOMENIUL COMUNICAȚII ȘI INFORMATICĂ PENTRU TOATĂ ARMATA ROMÂNIEI.***

La ceas aniversar, sunt deosebit de onorat să adresez celor care au lucrat, lucrează și vor lucra, în viitorul apropiat, în unitatea de instrucție a armei comunicații și informatică - ***BATALIONUL INSTRUCȚIE COMUNICAȚII ȘI INFORMATICĂ „FRAȚII BUZEȘTI”*** - un respectuos și călduros „**La mulți ani cu sănătate!**”

ABREVIERI:

- **I.M.S.** – Instrucție Militară de Specialitate;
- **I.M.G.** – Instrucție Militară Generală;
- **R.M.N.C.** – Rețeaua Militară Națională de Campanie;
- **RI-STI** – Rețea de Internet – Subrețea pentru Testare și Învățământ;
- **S.S.M.** – Sănătate și Securitate în Muncă;
- **C.B.R.N.** – Chimic, Bacteriologic, Radiologic și Nuclear;
- **I.T.A.I.** – Instrucția Tragerilor cu Armamentul de Infanterie;
- **E.F.M.** – Educație fizică Militară;
- **C.I.S.M.** – Conseil International du Sport Militaire (Consiliul Internațional al Sportului Militar)
- **C.I.S.** - Communications and Information Systems (Sisteme de Comunicații și Informatică).

SCURT ISTORIC AL BATALIONULUI INSTRUCȚIE COMUNICAȚII ȘI INFORMATICĂ „FRAȚII BUZEȘTI”

Maior Ionuț-Daniel ȘERBAN

Batalionul Instrucție Comunicații și Informatică „Frații Buzești”



La **01 iunie 1980**, în baza Ordinului General al ministrului apărării naționale nr. 008 din 02.04.1980, a luat ființă **Regimentul 46 Transmisiuni** în garnizoana Craiova (cazarma 878), cu personal și tehnică din garnizoanele București, Buzău,

Craiova, Cluj Napoca și Târgu-Mureș.



La **20 august 1981**, prin Decretul Prezidențial nr. 132, Regimentului 46 Transmisiuni i s-a înmănat **Drapelul de luptă**, simbol al onoarei, vitejiei și gloriei militare.

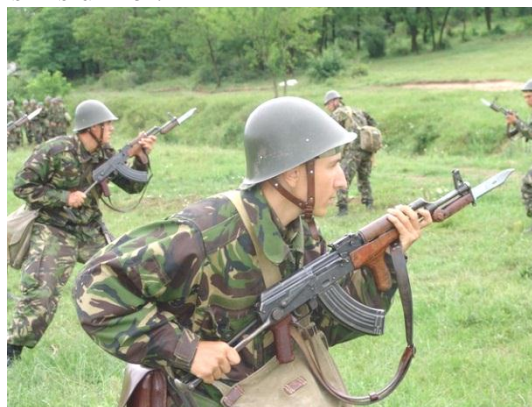


La **14 iulie 1995**, Regimentul 46 Transmisiuni a primit noul **Drapel de luptă** și i s-

a atribuit numele onorific de „**FRAȚII BUZEȘTI**”.



Începând cu data de **01.06.2001**, se înființează **Baza 14 Instrucție Transmisiuni** din garnizoana Craiova, subordonată Școlii de Aplicație pentru Transmisiuni, Informatică și Război Electronic a Comandamentului Transmisiunilor.



La **06 mai 2005** - Prin Decretul Prezidențial nr. 372/05.05.2005, Drapelul de Luptă a fost decorat cu **Ordinul Virtutea Militară în grad de Cavaler cu însemn pentru militari**.



Începând cu data de **01.08.2005**, prin Ordinul șefului SMG nr. B5/S/1187/2005, Baza 14 Instrucție Transmisiuni s-a transformat în **Batalionul Instrucție Transmisiuni**, subordonat Centrului de Pregătire pentru Comunicații și Informatică „Decebal”.



La data de **29.03.2006**, ministrul apărării a aprobat cu Ordinul nr. DR 1210 ca unității noastre să i se atribuie denumirea onorifică de „**FRĂȚII BUZEȘTI**”. În același timp, **Batalionul Instrucție Transmisiuni „Frații Buzești”** a devenit **continuatorul tradițiilor de luptă** ale Regimentului 46 Transmisiuni și Bazei 14 Instrucție Transmisiuni.



Începând cu data de **01.01.2007**, unitatea a trecut la instruirea soldaților voluntari, în conformitate cu legea **384/2006**.

Cu ocazia depunerii Jurământului Militar de către prima serie de soldați voluntari, în data de **16 iunie 2007**, unitatea a fost vizitată de către ministrul apărării.



Începând cu data de **01.07.2008**, unitatea trece în subordinea Comandamentului Comunicațiilor și Informaticii, conform ordinului ministrului apărării naționale nr. MS 17 din 25.02.2008.



În **14.07.2008** – Prin Ordinul șefului SMG nr. SPD1/12.07.2008, unității i-a fost conferită „**Emblema de Onoare a Comunicațiilor și Informaticii**”.

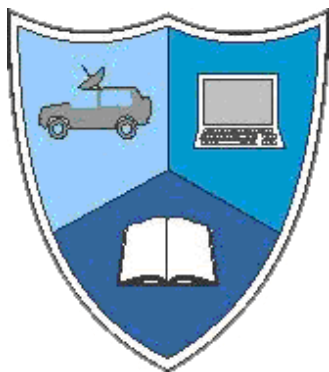
Începând cu data de **01.09.2008**, în baza Ordinului G2/S/1302 din 31.08.2008, Batalionul Instrucție Transmisiuni se restructurează și se transformă în **Batalionul Instrucție Comunicații și Informatică „Frații Buzești”** având ca misiune principală formarea luptătorului și specialistului în arma comunicații și informatică.



În data de **28.01.2009**, unitatea a fost vizitată de către șeful Statului Major General.



În ședința din data de **17.03.2010**, Comisia de heraldică și denumiri a Ministerului Apărării Naționale a aprobat *însemnele heraldice ale unității*.



Prin *Ordinul ministrului apărării naționale nr. MP 2 din 20.04.2010*, la data de **01.06.2010**, cu prilejul sărbătoririi a 30 de ani de la înființare, unității i-a fost conferită **Emblema de Onoare a Armatei României** și i s-a înmănat **Steagul de identificare**.



Cu prilejul aniversării a 140 de ani de la înființarea armei comunicații și informatică, *prin ordinul șefului Statului Major General nr. S.P.D. 19/03.06.2014*, în data de **14.07.2013**,

unității i s-a conferit **„Emblema de Onoare a Statului Major General”**.



În data de **18.07.2014**, unitatea a fost vizitată de către **șeful Statului Major al Forțelor Terestre – gl.mr. dr. Nicolae-Ionel CIUCĂ**.



La data de **18.07.2014**, cu ocazia ceremoniei de încheiere a misiunii Armatei României în provincia Zabul din Teatrul de Operații Afganistan, prin *ordinul ministrului apărării naționale nr. M.P. 408/15.07.2014*, unității i s-a conferit **„Emblema de Onoare a Armatei României cu însemn de război”**.



BATALIONUL INSTRUCȚIE COMUNICAȚII ȘI INFORMATICĂ „FRAȚII BUZEȘTI” – 35 DE ANI ÎN SLUJBA ARMEI COMUNICAȚII ȘI INFORMATICĂ

Locotenent-colonel Leonide CUNE

Batalionul Instrucție Comunicații și Informatică „Frații Buzești”



La data de 01.06.2015 se sărbătorește 35 de ani de existență, toți puși în slujba armeei cu abnegație și profesionalism de către personalul unității.

Batalionul Instrucție Comunicații și Informatică „Frații Buzești” este

continuatorul

tradițiilor Regimentului 46 Transmisiuni – U.M. 01662 care, în baza Ordinului General al Ministrului Apărării Naționale nr. 008 din 02.04.1980, se înființează în perioada 01.05. – 30.08.1980.

Regimentul a fost creat prin contopirea Companiei a 9-a Transmisiuni/R.45 Trs. București, Compania Transmisiuni/R.74 Trs. Târgu Mureș și 14 ofițeri, 5 maiștri militari, 9 subofițeri din R.47 Trs. Buzău.

În actuala locație-cazarma 878 din garnizoana Craiova, situată pe strada Vasile Alecsandri, nr.77-79, Regimentul 46 Transmisiuni a asigurat nevoile de legătură ale Comandamentului Armatei a 3-a.

Prin Decretul Prezidențial nr. 132 din 20.06.1981 și în baza Ordinului Ministrului Apărării Naționale nr. O.Z.U. 10 din 21.07.1981, în ziua de 20 august 1981, Regimentului 46 Transmisiuni i-a fost înmănat primul Drapel de luptă.

În perioada 1982-2001, regimentul demonstrează profesionalismul personalului în aplicațiile la care participă din care cele mai importante au fost:

- aplicația „OLTUL 82”;
- aplicația „HAȚEG 89”;
- aplicația „VEDEA 90”;
- aplicația „CRIȘUL 90”;
- aplicația „BEGA 91”
- aplicația „TIMIȘ 91”;

- aplicația „BANAT 93”;
- aplicația „JIUL 94”;
- aplicația de specialitate „ZENIT 97”;
- aplicația tehnică de specialitate „SARMIS 2000”;
- aplicația „FORȚA 2000” .

În data de 14.07.1995, în piața A.I.Cuza din centrul Craiovei, a avut loc ceremonialul înmănării și sfințirii noului drapel de luptă al R.46 Trs. și acordării denumirii onorifice de „Frații Buzești”, în baza decretului Prezidențial nr. 201/03.07.1995.

Anul 2001 reprezintă un moment de cotitură în viața regimentului, acesta transformându-se în Baza 14 Instrucție Transmisiuni, subordonată Școlii de Aplicație pentru Transmisiuni, Informatică și Război Electronic, în baza ordinului ministrului Apărării Naționale nr. MS 34/ 29.03.2001.

În contextul procesului de modernizare și transformare a societății în general și a armatei în mod special, Bazei 14 Instrucție Transmisiuni îi revin misiuni și responsabilități extrem de importante și precise în pregătirea și instruirea militarilor în termen din arma transmisiuni.

Astfel, misiunea de bază a unității se schimbă radical, aceasta devenind de a forma militarii în termen, militarii cu termen redus transmisioniști din toată Armata României.

La Baza 14 Instrucție Transmisiuni, efectivele unității au fost dispuse în trei locații:

- actuala locație, cazarma 878;
- un local în loc. Făcai, la ieșirea din municipiul Craiova;
- un local în cadrul Facultății de Educație Fizică și Sport din Craiova, fosta locație a Liceului Militar „Tudor Vladimirescu”.

Numărul militarilor instruiți în perioada 2001-2005 este de aproximativ 5800.

Procesul de modernizare și transformare al armatei continuă și, astfel, în anul 2005, Baza 14 Instrucție Transmisiuni se transformă în Batalionul Instrucție Transmisiuni. Unitatea continuă să rămână dislocată în locația din strada Vasile Alecsandri, respectiv cazarma 878.

Anul 2006 pune o nouă misiune în fața militarilor unității, astfel:

- un detașament format din peste 100 de militari participă la limitarea efectelor inundațiilor în zona Bistreț –Rast, județul Dolj;

- un alt detașament, format din 25 de militari, participă în loc. Băilești pentru descărcarea ajutoarelor acordate persoanelor sinistrate;

- la solicitarea Centrului Regional de Transfuzie, în ziua de 17.05.2006, a fost organizată o activitate de donare de sânge de către personalul unității (astfel de activități au fost organizate anual).

Batalionul continuă misiunea Bazei 14 Instrucție Transmisiuni și, începând cu anul 2007, în conformitate cu Legea 384 din 10.10.2006 privind statutul soldaților și gradaților voluntari, trece de la pregătirea și instruirea soldaților conșcripți la formarea luptătorului și specialistului în arma comunicații și informatică.

Anul 2007 reprezintă schimbarea mentalității de instruire a soldatului - SOLDATUL VOLUNTAR. Apar „modelul luptătorului”, „modelul specialistului”, „programul instrucției individuale de bază” și „programul instrucției individuale de specialitate”.

Alături de întreaga armată, Batalionul Instrucție Transmisiuni „Frații Buzești” este angrenat într-un amplu proces de modernizare a infrastructurii necesare asigurării condițiilor optime de instruire a soldaților voluntari pentru îndeplinirea misiunilor la cele mai înalte standarde.

Cu sprijinul Comandamentului Comunicațiilor și Informaticii, baza materială pentru instrucție suferă profunde transformări. Sunt realizate primele săli de specialitate pentru operatorii din RTP/RMNC, unitatea este dotată cu stații digitale de tipul Panther și Harris.

Începând cu data de 01.09.2008, Batalionul Instrucție Transmisiuni se transformă în Batalionul Instrucție Comunicații și Informatică „FRAȚII BUZEȘTI”, cu misiunea de a forma luptătorul și specialistul în arma comunicații și informatică.

Între anii 2009-2014, modernizarea bazei materiale pentru instrucție continuă și astfel:

- sunt schimbate total sălile de instrucție militară generală (IMG) în concordanță cu programul de instrucție editat în 2009;

- sunt modernizate sălile de instrucție militară de specialitate (IMS) existente și sunt realizate săli noi – sală operatori tehnică de calcul, sală centru

de instrucție tip „C”-RMNC, sală electroalimentare, sală reparatori tehnică de comunicații;

- în zona sălilor de specialitate este implementată rețeaua de internet pentru testare și învățământ cu 12 posturi de lucru – RI-STI;

- este realizată rețeaua de calculatoare a unității cu 25 posturi de lucru, acreditată și conectată la rețeaua INTRAMAN a M.Ap.N.;

- în Poligonul de instrucție Ghercești este realizată pista cu obstacole pentru militarii de toate armele – tip CISM.

Aria curriculară a suferit profunde transformări. Dacă în anul 2005 în unitate se desfășurau doar cursurile de formare (modulul instrucției individuale, respectiv modulul perfecționării instruirii de specialitate) și cursul de carieră (cursul avansat), în prezent, în unitate se desfășoară:

- cursuri de formare (modulul instrucției individuale și modulul perfecționării instruirii de specialitate);

- curs de carieră (curs avansat de instruire pentru gradați profesioniști, arma comunicații și informatică);

- cursuri de specializare (curs de specializare în arma comunicații și informatică a gradaților și soldaților profesioniști din alte arme, curs de specializare a operatorilor RTP/RMNC, curs operatori stații radio HARRIS, curs operatori stații radio PANTHER, curs de specializare operatori radioreleu numeric, curs de specializare electromecanici);

- cursuri de informatică (curs de utilizare WORD, EXCEL și ACCES).

Întreaga activitate a batalionului s-a desfășurat sub deviza „ONOARE ȘI PATRIE”, înscrisă pe drapelul de luptă.

Pentru rezultatele remarcabile obținute în îndeplinirea cu succes a misiunilor de mare complexitate și răspundere privind pregătirea profesională a specialiștilor de comunicații și informatică pentru toate categoriile de forțe ale armatei, Drapelul de luptă al unității a fost decorat de-a lungul anilor, astfel:

- în ziua de 05 mai 2005, președintele României a decorat Drapelul de luptă al unității cu ordinul „Virtutea Militară în grad de cavaler cu însemn pentru militari”;

- prin Ordinul ministrului apărării naționale nr. M.P. 2 din 20.04.2010, cu prilejul sărbătoririi a 30 de ani de la înființare, unității i-a fost

conferită „**Emblema de onoare a Armatei României**”;

- prin Ordinul șefului Statului Major General nr. S.D.P. 19 din 03.06.2013, cu prilejul sărbătoririi a 140 de ani de la înființarea armeei

transmișii, unității i-a fost conferită „Emblema de Onoare a Statului Major General”;

- prin Ordinul ministrului apărării naționale nr. M.P. - 408 din 15.07.2014, unității, i-a fost conferită „Emblema de Onoare a Armatei României cu însemn de război”.

35 ani

tradiție

GÂNDURI LA CEAS ANIVERSAR... ...O UNITATE CU STATUT DE CARTE DE VIZITĂ

Colonel Marian APOSTOL

Șeful Centrului Zonal de Pregătire de Protecție Civilă – Craiova



Sărbătorirea a 35 de ani de la înființarea **unității „noastre”** îmi oferă plăcutul și onorantul prilej de a-mi exprima gândurile și sentimentele care mă încercă în acest moment cu adevărat emoționant pentru mine, având în vedere că în urmă cu 30 de ani mi-am început cariera militară în această cazarmă.

Cazarmă în care funcționa atunci Regimentul 46 Transmisiuni, unitate cu misiuni specifice de maximă importanță pentru conducerea Armatei a 3-a – asigurarea legăturilor necesare exercitării actului de conducere. Un început de drum greu, cu sarcini multe (instrucție, exerciții și aplicații, asigurarea operativității tehnicii, munci agricole, lucrări de amenajare interioară etc), cu lipsuri și greutăți, care au fost surmontate prin abnegația și devotamentul de care au dat dovadă cadrele unității din acei ani. Cinste lor!

A urmat începând din anul 2001, odată cu transformarea în Baza 14 Instrucție Transmisiuni, o perioadă la fel de dificilă, în care s-au îmbinat sarcinile operative cu cele de instruire în cadrul S.M.F.T. și apoi instruirea centralizată a militarilor în termen și cu termen redus, transmisioniști din Armata României (în număr de 1567 militari în primul ciclu de instrucție), sub cupola Școlii de Aplicație și Comandamentului Transmisiunilor, ulterior Comandamentul Comunicațiilor și Informaticii.

Concluzia este scurtă și cuprinzătoare – misiuni îndeplinite!

Pentru mine, perioada petrecută în această unitate, până în anul 2005, a constituit o adevărată academie de pregătire multilaterală ca ofițer și specialist în armă.

Mă simt deosebit de onorat de faptul că am făcut parte din această unitate de elită a armeei și armatei. Poate că unii nu înțeleg de ce îmi

amintesc cu atât de multă dragoste și respect de **unitatea „noastră”**, însă eu mă consider în continuare membru al acestei unități pentru că aici mi-a rămas inima, pentru că aici m-am format ca ofițer, aici mi s-au întipărit în comportament caracteristicile, atitudinile și deprinderile specifice unui militar adevărat și devotat, pentru că nu am să pot uita vreodată clipele trăite alături de oamenii care reprezintă spiritul unității în a cărei revistă am ocazia și onoarea să aștern aceste rânduri.

Unitatea se poate mândri, pe drept, cu trecutul și realizările sale, dar o poate face și mai mult cu prezentul. Prezent în care îndeplinește cu profesionalism, prin organizare ireproșabilă, pregătire excelentă și înțelegerea conceptelor moderne de instruire, o misiune deosebit de importantă în actualul context, aceea de a pregăti viitorii specialiști de comunicații și informatică din categoria soldați și gradați profesioniști.

Revenirea după un timp în unitate te surprinde, descoperind lucruri noi și constatând transformări interesante. Pentru mine care, prin prisma relației personale cu colegul și prietenul meu, col. dr. Dincă Gheorghe – comandantul unității, și a relației instituționale dintre unitățile noastre, sunt aspecte binecunoscute care mă bucură.

Astfel, putem descoperi tinerețea majorității personalului sau „tinerețea veșnică” a celor cu care am lucrat și înainte de 1989, constatând cu satisfacție că aceștia au suferit transformări cu trecerea timpului, dar au reușit să țină pasul în condiții foarte bune cu vremurile actuale. De altfel, valoarea cea mai de preț a unității a fost și este factorul uman, care și-a demonstrat calitatea și pregătirea excepțională în întrebuințarea tehnicii militare și menținerea acesteia în stare operațională pe timpul executării misiunilor încredințate de-a lungul timpului, precum și instruirea militarilor în termen și cu termen redus, respectiv a soldaților și gradaților profesioniști, la standardele de performanță cerute.

Cea mai importantă descoperire este aceea situată în planul modernizării unității. Astfel, transformările făcute în dotarea acesteia cu tot

cea ce este necesar pentru un proces de instruire modern, de calitate, cu tehnică nouă, îmbunătățirile considerabile ale condițiilor de trai-cazare, hrană, echipare, toate amenajările din cazarmă nu fac decât să te bucure și să sădească speranța că această unitate militară va dăinui peste ani.

Specificul misiunilor și responsabilităților, realizările deosebite, posibilitățile și resursele actuale susțin în mod competitiv, fără echivoc, menirea „noastră”, determinând constituirea unității într-un adevărat creuzet al performanței în instruire, în arma comunicații și informatică.

Îmi permit să apreciez, ca ofițer care am muncit în această unitate timp de peste 15 ani, că toate realizările nu ar fi fost posibile fără eforturile tuturor, fără truda și sacrificiul unor oameni devotați, serioși, solidari, oameni adevărați, care au dat și dau numele unității – de la militari în termen și cu termen redus/soldați și gradați profesioniști, salariați civili și militari angajați, până la subofițeri, maiștri militari și ofițeri. Oameni cu care am muncit și de la care am învățat, oameni pe care m-am străduit să-i învăț, să-i ajut, să-i înțeleg. Nu o să dau nume pentru că, fiind foarte mulți, există riscul unor omisiuni pe care le-aș regreta; vreau însă să le mulțumesc că

au făcut parte dintr-o perioadă frumoasă și importantă a carierei mele, să-i asigur că vor fi permanent în sufletul meu și că nu am să uit niciodată clipele trăite împreună, la bine și la greu.

Astăzi ne reîntâlnim cu drag, redeșteptăm întâmplări, călătorim cu ochii minții la sălile de specialitate și poligoane, ne amintim de gerul iernilor tăioase sau căldura sufocantă a verilor toride din nenumăratele zile și nopți de trageri, exerciții și aplicații, reîntâlnim comandanți, subordonați, camarazi.

Să trăim intens și cu plăcere aceste clipe și să ne vedem cu bine!

În acest moment de sărbătoare se cuvine să îndreptăm **un gând curat și un pios omagiu** celor care nu mai sunt printre noi, pentru a ne bucura împreună. Din păcate, prea mulți și prea tineri!

Dragi colegi din **Batalionul Instrucție Comunicații și Informatică „Frații Buzești”** vă doresc sănătate, împlinirea tuturor aspirațiilor și succese în nobila misiune pe care o aveți.

Am să fiu permanent alături de dumneavoastră cu gândul, dar și cu fapta.

Dumnezeu să vă ajute și să vă dea putere, în faptă și în gând, să duceți lucrarea mai departe!

La mulți ani și viață lungă!

BAZA MATERIALĂ - ROL DETERMINANT ÎN PROCESUL DE INSTRUCȚIE DIN BATALIONUL INSTRUCȚIE COMUNICAȚII ȘI INFORMATICĂ „FRAȚII BUZEȘTI”

Locotenent-colonel Ionel CRĂCIUN

Batalionul Instrucție Comunicații și Informatică „Frații Buzești”



Instrucția este o activitate cu caracter predominant practic-aplicativ și are ca obiectiv principal formarea, dezvoltarea și menținerea deprinderilor de acțiune ale individului și ale structurilor militare în scopul îndeplinirii atribuțiilor

funcției/misiunilor. Ea se desfășoară pe două paliere distincte: la nivelul individului și la nivelul colectiv (al structurilor militare) și are rol decisiv în realizarea capacității operaționale a unităților militare. Batalionul Instrucție Comunicații și Informatică „FRAȚII BUZEȘTI” este o structură cu misiune specială, care execută instrucția la nivelul individului și la nivelul microcolectivului (echipaj/grupă de comunicații și informatică).

Atât instrucția individuală, cât și cea colectivă, cuprind laturile: teoretică, fizică, psiho-morală, tehnică și tactică. Pondere și conținutul acestor laturi în ansamblul activității se stabilesc în funcție de nivelul și caracteristicile personalului/forțelor și sarcinilor/misiunilor pentru care se instruiesc.

La nivelul individului și al eșaloanelor mici, al structurilor de execuție, accentul se pune pe laturile fizică, psiho-morală și tehnică, iar la eșaloanele superioare, ale structurilor de comandă, pe instrucția teoretică și tactică.

Fiecare din cele cinci laturi ale instrucției se materializează prin obiective specifice, astfel:

a) latura teoretică – cunoașterea caracteristicilor spațiului de luptă și formarea și dezvoltarea capacității de a gândi eficient, specifice nevoilor acestui mediu;

b) latura fizică și psiho-morală – formarea și dezvoltarea capacității fizice și psiho-morale necesare militarilor pentru îndeplinirea misiunilor în condițiile extreme de efort și stres, specifice operațiilor;

c) latura tehnică – cunoașterea echipamentelor militare, formarea și dezvoltarea deprinderilor necesare folosirii eficiente a acestora în spațiul tactic;

d) latura tactică – cunoașterea modului în care trebuie acționat în spațiul tactic și formarea și dezvoltarea deprinderilor acționale pentru îndeplinirea misiunilor.

Batalionul Instrucție Comunicații și Informatică „FRAȚII BUZEȘTI”, structură subordonată Centrului de Instruire pentru Comunicații și Informatică „Decebal”, are ca misiune fundamentală formarea luptătorului și specialistului în arma comunicații și informatică, deci instrucția trebuie să fie fundamentată la nivelul individului. Instrucția, metodică instruirii, asigurarea cu instructori specializați, pregătirea și verificarea modului de executare a procesului de instrucție a constituit și va constitui în permanență o preocupare esențială a comenzii unității și a factorilor cu responsabilitate în procesul instructiv-educativ din unitate. Pe lângă calitatea și numărul instructorilor, o componentă la fel de importantă a procesului instructiv-educativ este și baza materială destinată instrucției. Preocuparea pentru realizarea și modernizarea bazei materiale din Batalionul Instrucție Comunicații și Informatică „FRAȚII BUZEȘTI” s-a manifestat din plin începând cu anul 2007, când s-a trecut la stagiul militar pe bază de voluntariat, dar mai ales din anul 2008, când unitatea a fost resubordonată Comandamentului Comunicațiilor și Informaticii.

Cu sprijinul material și implicarea personală a factorilor de conducere și decizie din Comandamentul Comunicațiilor și Informaticii, prin implicarea personală și prin efortul depus de întregul personal, susținut de comanda unității, s-a realizat o bază materială modernă, modulară, pliată perfect pe misiunile unității și pe programele de instrucție și învățământ destinate formării și specializării soldaților și gradaților profesioniști.

Luptătorul modern, dincolo de capacități excepționale fizice și psiho-morale, trebuie să fie

și abil și foarte iscusit în mânuirea armamentului și tehnicii din dotare din ce în ce mai performante. Pe de altă parte, costurile din ce în ce mai mari ale tehnicii din dotare, necesitatea menținerii acesteia permanent în stare de operativitate, presupun o responsabilitate suplimentară în utilizarea acesteia în procesul de instrucție. Aici intervine rolul esențial al planșei, machetei și simulatorului, al softului educațional, dar și al valorii instructorului și calității luptătorului. Toate aceste componente ale instruirii practic-aplicative sunt atinse și materializate în Batalionul Instrucție Comunicații și Informatică „FRAȚII BUZEȘTI”. Formarea luptătorului necesită un proces instructiv – educativ având un caracter preponderent practic. Militarul trebuie format în primul rând ca executant, ca luptător activ, de aceea formele de organizare a activităților instructiv-educative sunt, mai ales, „ședințe practice”, în timp ce ședințele teoretice pregătesc doar și susțin demersurile practice. În pavilionul săli de instrucție militară generală din Batalionul Instrucție Comunicații și Informatică „FRAȚII BUZEȘTI” sunt amenajate 8 săli de instrucție tip cabinet de disciplină, dotate cu planșe specifice, machete, tehnică și armament secționat în care se execută ședințe teoretice, apercceptive înaintea ședințelor practice, care contribuie decisiv la crearea unei imagini și aprofundarea în detaliu a unei mișcări sau acțiuni ce va trebui formată sau perfecționată în cadrul ședinței practice. Desfășurarea grupei de infanterie, ofensiva, atacul sunt exemplificate pe machete instructive și prin proiecții video, apoi se trece la partea practică a însușirii și dezvoltării deprinderilor în poligonul de instrucție.

Celaltă componentă a misiunii fundamentale, formarea și specializarea în arma comunicații și informatică a soldaților și gradaților profesioniști, are aceeași dualitate teorie-practică, de această dată accentul punându-se pe 8 săli de pregătire militară de specialitate și pe tehnica de comunicații și informatică portativă,

containerizată sau dispusă pe șasiuri auto. Denumirea, dotarea și organizarea sălilor de specialitate sunt date de specializările în arma comunicații și informatică a soldaților și gradaților profesioniști și cerințele de formare impuse prin modelele absolventului pentru cursurile de specializare și de carieră care se execută în Batalionul Instrucție Comunicații și Informatică „FRAȚII BUZEȘTI”.

Poligonul de instrucție „Ghercești” este un „laborator” practic-aplicativ organizat pe aceleași principii modulare ale specialităților de instrucție militară generală și locul unde se execută instrucția practic-aplicativă și exercițiile de comunicații cu tehnică în teren. Situat în apropierea cazarmii de dislocare la pace (5 km), are următoarele amenajări destinate procesului de instrucție:

- poligon de instrucție complex (pregătire C.B.R.N., instrucție tactică și de specialitate, poligon supraviețuire, poligon ITAD);
- pistă cu obstacole pentru militarii din toate armele;
- portic de gimnastică;
- 2 săli IMG.

Pentru asigurarea concordanței între misiunea unității, oferta educațională și specialitățile militare de instruit, menținerea ritmului de dotare cu tehnică de comunicații și informatică la același nivel cu cel de înzestrare, comanda și factorii de răspundere din unitate se preocupă permanent de îmbunătățirea și transformarea/retehnologizarea bazei materiale pentru a desfășura procesul de instrucție la cele mai înalte standarde.

Concluzionând, apreciez că baza materială existentă în Batalionul Instrucție Comunicații și Informatică „FRAȚII BUZEȘTI” are un rol determinant în cadrul trinomului instructor – bază materială – instruit, cu un rol decisiv în obținerea calității și performanței în domeniul instrucției.

UNELE OPINII PRIVIND RELAȚIA INTRINSECĂ DINTRE EDUCAȚIE ȘI INSTRUCȚIE

Locotenent-colonel Torino NUȚĂ

Batalionul Instrucție Comunicații și Informatică „Frații Buzești”

„Educația este cea mai puternică armă pe care o poți folosi pentru a schimba lumea”

Nelson Mandela



Considerații generale

În educație, atitudinea prospectivă ține de conștientizarea faptului că formarea personalității umane, formarea profesională a tinerilor trebuie să ia în considerare perspectivele și provocările viitorului.

Astăzi se consideră că

relația trecut – prezent – viitor este o relație dialectică, raporturile reciproce dintre ieri, azi și mâine s-au schimbat și se schimbă permanent, azi nu mai apare determinat atât de ieri, cât de mâine. În sfera educației, consecința practică imediată este necesitatea adaptării instrucției și educației la ritmul rapid de dezvoltare a societății. Este foarte cunoscută afirmația lui Gaston Berger, potrivit căreia: „viitorul nu trebuie așteptat, ci construit și, în consecință, în primul rând inventat”. Astfel, trecutul este cel care configurează și explică viitorul, iar evenimentele viitorului prezintă rațiunea prezentului.

Activitatea de formare inițială a soldaților profesioniști ai Armatei României nu poate să nu țină seama de aceste abordări (dar oare se întâmplă așa?), de această poziționare a procesului de formare profesională pe axa trecut – prezent – viitor; prin urmare, învățământul militar și instrucția ar trebui concepute pe principiile prospecției în educație. Între principiile metodologice generale, care stau la baza elaborării strategiilor de formare, s-ar putea menționa:

– *a privi departe*, respectiv a examina alternativele, deciziile posibile, demersurile prezente și viitoare privind armata și rolurile sale, din perspectiva implicațiilor și a consecințelor pe termen lung, altfel existând pericolul unor nesincronizări cu cerințele societății;

– *a privi cuprinzător*, respectiv a analiza posibilele interacțiuni, corelații între fenomenele,

procesele, sistemele implicate, pentru a promova o viziune sistemică;

– *a analiza în profunzime*, respectiv a identifica toți factorii care influențează evoluția pe termen lung a armatei și a rolurilor sale, pentru a putea interveni oportun din punct de vedere educativ;

– *a și asuma riscuri*, respectiv a nu se limita la explicarea evoluțiilor viitoare posibile și realizabile, ci a se implica în realizarea acestora, a prelua anumite responsabilități umane, sociale, politice și militare;

– *a se gândi la om*, respectiv a avea tot timpul în vedere faptul că prospectiva educațională trebuie să se realizeze într-o viziune umanistă.

Educația ca fapt, fenomen, proces și relație socială

Trăim într-o epocă în care resursele umane (inteligenta, creativitatea, adaptabilitatea) au trecut pe primul plan, devenind sursele-cheie ale unei dezvoltări care integrează diferitele sale dimensiuni: pacea, economia, mediul înconjurător, justiția socială și democrația. Tot mai mult se înțelege ideea că dezvoltarea trece prin educație și cultură și că dezideratul poate deveni realitate socio-educatională numai în măsura în care toți membrii unei colectivități umane și-l însușesc ca perspectivă și ca program de lucru¹.

Educația ca fapt social poate fi înțeleasă ca o cauză, dar și ca un efect al unui alt fapt social, fie el economic, cultural, religios, militar ș.a., capabil să producă o schimbare de mentalitate. Educația acționează asupra omului ca ființă individuală, influențându-l în comportamentul său

¹În Raportul întocmit pentru UNESCO de Comisia Internațională asupra educației pentru secolul XXI, intitulat sugestiv: *L'éducation- un tresor est caché dedans* (1996), Jacques Delors sublinia că educația nu este un „remediu miraculos”, un fel de „sesam, deschide-te”, ci un atu indispensabil, o cale în serviciul dezvoltării umane, un strigăt de dragoste față de copii, față de generația tânără, un voiaj interior jalonat de cunoaștere, meditație și exercițiu practic.

cotidian, chiar dacă măsurile nu pot fi decât rezultatul unei acțiuni sociale. Un fapt educațional poate fi, de exemplu, și un calificativ/notă acordată unui cursant pe merit sau nu, căci ambele produc o modificare în comportamentul acestuia, fie prin sporirea motivației învățării, fie prin efecte contrare sensului dorit de instructor.

Educația devine un fenomen social când antrenează o colectivitate de masă și devine un reper, un criteriu de apreciere în analizele sociale. Ca orice fenomen social, educația are o condiționare obiectivă și subiectivă. Ea este influențată de *contextul social* în care se manifestă, influențat și el de condițiile materiale, voința politică, ansamblul politicilor educaționale etc., dar și de actorii sociali participanți în relație (educatori și educați). *Contextul social* generează și răspunde unor nevoi prezente pe care educația le satisface, dar a cărei finalitate nu o putem anticipa. Ea va fi confirmată sau infirmată de viitorul social. Proiectarea devine în aceste condiții o componentă a politicii educative care pornește de la evaluarea stării actuale a educației și identificarea actorilor sociali care realizează acest tip de schimbare.

Educația ca proces social pune în evidență o structură, funcționare, actori sociali, măsuri de politică educațională, se derulează în timp. Deosebirea dintre educația ca fenomen și conceperea ei ca proces are în vedere, în special, dimensiunea temporală, adică timpul necesar de la exercitarea influenței până la măsurarea efectelor și compararea lor cu finalitățile dezirabile și așteptate. Datorită caracterului permanent, pe durata întregii vieți, este dificil de identificat și exprimat care sunt contribuțiile fiecărui factor educațional.

Educația presupune o relație între cei care participă la proces. *Relația* între instructorii militari, pe de o parte, și cursanții/soldații profesioniști aflați la cursurile de formare, pe de altă parte, relația dintre educatori și educați, care în condițiile actuale, precum ar spune Leon Bloy „*nu se știe cine dă și cine primește*”. În relația educativă, aceasta înseamnă asigurarea unui permanent feed-back între partenerii procesului educativ. Chiar dacă există o asimetrie a relațiilor de putere între educator și educat, aceasta nu trebuie să fie un pretext pentru abuzul de putere, doar în numele vârstei, experienței, statutului socio-profesional ș.a. care plasează cei doi membri ai relației în poziții inegale.

Educatorul trebuie să înțeleagă că axioma mai veche conform căreia *trecutul explică viitorul*, trebuie înlocuită cu aceea că *viitorul este rațiunea de a fi a prezentului*, stimulând voința omului de a construi dezirabilul și de a ieși de sub domnia viitorilor probabili. Deși poartă în sine un grad de incertitudine, *el poate fi construit pentru că îl dorim* și poate tocmai de la acest deziderat începe munca noastră, de la ceea ce am dori să formăm pentru ceea ce este de așteptat.

Instrucția – prezent și perspective

Procesul de instruire a personalului, și în special a soldaților profesioniști din arma comunicații și informatică, pentru o mare varietate de operații militare are caracteristici care-l diferențiază de oricare alt tip de proces instructiv-educativ.

Instruirea presupune activități de predare – învățare - evaluare; acceptăm aici termenul de „predare” în sensul general – desemnând toate eforturile instructorului militar de a transmite informația specifică, de a forma capacități intelectuale, motrice și atitudini solicitate, mai ales, de acțiunile militare. În instruire este imperios necesară ordonarea logică, de la teoretic la practic-aplicativ, de la simplu la complex, de la individ sau structuri mici la eșaloane superioare, în vederea fundamentării instruirii personalului și forțelor pe principii, concepte și tehnologii moderne (specifice NATO).

Orice act instructiv-educativ performant impune și tinde spre o formă optimală de organizare. Din perspectivă sistemică, este necesar să se aibă în vedere că instruirea trebuie planificată coerent și riguros, desfășurată cu competență și realism, precum și evaluată în raport cu standardele de performanță stabilite și cât mai obiectiv.

Instrucția, în accepțiune generală, este învățătura, știința căpătată în școli/prin învățare, prin studiu organizat, dar și procesul de predare a cunoștințelor și deprinderilor într-o instituție de învățământ, iar, din perspectivă militară, aceasta reprezintă *totalitatea acțiunilor destinate însușirii cunoștințelor, formării, dezvoltării/perfecționării și menținerii deprinderilor individuale (intelectuale, senzoriale, motrice) și colective, necesare pentru îndeplinirea sarcinilor/misiunilor ce le revin în timp de pace, în situații de criză, la război și în etapa postconflict*.

Instrucția trebuie să fie procesul organizat și integrat² de educație și antrenament prin care se cultivă spiritul de învingător și virtuțile militare, se realizează coeziunea structurilor militare, spiritul de corp și se dezvoltă capacitatea forțelor de acțiune în concordanță cu standardele militare operaționale. Eficiența oricărei activități instructive implică echilibrarea relației dintre elementele ei componente. Obținerea unor performanțe înalte depinde de structurile organizatorice și conținutul instruirii, iar în instituția noastră, instrucția se desfășoară pe două paliere distincte: instrucția *individuală* de bază și instrucția *individuală* de specialitate.

Modernizarea activității instructiv-educative a implicat discuții/dispute serioase și în legătură cu formele de organizare a acesteia. Ele sunt sesizabile chiar la nivelul conceptual de bază. Se face, astfel, distincția – spre exemplu – între formă de organizare a procesului instructiv-educativ, formă de organizare a învățării, formă de organizare a activităților educative extrașcolare ș.a.m.d.

În principiu, *forma de organizare* se referă la modul sau maniera de lucru în care se realizează activitatea binomului instructor-instruit, modul de lucru cu grupul sau cu individul. Ea circumscrie o activitate cu durată variabilă și o structură specifică prin care se urmărește îndeplinirea scopurilor fundamentale ale instrucției, implică o articulare sistemică a tuturor elementelor procesului de instrucție.

Creșterea repertoriului formelor de instruire și educare impune clasificarea lor după numărul de participanți și al modului în care se înfăptuiește relația instructor-instruit în procesul instrucției (frontal, de grup, individual) și din punct de vedere al locului în care se desfășoară activitatea instructivă (instituționalizat, conex, operațional).

Instrucția militară reprezintă o activitate preponderent practică (aproximativ 75%), iar pentru asimilarea cunoștințelor și formarea deprinderilor intelectuale, senzoriale, motrice, individuale (forța fizică, rezistența fizică și psihică, îndemânarea ș.a.) - necesare soldatului profesionist – pentru a putea rezolva probleme tipice generate de activități militare, aplicarea în practică a cunoștințelor însușite anterior, formarea unor trăsături de personalitate tipice (curaj, spiritul

de ordine și disciplină, camaraderia, solidaritatea ș.a.) un rol deosebit revine instructorului.

Instructorul militar – lider educațional

Se cunoaște faptul că metodele de predare utilizate în cadrul instrucției militare nu devin eficiente prin ele însele, ci sunt puse în valoare de inteligența și priceperea instructorului militar. Binomul „*metode + calități personale*” asociază într-o formulă unitară și firească o cerință devenită evidentă. O metodă atestată ca fiind bună se poate transforma în contrariul ei în mâinile unui instructor militar care nu are abilități psihopedagogice. Rămânând în același cadru, este evident că, în timp ce metodele constituie tehnici transmisibile, aptitudinile personale rămân atributul fiecăruia.

În această optică, modul de proiectare și de realizare a procesului de învățământ militar devine „*în bună măsură o artă, întrucât depinde de însușirile personale*”³.

Se consideră necesară această precizare întrucât se dorește să se scoată în evidență importanța însușirilor de personalitate și rolul instructorului militar în cadrul activității de instruire a soldaților profesioniști.

Un bun instructor militar, pentru a-și îndeplini la un înalt nivel de performanță și eficiență complexă sa activitate, trebuie să-și formeze și să manifeste o serie de însușiri (calități) ale personalității sale, cum ar fi următoarele:

a) *vocația pedagogică* – după părerea majorității pedagogilor este principala însușire a instructorului;

b) *pregătirea de specialitate temeinică* – constituie calitatea esențială și fundamentală pentru exercitarea la un înalt nivel a muncii de instructor militar; dacă el nu este bine pregătit, nu poate pregăti pe alții;

c) *capacitatea de creație științifică* – un bun instructor militar trebuie să întreprindă o continuă activitate de documentare și să folosească în demersul său tot ceea ce este nou în domeniul disciplinei predate;

d) *orizont cultural larg* - pentru a se manifesta nu doar ca specialist militar, dar și ca un adevărat intelectual; instructorul militar trebuie să aibă o bogată cultură generală pe care să o folosească în complexa sa activitate.

²Doctrina instruirii Armatei României, București, 2006.

³ Ionescu, R., *Experiență didactică și creativitate*, Editura Dacia, Cluj-Napoca, 1987, p.86.

e) *pregătire psihopedagogică* – calitatea de educator, de pedagog nu este înnăscută. Această calitate se însușește și se dezvoltă sub forma profesiei de instructor, așa cum se însușește și calitatea de specialist. I. Bontaș subliniază faptul că, *acea concepție potrivit căreia dacă ești un bun specialist este și suficient să fi profesor este falsă*⁴.

Obținerea profesiei de instructor militar care să se manifeste cu competență și eficiență este cu siguranță numai rezultatul îmbinării armonioase a calităților de specialist militar cu calitatea de psihopedagog.

Empatia, ca însușire de personalitate, presupune capacitatea de transpunere a unei persoane într-un model uman exterior, condiționând înțelegerea și comunicarea implicită și o retrăire afectivă a stărilor emoționale ale modelului.

Concluzii

Educația prin instrucție, prin intermediul valorilor pe care le prelucrează, selectează și transmite sub formă de cunoștințe, priceperi și deprinderi, contribuie la formarea și dezvoltarea personalității raționale, precum și la perfecționarea tuturor capacităților intelectuale,

funcțiilor cognitive și instrumentale, necesare practicării profesiei militare.

Performanțele celui instruit rezultă nu doar din măsura în care acesta și-a atins obiectivele, ci mai ales din dezvoltarea capacității acestuia de a se adapta și a rezolva problemele nou apărute pe timpul instruirii. Pe scurt, de a găsi resursele necesare soluționării situațiilor create, pregătindu-l astfel pentru o gândire constantă, sănătoasă, creându-i bazele unui studiu consecvent, individual.

Concluzionând, se poate afirma că obiectivul principal al instrucției, pe lângă celelalte definiții și trăsături care o caracterizează, trebuie să fie educația, însușirea unui sistem de metode de lucru și investigație, astfel încât cel care se educă să fie capabil de continuarea efortului de instruire/autoinstruire, de adaptare la cerințele funcțiilor pe care va fi încadrat.

⁴ Bontaș, I., *Pedagogie- Tratat* Editura All, București, 1994, p.40.

OPINII PRIVIND INTERDEPENDENȚA/RELAȚIONAREA PROCESULUI PATRIMONIAL CU PROCESUL MANAGERIAL ÎN BATALIONUL INSTRUCȚIE COMUNICAȚII ȘI INFORMATICĂ „FRAȚII BUZEȘTI”

Maior Cornel DRĂGHICI

Batalionul Instrucție Comunicații și Informatică „Frații Buzești”



Personalul desemnat cu privire la inițierea și derularea operațiunilor supuse controlului financiar preventiv propriu din unitate sunt o resursă importantă a întregului ansamblu organizațional, pregătită să asigure cu cele necesare desfășurarea procesului de instruire a

soldaților și gradaților profesioniști din unitate.

Potrivit organizării interne, în conformitate cu Ordinul ministrului finanțelor publice nr. 1792/2002, personalul desemnat, cu atribuții pe linia gestionării patrimoniului unității, a parcurs și parcurge de fiecare dată fazele privind angajarea, lichidarea, ordonanțarea și plata cheltuielilor. De asemenea, acestea sunt persoanele care au competența necesară să dispună utilizarea resurselor din unitate. În acest sens, operațiunile promovate pentru acordarea vizei de control financiar preventiv propriu au la bază documente justificative avizate și întocmite în volum complet. Din acest motiv, nu s-au înregistrat operațiuni refuzate la viză.

Numai în anul 2014 au fost promovate un număr de 1426 operațiuni supuse controlului financiar preventiv propriu din sfera: achizițiilor, a consumurilor de materiale, a gestionării patrimoniului din punct de vedere al patrimoniului imobiliar, precum și al valorificării de bunuri rezultate în urma declasărilor și casărilor de bunuri. Toate aceste operațiuni cumulează o valoare totală pentru care s-a acordat viza de control financiar preventiv propriu de 43.028 mii lei.

Acest lucru a fost posibil și este în continuare posibil prin acțiunea unitară a întregului personal angrenat în procesul de administrare a patrimoniului și utilizare a resurselor, se pleacă de la inițiator și se merge până la compartimentele și/sau structurile responsabile de derulare, la structura de achiziții și

la personalul ce încadrează compartimentul financiar-contabil. La structura financiar-contabilă, controlul financiar preventiv se exercită asupra documentelor în care sunt consemnate operațiunile patrimoniale, înainte ca acestea să devină acte juridice, prin aprobarea lor de către titularul de drept al competenței sau de către titularul unei competențe delegate în condițiile legii.

În procesul de utilizare a resurselor se acordă o mare atenție în asigurarea cu cele necesare desfășurării etapelor de instruire. În baza cererilor de materiale și a rapoartelor de necesitate formulate de către personalul angrenat în asigurarea condițiilor de instruire, echipare, hrănire și cazare a soldaților și gradaților profesioniști ce urmează modulele de instruire și cele de perfecționare, compartimentele de specialitate verifică în permanență gradul de asigurare și de încadrare în normele de consum și numai după aceea, dacă este cazul, inițiază operațiunile specifice de achiziție pentru acoperirea deficitelor. Se pune accent pe utilizarea serviciului electronic de achiziții publice; în mod special și numai prin excepție este utilizată achiziția directă. Am reușit ca în ultimii doi ani să creștem procentul de achiziții prin intermediul serviciului electronic la un nivel mediu de peste 70%. Lucru cu care noi ne mândrim. Acest fapt demonstrează printre altele și transparența procesului de achiziții publice din unitatea noastră.

Despre planificarea bugetară, solicitarea, repartizarea și utilizarea creditelor bugetare cu privire la nivelul execuției bugetare, se fac analize și informări săptămânale în ședințele de lucru ale comandantului. Nu întâmplător, pe parcursul execuției bugetare, nivelul atins a fost de cele mai multe ori de 100%.

Toate aceste rezultate au la bază o bugetare obiectivă prin care sunt determinate costurile pe obiective, activități, misiuni, naturi de cheltuieli și ani, sunt încadrate și grupate pe structura clasificăției bugetare, rezultând proiecțiile de resurse financiare corespunzătoare nevoilor

viitoare pentru asigurarea condițiilor optime de instruire ale soldaților și gradaților profesioniști.

Putem concluziona că întregul angrenaj angajat în procesul de inițiere și derulare a operațiunilor supuse controlului financiar preventiv propriu este fundamentul procesului managerial și

are rolul de a identifica, de a contura și de a stabili ceea ce urmează să se facă. În esență, are menirea de a orienta eforturile viitoare, care sunt rațional alocate și eficient combinate în vederea realizării obiectivelor manageriale.

BATALIONUL DE INSTRUCȚIE – PARTICULARITĂȚI MANAGERIALE

Maior Ionuț-Daniel ȘERBAN

Batalionul Instrucție Comunicații și Informatică „Frații Buzești”



Armata este o instituție în care primează anumite particularități:

- conducerea este bazată pe autoritate formală, iar ordinele comandanților trebuie îndeplinite întocmai, la timp, în volum complet și fără șovăiri;
- o unitate militară este un sistem format din compartimente specializate, fiabile și stabile, bazat pe o ierarhie strictă, reglementări precise și comandă unică;
- stările de incertitudine și indisciplină sunt intolerabile;
- interesele generale, de grup, primează în fața celor individuale;
- reglementările specifice și detaliate și uniformitatea impusă conduc la o independență decizională din ce în ce mai redusă pe măsură ce se coboară pe scara ierarhiei;
- spiritul de echipă și coeziunea de grup capătă o importanță ridicată.

Managementul unei organizații militare este, prin prisma acestor particularități, dar nu numai, diferit de cel al unei organizații civile.

Mergând pe aceeași linie, managementul unei unități militare de instrucție este, la rândul lui, diferit față de managementul unei unități sau mari unități luptătoare.

O unitate de instrucție, în cazul acestui articol – batalion de instrucție, însumează două componente: ipostaza de unitate militară și ipostaza didactică, de „instructori-învățători”.

Având în vedere faptul că instruirea forțelor reprezintă activitatea esențială a procesului de realizare a capacității operaționale a Armatei României și că în batalionul de instrucție începe formarea inițială a soldaților și gradaților profesioniști prin parcurgerea și finalizarea programelor de formare inițială, rezultă clar că

într-o astfel de instituție apar particularități manageriale majore.

Prima particularitate derivă din vârsta pe care recruții o au la începerea programului de formare – între 18 și 46 de ani. Astfel, pe poarta unității intră la pregătire atât proaspeți absolvenți ai învățământului liceal, care sunt pregătiți și „deschiși” pentru acumularea de noi cunoștințe, cât și persoane ajunse la maturitate, dar care nu au mai „stat în bancă” de multă vreme. Din acest punct de vedere, de la comandantul de grupă – instructor, până la comandantul companiei, toți vor trebui să acorde o atenție deosebită integrării graduale a soldaților profesioniști și adaptării acestora la procesul de instruire și vor trebui să dea dovadă de tact, răbdare, putere de motivare, să aibă o bună capacitate de comunicare și un comportament exemplar.

O altă particularitate o reprezintă faptul că batalionul de instrucție este un mediu cu solicitări fizice și psihice intense, cu multiple activități curriculare, dar și extracurriculare, cu multe dintre acestea soldații profesioniști neîntâlnindu-se înainte. Astfel, instructorii trebuie să aibă un vast bagaj de cunoștințe, în același timp trebuind să dețină noțiuni de psihopedagogie necesare transmiterii cunoștințelor și experienței proprii, îndrumării și consilierii soldaților profesioniști.

Batalionul de instrucție presupune și uniformizarea condițiilor de cazare, de hrănire și de studiu. Soldații profesioniști provin din medii diferite, cu un grad de civilizație diferit, posibilități materiale diferite. Pentru unii dintre ei, de abia la acest moment apar primele responsabilități (întreținerea uniformei, a cazarmamentului, a sectoarelor) și, în același timp, pentru majoritatea apar primele îngrijiri ale unor libertăți.

Din nou, instructorii, împreună cu administratorii de subunități, trebuie să dea dovadă de preocupare și responsabilitate, să acorde sprijin susținut și să suplinească ajutorul pe care, acasă, soldatul profesionist l-ar primi de la mamă sau tată, de la soț sau soție, să îi transmită acestuia modul cum se păstrează, utilizează și valorifică resursele materiale puse la dispoziție.

Un alt element particular îl reprezintă caracterul practic-aplicativ al instrucției. Dacă în învățământul general și liceal, profesorul transmite foarte multe cunoștințe teoretice, iar exercițiile și partea practică sunt mai mult „pe post” de „teme pentru acasă”, în batalionul de instrucție se pune accent pe ședințele practice, în timp ce teoria pregătește și doar susține demersul practic-aplicativ. Acest lucru se datorează faptului că soldatul trebuie format în primul rând ca executant, ca luptător activ, iar programul de formare inițială este unul relativ scurt, de doar 18 săptămâni. De aici a rezultat necesitatea transformării și remodelării instrucției pe baza unor programe de instrucție individuală standardizate, care au prevăzute în componența lor activități standard de instrucție și evaluare.

Din alt punct de vedere, activitatea de cunoaștere a soldaților profesioniști reprezintă o altă particularitate a unui batalion de instrucție. Este imperios necesar ca un comandant de grupă sau pluton – instructor să fie și un bun psiholog, să cunoască aptitudinile psihosociale ale soldaților, abilitățile și punctele lor slabe, astfel încât acestea să fie fructificate sau, după caz, antrenate și dezvoltate, în scopul trecerii treptate la o coeziune de grup/echipă/echipaj cât mai bună și cu rezultate individuale și colective maxime.

În rezolvarea tuturor acestor particularități, în afara comandantului de grupă, pluton sau companie este necesară și implicarea celorlalte cadre militare sau personalului civil din batalionul de instrucție: structura de personal pentru verificarea dosarelor de candidat și transmiterea informațiilor extrase către instructori și prin consilierea soldaților profesioniști privind evoluția lor în carieră; compartimentul operații și instrucție pentru coordonarea și verificarea activităților de instruire; structura logistică pentru asigurarea condițiilor de cazare, echipare și hrănire; psihologul unității pentru asigurarea sprijinului de specialitate soldaților profesioniști în depășirea

anumitor momente grele; compartimentul medical pentru asigurarea măsurilor profilactice și acordarea tratamentelor de specialitate.

Toate acestea sunt imperios necesare pentru a crește eficiența actului de instruire, pentru a putea trimite la unitățile beneficiare soldați profesioniști bine instruiți, buni profesioniști, având temeinice cunoștințe acumulate și deprinderi corect formate.

Nu este de neglijat faptul că, într-un batalion de instrucție, pot apărea și erori sau deficiențe ce pot avea efecte negative asupra formării inițiale a soldaților profesioniști:

- o conducere excesiv autoritară, fără înțelegerea personalității fiecăruia în parte poate bloca dorința soldaților de a continua cariera militară;

- neglijarea regulilor medicale sau psihopedagogice în proiectarea programelor de instrucție poate conduce la apariția problemelor pe aceste linii/domenii;

- punerea la dispoziția cursanților a unor condiții de cazare, hrănire și recreere neadecvate conduc la apariția oboselii, surmenării și suprasolicitării, ceea ce poate duce la un interes scăzut în pregătire;

- neangrenarea soldaților profesioniști în activități de recuperare sau petrecere plăcută a timpului liber (vizite la muzee, teatre sau spectacole) poate conduce la stări de demoralizare sau chiar la dorința de abandonare a carierei militare.

Argumentele prezentate mai sus denotă clar și fără dubii că într-un batalion de instrucție există particularități manageriale diferite față de mediul civil, respectiv față de o unitate militară operaționalizată, de acestea orice comandant trebuind să țină cont pentru ca rezultatele să fie maxime, iar produsul final să fie reprezentat de un soldat profesionist bine pregătit și antrenat, apt să își îndeplinească misiunile specifice de execuție în domeniul CIS.

INSTRUCȚIA INDIVIDUALĂ ÎN DOMENIUL APĂRĂRII CIBERNETICE - FACTOR ESENȚIAL ÎN SECURITATEA SISTEMELOR INFORMATICE ȘI DE COMUNICAȚII

Maior Cătălin GHERGHEL

Centrul 42 Comunicații și Informatică de Sprijin



Pe parcursul ultimelor decenii, tehnologia informațiilor s-a dezvoltat deosebit de mult, devenind de la un instrument administrativ pentru optimizarea proceselor de birou la un instrument strategic al industriei, administrației și, nu în ultimul rând, al apărării. Astfel, a devenit evident că lumea cibernetică presupune vulnerabilități serioase în vederea atingerii obiectivelor strategice asumate de societate în ansamblu. Pentru gestionarea riscurilor și amenințărilor ce derivă din vulnerabilitățile spațiului cibernetic, apreciem că este necesar și obligatoriu ca acest domeniu al apărării spațiului virtual să devină primordial în pregătirea/instruirea generală și de specialitate în informatică.

Spațiul cibernetic se caracterizează prin lipsa frontierelor, dinamism și anonim. Cu cât o societate este mai informatizată, cu atât ea poate fi mai vulnerabilă. Asigurarea securității spațiului virtual trebuie să constituie o preocupare majoră a tuturor actorilor implicați, atât la nivel instituțional, unde se concentrează responsabilitatea elaborării și aplicării de politici coerente în domeniu, dar și în mediul privat, care operează în fapt 80% din internet.

Eliminarea acestor vulnerabilități implică o cooperare strânsă, permanentă, între actorii instituționali care generează politicile pentru securizarea spațiului cibernetic și cei privați, care gestionează segmente importante ale sistemelor informatice și de comunicații.

La nivel mondial există în jur de 150 de organisme naționale de tip CERT, care sunt conectate la o rețea în care schimbă informații și lansează alerte cu privire la atacurile cibernetic.

În România, încă din anul 2011, prin HG 494, s-a înființat Centrul Național de Răspuns la Incidente de Securitate Cibernetică – **CERT-RO**.

Informațiile și alertele folosite de CERT-RO pentru a preveni și a contracara atacurile cibernetic vin din această rețea, dar și de la utilizatori privați de pe internet, de la firme de securitate IT, telefonie sau telecomunicații. În cazul unui atac la nivel instituțional, CERT-RO este alertat prin măsurile tehnice cu care sunt securizate rețelele informatice ale instituțiilor.

CERT-RO pune la dispoziție ghiduri utile în asigurarea securității sistemelor informatice.

Asigurarea securității cibernetic se bazează pe cooperarea la nivel național și internațional pentru protejarea spațiului cibernetic.

Privind dinamismul evoluțiilor globale în spațiul cibernetic, precum și obiectivele României în procesul de dezvoltare a societății informaționale și implementare pe scară largă a serviciilor electronice, este necesară elaborarea unui program național detaliat, care – pe baza reperelor oferite de prezenta strategie – să asigure elaborarea și punerea în practică a unor proiecte concrete de securitate cibernetică.

AMENINȚĂRI CIBERNETICE

➤ **Amenințările de tip Drive-by** - când un utilizator vizitează un site ce conține exploit-uri drive-by, se pot exploata vulnerabilități în browser, în plugin-urile acestuia sau în sistemul de operare pentru a instala malware pe PC fără știrea utilizatorului.

În fiecare zi, atacatorii manipulează mii de site-uri web din întreaga lume și apoi injectează un cod malițios în conținutul acestora. Aceste site-uri, de regulă, sunt compromise prin furtul datelor de autentificare.

Exploit-urile de tip drive-by și-au extins aria de acțiune în 2012 și la terminalele mobile. Conform McAfee și F-Secure, începând cu luna mai 2012 apar primele rapoarte cu privire la folosirea acestui instrument de către atacatori pentru exploatarea vulnerabilităților sistemului de operare Android.

➤ **Viermi/Troieni:**

Viermi: programe care se pot auto-replica. Acestea folosesc rețeaua de calculatoare pentru a-și trimite propriile copii în alte noduri (calculatoare din rețea), reușind să facă acest lucru fără intervenția vreunui utilizator.

Spre deosebire de un virus informatic, un vierme informatic nu are nevoie să fie atașat la un program existent. Viermii provoacă daune rețelei, chiar și prin simplul fapt că ocupă bandă, în timp ce virusii corup sau modifică aproape întotdeauna fișiere de pe computerul țintă.

Troieni: programe care se prezintă sub forma unor programe legitime, dar, în realitate, sunt create cu scopul de a fura date confidențiale sau de a permite unor utilizatori sau programe neautorizate accesul la computerul infectat. Conform *ENISA Threat Landscape 2012*, troienii constituie marea majoritate a infecțiilor (80%).

În ceea ce privește aria terminalelor mobile, un raport al F-Secure din 2012 arăta că 84% din amenințări sunt reprezentate de către Troieni.

➤ **Injecție de cod:** tehnici de atac binecunoscute împotriva aplicațiilor web, cum ar fi SQL Injection (SQLi), cross-site scripting (XSS), cross-site request forgery (CSRF), Remote File Inclusion (RFI) etc. Atacurile de acest tip sunt populare în rândul grupurilor hacktivist (ex: Anonymus), grupurilor de hackeri (ex: LulzSec) și în rândurile infractorilor cibernetici (ex: LizaMoon25).

➤ **Kit-uri de exploatare:** software automatizat care ajută atacatorii mai puțin experimentați în compromiterea sistemelor prin exploatarea vulnerabilităților de tip client-side, în special a celor din browsere web sau aplicații ce pot fi accesate de site-uri web (ex: Adobe Reader, Flash, JRE etc.).

➤ **Botnet:** reprezintă un set de computere care se află sub controlul unui atacator. Rețeaua de tip botnet poate fi utilizată cu scopuri multiple: atacuri de tip „Distributed Denial of Service - DDoS”, spamming, furt de identitate, distribuire de malware, infectarea sistemelor informatice etc.

➤ **Denial of Service:** încercare de a afecta disponibilitatea unor sisteme/servicii informatice sau comunicații electronice. Sistemul țintă este atacat prin transmiterea unui număr foarte mare de solicitări nelegitime, ce consumă resursele hardware sau software ale acestuia, făcându-l indisponibil.

➤ **Phising:** o formă de înșelăciune în mediul online care constă în folosirea unor tehnici de manipulare a identității unor persoane/organizații pentru obținerea unor avantaje materiale sau informații confidențiale prin diverse tehnici de social engineering. Atacatorii se bazează pe naivitatea utilizatorilor.

➤ **Compromiterea informațiilor confidențiale:** încălcări ale securității datelor care au apărut prin dezvăluirea (fie intenționată, fie neintenționată) de informații confidențiale de către angajați.

➤ **Rogueware/scareware:** software fals utilizat de criminalii cibernetici pentru a atrage utilizatorii către scopurile lor malițioase. Odată instalat în sistem, furnizează alerte false de securitate și invită utilizatorul să cumpere programe de dezinfectie.

➤ **Spam:** mesaje trimise de către calculatoare infectate cu troieni, care fac parte dintr-un botnet.

➤ **Atacuri direcționate:** colectarea de date cu caracter personal/confidențial sau compromiterea sistemelor informatice țintă (ex. inginerie socială).

➤ **Furt/Pierderi/Distrugere fizică:** amenințare cauzată de device-uri mobile (laptop, telefon, tabletă).

➤ **Furt de identitate:** ținta atacatorilor fiind datele personale. Se urmărește efectuarea de tranzacții financiare.

➤ **Scurgere de informații:** dezvăluirea în mod voit sau nu de informații către o persoană neautorizată.

➤ **Manipularea motoarelor de căutare (SEP):** manipularea motoarelor de căutare pentru a afișa rezultate de căutare care te conduc spre site-uri malițioase.

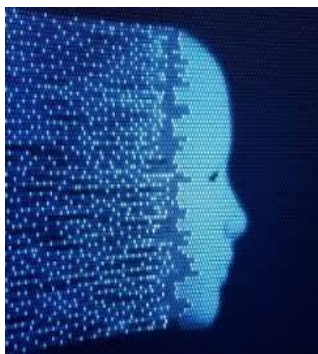
➤ **Certificate digitale false:** certificate pentru semnarea digitală a resurselor (site-uri web, aplicații, coduri sursă etc.) folosite în diverse atacuri cibernetice. Certificate false pentru semnarea aplicațiilor web malițioase de tip **e-banking sau e-commerce**, ce folosesc protocolul HTTPS.

MĂSURI DE APĂRARE CIBERNETICĂ:

- **Cognitec Systems a încheiat un contract de colaborare pentru dezvoltare și licențiere de software cu Intel Corporation.**

Fondată în 2002, **Cognitec** este o companie germană specializată în **soluții**

biometrice, în special în **tehnologie de detectare a feței**.



Prin intermediul colaborării, cele două companii vor implementa **tehnologia de recunoaștere facială** în dispozitivele electronice **Intel**. Autentificarea pe PC-uri, notebook-uri, tablete sau telefoane mobile va deveni mai

sigură după ce noua tehnologie va înlocui parolele obișnuite, informează **Source Security**.

„**Intel** coordonează avansări importante în domeniul **securității și al biometricii**. Colaborarea cu **Cognitec** este un ingredient cheie în **dezvoltarea metodelor de autentificare** bazate pe **recunoașterea facială**, care sunt sigure, însă ușor de utilizat pentru clienți și întreprinderi”, a declarat Manish Tangri, reprezentant **Intel Corporation**.

“**Cognitec** este mândră pentru că a fost aleasă de **Intel** pentru această implementare importantă a tehnologiei noastre. **Tehnologia de recunoaștere facială** va permite proprietarilor a milioane de dispozitive electrice să le protejeze și să le acceseze ușor, fără să fie nevoiți să memoreze parole”, a explicat Alfredo Herrera, Managing Director **Cognitec Systems**.

- Folosirea software cu licență;
- Folosirea pachetelor software care beneficiază de suport din partea producătorului (Pachetele software ce nu mai beneficiază de suport tehnic (actualizări) nu vă pot oferi protecție împotriva ultimelor tipuri de atacuri sau variante de malware);
- Folosirea software de securitate antimalware (antivirus, antispam, antirootkit, antiphishing, firewall, control parental);
- Securizarea rețelei Wi-Fi;
- Securizarea unei rețele.

VPN permite utilizatorilor să comunice printr-un *tunel* prin internet sau o altă rețea publică în așa fel încât participanții la *tunel* să se bucure de aceeași securitate și posibilități puse la dispoziție numai în rețelele private.

Pentru a utiliza internetul ca o rețea privată virtuală, de tip WAN (Wide Area Network), trebuie depășite două obstacole principale. Primul apare din cauza diversității de protocoale prin care comunică rețelele, cum ar fi IPX sau NetBEUI, în

timp ce internetul poate înțelege numai traficul de tip IP. Astfel, VPN-urile trebuie să găsească un mijloc prin care să transmită protocoale non-IP de la o rețea la alta. Când un dispozitiv VPN primește o instrucțiune de transmitere a unui pachet prin internet, negociază o schemă de criptare cu un dispozitiv VPN similar din rețeaua destinație.

În consecință, o soluție VPN trebuie să realizeze cel puțin următoarele funcții vitale:

- **Autentificarea utilizatorului.** Soluția trebuie să verifice identitatea utilizatorului și să permită accesul prin VPN numai utilizatorilor autorizați. În plus, soluția trebuie să permită monitorizarea și jurnalizarea activităților pentru a arăta cine și când a accesat o anumă informație.

- **Gestionarea adreselor.** Soluția trebuie să asocieze unui client o adresă din rețeaua privată și să asigure că adresele private rămân secrete.

- **Criptarea datelor.** Datele transferate prin rețeaua publică trebuie făcute ilizibile pentru clienții neautorizați.

- **Gestiunea cheilor.** Soluția trebuie să genereze și să împrășteze cheile de criptare pentru client și pentru server.

- **Support multiprotocol.** Soluția trebuie să fie capabilă să manevreze protocoalele existente în rețelele publice, cum ar fi Internet Protocol (IP), Internet Packet Exchange (IPX) etc.

Cel mai întâlnit dintre protocoalele VPN discutate anterior este IPSec – un „open-standard” de securitate folosit de cele mai mari firme, printre care se numără IBM, Sun sau BayNetworks – pentru stabilirea comunicațiilor directe private prin internet.

Internet Protocol Security (IPSec) oferă caracteristici de securitate extinsă, precum și algoritmi de criptare mai buni, pe lângă mecanisme de autentificare. IPSec are două moduri de criptare: tunel și transport. Tunelul criptează doar antetul, în timp ce transportul criptează și datele. IPSec poate cripta date între diverse echipamente: ruter-ruter, firewall-ruter, PC-ruter, PC-server.

IPSec vă protejează datele în trei moduri, folosind tehnici criptografice:

- **Autentificarea:** Procesul prin care este verificată identitatea unui host (stație de lucru).

- **Verificarea integrității:** Procesul prin care se semnalează orice modificări ale datelor survenite în procesul de transport prin internet, între sursă și destinație.

▪ **Criptarea:** Procesul de codificare a informației în tranzit prin rețea, pentru a asigura caracterul său privat.

- Securitatea rețelei WI-FI:
 - Schimbarea parolei de acces pentru configurarea routerului (parolă complexă, minim 8 caractere, caractere speciale :\$#*&, cifre, litere mari și mici);
 - Alegerea criptării WPA, WPA2 sau WPA + WPA2, o parolă de minim 10 caractere (cât mai complexă și schimbarea ei la o perioadă de 3-6 luni) pentru o securitate mai ridicată.
 - Schimbarea SSID-ului clasic sau debifarea opțiunii SSID broadcast;
 - Filtrarea, după adresa MAC, a echipamentului. Setarea DHCP pentru controlul numărului de IP-uri.
 - **Un alt sfat pentru o securitate mai bună a echipamentului Wi-Fi ar fi poziționarea acestuia în casă cât mai central, cât mai departe de fereastră ca să nu poată fi accesat din exterior (semnalul să fie cât mai slab sau inexistent).**

Programe utile

Aplicații pentru devirusare troian
FLAME/GAUSS

Bitdefender_Gauss_Removal_Tool
Bitdefender_Flame_Removal_Tool
Kaspersky_Virus_Removal_Tool

AntiMalware Free

Avast Free Antivirus
AVG Free Antivirus
Bitdefender Free Edition
Microsoft Security Essentials
Microsoft Malicious Software
Removal Tool
Kaspersky Free Virus Scan

Program testare rețele

Back Track Linux

Program testare web-server

Apache Benchmark

Forensic Tools

Mandiant Red Curtain

Mandiant Red Line
Acces Remote
PuTTY
Aplicații Criptare
Pretty Good Privacy - GnuPG
TrueCrypt.
Aplicații de tip Firewall
COMODO Free Firewall
ZoneAlarm Free Firewall
Aplicații Detectare Intruziuni
OSSIM
OSSEC
SNORT
Scanner de Porturi
Angry Ip Scanner
Net Scan
NMAP
Server Proxy
Paros Proxy
Monitorizare Trafic
Wireshark
Scanere de Vulnerabilități
Microsoft Baseline Security
Analyser
NESSUS
OpenVAS
W3AF
Scanare online
Bitdefender
Eset Online Scanner
Norton security scan
Microsoft safety scanner

BIBLIOGRAFIE:

- www.cert-ro.eu
- www.microsoft.com/windowsserver2003/technologies/networking/vpn/default.msp
- <http://www.nato.int/>
- <http://www.marketwatch.ro/>
- <http://www.securitatea-informatiilor.ro/carti/>
- Tannenbaum A.S. - "Rețele de calculatoare", Computer Press Agora, 1996

MOTIVAREA PERSONALULUI PENTRU ÎNDEPLINIREA OBIECTIVELOR

Căpitan Daniel DACICA

Batalionul Instrucție Comunicații și Informatică „Frații Buzești”



În jurul anului 210 Î.Hr., un general chinez numit Xiang Yu (Î.Hr. – 202 Î.Hr.) și-a dus armata peste fluviul Yangtze pentru a ataca armata dinastiei Qin. Trupele au înnoptat pe mal, iar dimineața s-au trezit în panică deoarece corăbiile

lor erau în flăcări. Au sărit repede la arme, însă generalul i-a oprit spunând că el a dat ordin să fie incendiate corăbiile și să fie distruse sursele de hrană. Generalul a explicat că fără cale de întoarcere și fără mâncare, aveau de făcut o alegere simplă: să învingă inamicul sau să moară pe câmpul de luptă. Rezultatul a fost că armata lui Xiang Yu a învins în 9 bătălii consecutive, distrugând întreaga armată a dinastiei Qin. Observăm cum generalul s-a folosit de instinctul de supraviețuire al oamenilor săi și a învins.

Instinctul de supraviețuire reprezintă, în această situație, *mobilul care a provocat, care a susținut energic și care a orientat acțiunea*. Este *motivul care a asigurat declanșarea comportamentelor corespunzătoare atingerii țintei propuse*.

Instinctul de supraviețuire este atât *motivul* care i-a făcut pe oameni (angajații armatei, subordonați) să nu renunțe, ci să lupte alături de general (și-a folosit abilitatea de a-i face pe oameni să lupte cu el și pentru el); dar și *motivația* = instrument folosit de conducător pentru obținerea unei performanțe superioare.

Arta motivării celorlalți în legătură cu scopurile comune este esențială pentru succesul oricărui manager. Deși este o artă veche, în cadrul organizațiilor, preocuparea pentru motivarea subordonaților de către manageri a avut loc la începutul secolului XX.

Motivația este un „concept fundamental în psihologie și, în genere, în științele despre om, exprimând faptul că, la baza conduitei umane, se află întotdeauna un ansamblu de mobiluri –

trebuințe, tendințe, afecte, interese, intenții, idealuri – care susțin realizarea anumitor acțiuni, fapte, atitudini”.

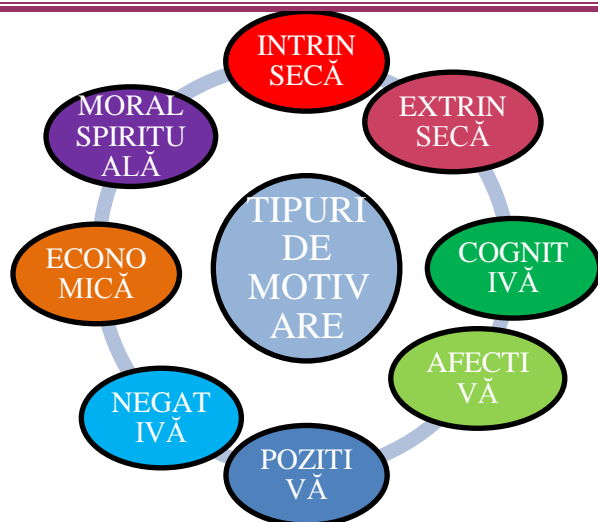
A cunoaște motivația unei persoane echivalează cu găsirea răspunsului la întrebarea „de ce” întreprinde o activitate. Răspunsul este dificil deoarece cauzele declanșatoare sunt multiple și nu se pot reduce la stimulii externi. Activitatea, reacțiile sunt declanșate și de cauze interne; ansamblul lor a fost numit motivație de la latinescul *motivus* (care pune în mișcare). Pentru unii psihologi, motivul este numele generic al oricărei componente a motivației, fiind definit ca fenomen psihic ce declanșează, direcționează și susține energetic activitatea.

În teoriile comportamentului organizațional, motivația apare ca o forță ce energizează, orientează și sprijină comportamentul uman. Din perspectiva organizației militare, motivația:

- este o forță ce impulsionează pe membrii acesteia să se comporte într-un anumit mod;
- orientează comportamentul personalului spre un anumit scop;
- necesită o perspectivă sistemică asupra forțelor intrinseci individului uman și celor aparținătoare mediului său pentru a o înțelege.

Din punctul de vedere al managementului organizației militare, motivația înseamnă abilitatea cadrelor de conducere din structurile acesteia de a crea un mediu în care subordonații pot și vor să realizeze răspunsurile solicitate. Ea apare, astfel, ca fundament, dar și măsură a succesului unui proces managerial.

Motivarea constă în corelarea necesităților, aspirațiilor și intereselor personalului din cadrul organizației cu realizarea obiectivelor și exercitarea sarcinilor, competențelor și responsabilităților atribuite în cadrul organizației. Motivarea personalului se poate clasifica, în funcție de diverse criterii, în mai multe tipuri, conform schemei:



➤ **Motivarea pozitivă și negativă**

Prin prisma criteriului influenței motivațiilor asupra mărimii satisfacțiilor personalului din participarea la procesele de muncă din cadrul organizației, motivarea poate fi pozitivă sau negativă.

Motivarea pozitivă are în vedere creșterea eforturilor și contribuției personalului la realizarea obiectivelor organizației, pe baza amplificării satisfacțiilor sale din participarea la procesul muncii ca urmare a realizării sarcinilor atribuite. Ea utilizează, preponderent, motivații generatoare de satisfacții sporite pentru salariați (măriri de salarii, acordări de titluri, avansări).

Motivarea negativă vizează sporirea eforturilor și contribuției personalului instituției la îndeplinirea obiectivelor sale pe baza diminuării satisfacțiilor în procesul muncii și a amenințării cu reducerea lor dacă sarcinile și obiectivele nu sunt realizate. Ea folosește predominant motivații generatoare de diminuări a satisfacțiilor pentru salariați (reduceri de salarii, retrogradări).

Se recomandă să se utilizeze motivarea pozitivă pentru că aceasta contribuie la instaurarea unui moral ridicat al personalului și a unui climat organizațional destins, propice dezvoltării profesionale, în timp ce motivarea negativă duce la un moral scăzut al personalului și la o atmosferă tensionată.

➤ **Motivarea economică și moral-spirituală**

În funcție de natura mijloacelor utilizate pentru motivarea personalului, motivarea poate fi economică și moral-spirituală.

Motivarea economică reprezintă motivarea realizată prin mijloace clasice, care vizează satisfacerea aspirațiilor și așteptărilor de ordin economic ale salariaților. Principalele motivații utilizate sunt: salariile, primele, penalizările la salarii, imputări financiare etc.

Motivarea economică are un rol decisiv în toate organizațiile și în toate țările.

Motivarea moral-spirituală are în vedere satisfacerea aspirațiilor și așteptărilor de natură moral-spirituală, ce vizează în primul rând sistemul de valori, atitudinile și comportamentele salariaților. În realizarea motivării moral-spirituale, se folosesc motivații ca: acordarea de titluri onorifice și medalii, exprimarea de laude și mulțumiri sau de critici și avertismente.

Se recomandă ca motivarea personalului să includă atât motivarea economică, după cum am spus esențială, cât și motivarea moral-spirituală, mai ales pentru personalul cu nivel ridicat de pregătire.

➤ **Motivarea intrinsecă și extrinsecă**

După criteriul naturii relațiilor motivaționale care se produc și amplasamentului sursei care generează efectul motivațional, motivarea poate fi intrinsecă și extrinsecă.

Motivarea intrinsecă se bazează pe determinarea salariatului să se implice, să depună efort și să obțină rezultate în cadrul organizației întrucât, din aceste procese, el obține satisfacții ce țin de eul, de personalitatea sa. Salariatul participă la procesul de muncă, la realizarea anumitor obiective organizaționale pentru că îi place ceea ce face, îi sporesc cunoștințele, învață lucruri noi, se simte realizat profesional.

Motivarea extrinsecă se bazează pe determinarea salariatului să se implice, să depună efort și să obțină rezultate în organizație pentru că acestea vor genera din partea organizației anumite reacții formale și informale, economice și moral-spirituale care îi vor produce satisfacții.

Se recomandă ca cele două tipuri de motivare să fie folosite combinat, deși în marea majoritate a organizațiilor predomină motivarea extrinsecă. Un mod de creștere a motivării intrinseci este îmbogățirea fișei postului.

➤ **Motivarea cognitivă și afectivă**

În funcție de componența personalității umane avută în vedere cu prioritate, motivarea poate fi cognitivă și afectivă.

Motivarea cognitivă are în vedere latura, dimensiunea intelectuală a salariatului, axându-se pe satisfacerea nevoilor individuale de a fi informat, de a cunoaște, de a învăța, de a inova, de a opera și controla mediul în care își desfășoară activitatea. Specific acestei motivări este însă faptul că utilizarea acestor motivații este centrată pe dezvoltarea și folosirea capacității intelectuale a salariaților, subordonată derulării proceselor de

muncă și îndeplinirii obiectivelor din cadrul organizației.

Motivarea afectivă vizează dimensiunea afectivă, strict umană a salariatului, concentrându-se asupra satisfacerii nevoilor sale de ordin sentimental în cadrul organizației. Motivarea afectivă urmărește ca salariatul să se simtă bine la locul de muncă și în cadrul organizației, să fie apreciat și simpatizat de colegi, șefi și subordonați.

Întrucât personalitatea umană are o latură cognitivă și o latură afectivă, ambele tipuri de motivare trebuie avute în vedere.

Dacă în organizațiile civile se folosesc foarte des motivarea pozitivă și cea economică, în organizațiile militare aceste tipuri de motivare sunt foarte greu, în majoritatea cazurilor imposibil de folosit. În firmele private, stau în puterea managerului mărirea salariilor, acordarea diverselor prime sau avansările, pe când în organizațiile militare nu se pot acorda mărirea de salarii sau prime, iar avansările trebuie să urmeze niște proceduri mult mai complicate decât în organizația civilă. Așadar, comandanții/șefii organizațiilor militare sunt în dezavantaj față de managerii din organizațiile civile, ei având la dispoziție o gamă mai restrânsă de instrumente motivaționale cu care să stimuleze subordonații pentru îndeplinirea obiectivelor.

În concluzie, putem spune că activitatea de motivare a personalului este o activitate complexă (o artă chiar, ar spune unii) în care managerii/șefii/comandanții trebuie să aplice, combinat, mai multe tipuri de motivare pentru a îndeplini obiectivele organizației.

Referindu-ne strict la motivarea soldaților aflați la instruire în Batalionul Instrucție Comunicații și Informatică „Frații Buzești”, putem spune că, începând cu anul 2007, atunci când s-a trecut la executarea serviciului militar pe bază de voluntariat, aceștia sunt puternic motivați pozitiv și economic de faptul că vor avea un loc de muncă stabil și că pot avansa și face carieră în această meserie.

Pe timpul desfășurării cursurilor organizate în Batalionul Instrucție Comunicații și Informatică „Frații Buzești”, pe lângă tipurile de motivare enumerate mai sus, comandanții de subunități și instructorii folosesc predominant motivarea intrinsecă și cea cognitivă (cursanților le place ceea ce fac, își sporesc cunoștințele, învață lucruri noi, încep să opereze și să controleze mediul din care fac acum parte, se simt realizați profesional), dar se încearcă și motivarea afectivă, făcându-se eforturi pentru ca militarul să se integreze cât mai bine și mai repede în colectiv, să se simtă cât mai bine în cadrul subunității și, în final, la sfârșitul perioadei de pregătire, acesta să ajungă să meargă cu plăcere la serviciu.

În final, câteva constatări de care trebuie să ținem cont:

- Motivele sunt forțele noastre interne mobilizatoare, invizibile și care nu pot fi măsurate;
- Același motiv poate da naștere la comportamente diferite;
- Același comportament, la diferiți oameni, poate fi determinat de motive diferite;
- Comportamentul poate servi pentru estimarea motivului individual care l-a generat;
- Motivele pot acționa în armonie sau în conflict;
- Motivele unui individ se modifică de-a lungul vieții sale;
- Mediul ambiant influențează întreaga gamă de motive umane.

Bibliografie:

- [1] Ausubel, D. P., Robinson, F. D., *Învățarea în școală. O introducere în psihologia pedagogică*, București, Editura Didactică și Pedagogică, 1981.
- [2] Golu, P., *Fenomene și procese psihologice*, București, Editura Științifică și Enciclopedică, 1989.
- [3] Kubr, M., *Introducere în management*, București, Editura Alternative, 1994.
- [4] Octavia, E., *Motivarea subordonaților de manageri*, Universitatea București, 2011.

CONCEPȚIA DE ELABORARE A PLANULUI ANUAL DE ACHIZIȚII PUBLICE ÎN VEDEREA ASIGURĂRII UNOR CONDIȚII OPTIME DE INSTRUIRE PENTRU SOLDAȚII ȘI GRADAȚII PROFESIONIȘTI

Căpitan Cezar MAICAN

Batalionul Instrucție Comunicații și Informatică „Frații Buzești”



În cadrul Batalionului Instrucție Comunicații și Informatică „Frații Buzești”, procesul privind achizițiile publice începe prin stabilirea cu precizie a responsabilităților, termenelor și activităților referitoare la identificarea nevoilor, a fondurilor necesare, a

procedurilor de urmat pentru elaborarea, realizarea și evidența PAAP.

Legi, Hotărâri folosite pentru elaborarea PAAP:

- Legea nr. 500/2002 privind finanțele publice, publicată în Monitorul Oficial nr. 597/2002, cu modificările și completările ulterioare.

- Legea nr. 554/2004 a contenciosului administrativ Hotărârea Guvernului nr. 782/2006 pentru aprobarea Regulamentului de organizare și funcționare al Consiliului Național de Soluționare al Contestațiilor.

- Legea nr. 337/2006 pentru aprobarea și modificarea Ordonanței de Urgență a Guvernului nr. 34/2006 privind atribuirea contractelor de achiziție publică, a contractelor de concesiune de lucrări publice și a contractelor de concesiune de servicii.

- Ordonanța de Urgență a Guvernului nr. 34/2006 privind atribuirea contractelor de achiziție publică, a contractelor de concesiune de lucrări publice și a contractelor de concesiune servicii, aprobată cu modificări prin Legea 337/2006.

- Ordonanța de Urgență a Guvernului nr. 30/2006 privind funcția de verificare a aspectelor procedurale aferente procesului de atribuire a contractelor de achiziție publică.

- Ordonanța de Urgență nr. 45/2003 privind finanțele publice locale, publicată în Monitorul Oficial nr. 431/2003, modificările și completările

ulterioare.

- Ordinul ministrului apărării nr. M-31/2008, privind competențele de achiziții, cu modificările și completările ulterioare;

- Ordinul ministrului apărării nr. M-141/2002 privind achizițiile publice și nr. M-25/2003 privind Normele metodologice de întocmire, avizare și aprobare a PAAP.

DOMENIUL DE APLICARE al PAAP

a. aprovizionarea unității cu bunurile și serviciile necesare îndeplinirii misiunilor stabilite, conform normelor;

b. utilizarea eficientă și în totalitate a fondurilor aprobate;

c. efectuarea achizițiilor de bunuri și servicii și evidența acestora în conformitate cu legislația națională și instrucțiunile specifice M.Ap.N. în vigoare.

În deplină concordanță cu indicatorii economico-financiar preluati în proiectul de buget, structurile planificare și logistică (prin compartimentul achiziții) întocmesc, în trimestrul IV al anului în curs, Proiectul programului anual de achiziții publice pentru anul următor, care cuprinde totalitatea bunurilor și serviciilor necesare de achiziționat.

La întocmirea acestui program, autoritățile contractante au obligația să țină seama de:

➤ anticipările cu privire la fondurile ce urmează să fie alocate prin bugetul anual;

➤ necesitățile de bunuri, servicii și lucrări și gradul de prioritate a acestora.

PAAP se întocmește, avizează și se aprobă în două faze distincte:

➤ faza 1 – proiectul PAAP;

➤ faza 2 – PAAP definitivat.

Programul anual al achizițiilor publice definitivat se întocmește în termen de 10 zile de la primirea bugetului de cheltuieli aprobat, de către structurile planificate de logistică (prin compartimentul achiziții) și se prezintă spre aprobare comandantului unității.

Documentul se întocmește pe capitole și articole bugetare, în limitele creditelor aprobate

prin buget și ale competențelor de achiziție acordate.

Produsele, serviciile și lucrările necesare unității pentru îndeplinirea obiectivelor, dar care fac obiectul achizițiilor publice centralizate, se solicită ierarhic structurilor care au competențe pentru achiziționarea lor, la ordin sau odată cu înaintarea proiectului de buget anual.

Pentru realizarea unei baze de date cu aceste produse, servicii și lucrări, compartimentul achiziții centralizează aceste solicitări de la toate structurile din unitate, concomitent cu propunerile anuale de cheltuieli.

Pe parcursul derulării exercițiului bugetar, compartimentul achiziții actualizează Programul anual al achizițiilor publice în concordanță cu modificările de buget și cu nevoile apărute.

De asemenea, compartimentul achiziții ține lunar evidența realizării PAAP pe baza achizițiilor efectuate.

Pentru a asigura transparența, autoritățile contractante au obligația de a permite accesul persoanelor interesate la informațiile cuprinse în dosarul achiziției publice, după finalizarea procedurii de atribuire, cu respectarea prevederilor legale referitoare la liberul acces la informațiile de interes public. În acest sens, dispozițiile art. 215 din O.U.G. nr. 34/2006 prevăd că dosarul achiziției publice are caracter de *document public*, în forma în care se află la momentul solicitării accesului la informațiile din cuprinsul acestuia. Accesul persoanelor la aceste informații se realizează cu respectarea termenelor și procedurilor prevăzute de reglementările legale privind liberul acces la informațiile de interes public și nu poate fi restricționat decât în măsura în care aceste informații sunt confidențiale, clasificate sau protejate de un drept de proprietate intelectuală, potrivit legii. Se poate observa că legiuitorul instituie o excepție de la caracterul public al documentelor ce fac parte din dosarul achiziției publice, respectiv situația în care aceste informații sunt confidențiale, clasificate sau protejate de un drept de proprietate intelectuală, potrivit legii.

Definită ca fiind un principiu fundamental în procesul achizițiilor publice, *transparența* constituie un veritabil instrument de control, o garanție a utilizării eficiente și legale a resurselor financiare ale autorităților contractante, reprezentând o condiție esențială pentru integritate și prevenirea corupției în domeniul achizițiilor publice. Aplicarea principiului transparenței vine

în sprijinul consolidării procesului de achiziție publică, asigurând credibilizarea publică a acestui proces. La nivelul legislației naționale în materia achizițiilor publice, *principiul transparenței* este reglementat prin dispozițiile art. 2 lit. d) din Ordonanța de urgență a Guvernului nr. 34/2006, cu modificările și completările ulterioare și reprezintă, în esență, aducerea la cunoștința celor interesați a tuturor informațiilor referitoare la aplicarea procedurilor de atribuire a contractelor de achiziție publică.

În acest sens, la nivelul legislației naționale, există o serie de dispoziții care reglementează protecția anumitor informații cuprinse la nivelul ofertelor, în măsura în care divulgarea unor asemenea informații ar prejudicia interesele operatorilor economici.

În lipsa stabilirii la nivel legislativ a unor repere obiective pentru delimitarea informațiilor confidențiale, se pune problema de a stabili în ce măsură o astfel de măsură legislativă vine în contradicție cu dispozițiile *Legii nr. 544/2011 privind liberul acces la informațiile de interes public*, care prevăd că accesul liber și neîngrădit al persoanei la orice informații de interes public, constituie unul dintre principiile fundamentale ale relațiilor dintre persoane și autoritățile publice, în conformitate cu Constituția României și cu documentele internaționale ratificate de Parlamentul României.

Concluzii:

- În urma analizei prezentate, apreciez că o corectă fundamentare și o derulare ritmică a PAAP conduce la determinări pozitive importante asupra misiunii unității, aceea de formare a luptătorului și inițiere a specialistului în domeniul CIS.

- PAAP se poate constitui într-un instrument modern de utilizare eficientă a două dintre resursele fundamentale care determină procesul de instrucție – financiară și materială, cu aplicații directe asupra eficienței procesului instructiv-educativ.

Bibliografie:

- Ordonanța de Urgență a Guvernului nr. 34/2006 privind atribuirea contractelor de achiziție publică.

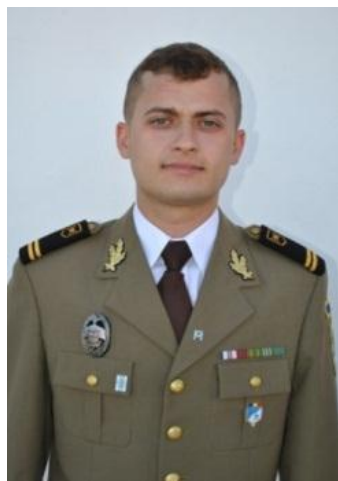
- Ordinul ministrului apărării nr. M-141/2002 privind achizițiile publice și nr. M-25/2003 privind Normele metodologice de întocmire, avizare și aprobare a PAAP.

- Legea nr. 544/2011 privind liberul acces la informațiile de interes public.

STILURILE DE LEADERSHIP UTILIZATE DE CĂTRE COMANDANTUL DE PLUTON ÎN INSTRUIREA SOLDAȚILOR PROFESIONIȘTI ȘI EFICIENȚA ACESTORA

Locotenent Răducu OPREA

Batalionul Instrucție Comunicații și Informatică „Frații Buzești”



Activitatea militarului, în special a celui specializat în arma comunicații și informatică, constituie un proces continuu de învățare, de adaptare, de competiție și de selecție. În contextul actual, al modernizării armatelor lumii, în urma creșterii rapide a concurenței fără

precedent, rolul liderilor devine tot mai important. Astfel, liderii își câștigă sprijinul subordonaților și simpatia acestora prin calitățile pe care le posedă și le utilizează în relațiile cu cei din jur.

În cadrul *Batalionului Instrucție Comunicații și Informatică „Frații Buzești”* din garnizoana Craiova, unde instruirea militarilor are loc într-un flux continuu, cunoașterea problematicei legate de leadership de către persoanele cu funcții de conducere constituie un fundament important în formarea soldaților și gradaților profesioniști, atât în instruirea individuală, cât și în instruirea de specialitate, pentru pregătirea specialiștilor în arma comunicații și informatică.

Liderii trebuie, în cele din urmă, să asigure un *cadru organizațional adecvat* pentru ca subordonații să-și manifeste abilitățile și inițiativa, să-și valorifice cunoștințele la cele mai înalte standarde, în special când vorbim despre unitățile de instrucție unde comandanții de grupe/plutoane sunt încadrați pe funcții de instructori, fără a fi nevoie de o mulțime de supervizori sau de a construi sisteme de control rigide sau sofisticate.

În teorie, *leadershipul reprezintă procesul prin care o persoană, un lider, determină, prin utilizarea relațiilor interpersonale, una sau mai multe persoane să acționeze în vederea realizării unor obiective bine stabilite, pe baza unei viziuni puternice și atractive.*

Una dintre *provocările majore* cu care se confruntă un lider, o persoană cu o poziție cheie în cadrul unei subunități, este aceea de a crea și menține o cultură organizațională care să fie în concordanță cu obiectivele subunității și natura activităților desfășurate în cadrul acesteia.

În urma experienței dobândite în funcția de comandant de pluton (și instructor), în cadrul *Batalionului Instrucție Comunicații și Informatică „Frații Buzești”* și în urma aplicării diferitelor stiluri de leadership în cadrul subunității, am concluzionat că stilurile de leadership pot fi utilizate în paralel și procentual astfel: 28% *leadershipul tranzacțional*, 24 % *leadershipul cultural*, 22% *leadershipul autoritar*, 18% *leadershipul charismatic*, 5% *leadershipul transformațional* și 3% *leadershipul „laissez-faire”*. Aceste procente sunt materializate și în diagrama de mai jos:



1. Leadershipul charismatic

Acest stil de leadership este întâlnit la persoanele care au charismă, care au un talent nativ de a-i influența într-o manieră profundă pe cei din jur prin acțiunile pe care le fac și prin convingerile pe care le au. Liderii charismatici au avut realizări mari încă de la vârste fragede și evoluția lor confirmă calitățile pe care le-au moștenit de la generațiile anterioare.

În cazul în care calitățile native ale liderului sunt șlefuite prin diferite experiențe personale și prin educație, acesta devine o personalitate marcantă a subunității în cadrul căreia își desfășoară activitatea.

Un leader charismatic este caracterizat prin încredere foarte mare în propriile resurse și în propriile valori, dar și în abilitatea acestuia de a obține tot ceea ce își dorește, având următoarele calități: *capacitatea de a crea o viziune, capacitatea de a energiza și capacitatea de a dezvolta și utiliza potențialul susținătorilor săi.*

De altfel, mult timp s-a considerat că poți fi un lider adevărat doar în măsura în care te naști cu un anumit talent, așa cum nu poți fi un pictor sau un artist strălucit dacă nu ai un talent înnăscut.

În cazul nostru, leadershipul charismatic poate fi folosit de către instructorii care au charismă și astfel le este foarte ușor să lucreze cu soldații profesioniști pentru a-i instrui cât mai lesne cu putință și a le forma comportamentul și obiectivele de performanță dorite.

Folosind exemplul personal, liderul charismatic își poate influența subordonații să-și propună obiective mult mai înalte pe care să le atingă față de cele stabilite anterior, aceștia considerând că vor avea un ajutor și un sprijin în plus din partea comandantului de pluton.

2. Leadershipul autoritar

Leadershipul autoritar, cunoscut și sub denumirea de leadership instituțional, valorizează foarte puternic sistemul și inteligența sistematică a procedurilor și politicilor bine stabilite. Liderul autoritar se bazează pe avantajul competitiv pe care i-l oferă funcția și pe siguranța pe care i-o oferă sistemul organizațional.

Dacă acest tip de leadership este dus la extrem, poate genera o formă birocratică de funcționare, dar face lucrurile să se întâmple. Atunci când acesta este convins de un anumit lucru, toată subunitatea va fi antrenată în direcția deciziei luate, iar acest lucru poate fi extrem de favorabil în cazul schimbării.

În cazul acestui stil de conducere, cultura organizațională propulsează opinia liderului ca fiind cea mai bună. Chiar dacă pare o formă tiranică de conducere, funcționarea cu succes a unei subunități conduse de un lider autoritar depinde foarte mult de valorile și personalitatea acestuia. Un lider autoritar poate fi un adevărat model, respectat și apreciat de către oamenii pe care acesta îi are în subordine.

Folosirea leadershipului autoritar în cadrul instruirii soldaților profesioniști poate fi o variantă de succes, dar liderul trebuie să fie atent și să știe când să elimine tensiunile create în urma acestui

stil de conducere pentru a nu ajunge la o extremă care să îi creeze antipatia subordonaților.

În urma transmiterii convingerilor personale soldaților profesioniști, aceștia văd în comandantul de pluton o autoritate importantă în cadrul subunității care trebuie urmată pentru a atinge cele mai înalte standarde profesionale.

3. Leadershipul tranzacțional

Leadershipul tranzacțional se bazează pe capacitatea liderului de a negocia cu subordonații săi pentru a obține implicarea acestora și pentru a-i atrage de partea sa. Acesta promite o serie de recompense în schimbul adoptării anumitor decizii și comportamente.

Pentru a direcționa energia subordonaților săi, liderul trebuie să-și dezvolte în permanență abilitățile de negociere și să fie empatic cu ei, astfel încât să reușească să înțeleagă pe deplin factorii ce-i motivează pe aceștia.

Dacă liderul promite anumite recompense în schimbul anumitor comportamente, decizii, performanțe care îi sunt satisfăcute, dar acesta nu reușește să ofere într-un timp rezonabil recompensele promise subordonaților, acest lucru va conduce la pierderea credibilității acestuia în fața lor.

Acest stil de leadership este foarte ușor de pus în aplicare în contextul în care soldații vor trebui să obțină rezultate cât mai bune pentru a beneficia de cât mai multe învoiri și permisiile, cea mai mare recompensă pentru aceștia constituind-o zilele în plus la permisie.

De asemenea, în cazul nostru, leadershipul tranzacțional nu poate fi folosit independent, fiind necesară îmbinarea acestuia cu unul sau mai multe stiluri de conducere.

4. Leadershipul transformațional

Acest tip de leadership caracterizează liderii care reușesc să perceapă nevoia de schimbare în cadrul subunității, să conducă și să proiecteze în mod eficace schimbări organizaționale majore.

Pentru a reuși acest lucru, este nevoie de o serie de calități și de un set de abilități care să-i ofere unei persoane capacitatea de a lucra într-un mediu turbulent, de a fi deschisă provocărilor venite din mediul intern, cât și din mediul extern.

Liderii care adoptă acest stil de leadership reușesc, asemenea liderilor charismatici, să creeze o viziune atractivă și să-și inspire subordonații în

deciziile și comportamentele lor. Leadership-ul transformațional este considerat ca fiind opusul leadershipului clasic, care se manifestă în perioade de relativă stabilitate, cu schimbări rare și, în general, previzibile, ce oferă un timp suficient de mare pentru pregătire și reacție.

În cadrul instruirii soldaților profesioniști, acest tip de leadership este folosit într-o măsură foarte scăzută sau chiar deloc deoarece nu apar schimbări pe parcursul etapelor de instruire.

Schimbările apărute în programele de instruire anuale sunt luate la cunoștință de către instructorii din cadrul subunității în perioada cuprinsă între seriile de instrucție, perioadă în care aceștia execută instrucția conform noilor precizări și, astfel, aici putem discuta despre leadershipul transformațional.

5. Leadershipul de tip „laissez-faire”

Leadership-ul de tipul „laissez-faire” este specific liderilor care preferă să creeze un cadru general de referință, să construiască o viziune și să stabilească obiective, după care să lase susținătorilor săi deplină libertate asupra modalităților de realizare a acestora.

În cazul acesta, liderul se implică doar la partea de concepție, la partea macro și nu intervine la nivel micro, în zona operațională. Subordonații liderului își definesc și împart rolurile, își stabilesc propria strategie, adoptă decizii și acționează, fără ca în aceste decizii să intervină liderul lor.

De asemenea, la fel ca în cazul leadershipului transformațional, leadershipul de tip „laissez-faire” nu poate fi utilizat în instruirea de bază a soldaților profesioniști deoarece aceștia ating în permanență noi obiective, conform modelului luptătorului, și nu sunt capabili încă să-și stabilească propria strategie de acțiune în diverse situații.

6. Leadershipul cultural

În ceea ce privește leadershipul cultural, un element important ce trebuie avut în vedere este acela al unicității culturii. Fiecare cultură organizațională, reprezintă o *construcție socială cu propria identitate*, asemănătoare indivizilor. În cadrul acestora, subordonații desfășoară o serie de activități, comunică și interacționează pentru atingerea obiectivelor de performanță stabilite în fișa postului.

Prin leadership cultural înțelegem *capacitatea unei persoane de a influența și a motiva alte persoane, de a crea o viziune atractivă, de a se implica major, rațional, emoțional și fizic în stabilirea și realizarea unor obiective, prin luarea în considerare la un nivel înalt a atitudinilor, simbolurilor, normelor și valorilor de comportament specifice unor indivizi sau grupuri de persoane.*

Rolul liderului nu este unul ușor, deoarece el trebuie să creeze mai întâi o viziune bazată pe un set de valori proprii, care să țină seama de elementele culturale organizaționale și să fie acceptate de către subordonați.

Principala diferență a leadershipului cultural față de leadershipul clasic o reprezintă *accentuarea elementelor culturale*, atât din punct de vedere al liderului în construirea viziunii organizaționale, cât și din punct de vedere al așteptărilor subordonaților acestuia.

Din punct de vedere al leadershipului cultural, liderul poate influența dorința acumulării de noi cunoștințe a soldaților profesioniști atât prin profesionalismul de care acesta dă dovadă, cât și prin modul în care le transmite acestora cunoștințele pe care le deține.

Prin cultura organizațională pe care liderul o creează în cadrul subunității, acesta își poate motiva subordonații prin crearea unui climat competițional foarte strâns între aceștia.

Odată stabilite obiectivele de performanță de către comandantul de pluton, prin nevoia de cunoaștere, soldații profesioniști prezintă un interes major în ceea ce privește pregătirea personală, deoarece, în arma comunicații și informatică, nevoia de cunoaștere este alimentată continuu datorită evoluției într-un ritm foarte rapid a tehnologiei.

Concluzii

În concluzie, ar trebui să vorbim despre un stil de leadership implementat cu strictete care este unic în conducerea liderului. În mod ideal, un lider ar trebui să-și configureze stilul de conducere în funcție de circumstanțe. În realitate, lucrurile nu se întâmplă așa, deoarece foarte mulți lideri rămân cantonați într-un anumit stil de conducere, indiferent de situație. Flexibilitatea stilului de conducere este o calitate a unui lider de succes.

Cunoașterea stilurilor de leadership, din diferite perspective este extrem de necesară pentru un lider. În primul rând îi permite să-și înțeleagă punctele slabe și punctele forte, iar în al doilea

rând, aceasta îi permite înțelegerea comportamentului subordonaților.

Deși este greu ca un stil de leadership să atingă perfecțiunea, poate tinde spre cristalizarea unui asemenea stil. Cu cât ponderea unor efecte pozitive ale unui stil de leadership este mai mare, cu cât practicarea lui îndelungată se asociază cu mai multe efecte pozitive, cu cât el este adaptat și corespunzător nu numai din grup, ci și celor social-istorice, cu atât stilul respectiv va fi mai eficient.

Concluzionăm, astfel, că, pentru instruirea soldaților profesioniști, se pot folosi patru stiluri importante de leadership: *leadershipul tranzacțional*, care de altfel și predomină, *leadershipul charismatic*, *leadershipul autoritar* și *leadershipul cultural*.

Ideal pentru comandantul de pluton în conducerea subunității ar fi îmbinarea acestor patru stiluri de leadership, în funcție de calitățile subordonaților, de experiența dobândită în leadership, de expertiză, precum și de trăsăturile de personalitate și comportament.

NOTE BIBLIOGRAFICE:

1. Avolio Bruce J., „*Full leadership management*”, Editura Sage Publications Wiley And Sons Ltd, Washington, 2010.
2. Năstase Marian, Revista „*Economia. Seria management*”, Anul X, Nr. 1, Editura ASE, București, 2007.
3. Năstase Marian, Revista „*Economia. Seria management*”, Anul IX, Nr. 2, Editura ASE, București, 2006
4. Năstase Marian, „*Cultura organizațională și managerială*”, Editura ASE, București, 2004.
5. Nicolescu O., Verboncu I., „*Fundamentele managementului organizației*”, Editura Economică, București, 2001.
6. Petrovici Virgil, „*Stiluri de conducere și eficiența managementului*”, Editura Economică, București, 2001.
7. Schein Edgar H., „*Organizational culture and leadership*”, Editura John Wiley and Sons Ltd, San Francisco, 2010.
8. Zlate Mielu, „*Leadership și management*”, Editura Polirom, Iași, 2004.

RADIAȚIILE ELECTROMAGNETICE ȘI EFECTUL LOR ASUPRA SĂNĂȚĂII POPULAȚIEI Un pericol pentru sănătate?

Locotenent-colonel Dinu BUTALIU

Batalionul Instrucție Comunicații și Informatică „Frații Buzești”



Preocuparea constantă pentru îmbunătățirea calității vieții și pentru utilizarea unor tehnologii industriale performante a determinat, la sfârșitul secolului XX, explozia numărului de surse de radiații electromagnetice, concomitent cu creșterea interesului populației și al specialiștilor pentru evaluarea riscurilor pentru sănătate. În acest context, este lesne de înțeles preocuparea atât a cercetătorilor, cât și a populației cu privire la identificarea și evaluarea riscurilor pentru sănătate.

DEFINIȚIE

Radiațiile electromagnetice sunt, în esența lor, un flux variabil de linii invizibile de forțe de natură electrică și magnetică, ce se propagă simultan în spațiu și în timp cu viteza de trei sute mii k/s.

EPECTELE RADIAȚIILOR

Experiențele cercetătorului american Georges Lakhovsky au demonstrat că cromozomii din nucleul fiecărei celule vii au forma unui filament tubular alcătuit dintr-o materie dielectrică umplută cu o substanță conductivă și că un cromozom poate fi comparat cu un circuit oscilant echipat cu inductanță, rezistență și capacitate electrică. Cu alte cuvinte, celulele corpului uman sunt de fapt rezonatoare (circuite oscilante), capabile să vibreze electric la cele mai fine influențe electromagnetice, cosmice, atmosferice, telurice. În epoca noastră însă, pe lângă aceste unde naturale, există o multitudine de radiații electromagnetice, care influențează și ele celulele, perturbând buna funcționare a corpului uman. Pornind de la cele mai banale radiații cu care suntem atât de obișnuiți încât nici nu le mai

considerăm nocive pentru noi (de la radiațiile rețelelor electrice de 50 Hz și până la frecvențe foarte înalte în gama microundelor), toate interferează cu câmpul vital uman și perturbă activitatea celulelor vii.

Suntem atât de obișnuiți, de exemplu, cu rețeaua de curent electric, avem fire prin toți pereții caselor, încât pare greu de crezut că acestea ar putea avea de fapt și efecte negative asupra sănătății noastre și asupra stării noastre psihice. Experiențe realizate însă în Laboratorul Marinei din Pensacola au demonstrat clar că la radiații magnetice de 1 Gauss (un câmp foarte slab) și frecvențe cuprinse între 45-60 Hz, memoria ființei umane scade semnificativ. Memoria nu este doar capacitatea unei persoane de a-și aminti și a reproduce un text, ci, într-un sens mult mai profund, memoria este alcătuită din straturile cele mai profunde ale ființei umane și ea este responsabilă inclusiv de starea de sănătate fizică și psihică.

În Elveția, s-a făcut un experiment sugestiv legat de influența nocivă a radiațiilor electromagnetice asupra organismului uman. Au fost luați pacienți suferind de diverse maladii, în special dezechilibrări ale anumitor ritmuri, și au fost ținuți timp de câteva săptămâni într-o zonă montană, la o cabană lipsită complet de curent electric. Lipsa radiațiilor electrice a făcut ca, în timp de doar două săptămâni, toți pacienții să-și revină complet. Rezultatele s-au menținut stabile chiar și doi ani după experiment.

Cercetările nocivității radiațiilor electromagnetice de foarte înaltă frecvență au demonstrat că acestea generează o hiperactivitate, îmbătrânire, stres și perturbă ciclurile de somn.

Alți cercetători, precum J.J. Noval, au concluzionat că radiațiile electromagnetice de foarte înaltă frecvență blochează producerea neurotransmițătorilor și generează o epuizare la nivelul cortexului și a sistemului imunitar.

Medicul american Beeker a realizat studii aprofundate și a concluzionat că multitudinea câmpurilor electromagnetice artificiale care se întâlnesc într-un oraș modern (emițătoare radio și

TV, linii de înaltă tensiune, radiațiile aparatelor menajere, cuptoare cu microunde, aparate TV, calculatoare etc.), generează un fel de zgomot electronic care afectează memoria, degradează sistemul imunitar și provoacă maladii, cum ar fi cancerul, sau diverse tulburări mentale și comportamentale, de exemplu depresia. Conform studiilor lui Beeker, victimele sinuciderilor trăiesc în majoritatea cazurilor într-un mediu electromagnetic cu 22% mai intens decât alte persoane. De asemenea, expunerea la câmpuri electromagnetice puternice anihilează producerea norepinefrinei (neurotransmițător), ceea ce favorizează apariția depresiei. Numărul de accidente este cu 40% mai mare în zonele supuse unor câmpuri electromagnetice intense.

Influența radiațiilor liniilor electrice asupra comportamentului și funcționării organismului este atât de puternică, încât atunci când s-a realizat un test în care li s-a cerut subiecților să aleagă o notă muzicală la alegere, peste 95% dintre europeni au ales nota SOL diez, (aproximativ 50 Hz – frecvența liniilor electrice europene) și majoritatea americanilor au ales un SI (care era foarte aproape de frecvența rețelei americane de 60 Hz).

Organizația Mondială a Sănătății (OMS) a actualizat simptomele provocate de electromagnetism. Această listă cuprinde și durerile de cap, starea de iritabilitate și chiar agresivitatea. Tot aici găsim dereglările menstruale, nașterea prematură, avortul sau unele malformații ale fetoșilor. Lista menționează și scăderea apetitului sexual, insomnia și reducerea vitalității, dar include și problemele cardiovasculare și riscul ridicat al apariției leucemiei.

REZULTATUL CERCETĂRILOR:

- riscul îmbolnăvirii de leucemie acută, care se termină cu deces, a persoanelor care lucrează în domeniul electronic, se mărește de 2,6 ori;

- posibilitatea ca oamenii care sunt expuși radiațiilor electromagnetice neionizante de a se îmbolnăvi de cancerul măduvei osoase și leucemie este 7 ori mai mare, iar posibilitatea de a se îmbolnăvi de tumora glandei tiroide, crește de 4 ori. În jur de 10 – 15 % din copiii care se îmbolnăvesc de cancer au fost expuși razelor electromagnetice emise de aparatele de uz casnic. Copiii care trăiesc în apropierea transmițătorilor de înaltă tensiune sunt expuși bolilor cu 5 % mai mult, în comparație cu cei care nu se află în aceste

zone. Un număr însemnat de nașteri premature au drept cauză razele emise din plăpumile electrice și paturile cu apă, încălzite electric, pe timp de iarnă. Câmpul electromagnetic de 45Hz, cu capacitatea de 100 mT, stârnește formarea rapidă a trigliceridelor, iar drept consecință apar probleme cardiace. 100% dintre femeile al căror serviciu se desfășoară în fața aparatelor tv și a monitoarelor nasc înainte de termen, în comparație cu femeile care n-au lucrat niciodată la astfel de locuri de muncă. În acest scop, a fost cercetată o grupă de 1593 de femei. Depresia clinică și crimele, la fel, apar drept consecințe ale expunerii la radiații.

- la muncitorii expuși la câmp electromagnetic ce nu depășea valorile maxime admisibile legal s-a demonstrat că a fost afectat atât sistemul nervos central, cât și cel cardiovascular, lucru demonstrat de indicii hematologici și biochimici modificați. Reacțiile adverse includ dureri de cap, dureri cardiace, insomnie, stare de oboseală avansată și iritabilitate, pierderi de memorie – ca tulburări principale. Tulburările funcționale ale sistemului nervos s-au manifestat ca disfuncții vegetative, sindrom de astenie vegetativă și neurastenii. Printre tulburările sistemului cardiovascular s-au numărat distonia neurocirculatorie, hipertensiunea, presiunea arterială scăzută.

- la operatorii care lucrau cu echipamente de transmisie s-au constatat niveluri scăzute de testosteron în serul sangvin. În cazul unei expuneri la câmpuri electromagnetice mai mare de 10 ani apare scăderea funcției testiculare. Operatorii echipamentelor de transmisie radio s-au plâns de dureri de cap, dureri cardiace, tulburări de somn, dureri epigastrice și oboseală sporită semnificativ mai mult decât muncitorii din alte grupuri. Rata tulburărilor somatice apărute în acest grup a fost semnificativ mai mare față de cea a grupului de control (77,8% în comparație cu 28,9%). Nivelul patologic pentru sistemul nervos central și cel cardiovascular al persoanelor expuse la câmpuri electromagnetice sau care au fost expuse în trecut este semnificativ mai ridicat decât la grupurile de control. Schimbările stării de sănătate induse de expunerea la câmpuri electromagnetice persistă. Procentul de perturbări funcționale ale sistemului nervos central la muncitori cu durate de activitate mai mici de 20 de ani a fost practic la fel cu cel al muncitorilor cu 10-20 de ani de activitate. Incidența perturbărilor funcționale ale sistemului nervos central scade la grupul cu perioada de activitate mai mare de 20 de

ani, dar aici se înregistrează ateroscleroza cerebrală. Procentul total al subiecților cu manifestări patologice ale sistemului nervos central este cel mai ridicat la ultimul grup. Manifestările patologice ale sistemului cardiovascular observate la muncitorii expusi la radiație de înaltă frecvență au fost distonie vasculară vegetativă, hipertonie, arteroscleroză și miocardită. Cu alte cuvinte, iradierea la înaltă frecvență a contribuit în mod semnificativ la dezvoltarea afecțiunilor cardiace.

Frecvențele joase și tipurile de modulare au ca influență diferite anomalii care apar la oameni. Deseori, sunt afectate creierul și sistemul de reproducere. În general, tabloul clinic al expunerii la câmpuri electromagnetice indică îmbatrânir eprematură.

În final, au fost menționate câteva informații specifice despre efectele metabolice ale radiației câmpurilor electromagnetice în rândul populației studiate; 76 % din grupul expus a avut un nivel al lipoproteinei ce depășea în mod semnificativ standardele în comparație cu 36,4 % din grupul de control. La grupul expus a existat o

tendință de creștere a concentrației totale de lipide în sânge. Modificarea metabolismului carbohidraților a demonstrat statistic, la grupul expus, creșteri semnificative ale nivelului de acid lactic (23 % creștere), acid piruvic (17% creștere) și concentrației de glucoză (21 %), creștere în comparație cu grupul de control. Patru subiecți cu niveluri ale glucozei ce depășesc standardele fiziologice aparțineau, de asemenea, grupului expus.

În concluzie, efectul câmpurilor electromagnetice asupra oamenilor se manifestă la:

- sistemul nervos, ducând în timp la scleroza cerebrală;
- sistemul neuro-vegetativ, producând dezechilibre;
- sistemul cardiovascular, cauzând boli de inimă și arteroscleroză;
- sistemul reproducător, cu descreșterea nivelului de testosteron și creșterea celui de FSH;
- tulburări gastrointestinale etc.

INIȚIATIVA FORȚE INTER-CONECTATE

*Locotenent-colonel dr. Gheorghe-Adrian GÎRTONEA
Baza 191 Logistică pentru Comunicații și Informatică*



În prezent, în domeniul militar se vehiculează din ce în ce mai des concepte precum capabilitate, dezvoltarea de capabilități, punerea în comun și lucrul în mediu întrunit și multinațional a acestora.

Dar ce înseamnă, de fapt, o capabilitate?

Conform prevederilor Cartei Albe a Apărării, elaborată de Ministerul Apărării Naționale în anul 2013, „*Capabilitatea reprezintă abilitatea de a executa acțiuni în scopul îndeplinirii unor obiective. Constituirea unei capabilități are în vedere un complex de măsuri și acțiuni într-o perspectivă largă cuprinzând elemente de doctrină, organizare, pregătire, echipamente, comandă, infrastructură, personal și interoperabilitate*”.[1]

În acest sens, pentru dezvoltarea capabilităților, punerea în comun și lucrul în mediu întrunit și multinațional, în contextul crizei economice și financiare, la nivelul Organizației Tratatului Atlanticului de Nord (North Atlantic Treaty Organization – NATO) și Uniunii Europene (European Union – EU) a fost subliniată oportunitatea dezvoltării unor abordări multinaționale în domeniul apărării, ducând, astfel, la apariția unor noi concepte, precum;

- Apărare Inteligentă (Smart Defence – SD) și Inițiativa Forțe Inter-Conectate (Connected Forces Initiative – CFI) – concepte NATO;

- dezvoltarea și utilizarea în comun a capabilităților europene de apărare (Pooling & Sharing – P&S) – concept la nivelul EU.

Deși diferite ca denumire, cele două concepte, SD și P&S, presupun, în linii mari, același lucru – comasarea și utilizarea capabilităților în mod comun, având scopul de a face ca investițiile în securitate și apărare să fie mai eficiente [2], gestionarea resurselor presupunând adoptarea de soluții inovatoare, precum prioritizarea investițiilor și finanțarea

multinațională a capabilităților de interes comun. Toate acestea au ca obiect creșterea securității statelor membre, limitarea efectelor unei subfinanțări a sectorului de apărare [1] bazându-se pe cooperarea multinațională și intersectorială între domeniul militar și industria de apărare.[3]

Menționez că, în cadrul articolului, am ales această introducere considerând că nu se poate vorbi de conceptul CFI fără a aminti și prezenta pe scurt rolul conceptului SD, concepte agreate la Summit-ul NATO de la Chicago, din luna mai 2012.

Importanța SD privind modul de realizare în comun a capabilităților la nivelul NATO, precum și nevoia de interoperabilitate⁵ a acestora pentru a putea lucra împreună la nivelul Alianței, aspect ce presupune înțelegere comună, aranjamente de comandă și control (Command and Control – C2) comune, standarde comune, limbaj comun, doctrine și proceduri comune, a fost subliniată de Secretarul General al NATO, dl. Anders Fogh Rasmussen, pe timpul desfășurării Conferinței de Securitate de la Munchen, din 2012.[4]

Interoperabilitatea nu necesită neapărat echipamente militare comune. Este important ca echipamentele să poată partaja facilități comune și să fie capabile să interacționeze, să se conecteze și să comunice, să facă schimb de date și servicii cu alte echipamente.[5]

Prin dimensiunile sale tehnice (hardware, echipamente, armamente și sisteme), procedurale (doctrine și proceduri) și umane (terminologie și instruire), completate de informații, ca un element transversal critic, interoperabilitatea sprijină implementarea unor astfel de inițiative NATO reunite, cum ar fi SD și CFI.

Soluțiile necesare pentru obținerea interoperabilității pot fi atinse numai printr-o angajare eficientă a standardizării, instruirii,

⁵ Conform prevederilor Cartei Albe a Apărării din 2013, „*Interoperabilitatea reprezintă capacitatea forțelor (întrunite, multinaționale) de a acționa împreună, într-un mod coerent, eficace și eficient, pentru îndeplinirea unor obiective comune de nivel tactic, operativ sau strategic*”.

exercițiilor, lecțiilor învățate, demonstrațiilor, testelor și încercărilor.

În acest sens, pentru ca aceste capacități să poată lucra împreună, la conferința lunară de presă din data de 05 martie 2012, Secretarul General al NATO a precizat motivul pentru care a fost lansat conceptul CFI, concept ce pune accent pe:[4]

- instruire și educație;
- exerciții;
- utilizarea mai eficientă a tehnologiilor.

Ulterior, la Summit-ul de la Chicago din 20 mai 2012, liderii aliați au stabilit obiectivul „Forțele NATO 2020”, avându-se în vedere realizarea unui pachet de forțe dislocabile, interoperabile și bine echipate, instruite și comandate, astfel încât să îndeplinească nivelul de ambiție al NATO de a putea opera împreună în cadrul Alianței și cu partenerii în orice mediu. În acest context, CFI este esențială pentru a asigura că Alianța rămâne bine pregătită pentru a-și asuma întreaga gamă de misiuni, precum și pentru a răspunde viitoarelor provocări, oriunde ar putea să apără acestea, iar implementarea conceptului CFI este unul din principalele mijloace pentru asigurarea Forțelor NATO 2020.[6]

Elementele componente ale CFI sunt:[7]

- Forța de Răspuns a NATO (NATO Response Forces – NRF);
- Educația și instruirea;
- Exercițiile;
- Tehnologiile;
- Forțele de Operații Speciale (Special Operations Forces – SOF).

În ceea ce privește educația și instruirea, principalele trei scopuri ale NATO sunt:

- creșterea eficienței forțelor multinaționale conduse de NATO și a abilității acestora de a opera împreună;
- sprijinul acordat țărilor partenere în eforturile lor de reformă;
- ajutorul în construirea păcii și stabilității în zonele afectate de criză.

Referitor la exerciții, acestea sunt instrumente importante ale Alianței pentru testarea și validarea conceptelor, procedurilor, sistemelor și tacticilor. Mai pe larg, ele permit organizațiilor militare și civile dislocate în teatrele de operații să se antreneze în lucrul împreună. Exercițiile au multe alte funcții, nu doar de a identifica „cele mai bune practici” (ce funcționează) și „lecțiile învățate” (ce trebuie îmbunătățit).

De asemenea, privitor la tehnologii, o mai bună utilizare a acestora va ajuta Alianții și forțele partenere să lucreze împreună, acest lucru contribuind la asigurarea interoperabilității și conectivității între sistemele și echipamentele proprii.

Totodată, tehnologiile și capacitățile moderne sprijină instruirea, educația, exercițiile, dislocarea și susținerea forțelor.

Conform Declarației Summit-ului din Țara Galilor adoptată de șefii de stat și de guvern participanți la reuniunea Consiliului Nord Atlantic din Țara Galilor din perioada 4 - 5 septembrie 2014, obiectivul NATO de a realiza Forțele NATO 2020 (moderne, forțe strâns conectate, echipate, pregătite, instruite și comandate astfel încât să fie în măsură să îndeplinească Nivelul de Ambiție NATO și în acest mod să poată opera împreună și cu partenerii în orice mediu) a rămas valid și s-a reafirmat angajamentul de a fi îndeplinit, menționându-se că Planul de Acțiune al Alianței (Readiness Action Plan - RAP) pentru creșterea nivelului de reacție completează și întărește Forțele NATO 2020, prin îmbunătățirea gradului de pregătire și reacție, în ansamblu.[8]

De asemenea, potrivit aceleiași Declarații, „*Vom stabili un program intensificat de exerciții, cu o atenție sporită pentru exercițiile de apărare colectivă, inclusiv exersarea răspunsurilor cuprinzătoare la scenarii complexe de tip civil-militar. CFI, pe care am agreat-o la Chicago, va fi utilă pentru atingerea coerenței depline a elementelor de instruire și de exerciții ale Planului de Acțiune al Alianței pentru creșterea nivelului de reacție*”, menționându-se faptul că CFI ia în considerare întreaga paletă de misiuni, inclusiv cele mai solicitante, demonstrând astfel coeziunea constantă și determinarea Alianței, inițiativa fiind caracterizată de următoarele elemente:

- furnizează structura necesară ca alianții să se pregătească și să exerseze într-o manieră coerentă;
- întărește întreaga paletă a instruirii multinaționale și întrunite;
- promovează interoperabilitatea, inclusiv cu partenerii;
- fructifică progresele în domeniul tehnologiei, cum ar fi asigurarea unui mediu federalizat de rețea pentru misiune (Federated Mission Network – FMN) care va spori schimbul de informații în cadrul Alianței și cu partenerii, în sprijinul pregătirii exercițiilor și operațiilor.

Dintr-un volum mare de activități pe care CFI le cuprinde, NATO a aprobat la Summit-ul din Țara Galilor, următoarele șase pachete cheie ale inițiativei:[6]

a) *Politica NATO actualizată pentru învățământ, instrucție, exerciții și evaluare (Education, Training, Exercise and Evaluation – ETEE).*

Această politică asigură Comandamentelor Strategice îndrumarea și ghidarea referitoare la ETEE, în vederea aplicării în cadrul NATO. Este un document pe termen lung care prezintă ghidările politice și pune la dispoziție politica necesară între aliați, în vederea desfășurării educației, instruirii, exercițiilor și evaluărilor individuale, a unităților, formațiunilor și comandamentelor din Forța NATO și structurile de comandă.

De asemenea, se adresează procesului de conectare a exercițiilor naționale la exercițiile NATO, furnizând detalii pentru angajarea partenerilor și entităților care nu fac parte din NATO. Ajută prin faptul că acele unități, formațiuni și comandamente pot să ia parte la întreaga gama de misiuni a Alianței și să atingă nivelul de ambiție al NATO.

b) *Un concept de instruire NATO pe termen mai lung: 2015-2020.*

Acest concept caută să operaționalizeze Politica NATO ETEE, punând la dispoziție îndrumarea specifică necesară și alocând responsabilitățile pe aproape toate domeniile indicate de politica menționată.

De asemenea, ajută la promovarea CFI, în special prin sprijinirea NRF, angajarea SOF și sporirea legăturilor și interacțiunilor dintre Structura de Comandă NATO, Structura de Forțe NATO, iar în cazurile în care există avantaje reciproce, și comandamentele naționale.

c) *Exercițiu cu o mare vizibilitate în anul 2015.*

Ca eveniment reprezentativ pentru CFI, exercițiul „Trident Juncture 2015” va fi găzduit de Portugalia, Spania și Italia. Având la bază un scenariu de răspuns la criză, va fi folosit și pentru a certifica capacitatea operațională a NRF 2016.

25.000 de militari vor participa la acest exercițiu, inclusiv din statele partenere, dar se va desfășura și un număr de exerciții naționale conectate la acesta. Exercițiul „Trident Juncture 2015” demonstrează credibilitatea, coeziunea și hotărârea NATO.

d) *Exerciții NATO majore începând din anul 2016.*

Acest program asigură un cadru conceptual pentru determinarea și stabilirea cerințelor pentru exerciții, în vederea atingerii nivelului de ambiție al NATO. Programul sprijină operaționalizarea Politicii NATO ETEE în domeniul de vizibilitate al exercițiilor majore NATO.

e) *Progresul continuu în implementarea aspectelor tehnologice ale CFI.*

Exploatarea tehnologiei în sprijinul interoperabilității este un element cheie al CFI. Asigurarea unui mediu federalizat de rețea pentru misiune (FMN) este piesa de rezistență, iar implementarea lui va permite o interconectare rapidă în cadrul Alianței, dar și cu partenerii, în sprijinul instruirii, exercițiilor și operațiilor, dar și în sprijinul comunicațiilor și activităților zilnice.

f) *Capabilitatea unor comandamente ale Componentei de comandă a operațiilor speciale, aflate sub comanda operațională a SACEUR.*

Aceste comandamente de bază dislocabile au obținut capabilitatea operațională completă în iulie 2014, asigurând o nouă capabilitate pentru comanda și controlul SOF, coordonarea, interoperabilitatea și conectivitatea acestora.

Acest lucru asigură comandantului suprem al Forțelor Aliate din Europa (Supreme Allied Commander Europe – SACEUR) capabilități de comandă a SOF pe timpul exercițiilor și operațiilor, cu elementele de conducere menținute la un nivel foarte ridicat de reacție.

Personal, consider că aceste pachete cheie ale CFI sunt de interes pentru Comandamentul Comunicațiilor și Informaticii, în special în ceea ce privește FMN, ținând cont de preocupările actuale ale comandamentului privind dezvoltarea capabilităților de comunicații și informatică în domeniul rețelelor fixe, rețelelor dislocabile, precum și în domeniul securității informaționale și apărării cibernetice. Realizarea la nivelul unităților militare subordonate Comandamentului Comunicațiilor și Informaticii a unor capabilități/rețele care să poată fi integrate în mediul federalizat de rețea pentru misiune reprezintă plus valoare în posibilitatea participării la exerciții în cadrul CFI, în viitorul apropiat.

Concluzionând, doresc să prezint două aspecte care mi-au atras atenția pe timpul documentării pentru prezentul articol, și anume:

- în cadrul Seminarului „Smart Defence and Defence Investment”, organizat de

Universitatea Națională de Apărare „Carol I”, Academia Oamenilor de Știință din România și Centrul de Analiză și Studii de Securitate la Biblioteca Centrală Universitară „Carol I” în data de 31 octombrie 2012, domnul Patrick Auroy, asistentul Secretarului General al NATO pentru Investiții de Apărare, a subliniat esența conceptului Smart Defence, declarând că „apărare inteligentă nu înseamnă să cheltuim mai mult, ci să cheltuim mai bine”. Domnia sa a enumerat cele trei etape de implementare a apărării inteligente la nivelul statelor aliate: „Prioritizare, cooperare și specializare. Prioritizarea înseamnă felul în care selectăm de comun acord ce anume să tăiem și ce să păstrăm. Cooperarea se referă la ce trebuie să facem împreună pentru a oferi capacități la nivel multinațional, care în mod normal ar fi prea scumpe pentru mulți dintre noi, luați separat. Specializarea înseamnă ca aliații să-și coordoneze mai îndeaproape planurile astfel încât să se poată concentra pe ce poate face fiecare cel mai bine și să contribuie efectiv la capacitățile de care este nevoie pentru a atinge țelurile NATO”;[9]

- Inițiativa Forțe Conectate oferă oportunitatea pentru a asigura că Alianța rămâne agilă și are abilitatea de a se adapta la noul mediu de securitate în anul 2015 și în anii următori [10], reprezentând fundamentul pe care trebuie construită cooperarea militară viitoare.[3]

În încheiere, doresc să evidențiez faptul că, în ceea ce privește achiziția de sisteme/ dezvoltarea de capacități, achiziția/dezvoltarea acestora nu presupune numai costurile inițiale de achiziție, ci și costuri de testare, instruire, operare, mentenanță, transport, depozitare, casare etc., aspecte care trebuie luate în considerare pentru planificarea resurselor umane, materiale și financiare necesare funcționării acestora pe întreg ciclul de viață.

De asemenea, pentru un sistem sau o capacitate realizată, atât în domeniul comunicațiilor și informaticii, cât și în alte domenii, este foarte important să se urmărească cât de des producătorul aduce modificări sau modernizări asupra echipamentelor componente ale sistemului (din punct de vedere hardware și software), astfel încât acestea să poată fi achiziționate și implementate în sistemele deja existente.

BIBLIOGRAFIE ȘI SURSE INTERNET:

[1] ***, *Carta Albă a Apărării*, avizată prin Hotărârea Consiliului Suprem de Apărare a Țării nr. 77 din 17.06.2013, [https://www.semperfidelis.ro/e107_files/public/1384498223_1234_FT37324_carta-alba-apararii .pdf](https://www.semperfidelis.ro/e107_files/public/1384498223_1234_FT37324_carta-alba-apararii.pdf).

[2] Frunzeti T., Zodian V., *Lumea 2013, Enciclopedie politică și militară, Studii strategice și de securitate*, Editura RAO, București, 2013.

[3] Atanasiu M., *Implicațiile participării României la dezvoltarea capacităților în cadrul multinațional organizat de NATO și UE prin inițiativele „Smart Defence” și „Pooling and Sharing” asupra revizuirii Strategiei de transformare a Armatei României*, Centrul de Studii Strategice de Apărare și Securitate, Universitatea Națională de Apărare „Carol I”, București, 2014,

http://cssas.unap.ro/ro/pdf_studii/implicatiile_participarii_Romaniei_la_dezvoltarea_capabilitatilor_in_cadrul_multinational_organizat_de_NATO_si_UE.pdf.

[4] <http://www.natolibguides.info/Smartdefence>

[5] http://www.nato.int/cps/nl/natohq/topics_84112.htm

[6] *Connected Forces Initiative*, http://www.nato.int/cps/en/natolive/topics_98527.htm

[7] *The Connected Forces Initiative Components*, http://www.nato.int/cps/en/SID-DOD702C7-F616F1F6/natolive/topics_105883.htm?selectedLocale=en

[8] ***, *Declarația Summit-ului din Țara Galilor adoptată de șefii de stat și de guvern participanți la reuniunea Consiliului Nord Atlantic din Țara Galilor din perioada 4 - 5 septembrie 2014*, <http://www.mae.ro/node/28465>.

[9] *Seminarul „Smart Defence and Defence Investment”*, Biblioteca Centrală Universitară „Carol I”, 31 octombrie 2012, <http://www.unap.ro/index.php/ro/evenimente?id=187>

[10] Lieutenant General Karlheinz Viereck, German Air Force, Deputy Chief of Staff Joint Force Trainer, *Connected Forces Initiative: Reshaping Priorities*, publicat la data de 29 Martie 2012, <http://www.act.nato.int/article-2013-1-4>

CRIPTOGRAFIE BAZATĂ PE MATEMATICA CURBELOR ELIPTICE

Maior George ZAMĂ

Centrul 346 Comunicații R.M.N.C.



Data de 11 septembrie 2001 a marcat faptul că amenințările la adresa securității, așa cum erau raportate la regulile militare de spațiu și timp, s-au schimbat, în sensul că orice lucru putea deveni o armă care putea depăși orice graniță. Evident, aceasta s-a reflectat și în mediu virtual, unde

tehnologia informațiilor, care la început era un instrument administrativ pentru optimizarea proceselor de birou, a ajuns acum să fie un instrument strategic al industriei, administrației și armatei, definind ceea ce numim spațiul cibernetic. Dar dezvoltarea pe care lumea cibernetică o cunoaște pe zi ce trece presupune și vulnerabilități serioase pentru diferitele societăți, care sunt din ce în ce mai interdependente.

Web-ul răspândit la scară globală, o invenție veche de câteva decenii, a evoluat. Dar la fel au făcut și amenințările. Viermii și virușii s-au transformat din simple mici probleme agasante în serioase provocări de securitate și instrumente perfecte ale spionajului cibernetic. Se pot astfel formula principalele cerințe de securitate pentru sistemele informatice, și anume: stocarea în siguranță a datelor, autentificarea utilizatorului pentru acces, serviciul E-mail, interfața cu alte dispozitive, ștergere date, Data Lost Prevention (DLP), ștergerea datelor la distanță. Una dintre căile de apărare a informațiilor vehiculate în și între sistemele de comunicații și informatică este aproape în mod obligatoriu implementarea mecanismului de criptare a informațiilor. Algoritmii de criptare trebuie să fie puternici, pentru a putea garanta siguranța datelor, utilizându-se atât cei cu chei simetrice, cât și cei cu chei asimetrice.

Unul dintre sistemele de criptare bazat pe chei publice și care se găsește la acest moment în plin proces de dezvoltare și maturizare este cel bazat pe matematica curbilor eliptice (ECC).

Folosirea curbilor eliptice în criptografie a fost propusă pentru prima dată în anul 1985 de către Victor Miller și, independent, de Neal Koblitz. Ideea de bază era folosirea grupului punctelor de pe o curbă eliptică în locul grupului Z_p^* din sistemele criptografice existente. Studiile făcute până acum și publicate în literatura de specialitate arată faptul că sistemele de tip ECC sunt cele mai eficiente din categoria celor cu chei publice. Comparativ cu sistemul criptografic RSA, sistemele ECC permit obținerea unui nivel de securitate echivalent cu folosirea unor chei mai reduse (aproximativ cu un nivel de mărime), ceea ce duce la creșterea performanțelor sistemului prin scurtarea timpilor de execuție și reducerea spațiului de memorare, a benzii de rețea și a puterii consumate. S-a demonstrat faptul că, pentru a obține un anumit nivel de securitate, de exemplu RSA/DSA necesită chei de 1024 biți, pe când în cazul ECC sunt necesari 160 biți. Pe măsură ce nivelul de securitate crește, adică dimensiunea cheilor se mărește, raportul privind dimensiunile cheilor respective și implicit al performanțelor amintite este net în favoarea ECC. Implementările optimizate, software sau hardware ale acestor sisteme au demonstrat faptul că generarea de semnături electronice este cu un ordin de mărime mai rapidă în cazul ECC față de RSA/DSA. Timpii de verificare a semnăturilor sunt însă comparativi ca valoare.

O curbă eliptică E constă din elemente (numite puncte) de tipul (x,y) ce satisfac ecuația:

$$y^2 = x^3 + ax + b \pmod{p},$$

unde a, b fac parte din Z_p astfel încât

$$4a^3 + 27b^2 \neq 0 \pmod{p}, \text{ iar } p \text{ este un număr prim.}$$

Operația de bază în criptografia pe curbe eliptice este cea de multiplicare a unui punct de pe curba eliptică cu un scalar, adică calculul lui $Q = mP$ unde m este un scalar (număr întreg mare), iar P este un punct al curbei. Calculul lui $Q = mP$ este realizat în general printr-o secvență de adunări de două puncte și de dedublări a unui punct, operațiile de bază necesare la nivelul curbei eliptice.

Mai exact, modul de aplicare a ecuației curbei eliptice în criptografie este transpus mai jos pentru sistemul criptografic ElGamal bazat pe aceasta. Vom avea curba eliptică

$E: y^2 = x^3 + a*x + b \pmod{p}$ și punctul $G = (x_1, y_1)$ un punct generator în E .

Utilizatorul A selectează o cheie privată n_A și calculează cheia publică $P_A = n_A * G$.

Utilizatorul B selectează cheia sa privată n_B și calculează cheia publică corespunzătoare $P_B = n_B * G$.

Pentru a cripta un mesaj P_m , utilizatorul A alege aleator un număr întreg pozitiv k . Calculează textul cifrat C_m (format dintr-o pereche de puncte): $C_m = \{kG, P_m + k * P_B\}$.

Pentru a decripta textul cifrat C_m , utilizatorul B calculează:

$$P_m + k * P_B - n_B(kG) = P_m + k(n_B * G) - n_B * (k * G) = P_m.$$

Aplicabilitatea curbelor eliptice în criptografie și relevanța operației de multiplicare a unui punct cu un scalar se bazează pe dificultatea rezolvării problemei logaritmului discret pe curba eliptică, enunțată astfel:

*Fiind dat un punct G pe o curbă eliptică, de ordin r (numărul de puncte de pe o curbă) și un alt punct Y , să se găsească un unic x , $0 \leq x \leq r-1$, astfel încât $Y = x * G$.*

Securitatea criptosistemelor care sunt dezvoltate pe aplicarea curbelor eliptice se bazează pe dificultatea rezolvării problemei logaritmilor discreți pe o curbă eliptică, adică pe determinarea lui x , dându-se G și Y . Din punct de vedere al complexității calculului, se poate face în timp polinomial, însă obținerea lui x când sunt date Y și G implică complexități de calcul mult mai mari. În

aceste condiții, unul din obiectivele principale urmărite în implementările schemelor de tip ECC este acela de a obține metode cât mai optime de calcul pentru $Y = x * G$.

Iată care sunt principalele avantaje ale criptosistemelor bazate pe curbe eliptice:

- Securitate crescută: tăria criptografică per bit este mult mai mare decât a oricărui alt sistem de criptare cu chei publice cunoscut la ora actuală;
- Lărgime de bandă redusă datorită semnăturilor și certificatelor de dimensiune mică;
- Viteză mare de criptare și semnare, atât în implementările software, cât și în cele hardware (transferuri de date sensibile, rețele radio);
- Economii substanțiale față de alte criptosisteme la calcule, lărgimea de bandă și necesitățile de memorare;
- Sunt ideale pentru implementările pe hardware de dimensiuni reduse (cum ar fi cartelele inteligente – smart cards criptografice, dispozitive de calcul mobile – telefoane inteligente, dispozitive wireless).

Bibliografie:

1. <http://www.nato.int/docu/review/2011/11-september/Cyber-Threads/RO/index.htm>
2. <http://webhost.uoradea.ro/cpopescu/cryptograpcr>
3. <http://www.certsig.ro/certsig/files/RST-Etapa1-ADECS.PDF>

MENTENANȚA ECHIPAMENTELOR MILITARE

Maior Silviu SĂPOI

Batalionul Instrucție Comunicații și Informatică,,Frații Buzești”



Mentenanța cuprinde totalitatea acțiunilor întreprinse pentru menținerea sau restabilirea caracteristicilor specifice de funcționare a echipamentelor.

Componentele vitale necesare desfășurării în bune condiții a activității de mentenanță sunt:

- resursele financiare;
- încadrarea cu personal de specialitate a grupelor de întreținere tehnică;
- nivelul de dotare cu utilaje și S.D.V. (scule, dispozitive, verificatoare) specifice.

Resursele financiare au fost stabilite prin buget și au la bază estimarea necesarului de fonduri bănești pentru echipamentele generale și specifice aflate în dotarea unității, în vederea executării mentenanței în sistem propriu și externalizat.

Încadrarea cu personal de specialitate a grupelor de întreținere tehnică s-a făcut în raport cu nevoile de execuție a activităților de mentenanță specifice echipamentelor din dotare, pentru menținerea permanentă a acestora în stare de operativitate.

Nivelul de dotare cu utilaje și S.D.V.-uri specifice a fost conceput pentru a asigura lucrări de testare/diagnosticare, control, reglaje, lucrări de conservare și lucrări de înlocuire a materialelor cu perioadă determinată de utilizare.

În ceea ce privește executarea mentenanței în sistem propriu, estimarea fondurilor la categoriile de echipamente aflate în dotarea unității s-a făcut pe baza numărului necesar de reparații cuprins în planul anual de mentenanță a echipamentelor.

Pentru echipamentele tehnice, la care estimările depășesc 60% din valoarea de înlocuire a acestora, precum și pentru cele scoase din înzestrare, s-a dispus scoaterea din funcționare și

valorificarea acestora în conformitate cu prevederile legale în vigoare.

Activitățile de mentenanță ce au necesitat imobilizări ale echipamentelor pe durată medie și mare de timp au fost executate cu sprijinul eșalonului superior la Baza 191 Logistică Comunicații și Informatică și la Secția 116 Mentenanță, conform ordinelor de reparații emise.

Conceptul de mentenanță redefinit, în funcție de starea echipamentelor și momentul efectuării lucrărilor, are două componente: preventivă și corectivă.

Mentenanța preventivă a constat într-o serie de activități întreprinse pentru menținerea sistemelor tehnicii în condiții normale de funcționare, prin înlocuirea sistematică a elementelor și executarea unor lucrări de revizie periodică, reglaj, diagnosticare și control, planificate și executate în cadrul întreținerilor tehnice periodice. Activități specifice mentenanței preventive s-au executat și cu ocazia întreținerilor tehnice de sezon.

Mentenanța corectivă a cuprins activități desfășurate pentru restabilirea capacității normale de funcționare a sistemelor defecte, care au avut ca scop repunerea în stare de funcționare a tehnicii defecte ca urmare a uzurii normale.

Atenția deosebită acordată pe timpul exploatarei echipamentelor în ceea ce privește monitorizarea funcționării acestora din perspectiva componentelor conceptului de mentenanță a dus la menținerea la un nivel ridicat a ponderii intervențiilor executate în sistem propriu de către grupele de întreținere tehnică la nivelul unității. Nivelurile de mentenanță pe care este structurat sistemul de mentenanță a echipamentelor militare, stabilite în funcție de complexitatea lucrărilor și durata de imobilizare, sunt următoarele:

- mentenanță de nivel de luptă – cuprinde intervențiile de mentenanță preventive și corective, cu imobilizări ale tehnicii de scurtă durată;
- mentenanță de nivel intermediar – cuprinde intervențiile de mentenanță preventive și

corective, cu imobilizări ale tehnicii pe durată medie de timp;

➤ mentenanță de nivel complex – cuprinde intervențiile de mentenanță preventive și corective cu imobilizări ale tehnicii pe durată mare de timp.

În funcție de tipul tehnicii, gradul de uzură și volumul de manoperă, de regulă, la tehnică se execută reparații care pot fi:

- ✓ reparații curente și de complexitate redusă – RC;
- ✓ reparații de complexitate medie – RM;
- ✓ reparații de complexitate ridicată – RR.

Duratele acestor tipuri de reparații sunt reglementate prin norme specifice, elaborate de către structurile cu atribuții în domeniu din cadrul categoriilor de forțe ale armatei și comandamentelor de arme.

La nivelul unității, s-au întocmit „Planurile suport logistic integrat” pentru fiecare tip de echipament esențial din dotare.

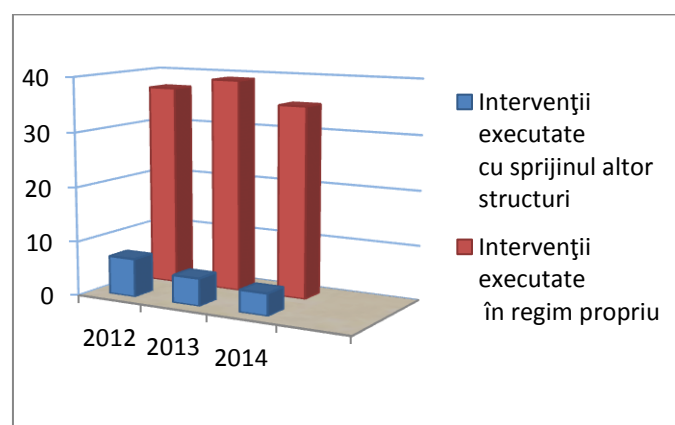
Lucrările de mentenanță preventivă/corectivă executate, precum și costurile acestora au fost consemnate în cărțile tehnice ale echipamentelor.

Evidența centralizată a datelor și a intervențiilor executate și activitatea desfășurată de către personalul care încadrează structura de

mentenanță au contribuit la menținerea în stare de operativitate a echipamentelor militare.

În concluzie, alături de alte activități specifice, care potențează procesul de instrucție, activitatea de mentenanță a echipamentelor militare este una de o remarcabilă importanță, cu determinări esențiale asupra stării de operativitate a unității, dar și asupra bazei materiale a instrucției, componentă hotărâtoare în derularea procesului de instrucție și educație ce se desfășoară, ca misiune de bază, în Batalionul de Instrucție Comunicații și Informatică „Frații Buzești”.

SITUAȚIA INTERVENȚIILOR EXECUTATE LA ECHIPAMENTELE DIN DOTARE



PLANIFICAREA, ORGANIZAREA ȘI EXERCITAREA CONTROLULUI MANAGEMENTULUI LOGISTIC LA NIVELUL UNITĂȚII

Maior Cristian STATE

Batalionul Instrucție Comunicații și Informatică „Frații Buzești”



Activitatea de planificare și organizare a controlului managementului logistic a avut ca scop protejarea patrimoniului unității, respectarea și asigurarea legalității activităților desfășurate, prevenirea, descoperirea și recuperarea pagubelor, precum și perfecționarea procesului decizional.

Exercitarea controlului managementului logistic s-a realizat de către structura logistică și comisiile nominalizate conform unei concepții întocmite la nivelul unității.

Personalul cu funcții de răspundere are atribuții clare de control pe domeniile funcționale ale logisticii și periodicitatea stabilită în funcție de complexitatea activității, acestea constând în operațiuni de verificare, inventarieri, distribuirea materialelor cu respectarea graficului de circulație al documentelor, precum și folosirea eficientă și cu prioritate a bunurilor materiale.

Pe linia managementului administrării resurselor materiale, s-a acționat pentru cunoașterea permanentă a bunurilor aflate în evidență și întocmirea la timp a cererilor necesare asigurării unei baze materiale optime.

În domeniul transportului prin personalul specializat, s-au asigurat nevoile planificate și misiunile de aprovizionare cu bunuri materiale necesare fiecărei serii de instruire. Menținerea tehnicii s-a asigurat în cadrul grupei de întreținere tehnică, precum și la nivel de garnizoană prin secția de mentenanță nr. 116 Craiova- U.M. 01395 CRAIOVA.

Pe linie de infrastructură, s-a acționat permanent pentru evaluarea stării tehnice a clădirilor, alocarea la drepturile de consum, executarea expertizelor și asigurarea mentenanței

acestora. Pentru îmbunătățirea condițiilor de trai ale cursanților cu sprijinul acordat de Centrul de domenii și Infrastructuri nr. 2 – U.M. 02517 CRAIOVA, pe parcursul anului 2015 se va construi o centrală termică ce va asigura apa caldă și încălzirea spațiilor cu destinația dormitoare și săli de specialitate, precum și aburul tehnologic necesar preparării hranei.

Echiparea cursanților aflați la pregătire, precum și a personalului propriu, s-a executat conform concepției de echipare și a normelor de înzestrare, atât la soldații și gradații profesioniști cursanți, cât și la personalul militar propriu. Au fost valorificate rezultatele revistelor de front planificate și, cu sprijinul eșalonului superior, s-a asigurat necesarul de articole de echipament.

Hrănirea se execută cu operatorul economic S.C. Ro-Armycatering S.A. încă din anul 2012, acesta reușind să-și îndeplinească obligațiile contractuale, hrana fiind de bună calitate și apreciată de întregul personal și cursanții aflați la pregătire.

În luna iulie 2014, unitatea a fost în măsură să-și evalueze capacitățile de cazare și hrănire pe timpul Ceremoniei de sosire din misiune a B 20 Infanterie „DOLJ” și încheiere a misiunii Armatei României în provincia ZABUL – Afganistan, asigurând din punct de vedere logistic un număr de 214 militari din S.M.F.A., C.Op.Psiho., R. 30 Gardă, Bg.Inf. Mil și Bg. 6 Op. Spec.

Concluzionând, activitatea de control al managementului logistic planificată, organizată și exercitată la specificul unității noastre constituie un instrument managerial eficient pentru furnizarea informațiilor reale, necesare unui proces decizional oportun și eficace cu determinări importante asupra modului de îndeplinire a misiunii de bază a unității, aceea de formare a luptătorului și inițiere a specialistului în arma comunicații și informatică.

ANALIZĂ COMPARATIVĂ PRIVIND HRĂNIREA PERSONALULUI ARMATEI ROMÂNIEI

Maior Marius CHIRIȚĂ

Batalionul Instrucție Comunicații și Informatică „Frații Buzești”



INTRODUCERE

Alinierea și coordonarea efortului logistic al Armatei României cu standardele și procedurile impuse de cadrul și misiunile Alianței Nord-Atlantice a impus și modernizarea serviciilor care sprijină resursa umană pentru a

răspunde cerințelor curente, a susține sănătatea fizică și psihică a militarilor și a asigura toate condițiile de trai și luptă la nivelul secolului XXI.

Unul dintre aceste servicii, de o importanță deosebită, este acela de *hrănire a efectivelor*.

Hrănirea militarilor este reglementată de acte legislative și norme interne ale M.Ap.N. Astfel, cadrul general este dat de *Ordonanța Guvernului României nr. 26 din 22 iulie 1994* privind drepturile de hrană în timp de pace, ale personalului din sectorul de apărare națională, ordine publică și siguranță națională, aprobată cu modificări prin *Legea 143/1994*, republicată, modificată și completată prin *Legea 523/2003*.

Restructurarea și modernizarea impuse de procesul de aderare la NATO au reliefat necesitatea externalizării unor servicii, printre acestea situându-se și serviciul de hrănire. Finalitatea dorită pentru acest demers a fost adoptarea unui sistem de hrănire modern și flexibil, obținerea de economii la bugetul apărării și degrevarea comandanților unităților militare de unele probleme logistice, care le ocupau mult din timpul necesar pentru planificarea, conducerea și execuția misiunii de luptă.

Ca urmare, în luna decembrie 2003, cadrul legislativ a fost completat cu un nou articol care stipulează că „pe bază de criterii de eficiență economică, hrănirea personalului din instituțiile publice.....se poate asigura și prin operatori economici de profil, cu aprobarea conducătorilor instituțiilor publice respective, în limita plafonului caloric și al structurii normelor de hrană la care

au dreptul”⁶. Ulterior, în baza experienței acumulate încă din anul 1999, când sistemul de hrănire externalizat a fost implementat experimental la Bg. 81 Mc. din garnizoana Dej, normele interne au fost modificate și completate, astfel încât „*în situația în care nu se poate realiza hrănirea în sistem propriu sau prin reciprocitate, la propunerea șefilor/comandanților categoriilor de forțe ale armatei și comandamentelor, pe baza criteriilor de eficiență economică, stabilite la nivelul acestora, hrănirea efectivelor se realizează prin S.C. RO-ARMYCATERING S.A.*”⁷, operator economic de profil, constituit în cadrul C.N. ROMTEHNICA R.A.

Indiferent de modalitatea de asigurare, în sistem propriu sau externalizat, hrănirea militarilor se execută astfel:

- în cazarmă, cel puțin o masă caldă pe zi;
- pe durata exercițiilor, taberelor de instrucție, tragerilor etc., atunci când activitățile durează mai mult de 24 de ore, sub formă de hrană caldă/rece, masa de dimineață, masa de prânz și masa de seară;
- în situații de criză, urgență, calamități naturale și la alertă, atunci când acțiunile durează mai mult de 24 de ore, sub formă de hrană caldă/rece, masa de dimineață, masa de prânz și masa de seară.

De asemenea, trebuie evidențiate ca având un caracter determinant în asigurarea hrănirii militarilor condițiile în care această activitate trebuie organizată și executată, astfel:

- alocații bugetare reduse și neacoperitoare pentru toate nevoile unităților militare;
- lipsa personalului specializat datorată restructurărilor și reorganizărilor succesive care s-au petrecut în cadrul tuturor structurilor militare în ultimii ani;
- deteriorarea capitală a infrastructurii dedicate asigurării hrănirii din cauza desființării unui număr important de unități militare, lipsei alocației pentru materiale de întreținere și reducerii efectivelor alocate la drepturi;

⁶ art. 4¹ din O.G. nr. 26/1994

⁷ art. 5, alin. 3 din Instrucțiunile L4/1/2008

- obligativitatea respectării angajamentelor internaționale care decurg din calitate de membru NATO și UE;

- necesitatea asigurării hrănirii efectivelor participante la exerciții, tabere, aplicații și în situații de criză, urgență, calamități naturale, precum și cele care participă la acțiuni în teatrele de operații.

MODALITĂȚI DE EXECUTARE A HRĂNIRII MILITARILOR

Hrănirea militarilor în sistem externalizat prin S.C. RO-ARMYCATERING S.A.

- asigură:

a) servirea sub formă de hrană caldă, în zilele lucrătoare, a minimum unei mese pe zi;

b) servirea sub formă de hrană caldă a mesei de dimineață, gustării, prânzului sau a mesei de seară, la cererea personalului.

- achiziția serviciului de hrănire prin S.C. RO-ARMYCATERING S.A. se face de către autoritățile contractante delegate din M.Ap.N., cu respectarea legislației care reglementează achizițiile publice și a H.G. nr. S-410/2011.

- Militarii care se hrănesc prin S.C. RO-ARMYCATERING S.A. nu primesc valoarea financiară a normei respective pentru zilele de hrană sau mesele servite; pentru regimul de hrănire cu 3 mese pe zi se rețin 35% pentru masa de dimineață și gustare, 50% pentru masa de prânz și 15% pentru masa de seară, în funcție de mesele servite, iar pentru regimul de hrănire cu cel puțin o masă caldă pe zi, suma ce se reține se aprobă de către comandantul unității militare și nu poate fi mai mică de 25% din valoarea financiară a normei de hrană, corespunzătoare mesei servite;

- prețul maxim de achiziție a serviciului de hrănire pentru fiecare normă de hrană cuprinde: valoarea financiară a normei de hrană din care se deduce TVA, cheltuieli directe și indirecte nu mai mult de 30% din valoarea financiară a normei fără TVA, profitul în cuantum de până la 3% din suma primelor două sume și TVA.

Hrănirea militarilor în sistem propriu

- asigură:

a) servirea sub formă de hrană caldă, în zilele lucrătoare, a minimum unei mese pe zi;

b) servirea sub formă de hrană caldă a mesei de dimineață, gustării, prânzului sau a mesei de seară, la cererea personalului.

- achiziția produselor agroalimentare necesare se face de către autoritățile contractante delegate din M.Ap.N., cu respectarea legislației care reglementează achizițiile publice și a H.G. nr. S-410/2011.

- impune unității militare:

a) existența unei infrastructuri adecvate (bloc alimentar, spații de depozitare, utilaje și materiale de resort etc.) și încadrarea cu personal de specialitate, care să asigure un flux tehnologic corect pentru păstrarea și distribuția alimentelor, preparare și servirea hranei în condiții de securitate alimentară și calitate.

b) organizarea, planificarea și executarea în volum complet a activității de hrănire.

c) asigurarea condițiilor optime pentru igiena personalului care lucrează la depozite și blocul alimentar, precum și a personalului care servește masa.

d) recoltarea probelor de mâncare.

e) asigurarea funcționării spațiilor frigorifice, instalațiilor de alimentare cu apă, energie, de evacuare a deșeurilor menajere și resturilor alimentare și de ventilație.

f) executarea lucrărilor periodice de curățenie, întreținere, dezinsecție, deratizare, dezinsecție la spațiile destinate hrănirii.

g) autorizarea sanitară și sanitar-veterinară a spațiilor și a autovehiculelor destinate hrănirii.

h) modificarea și completarea statelor de organizare ale unităților pentru încadrarea personalului de specialitate necesar desfășurării activității de hrănire.

i) aprovizionarea cu produse agroalimentare, materiale de întreținere și materiale pentru prepararea și servirea hranei, recepția, depozitarea și păstrarea acestora.

j) pregătirea și verificarea personalului implicat în activitatea de hrănire.

k) stabilirea de responsabilități personalului cu atribuțiuni specifice și organizarea controlului intern.

l) monitorizarea activității de hrănire pentru respectarea calității impuse de reglementările în domeniu.

După cum reiese din cele prezentate succint în tabelul următor, este evident că efectuarea hrănirii în sistem externalizat este mai avantajoasă decât sistemul de hrănire propriu, sub toate aspectele: uman, material și financiar.

Tabel de analiză comparativă a sistemelor de hrănire din Armata României

CRITERII ANALIZATE	SISTEM EXTERNALIZAT (1)	SISTEM PROPRIU (2)	ELEMENTE COMUNE	APRECIERE
Comandantul unității	- timpul alocat pentru organizarea, conducerea și îndrumarea activității se reduce substanțial, în favoarea organizării și conducerii misiunii unității.	- activitatea este grevată mai mult de asigurarea hrănirii militarilor în defavoarea executării pregătirii pentru luptă.	- poartă întreaga răspundere pentru activitățile care se desfășoară în unitate, le organizează, conduce și îndrumă nemijlocit.	Mai avantajos (1)
Structura de logistică	- îndrumă, coordonează și controlează activitatea, urmărind respectarea clauzelor contractuale.	- organizează, planifică, conduce, gestionează, controlează și execută în totalitate toate activitățile incumbate de această activitate (documente, aprovizionare, recepție, depozitare, control, întreținere spații și utilaje etc.).		Mai avantajos (1)
Personalul de specialitate/ execuție	- asigurat în totalitate de către operatorul economic, care este responsabil de toate implicațiile pe linia resurselor umane.	- este nevoie de încadrarea funcțiilor care au fost restructurate, detașări, pregătire în a doua specializare.		Mai avantajos (1)
Cheltuieli de personal	- în sarcina operatorului prestator și sensibil mai mici decât în sistemul militar.	- mai mari prin creșterea numărului de funcții încadrate cu specialiști militari.	- în final, sunt suportate de către unitatea militară.	Mai avantajos (1)
Cheltuieli materiale	- toate cheltuielile cu utilitățile, întreținerea, dotarea și asigurarea integrității bunurilor puse la dispoziție sunt în sarcina operatorului economic.	- costuri mai mari pentru întreținere și plata utilităților.		Mai avantajos (1)

CRITERII ANALIZATE	SISTEM EXTERNALIZAT (1)	SISTEM PROPRIU (2)	ELEMENTE COMUNE	APRECIERE
Costuri	- costul total al prestației poate fi cu până la 60% mai mare decât valoarea financiară a normelor de hrană.	- costul executării activității este mai mare decât valoarea financiară a normelor de hrană, dar mai mic decât cel în sistem externalizat, datorită lipsei cotei de profit, dar avantajul poate fi contrabalansat de cheltuieli mai mari cu drepturile de personal.		Mai avantajos (2)
Dotări	- se asigură de operatorul economic și pot fi puse la dispoziție de către achizitor, avantajul fiind dat de faptul că la sfârșitul contractului, bunurile trebuie returnate în aceeași stare ca la data primirii spre folosință și orice depreciere cade în sarcina operatorului.	- uzura bunurilor materiale folosite în această activitate nu se recuperează, fiind necesară înlocuirea acestora, ceea ce duce la costuri suplimentare.		Mai avantajos (1)
Alte aspecte	- obținerea tuturor avizelor sanitare, sanitar-veterinare, efectuarea examenelor medicale periodice pentru personal sunt obligativitatea operatorului.	- obținerea tuturor avizelor sanitare, sanitar-veterinare, efectuarea examenelor medicale periodice pentru personal sunt obligativitatea unității militare.		Mai avantajos (1)
	- degrevează unitatea de transportul hranei în alte locații unde personalul servește hrana.	- unitățile militare nu mai dispun de mijloace adecvate pentru transportul alimentelor și hranei gata preparate.		Mai avantajos (1)

CONCLUZII

Fără a ignora sau minimaliza importanța și aportul sistemului de hrănire propriu în asigurarea drepturilor militarilor și în susținerea efortului acestora pentru îndeplinirea misiunilor ce le revin, putem afirma că sistemul de hrănire externalizat răspunde mult mai bine realităților cu care se confruntă sistemul militar românesc actual.

Sintetizând, sistemul de hrănire externalizat corespunde standardelor și procedurilor NATO, fiind agreeat și folosit în cadrul Alianței, la scară largă, inclusiv în teatrele de operații cele mai dificile.

De asemenea, realizează o convergență cu unele dintre obiectivele prioritare ale Armatei României, de restructurare și modernizare, concomitent cu realizarea raportului optim între personalul luptător și cel administrativ, precum și diminuarea unor categorii importante de cheltuieli impuse de aprovizionare, transport, depozitare, gestionare, dotare și consum de utilități.

Totodată, sistemul externalizat, ca și cel propriu, asigură respectarea fluxului tehnologic impus de siguranța în alimentație, plafonul caloric și structura normelor de hrană și ceea ce este cel mai important, *satisfația personalului care beneficiază de acest serviciu.*

SECURITATEA CIBERNETICĂ – NECESITATE A SECOLULUI AL XXI-LEA

Căpitan Gabriel-Nicușor IANCU-IACOB

Batalionul Instrucție Comunicații și Informatică „Frații Buzești”



Evoluția economică mondială și transformările permanente ale omului autonom, dornic de putere și devorator de informație, lipsa de timp și „goana” după un confort material și spiritual au făcut din individul-social, care interacționează direct, conștient și afectiv cu semenii, individul-robot, conectat permanent la „rețea”.

Pe măsură ce factorul economic al țărilor dezvoltate exploatează avantajele oferite de internet, infrastructura și secretele țărilor devin din ce în ce mai vulnerabile atacurilor cibernetice. Dacă, în secolul trecut, războaiele aveau loc pe câmpul de luptă, astăzi obținerea resurselor adversarilor implică din ce în ce mai des o bătălie în teritoriul virtual. Teoreticienii consideră ciberspațiul ca fiind al cincilea domeniu în care se poate desfășura un război, după sol, mare, aer și spațiu.

Printre infrastructurile cibernetice vulnerabile se numără rețelele electrice, cele ale spitalelor, băncilor, ale companiilor de telecomunicații sau din domeniul apărării, iar pe măsură ce tot mai multe informații devin conectate la spațiul virtual, lista potențialelor ținte se mărește. Pentru că toate aceste sisteme sunt interconectate, un atac cibernetic poate dezactiva în câteva minute o rețea electrică, cu consecințe devastatoare asupra rețelelor bancare, de transport, de comunicare, afectând chiar și lanțurile logistice ce asigură alimentarea cu hrană a populației.

Pe lângă avantajul pe care ciberspațiul îl oferă potențialilor atacatori prin ușurința și viteza cu care resursele adversarului pot fi obținute sau distruse, ciber-războiul poate aduce un alt atu forței agresoare: *identitatea atactorilor poate fi disimulată*.

Dacă în secolul al XX-lea, arma nucleară a fost armă-cheie, în sensul că țările care o puteau folosi erau conștiente și descurajate de un eventual contraatac al inamicului la fel de devastator,

atacul cibernetic, ce se anunță a fi instrumentul militar esențial al secolului al XXI-lea, ar putea evita acest impendiment dacă victima atacului nu știe împotriva cărei țări să lanseze contraatacul.

Criminalitatea cibernetică este în continuă creștere și, pe măsură ce tehnologia evoluează, impactul atacurilor cibernetice devine din ce în ce mai puternic. Iar infractorii de pe internet nu fac discriminări atunci când vine vorba de țintele lor. Dovada? Când giganți precum Facebook sau Agenția de Securitate Națională a SUA, aparent greu de clintit, cad victime atacurilor.

Indiferent de percepția personală a fiecărui utilizator de internet vizavi de atacurile cibernetice, cu siguranță persistă o preconcepție în rândul majorității acestora: cu cât o companie este mai mare și mai importantă, cu atât sistemele sale de securitate ar trebui să fie mai bune și mai sigure. Însă... nu invincibile, după cum o demonstrează atacurile cibernetice „răsunătoare”, care au avut drept țintă cunoscute (și presupus sigure) mari organizații din lume.

58.000 de documente secrete, furate de la NSA, 50 de milioane de conturi compromise pe Evernote, 318.000 de parole furate de la Facebook și alte informații de login de pe Facebook, 250.000 de conturi de Twitter, compromise și 600.000 de conturi ale clienților furate de la lanțul de fast-food Domino's Pizza, sunt numai câteva din urmările atacurilor cibernetice într-o perioadă de 2 ani.

Criminalitatea cibernetică ce are în vedere giganții din diversele industrii este doar o mică parte din amenințările de care se tem specialiștii în securitate. Un atac cibernetic de proporții, cu impact deosebit de puternic asupra societății actuale, reprezintă un risc care planează de multă vreme la nivel mondial. Cea mai recentă referire la un potențial astfel de dezastru informațional a fost făcută la sfârșitul lunii septembrie 2014 de către un reprezentat al unei importante autorități de supraveghere financiară din Statele Unite. Astfel, conform lui *Benjamin LAWSKY, Chief, New York State Department of Financial Services*, vulnerabilitatea tehnologică a sistemului financiar

reprezintă o problemă presantă, potențial catastrofică.

Acesta a declarat că se teme de posibila declanșare a unui eveniment cibernetic major în sistemul financiar, un fel de Armagedon cibernetic, care ar putea lăsa urme adânci la nivelul sistemului financiar pe o perioadă mai lungă de timp, comparându-l cu atacurile de la 11 septembrie.

Primul atac informatic a avut loc în 1982, când spionii sovietici au furat un sistem de control computerizat de la o companie canadiană. Ceea ce nu au știut spionii sovietici era că CIA reușise să introducă în software-ul furat un cod care, introdus în programele de computer, activează o funcție malițioasă. În cazul sistemului de control furat de spionii URSS, bomba logică inserată de CIA a condus la o explozie masivă ce a avut loc la o conductă de gaz din Siberia. Deflagrația a fost atât de mare, încât a fost detectată din spațiu de sateliții americani, iar Thomas Reed, un fost comandant al aviației SUA, a descris-o în autobiografia sa ca fiind „*cea mai mare explozie non-nucleară detectată vreodată din spațiu*”.

La 25 de ani după, în aprilie 2007, Estonia a fost supusă unui atac cibernetic fără precedent, site-urile parlamentului, ministerelor, băncilor, principalelor ziare și televiziuni fiind țintele răufăcătorilor virtuali. Timp de trei săptămâni, țara a fost paralizată, ministerele, băncile și numeroase companii fiind nevoite să-și oprească activitatea, iar cetățenii au avut probleme în a accesa internetul.

Georgia a suferit atacuri similare în 2008, într-o perioadă ce a coincis cu conflictul georgiano-rus din Osetia de Sud. Din cauza atacurilor venite dinspre Rusia, routerele din Turcia și Rusia ce făceau legătura cu Georgia erau supraîncărcate cu date spre țara gruzină, astfel că traficul spre lume era complet sufocat. Din acest motiv, cetățenii Georgiei nu puteau accesa niciun site străin pentru a se informa și nici nu puteau trimite emailuri sau alte tipuri de pachete de date în afara țării. De asemenea, Georgia a pierdut controlul asupra domeniului .ge, fiind nevoită să transfere site-urile guvernamentale pe servere din afara țării. Pagina președintelui țării a fost mutată în „exil virtual” pe un blog găzduit de Google în California.

Cea mai sofisticată armă cibernetică ce a ieșit până acum la iveală este Stuxnet, un vierme informatic ce a fost folosit pentru a întârzia programul nuclear iranian. Un virus extrem de

complex, Stuxnet a impresionat analiștii din domeniul securității informatice prin numărul de vulnerabilități pe care acesta le-a exploatat, fiind de departe cel mai ingenios și complex vierme informatic descoperit vreodată. Atacul informatic a fost la fel de eficient ca unul militar, estimează analiștii, provocând o întârziere de aproximativ 2 ani programului nuclear iranian.

În ultimii ani, hackerii chinezi au lansat din ce în ce mai multe atacuri asupra computerelor ce aparțin guvernului SUA și companiilor din industria apărării. Din 2006 până în 2011, numărul atacurilor lansate împotriva computerelor aparținând guvernului federal american a crescut cu 650%. Printre oficialii de rang înalt atacați de agenții chinezi s-au numărat Secretarul Apărării, Robert Gates, și Secretarul Comerțului, Carlos Gutierrez, căruia i s-au copiat toate datele de pe laptop cu ocazia unei vizite la Beijing, pentru ca apoi să se încerce conectarea cu ajutorul lor la serverele Departamentului Comerțului din SUA.

SUA nu este singura țară afectată. În 2011, instituții precum Comisia Europeană și FMI au fost ținta unor atacuri semnificative, iar computerele guvernului francez au căzut victimă hackerilor cu puțin timp înainte ca această țară să găzduiască summitul G20. Guvernul german susține că hackerii chinezi au accesat computerul personal al premierului Angela Merkel, o altă victimă a acestora fiind premierul Australiei. Directorul MI5 a comunicat celor mai importante 300 de companii din Marea Britanie că rețelele lor au fost penetrate de agenții guvernului chinez.

Ca răspuns la numeroasele atacuri la care infrastructura SUA a fost supusă în ultima vreme, Pentagonul a anunțat recent noua strategie asupra spațiului virtual. Aceasta cuprinde o schimbare dramatică, guvernul american anunțând că intenționează să clasifice sabotajul computerizat drept *un act de război*. Acest lucru înseamnă că, pentru prima dată, SUA afirmă deschis că este dispusă să folosească forțele militare tradiționale pentru a răspunde la un atac cibernetic. „Dacă folosești atacuri cibernetică pentru a ne dezactiva rețelele electrice, nu fi surprins dacă te vei trezi lovit de o rachetă”, a descris un oficial din armata SUA noua doctrină.

Pentagonul intenționează să folosească conceptul de „echivalență” pentru a decide căror atacuri cibernetică să răspundă cu arme convenționale. Astfel, dacă un atac cibernetic va produce victime, daune materiale și perturbări în funcționarea normală a societății similare cu

efectul unui atac militar tradițional, armata SUA va lua în calcul posibilitatea de a răspunde prin forță militară convențională.

De asemenea, Pentagonul a anunțat că lucrează la un sistem intitulat *National Cyber Range*, ce reprezintă o „clonă” a internetului în care vor putea fi simulate ciber-războaie. Terenul de antrenament virtual va permite armatei americane dezvoltarea de strategii și tehnici de atac și de apărare în spațiul virtual. Acest sistem a intrat în funcțiune în 2012, fiind conceput de DARPA, agenția care a conceput ARPANET, precursorul internetului de azi.

Recent, Agenția de Securitate Națională a SUA a anunțat un parteneriat cu majoritatea furnizorilor de conexiuni la internet din SUA în cadrul căruia vor scana traficul de date transportat de acestea, în scopul detectării atacurilor cibernetice și eliminării lor.

Apărarea în fața potențialelor atacuri cibernetice ocupă un loc central în strategia de securitate a României și este, în același timp, o dimensiune importantă a profilului extern al țării noastre, a carei activitate în acest sens s-a dovedit deja remarcabilă în planul cooperării internaționale. Pentru NATO, de asemenea, acest domeniu de responsabilitate este încă nou, dar extrem de important, dată fiind dependența permanent crescândă a societății față de accesul la

internet și de rețelele informatice și de telecomunicații.

Un potențial atac, favorizat de vulnerabilitățile sistemelor informatice, ar avea o viteză mare de propagare la un cost relativ scăzut pentru autor, iar impactul său va fi resimțit la nivelul întregului sistem virtual și capabil să periclitizeze existența zilnică a tuturor cetățenilor, având în vedere că vulnerabilitățile sistemice nu se opresc la instalații militare, ci implică ansamblul administrației și mare parte din infrastructura esențială funcționării unei societăți moderne.

Furnizarea zilnică de informații căreia omul modern îi devine rob, timpul aproape instantaneu în care acesta are acces la aproape orice tip de informație, calea din ce în ce mai facilă către diferite surse de informație fac din individul contemporan o victimă posibilă și aproape sigură oricărui atac cibernetic ce poate avea un impact devastator, atât asupra lui, cât și asupra organizației.

Fie că vorbim de date personale, informații financiare sau date comerciale confidențiale stocate digital, toate acestea trebuie să fie păstrate în siguranță. Astfel, *securitatea cibernetică* trebuie să fie o constantă a vieții noastre zilnice în mediul online, precum centura de siguranță în conducerea mașinii.

Abrevieri:

1. NSA – Agenția de securitate națională (SUA);
2. CIA – Agenția Centrală de Informații (SUA);
3. FMI – Fondul Monetar Internațional;
4. DARPA (*Defense Advanced Research Projects Agency*) – agenție a Departamentului Apărării al SUA responsabilă pentru dezvoltarea de tehnologii emergente pentru a fi utilizate de către armată;
5. ARPANET (*The Advanced Research Projects Agency Network*) – rețea de calculatoare descentralizată, ce consta în legături între mașinile (calculatoarele) din 4 instituții academice americane.

Bibliografie:

1. H.G. 271 din 15.05.2013 pentru aprobarea Strategiei de securitate cibernetică a României și a Planului de acțiune la nivel național privind implementarea Sistemului național de securitate cibernetică.
2. www.wikipedia.org.
3. www.futurelearn.com.
4. www.mediafax.ro.
5. www.agerpres.ro.

UNELE OPINII PRIVIND ADAPTAREA INSTRUCȚIEI DE COMUNICAȚII ȘI INFORMATICĂ LA MEDIUL INTERNAȚIONAL ACTUAL

Locotenent Iulian ACSINTE

Batalionul Instrucție Comunicații și Informatică „Frații Buzești”

„Military education is key component to a fitter, faster and more flexible NATO.”

General Knud Bartels, Chairman of the NATO Military Committee



Schimbările survenite în mediul internațional de securitate, în special după data de 24 februarie 2014⁸, au condus la o serie de măsuri, atât de ordin economic, cât și de ordin militar, împotriva principalului factor destabilizator din regiune. Europa și

NATO trebuie să facă față celei mai mari provocări de securitate de la încheierea Războiului Rece.

În cadrul summit-ului care a avut loc în perioada 4-5 septembrie 2014 în Țara Galilor, membrii Alianței Nord-Atlantice au reiterat importanța implementării standardelor și doctrinelor convenite la nivel NATO, „se vor asigura că forțelor lor terestre, aeriene și maritime corespund liniilor directe convenite la nivelul NATO în privința capacității de dislocare și sustenabilității și a altor rezultate cuantificabile convenite”⁹ și și-au asumat creșterea cheltuielilor de apărare la minimum 2 % din PIB.

La reuniunea miniștrilor Apărării de la Bruxelles s-a decis constituirea imediată pe teritoriile aliaților din est¹⁰ a unor Unități pentru Integrarea Forțelor NATO, acestea fiind structuri multinaționale de comandă și control ale Alianței Nord-Atlantice, care vor asigura o prezență vizibilă și continuă a NATO pe teritoriul aliaților estici. Pe lângă acest centru, România va găzdui un Comandament Multinațional de Divizie Sud-Est care va funcționa ca un centru de comandă-

control în situația dislocării de forțe pe flancul estic al NATO¹¹.

Pentru țara noastră, un prim pas important în realizarea acestor obiective l-a constituit semnarea „Acordului politic național privind creșterea finanțării pentru Apărare”¹², în scopul asigurării predictibilității politicii de înzestrare a Armatei României cu tehnică modernă de luptă. Decidenții factorului politic au convenit creșterea finanțării pentru apărare, astfel încât, la nivelul bugetului pentru anul 2017, să se atingă 2% din PIB, iar pentru următorii 10 ani acest nivel să se mențină constant.

Continuarea dezvoltării sistemului de comunicații și informatică conform arhitecturii de comandă-control și dezvoltarea rețelelor, sistemelor și serviciilor de comunicații și informatice, în paralel cu realizarea punctelor de comandă de nivel batalion și inițierea realizării unui punct de comandă tip brigadă tip redus¹³ sunt stipulate în direcțiile de acțiune stabilite pentru îndeplinirea obiectivului strategic al politicii de apărare.

Considerăm că asigurarea unui climat financiar stabil și a unei politici de înzestrare a Armatei României pe termen mediu și lung va determina, fără echivoc, o serie de schimbări în domeniul instrucției, în scopul adaptării la noile cerințe ale partenerilor aliați și, implicit, în procesul de instrucție a soldaților și gradaților profesioniști din arma comunicații și informatică.

Metodele, mijloacele și tehnicile de predare-învățare utilizate în instrucție¹⁴ în princi-

⁸Intervenția armatei ruse în Ucraina, http://ro.wikipedia.org/wiki/Intervenția_armată_rusă_în_Ucraina_din_2014-2015

⁹<http://www.mae.ro/node/28465>

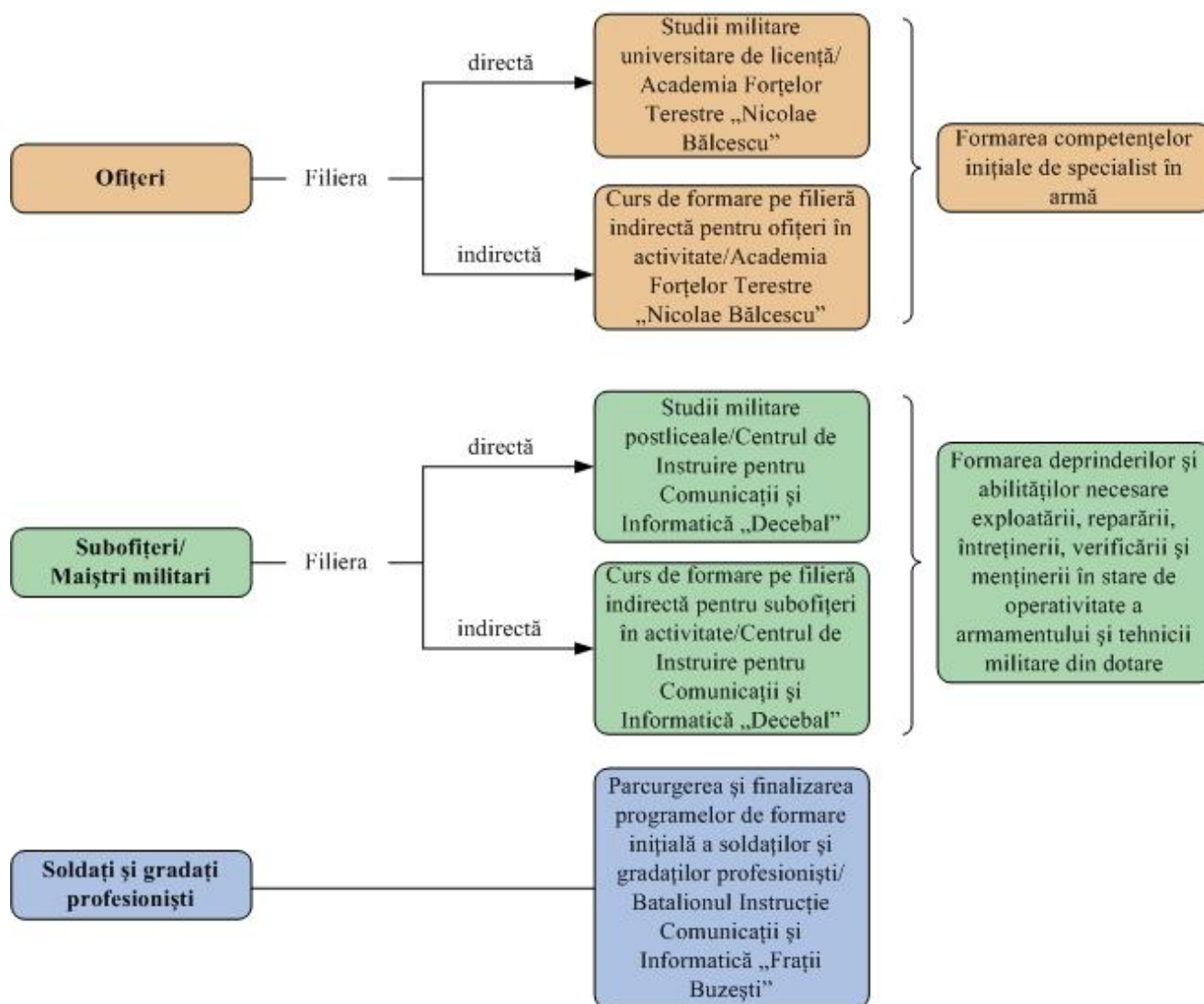
¹⁰ România, Polonia, Bulgaria, Estonia, Letonia și Lituania

¹¹ <http://www.mediafax.ro/politic/dusa-in-zilele-urmatoare-vom-stabili-amplasamentele-celor-doua-comandamente-nato-13817544>

¹²<http://www.presidency.ro/static/Acordul%20politic%20național%20privind%20cresterea%20finantarii%20pentru%20Aparare.pdf>

¹³ www.resboiu.ro

¹⁴ Ghe.Dincă în Revista comunicațiilor și informaticii, Sibiu, 2010



piu rămân aceleași, obiectul modificărilor fiind disciplinele de studiu din cadrul cursurilor de nivel/specializare.

Formarea profesională inițială a militarilor din arma comunicații și informatică se realizează, conform reglementărilor legale, pe categorii de personal, astfel:

Misiunea¹⁵ Batalionului Instrucție Comunicații și Informatică „Frații Buzești” este aceea de a forma și specializa soldați și gradați profesioniști ca luptători și specialiști în arma comunicații și informatică. Împreună cu Centrul de Instruire pentru Comunicații și Informatică „Decebal”, pune la dispoziția soldaților profesioniști din toate armele (nu doar din arma comunicații și informatică) o ofertă educațională¹⁶ suficient de variată și atractivă, astfel încât să

corespundă nevoilor de instruire și evoluție în carieră a acestora.

În mod cert și aceste cursuri de specializare trebuie să se adapteze în permanență la cerințele sistemului militar și la standardele nord-atlantice, Școala NATO de Comunicații și Informatică reprezentând un etalon important pentru toate statele membre.

Prin tabelul de mai jos, propunem inițierea unui demers cu scopul de a analiza și a desprinde unele concluzii, atât de către noi, cât și de cei care sunt preocupați de rolul și evoluția viitoare a BICI și CICI. Am selectat dintre cursurile din domeniul comunicațiilor destinate soldaților și gradaților profesioniști aprobate pentru anul învățământ 2014-2015 ale celor două unități de învățământ și instrucție elementele comune cu cele prezente în oferta educațională a Școlii NATO¹⁷ de la

¹⁵http://smg.mapn.ro/site_CCI/istoric%20subordonate.htm

¹⁶http://www.cissb.ro/Oferata_educationala.html,

¹⁷https://www.nciss.nato.int/courses_description.php

Latina/Italia, ordinea prezentării informațiilor nereprezentând neapărat o corespondență/echivalare a acestora.

O caracteristică foarte importantă a cursurilor desfășurate în cadrul Școlii NATO o reprezintă precizarea clară a categoriilor de personal cărora le sunt destinate cursurile, acest aspect fiind relevant, în comparație cu oferta educațională națională, mai ales la cursurile din domeniul informaticii.

Consider că ultimul curs menționat în tabel, *Deployable Optical Fibre Cable*, se poate transpune într-un orizont de timp foarte redus și cu costuri relativ mici în oferta educațională a Batalionului Instrucție Comunicații și Informatică „Frații Buzești”, microstructurile de execuție a serviciilor informatice fiind formate cu preponderență din soldați și gradați profesioniști.

DENUMIREA CURSULUI	ȘCOALA CIS NATO	CICI	BICI
	Long Range Line of Sight Communications System Operator/Technician.	Curs de specializare a operatorilor din centrele de comunicații ale RTP/RMNC	Curs de specializare pentru operatori tehnică de comunicații radioreleu numeric de capacitate mare
	Short Range Line of Sight Communications System Operator/Technician	Curs de specializare a operatorilor din centrele de management ale RTP/RMNC	Cursul de specializare a operatorilor din centrele de comunicații ale RTP/RMNC
	NATO HF	Curs de operatori stații radio numerice HARRIS (VHF și HF) și proceduri de comunicații NATO	Cursul de operatori stații radio numerice HARRIS (VHF și HF) și proceduri de comunicații Cursul de operatori stații radio numerice PANTHER (VHF și HF) și proceduri de comunicații
	NATO Video Tele Conferencing Servers (VTC MCU)	Curs pentru cunoașterea, operarea și mentenanța echipamentelor din Modulul de comunicații și informatică desfășurabil (MCID), autostației de videoteleconferință (VTC) și a stațiilor radio utilizate în misiuni	
	NATO Video Tele Conferencing Endpoint (VTC CODEC)	Curs de operatori pentru echipamente VTC	
	AN/PRC-117F (TACSAT) Applications and database manager	Curs de instruire pentru planificarea și organizarea rețelelor radio utilizând stații radio de tip HARRIS ANPRC 117 G	
	NATO Very Small Aperture Terminals (VSAT) Operator Course	Curs de comunicații militare prin satelit	
	NATO Satellite Communications System Technician		
	NATO Transportable Satellite Ground Terminal Technician		
	NATO Deployable Satellite Ground Terminal Operator		
	New Transportable Satellite Ground Terminal Course		
	UHF TACSAT Basic		
Deployable Optical Fibre Cable	Curs de operatori pentru echipamente de comutație multiprotocol	Curs de specializare pentru electromecanici în comunicații și informatică	

În procesul de instruire, modernizare și operaționalizare, structurile de comunicații și informatică naționale pot beneficia de experiența dobândită de către Modulul NATO de comunicații și informatică dislocabil DCM „E”. Acțiunile întreprinse în scopul îndeplinirii misiunii modulului¹⁸, respectiv extinderea serviciilor de comunicații și informatice în sprijinul comandamentelor NATO, prin interconectarea punctelor de comandă fixe din Europa cu teatrele de operații, folosind *mijloace de legătură prin satelit*, dar mai ales activitățile de instruire executate în vederea atingerii capacității operaționale au fost verificate în mod real pe timpul dislocării în teatrul de operații Afganistan, iar instruirea personalului s-a executat atât în țară, cât și în cadrul Școlii NATO de Comunicații și Informatică.

Și în tabelul prezentat anterior se poate observa cu ușurință multitudinea de cursuri din cadrul Școlii NATO referitoare la cunoașterea și exploatarea stațiilor/autostațiilor satelitare și de videoteleconferință. Motivele pentru care asemenea echipamente moderne și performante nu sunt în dotarea tuturor structurilor de comunicații și informatică sunt desigur, în primul rând, financiare.

Armata României este în curs de implementare a unor tehnici și tehnologii deosebite¹⁹, compatibile cu tehnica partenerilor din NATO. Fără a detalia fiecare tip de tehnică în parte, menționăm câteva echipamente de comunicații și informatică pe care le așteptăm să intre și în dotarea unităților de învățământ și instrucție:



¹⁸ Nota ministrului apărării naționale privind constituirea și găzduirea pe teritoriul statului român a unui Modul NATO dislocabil, disponibilă pe adresa:

<http://www.cddep.ro/bperm/2010/F970471513-SCAN0004.PDF>

¹⁹ A se vedea <http://www.rumaniamilitary.ro/inteligența-romaneasca-transmisiunile-in-armata-romana>

1. **Autospeciala de telecomunicații prin satelit „Anchor Station”** a intrat recent în înzestrarea Centrului 48 Comunicații și Informatică Strategice din subordinea Comandamentului Comunicațiilor și Informaticii.²⁰

Pentru asigurarea securității comunicațiilor de orice fel, autospeciala dispune de aparatura de criptare a aplicațiilor IP sau a fluxurilor. De asemenea, componenta radio a autospecialei este reprezentată în benzile scurte și ultrascurte cu stații de tip „Harris”, integrate printr-un Hub tactic.

2. **Modulul de comunicații și informatică dislocabil** reprezintă extensia RMNC destinată asigurării legăturii unor structuri de nivel tactic, dislocate într-o arie de operații în țară sau în afara granițelor țării, având capabilitatea de operare independentă. Modulul este proiectat astfel încât legăturile operative între teatrele de operații și platforma centrală de integrare în RMNC să poată fi asigurate prin una sau mai multe căi de comunicații alternative, în funcție de situația operativă și infrastructura existentă în locația respectivă. MCID este echipat cu tehnică de comunicații rigidizată, identică cu cea care echipază centrele de comunicații din RMNC, la care se adaugă echipamente multicanal de satelit (în benzile civile și militare), precum și o rețea de calculatoare pentru integrarea în intranetul militar. Segmentele satelitare se închiriază de la operatorii publici sau de la organismele militare care controlează activitatea sateliților militari de telecomunicații.

3. **Videoteleconferința/VTC - S.M.G.-23/2013** reprezintă un serviciu multimedia constituit dintr-un set de tehnologii care permit interacțiunea între două sau mai multe locații printr-o comunicație bidirecțională audio și video simultană. Serviciul permite realizarea unor activități de grup, în care participanții, deși sunt dispersați în spațiu, la anumite distanțe unii față de alții, colaborează în condiții aproape identice cu cele în care lucrează persoane aflate împreună, în aceeași sală. Pentru a realiza acest lucru, sistemele VTC trebuie să asigure o comunicare vizuală și auditivă eficientă între participanți și un schimb de informații în timp real prin transfer de documente, imagini, date statistice etc.

²⁰http://www.rft.forter.ro/_wsn/2014_2/07-arm/04.htm

CONCLUZII ȘI PROPUNERI

1. Continuarea participării instructorilor din BATALIONUL INSTRUCȚIE COMUNICAȚII ȘI INFORMATICĂ la aplicații și exerciții tehnico-tactice de nivel operativ și strategic, pentru crearea unei imagini de ansamblu asupra funcționării CIS.

2. Continuarea colaborării cu structuri militare care au fost dislocate în teatrele de operații și oportunitatea extinderii acestora în afara garnizoanei Craiova cu privire la îmbunătățirea nivelului de informații referitoare la funcționarea tehnicii de comunicații în operațiile militare executate în mod real, disfuncțiile apărute și mai ales soluțiile adoptate pentru remedierea imediată a acestora, în scopul eficientizării procesului de instrucție al soldaților și gradaților profesioniști.

3. Analiza oportunității demarării demersurilor legale în vederea inițierii unor schimburi de experiență cu unități de instrucție în arma comunicații și informatică ale partenerilor

nord-atlantici și, desigur, cu Școala NATO de comunicații și informatică de la Latina.

Instrucția desfășurată în scopul creșterii nivelului de pregătire al soldaților și gradaților profesioniști influențează, inevitabil, modul de operaționalizare al forțelor, mai ales dacă nu este executată la standardele impuse.

Corpul de instructori din BATALIONUL INSTRUCȚIE COMUNICAȚII ȘI INFORMATICĂ „FRAȚII BUZEȘTI”, prin pasiunea față de armă, prin profesionalismul autoimpus și exprimat, la fiecare serie de formare a soldaților profesioniști și la fiecare curs de specializare, prin rezultatele obținute de cursanți și prin feedback-ul pozitiv primit de la unitățile care beneficiază în mod real de pregătirea acestora, a demonstrat că este în măsură să se adapteze la standardele și nevoile de instruire ale Armatei României.

La mulți ani !

SPAȚIUL CIBERNETIC – PRINCIPALA SURSĂ DE AMENINȚĂRI

Locotenent Daniel CALCIU

Centrul 105 Comunicații RMNC



Spațiul cibernetic se caracterizează prin lipsa frontierelor, dinamism și anonim, generând deopotrivă oportunități de dezvoltare a societății informaționale bazate pe cunoaștere, dar și riscuri la adresa funcționării acesteia.

Alături de beneficiile incontestabile pe care informatizarea le induce la nivelul societății moderne, aceasta introduce și vulnerabilități, astfel că asigurarea securității spațiului cibernetic trebuie să constituie o preocupare majoră.

Amenințările de natură informatică asupra spațiului cibernetic s-au diversificat, fiind relevate tendințe evolutive, atât din perspectivă cantitativă, cât și din punct de vedere al complexității tehnice evidențiate. Majoritatea incidentelor analizate sunt îndreptate către sisteme învechite, depășite moral, fără posibilități native de securizare (ex: sistemele afectate de Conficker) sau care nu sunt actualizate cu ultimele patch-uri/update-uri de securitate.

Este de remarcat faptul că multe entități devin din ce în ce mai frecvent ținta amenințărilor de tip atacuri cibernetică cu un grad ridicat de complexitate, lansate de către grupuri ce au capacitatea și motivația necesară pentru a ataca în mod persistent o țintă în scopul obținerii anumitor beneficii (de obicei acces la informații sensibile).

Pentru aceasta, se consideră absolut necesară cunoașterea, de către utilizatorii casnici, cel puțin a recomandărilor de securitate expuse mai jos:

1. Se folosește numai software cu licență. Sistemele de operare, aplicațiile de securitate, filmele, muzica precum și alte pachete software pirat, descărcate de pe site-uri de tip „torrent” sau hub-uri de DC, pot conține cod malițios ascuns (rootkits, backdoors etc.) ce poate transforma computerul într-un „zombie”, parte dintr-o rețea de tip botnet, controlat de către atacator.

2. Se folosesc, în măsura posibilităților, pachete software (sisteme operare și aplicații) ce beneficiază de suport din partea producătorului, pentru care update-uri de securitate sunt publicate periodic. Pachetele software ce nu mai beneficiază de suport tehnic (actualizări) nu vă pot oferi protecție împotriva ultimelor tipuri de atacuri sau variante de malware.

Dacă, din diverse motive, este necesară folosirea de pachete software ce nu mai beneficiază de suport din partea producătorului (declarate „end of life”), asigurați-vă de securizarea suplimentară a acestora prin instalarea de aplicații dezvoltate de terți (antimalware, firewall, aplicații de control parental etc.), care să acopere breșele de securitate neacoperite de producător.

3. Se folosește întotdeauna, indiferent de sistemul de operare sau tipul de echipament folosit, software de securitate de tip antimalware, care să dispună de multiple module de protecție (ex: antivirus, antispam, antirootkit, antiphishing, firewall, control parental etc.). În prezent, există variante de malware pentru fiecare tip de sistem de operare, instalat fie pe sisteme convenționale (desktop, laptop), fie pe dispozitive mobile (tablete, smartphone). Indiferent de soluția folosită, aceasta trebuie actualizată permanent.

4. Se securizează rețeaua locală wireless. În cazul în care se dispune de mai multe dispozitive ce necesită acces la internet și se folosește o rețea locală wireless, router-ul folosit pentru conectarea dispozitivelor și partajarea conexiunii la internet trebuie securizat corespunzător.

5. Se protejează corespunzător calculatorul sau dispozitivul folosit în comun de mai mulți membri ai familiei. Crearea de conturi de utilizator individuale sau folosirea de software de control parental sunt doar câteva din măsurile pe care se pot implementa.

6. Se folosesc parole puternice și nu se dezvăluie nimănui credențialele de acces la diferite aplicații, servicii sau sisteme.

7. Se navighează prudent pe internet și se acordă o atenție sporită informațiilor disponibile pe rețelele sociale (link-uri, aplicații etc.), acestea fiind folosite mai nou ca vector pentru distribuirea de malware.

8. Se evită folosirea calculatoarelor/dispozitivelor publice pentru accesarea diverselor servicii online (rețele socializare, aplicații de mesagerie instant etc.). De

asemenea, nu se realizează tranzacții financiare sau cumpărături online de pe calculatoarele/dispozitivele publice.

Bibliografie:

1. http://www.mcsi.ro/Strategie_Cyber
2. <http://www.cert-ro.eu/articol.php?idarticol=743>

DESPRE CRIPTOGRAFIE, CRIPTANALIZĂ ȘI CRIPTOLOGIE

Locotenent Adrian VĂTAFU
Centrul 105 Comunicații RMNC

**Criptografia**

este arta și știința ascunderii semnificației unei comunicări împotriva unor interceptări neautorizate. Cuvântul își are originile în limba greacă, unde înseamnă scriere ascunsă: kryptos graphen. Aceasta este o știință destul de veche, care s-a născut din

necesitatea de a transmite mesaje secrete și de a comunica eficient fără ca dușmanul să cunoască conținutul acestora.

Criptanaliza este actul obținerii textului clar sau a cheii din textul cifrat, care este folosit pentru obținerea informațiilor necesare acestui scop.

Criptologia, pe de altă parte, cuprinde atât criptografia, cât și criptanaliza. Aceasta poate fi împărțită în două subdiviziuni: transpoziția și substituția.

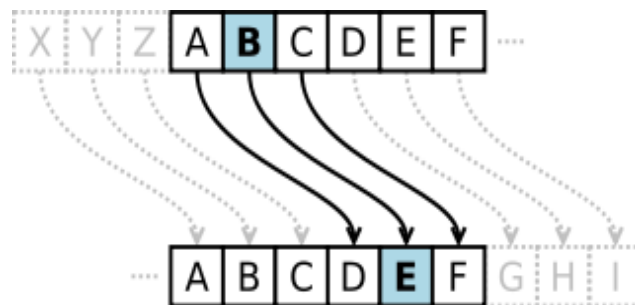
Transpoziția presupune ca literele dintr-un mesaj să fie pur și simplu rearanjate cu scopul de a crea anagrame. Această metodă este folosită în special pentru mesajele scurte și nu este foarte sigură având în vedere că, în acest caz, există un număr limitat de litere ce pot fi rearanjate relativ repede. În textele lungi, transpoziția oferă oarecare siguranță. Pe măsură ce numărul literelor crește, numărul combinațiilor posibile se multiplică, iar descifrarea mesajului se poate face doar cunoscând sau aflând procedeu exact de codificare.

Substituția, pe de altă parte, ca metodă de codificare, este una dintre cele mai vechi modalități de criptare și unele dintre cele mai vechi descrieri ale sale apar în Kama-sutra, text scris în secolul al IV-lea de învățatul brahman Vatasayana. Una dintre tehnicile recomandate de brahman este gruparea alfabetului pe perechi alese la întâmplare pentru ca, apoi, fiecare literă să fie substituită cu perechea ei.

A	C	F	H	I	J	N	O	R	S	Ș	T	U	V
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
G	L	P	B	Ă	Ț	D	Z	K	I	Ă	Q	M	X

NE VEDEM DISEARĂ => DÎ XÎNÎU NSÎGKI

Unul din primele cifruri cu substituție a fost **Cifrul lui Cezar**, numit și cifru cu deplasare, codul lui Cezar sau deplasarea lui Cezar. Este una dintre cele mai simple și mai cunoscute tehnici de criptare, în care fiecare literă din textul clar era înlocuită cu o literă aflată la un număr fix de poziții distanță de ea în alfabet. Cifrul a fost denumit astfel după Iulius Cezar despre care se spune că l-a folosit, cu o deplasare de 3, în comunicația cu generalii săi în timpul campaniilor militare. De exemplu, cu o deplasare de 3 poziții, A este înlocuit cu D, Ă devine E și așa mai departe.



Aplicarea cifrului lui Cezar asupra unui text oarecare constă în înlocuirea fiecărei litere din textul inițial cu una care se află la o distanță fixă în alfabet. Acest exemplu este cu o deplasare de trei poziții, astfel încât B din textul inițial devine E în textul criptat.

Ca orice alt cifru bazat pe substituții alfabetice, cifrul lui Cezar este simplu de descifrat și în practică nu oferă securitate suficientă.

Cifrul Vigenère folosește un cifru Cezar cu o deplasare diferită la fiecare poziție din text; valoarea deplasării este definită folosind un cuvânt-cheie care se repetă. Dacă o cheie este la fel de lungă ca și mesajul și aleasă aleatoriu, atunci acesta este un cifru care nu poate fi spart atât timp cât cheia este secretă. Cuvintele cheie mai scurte decât mesajul introduc un șablon ciclic care poate fi detectat cu o versiune statistică avansată a analizei frecvenței.

Textul clar: This is an example of the Vigenere Cipher

Cheia: vector

Textul cifrat: olklwjvrgqodkpghtkcixbuviiqxzklgk

Între timp, dându-și seama de importanța cifrului, marile puteri au optat pentru îmbunătățirea lui. Una din cele mai simple modificări a fost adoptarea **nulelor**, a acelor simboluri care nu înlocuiesc litere, ci care au rolul de a-l induce în eroare pe inamic.

Spargerea cifrului

Cifrul Cezar poate fi spart ușor chiar și având la dispoziție numai criptotextul. Pot fi luate în considerare două situații:

- atacatorul cunoaște (sau ghicește) că a fost folosită un fel de substituție simplă, dar nu neapărat o schemă Cezar;

- atacatorul știe că s-a folosit cifrul Cezar, dar nu cunoaște valoarea de deplasare.

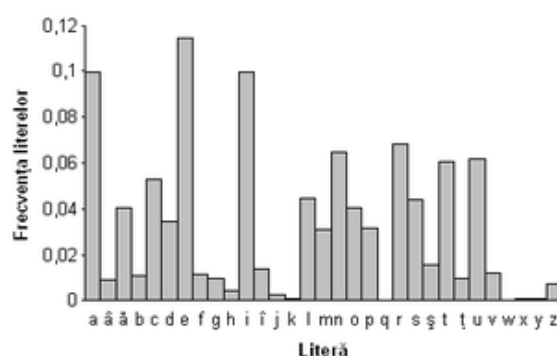
În primul caz, cifrul poate fi spart folosind aceeași tehnică ca pentru cazul general de substituție simplă, precum analiza frecvenței sau cuvinte șablon. În timpul decriptării, este foarte probabil ca atacatorul să observe regularitatea în soluție și să deducă că cifrul Cezar este algoritmul folosit.

În al doilea caz, spargerea schemei este mult mai simplă. Deoarece numărul de deplasări posibile e limitat (31 în română), fiecare din ele poate fi testată printr-un atac prin forță brută. O cale de a realiza acest lucru este de a scrie un fișier cu criptotextul într-un tabel cu toate deplasările posibile - tehnică numită uneori „completarea componentei normale”. Exemplul este dat pentru criptotextul „DXDHJȘUYDX”.

Deplasare în decriptare	Text candidat
0	dxdhjșuydx
1	cwcgîstxcw
2	bvbfirtwbv
3	âuâehqșvâu
4	ățădgpsuăț
5	atacforțat
6	zșzbenqtzș
7	ysyâdmpșys
...	
28	gagjmxăga
29	fzfîlțwafz
30	eyeiktvezey

Textul normal este imediat recognoscibil de ochi la valoarea cinci. O altă cale de a vizualiza această metodă este de a scrie sub fiecare literă alfabetul înapoi față de literă. Acest atac poate fi accelerat folosind șiruri cu alfabetul scris invers. Șirurile sunt apoi aliniate astfel încât criptotextul să apară pe un rând, iar astfel textul inițial va apărea pe un alt rând.

O altă abordare a atacului prin forță brută este identificarea literelor conform distribuției lor în limba în care a fost scris textul. Prin crearea graficului frecvențelor literelor din criptotext și prin cunoașterea distribuției obișnuite, un om poate descoperi valoarea deplasării prin observarea decalajului dintre anumite caracteristici ale graficului. Aceasta este cunoscută ca **analiza frecvenței**.



Distribuția literelor într-un text din limba română are o formă cunoscută și predictibilă. Un cifru Cezar rotește această distribuție și de aceea e posibilă aflarea valorii de deplasare prin analizarea graficului de frecvență rezultat.

Dezvoltarea criptanalizei a dus mai departe la dezvoltarea criptografiei.

Astfel, în anul 1918, inventatorul german Arthur Scherbius a construit o mașină criptografică care avea la bază discul de cifrare creat în secolul al XV-lea, o invenție a unui arhitect italian, pe numele său Leon Alberti. **Enigma**, așa cum a fost botezată mașina, a devenit în scurt timp cel mai de temut sistem de criptare din istorie. Cu ajutorul acestei mașini, expeditorul putea să tasteze textul în clar, iar mașina genera mesajul criptat. La rândul său, destinatarul, dotat și el cu o Enigma și un exemplar al cărții de coduri, tasta textul cifrat pentru a genera mesajul în clar. În acest caz, chiar dacă inamicul captura o astfel de mașină, decriptarea mesajului era una dificilă în lipsa configurațiilor inițiale folosite pentru scrierea mesajului. Fără cartea de coduri, inamicul trebuie

să încerce toate cele 17.576 configurații posibile de codare. Cu timpul, mașina a primit îmbunătățiri datorită cărora Germania ajunsese să se bucure de cel mai sigur sistem de comunicații din lume.

Mașina este dotată cu o tastatură prin care se introduce textul clar simbol cu simbol, iar la capătul celălalt (imprimantă sau tablou cu becuri) rezultă simbolurile criptate. Acestea sunt calculate în funcție de starea rotoarelor (care se actualizează cu fiecare tastă apăsată), rotoare care controlează traseele circuitelor electrice de la intrare la ieșire. Versiunile inițiale au fost simple, dar în mod constant s-au adăugat complicații la mecanism, pentru creșterea securității cifrului, cum ar fi creșterea numărului de rotoare și adăugarea unui tablou de prize prin care se puteau substitui suplimentar perechi de simboluri.

Deși cifrurile Enigma au slăbiciuni criptografice, în practică, doar în combinație cu alți factori semnificativi (greșeli de operare, defecte procedurale, o mașină sau un caiet de coduri capturate ocazional) criptografii Alianților au reușit să descifreze mesajele.

În al doilea Război Mondial, situația se schimbă, iar supremația în domeniul decriptării o dețin englezii, care au inventat dispozitivul de decodificare numit Colossus, artizanul principal fiind strălucitul matematician Alan Turing. Această mașinărie a fost considerată părintele computerului modern și a determinat dezvoltarea criptografiei în timpul ultimei jumătăți a secolului XX.

Timp de 2000 de ani, criptografia a fost importantă pentru regi, regine, guverne și armată, dar, odată cu apariția internetului și a revoluției digitale, ea facilitează și dezvoltarea afacerilor și chiar protejarea intimității.

Bibliografie:

- 1.<http://www.descopera.ro/cultura/10056537-criptografia-si-codurile-secrete-care-au-marcat-istoria>
- 2.http://ro.wikipedia.org/wiki/Cifrul_Cezar
- 3.http://ro.wikipedia.org/wiki/Mașina_Enigma
- 4.http://ro.wikipedia.org/wiki/Cifrul_Vigenere

VOICE OVER IP – SOLUȚIE UNIFICATĂ DE COMUNICAȚII CA PREMISĂ A COMUNICAȚIILOR INTELIGENTE

Sublocotenent Teodor MITREA

Batalionul Instrucție Comunicații și Informatică „Frații Buzești”

Abstract

Convergența serviciilor de voce, date a creat premisa trecerii la etapa de unificare a comunicațiilor și a celei de definire a comunicațiilor inteligente. Unificarea comunicațiilor a eliminat nivelul ridicat al latenței induse, prin unificarea interfețelor pentru managementul comunicațiilor. Deși dezvoltarea și implementarea tehnologiei VoIP nu este la început, organizațiile urmăresc tot mai mult implementarea unui management bazat pe instrumentele și serviciile puse la dispoziție de această tehnologie. Din păcate, potențialul acestei importante resurse tehnologice nu a fost pe deplin exploatat.



Introducere

Actualul context al comunicațiilor prin internet cunoaște o efervescentă tot mai crescută, oferind o gamă din ce în ce mai variată de servicii ce vin în întâmpinarea nevoilor utilizatorilor. În spatele acestor servicii recent apărute se află de cele mai multe ori tehnologii noi, ce oferă posibilitatea schimbului de date la viteze din ce în ce mai mari, noi paradigme de accesare a informației și, nu în ultimul rând, noi metode de partajare a resurselor din infrastructurile de comunicații existente.

Ritmul alert în care se dezvoltă și converg serviciile de telecomunicații și IT poate duce cu ușurință la apariția unor decalaje informaționale și, chiar dacă nu suntem specialiști, este vital să rămânem permanent informați cu privire la noutățile și realizările din aceste domenii pentru că implementarea și utilizarea eficientă a acestor servicii se reflectă direct în sporirea productivității organizației și în îmbunătățirea și simplificarea proceselor interne specifice. Astfel, schimbul de informații în timp real nu mai este doar un deziderat, noile tehnologii ne permit să rămânem permanent conectați, oriunde ne-am afla.

Convergența serviciilor de date, voce a creat premisa trecerii la etapa de unificare a comunicațiilor și a celei de definire a comunicațiilor inteligente. Tot mai frecvent, procesele interne specifice organizațiilor au de suferit din cauza lipsei de informații vitale din zona comunicațiilor care să dinamizeze procesele de management în scopul obținerii unui coeficient de productivitate superior. În cazul organizațiilor cu mai multe puncte de lucru sau angajați în diverse locații, acest mod de comunicare este

extrem de important și eficient. Unificarea comunicațiilor a eliminat astfel nivelul ridicat al latenței induse prin unificarea interfețelor pentru managementul comunicațiilor. Din păcate, potențialul acestei importante resurse tehnologice nu a fost pe deplin exploatat.



Fig. 1. Arhitectură orientată pe servicii.

Comunicațiile inteligente combină funcționalitățile comunicațiilor unificate cu aplicațiile de business, iar serviciile web și arhitecturile orientate pe servicii (SOA²¹) furnizează metoda prin care aplicațiile de business interacționează cu comunicațiile.

1. VoIP - soluție unificată de comunicații

VoIP (Voice over IP) este tehnologia care permite efectuarea de convorbiri telefonice și trimiterea faxurilor folosind rețeaua existentă bazată pe protocolul IP ca și infrastructură de voce, reușind să asigure o anumită calitate a serviciului (QoS – Quality of Service) și aducând un prim important beneficiu – reducerea costurilor asociate atât la implementare, cât și prin exploatare. VoIP poate fi primul pas către o soluție unificată de comunicații, un sistem complet de comunicații care îmbină vocea cu datele și video.

Utilizarea în masă a VoIP-ului a început în 2004 și a permis utilizatorilor să efectueze și să

²¹SOA (Service Oriented Architecture - Arhitectură software bazată pe servicii).

primească apeluri ca și în telefonia clasică. Apelurile VoIP sunt similare apelurilor clasice digitale implicând partea de semnalizare, canalul de transmitere și codarea (împachetarea vocii pentru a putea fi trimisă sub formă de pachete de date). Codecurile folosite sunt responsabile pentru calitatea transmisiei și lățimea de bandă ocupată de un apel. Cu cât un codec este mai performant, el conferă o calitate mai bună și o ocupare mai mică a benzii disponibile; aceste codec-uri au ajuns atât de performante, încât oferă calitate HD Voice²² la numai 6,4kbps.

2. Servicii VoIP

Orientarea pe servicii reprezintă abordarea în baza căreia poate fi organizată distribuirea resurselor IT într-o soluție integrată care fluidizează concentrările de informații și maximizează eficiența organizației. Orientarea pe servicii modularizează resursele IT, facilitând conectarea flexibilă și accesul la informațiile furnizate de diverse servicii prin utilizarea protocoalelor standard și a interfețelor convenționale. Arhitectura SOA furnizează principiile pe baza cărora se poate realiza transformarea resurselor IT eterogene, distribuite, de mare complexitate și inflexibile într-o variantă integrată, simplă și flexibilă a resurselor care pot fi mai ușor configurate în funcție de obiectivele organizației.

Într-o arhitectură *orientată pe servicii*, aplicațiile și serviciile utilizează protocoale comune în vederea comunicării, la care se adaugă un format comun, ce stă la baza schimbului de date. În plus, SOA furnizează o infrastructură pentru instalarea și avertizarea disponibilității serviciilor în rețea. Prin urmare, serviciile web pot fi utilizate la implementarea unei arhitecturi bazate pe servicii, care se constituie în elemente funcționale constitutive accesibile protocoalelor internet standard, care sunt independente de platformă și limbajele de programare. Comunicarea între aplicații în cadrul SOA se realizează cu ajutorul protocoalelor web și a limbajelor de marcare HTML, CCXML,

VoiceXML etc. La debutul său, SOA nu a interferat cu ideea convergenței comunicațiilor pentru că vocea și datele făceau parte din două paradigme diferite, dar care între timp au înregistrat un proces de unificare. Mai mult decât atât, SOA creează importante oportunități în industria telecom, prin faptul că vocea și datele pot interopera la nivelul serverelor HTTP. Aplicațiile pentru procesarea vocii sunt instalate și rulează pe serverele HTTP aparținând infrastructurii organizației și conectate la rețeaua de voce.



2.1. Telefonie IP

Convergența comunicațiilor a creionat începuturile VoIP, iar utilizarea WAN în cadrul organizației ca alternativă a rețelei publice de telefonie în scopul reducerii costurilor aferente convorbirilor *long-distance* a condus la o scădere a costurilor destinate comunicațiilor. Folosind rețeaua IP ca infrastructură de bază pentru telecomunicații, serviciile de telefonie IP reprezintă forma evoluată de telecomunicații (voce, fax, SMS și/sau aplicații voce-mesagerie) cu ajutorul căreia se poate realiza un management mai bun al costurilor, dar și al modului în care sunt utilizate aceste servicii de către beneficiari. În varianta tradițională a comunicațiilor, rețeaua de voce este separată de cea de date, convergența se realizează la nivelul end-user-ului, care transferă date, în principal manual, între sisteme.

2.2. Audio și videoconferință VoIP

Soluțiile de audio și videoconferință rezolvă pe de o parte necesitatea elementară de comunicare la distanță (voce), dar aduc în plus componenta de interacțiune directă, extraverbală, prin elementul video. Acest gen de soluție rezolvă necesitatea inițială de deplasare și atrage scăderi substanțiale de cheltuieli și efort.

Cu serviciul audioconferință se poate comunica în timp real între abonați aflați în locații diferite, fiind un instrument eficient de comunicare cu un număr mare de persoane aflate la distanță. Prin simpla apelare a unui număr dedicat, toți participanții se pot conecta la conferința audio, în locul unei întâlniri clasice într-o sală de ședințe. Aceste teleconferințe pot fi organizate de la birou, sau chiar de oriunde sunând de pe mobil sau notebook la numărul centrului de teleconferințe audio.

²²Presupune utilizarea tehnologiei de bandă largă pentru a oferi o claritate sporită și o mai bună experiență audio în comunicațiile VoIP. HD Voice îmbunătățește calitatea sunetului prin dublarea numărului de secvențe preluate pe secundă (16kHz) față de telefonia clasică (8kHz). În plus, zgomotul de fond e mult redus, pentru a permite o convorbire impecabilă, în care nu pierzi timp și bani rugând persoana de la capătul firului să repete ceea ce nu ai înțeles.

Noile tehnologii de videoconferință au depășit și provocările inițiale calitative – ca atare, în prezent, alegerea unei soluții optime va ține cont de posibilitatea acesteia de a asigura o cât mai bună calitate a imaginii și o utilizare minimă a benzii.

3. IP-PBX – simplu și eficient

Instalarea unui sistem PBX (o centrală telefonică) înseamnă uneori echipamente complexe ce trebuie instalate și întreținute. IP-PBX este o soluție flexibilă, gata de lucru în câteva ore și care nu necesită investiții în echipamente suplimentare, ci doar asigurarea telefoanelor de birou sau instalarea „softphones” pe stațiile de lucru disponibile.

Serviciile de telefonie furnizate sunt livrate prin rețeaua de date ca un serviciu PBX. Furnizorul menține infrastructura hardware, software și upgrade-ul periodic și alocă clienților numerele de telefon pentru recepționarea apelurilor. Abonații IP-PBX beneficiază de o varietate de facilități: pot transfera apelurile primite către altă locație sau către voicemail, pot înregistra convorbirile sau pot activa funcția IVR (Interactive Voice Response) pentru distribuția automată a apelurilor către extensii, ca în cazul unei centrale performante. Principalele beneficii pot fi sintetizate astfel:

- se reduc costurile operaționale;
- se asigură o calitate mai bună și fiabilitate crescută a serviciilor;
- se pot implementa funcții PBX avansate ce sporesc mobilitatea abonaților;
- disponibilitatea serviciilor indiferent de terminale: telefon VoIP sau clasic, smartphone, tabletă, PC;
- utilizarea optimă a lărgimii de bandă.

Prin serviciul SIP trunking se poate conecta centrala IP-PBX la rețeaua publică de telefonie (PSTN) pentru a realiza tranziția către serviciile multimedia VoIP. Serviciile de SIP trunking sunt o alternativă la circuitele telefonice digitale ISDN și elimină necesitatea achiziționării unor echipamente costisitoare de tipul BRI/PRI gateways. În plus, serviciile de SIP trunking deschid noi oportunități pentru integrarea aplicațiilor de comunicații unificate: mesagerie instant și prezență, video, Internet Fax etc.

SIP (Session Initiation Protocol) este protocolul de semnalizare destinat telefoniei IP și se bazează pe HTTP și MIME, elemente care îl fac ideal pentru integrarea aplicațiilor date-voce.

Trebuie menționat faptul că a fost proiectat pentru transmisii în timp real, fiind un consumator redus de resurse și mult mai simplu decât H.323, schema de adresare fiind una de tip URI (sip@domain.tld). SIP operează pe baza unui protocol de descriere a sesiunii SDP (Session Description Protocol) și a protocolului de transport în timp real RTP. SIP include posibilitatea de alertă legată de prezența unui utilizator în fluxul de procesare al unei cereri. Prezența este interpretată în acest context ca fiind capacitatea unui utilizator de a comunica cu alți utilizatori în rețea. Cu alte cuvinte, prezența a fost limitată la faptul că abonatul să fie „on-line”. Notificarea prezenței este realizată de definirea unui pachet de evenimente în contextul general al evenimentelor de notificare SIP.

4. Determinări ale noilor tehnologii asupra pregătirii specialiștilor

Instruirea de specialitate reprezintă una dintre cerințele esențiale pentru dezvoltarea competențelor, deprinderilor și aptitudinilor tehnice ale specialiștilor de comunicații și informatică necesare exploatarea sistemelor de comunicații unificate. Pentru asigurarea unui proces de instruire de înalt nivel calitativ este necesară elaborarea unor programe de studii care să ofere o imagine globală asupra rețelelor și serviciilor VoIP în vederea familiarizării cu noile tehnologii a celor care doresc să planifice, implementeze, administreze sau să evalueze rețele, aplicații sau servicii VoIP. Pregătirea tehnică teoretică completată de activitatea practic-aplicativă din cadrul laboratoarelor va contribui la formarea viitorilor specialiști pentru a face față noilor provocări și a valorifica potențialul resurselor tehnologiei VoIP.

Concluzii

Serviciile orientate spre comunicații vor juca un rol important în găsirea soluțiilor pentru managementul evenimentelor critice, dublate de realizarea unor conexiuni între decidenții importanți, de la nivelul organizației, în scopul agregării optime a competențelor necesare soluționării acestor evenimente.

Deși dezvoltarea și implementarea tehnologiei VoIP nu este la început, organizațiile urmăresc tot mai mult implementarea unui management bazat pe instrumentele și serviciile puse la dispoziție de această tehnologie. Succesul implementării unor astfel de soluții trebuie privit

ca o corelare între procesele de performanță, monitorizare și management proactiv în faza inițială a componentelor VoIP și a aplicațiilor integrate real time din cadrul organizației. Tehnologia Voice over IP a revoluționat modul în care se comunică în general și nu doar în ceea ce privește comunicațiile de voce.

Dezvoltarea VoIP a însemnat în primul rând una dintre primele strategii complete prin care sunt unificate elementele de voce, date și comunicații video. Fără îndoială că avantajele implementării tehnologiei VoIP sunt evidente, integrarea rețelelor ducând la scăderea costurilor de investiții și la îmbunătățirea productivității membrilor organizațiilor.

Bibliografie

1. Jim Van Meggelen, Leif Madsen, Jared Smith, *Asterisk™: The Future of Telephony, Second Edition*, O'Reilly Media, Inc., 2007
2. [Cristian Kevorchian](#), *Servicii Orientate Comunicații - o abordare introductivă*, 2013
3. Bruce Hartpence, *Packet Guide to Voice over IP*, O'Reilly Media, Inc., 2013
4. Timothy Kelly, *VoIP for dummies*, Wiley Publishing, Inc., Indianapolis, Indiana, 2005.
5. http://en.wikipedia.org/wiki/Voice_over_IP, accesat 2015
6. <http://voipfreak.net/how-voip-is-taking-place-in-the-communication-world/>, accesat 2015
7. <http://it.toolbox.com/blogs/voip-news/always-keep-voip-security-in-mind-65520>, accesat 2015
8. <http://it.toolbox.com/blogs/voip-news/4-top-trends-in-uc-and-voip-communications-65501>, accesat 2015
9. <http://www.voipsupply.com/hd-voice-codecs>, accesat 2015

RĂZBOIUL BAZAT PE REȚEA ȘI IMPORTANȚA SPECIALIȘTILOR DE COMUNICAȚII ȘI INFORMATICĂ

Sublocotenent Alexandra-Cerasela AVRAM

Centrul 54 Comunicații R.M.N.C.

Motto: „Războiul este o problemă de o importanță vitală pentru Stat, domeniu al vieții și al morții, calea care duce spre supraviețuire sau nimicire. E necesar să fie studiat temeinic.”

Sun Tzu



Revoluția permanentă ce are loc în domeniul tehnicii și științei, în special în dezvoltarea tehnologiei informațiilor, cu un impact imediat în domeniul militar, a determinat schimbări profunde în gândirea militară contemporană

prin apariția unor concepte noi de ducere a războiului, modificarea continuă și rapidă a tacticilor, strategiilor, tehnicilor, metodelor și procedurilor de desfășurare a acțiunilor militare.

Viitorul război nu se va mai manifesta numai prin luptă armată, ci și prin alte forme și mijloace politice, mediatice, economice, informaționale și psihologice. Esența violenței va avea la bază întrebuintarea noilor arme și tehnologii care permit confruntarea în spațiul cibernetic. În acest context, cea mai dezbătută și importantă temă a ultimilor ani, prin multilateralitatea și complexitatea sa, este conceptul de război centrat pe rețele NCW (*Network Centric Warfare*), cunoscut și ca războiul bazat pe rețea (RBR).

Începuturile RBR se află în ceea ce militarii numesc „sistemul nervos” al războiului și al oricărui sistem militar, adică sistemul de comunicații. Ducerea acestui tip de război presupune utilizarea rețelelor integrate de calculatoare și de comunicații pentru comanda și controlul acțiunilor militare în contextul mai larg al sistemelor C4I2SR (comandă, control, comunicații, calculatoare, informații și informatică, supraveghere și recunoaștere).

Acest concept este definit „drept o modalitate de a genera putere de luptă prin integrare într-o rețea informațională a senzorilor, decidenților și executanților în scopul cunoașterii cuprinzătoare și permanente a spațiului de luptă,

măririi eficienței conducerii (prin viteză, forță și stabilitate), accelerării dinamicii operațiilor (prin ritm, intensitate și densitate adecvate), realizării sinergiei efectelor planificate pe obiective, sporirii viabilității și obținerii unui anumit grad de autosincronizare acțională”[1].

Fundamentul RBR îl reprezintă comunicarea în rețea. Această comunicare nu se realizează pe principiul rețelelor clasice de transmisiuni (unul vorbește, ceilalți ascultă, fiecare așteptându-și rândul să poată vorbi, în funcție de priorități prestabilite), ci pe rețele care asigură o comunicare complexă (simultană, selectivă și direcțională, în timp real, în funcție de cerințele concrete ale misiunii).

„Un sistem militar de comunicații flexibil, dinamic, complex și în permanentă funcționare este alcătuit din patru componente esențiale: informația, infrastructurile de comunicații, rețelele virtuale și sistemele de comunicare”[2]. Tehnologia de vârf și tehnologia informației permit, în prezent, realizarea maximă a tuturor acestor caracteristici, nu doar la nivelul unei structuri militare, ci și la nivelul teatrelor de operații.

Pentru a acționa potrivit exigențelor conceptului RBR, pregătirea forțelor trebuie să se axeze, în principal, pe formarea abilităților necesare folosirii eficiente a informației în rețea. Acest aspect necesită adaptarea rapidă la cerințele lucrului în rețea, cunoașterea și folosirea calculatorului și modului de acces în bazele de date. În același timp, specializarea forțelor în RBR cere o bună cunoaștere a filozofiei acestui tip de război și o bază solidă de cunoștințe în domeniul tehnologiei informației și funcționării rețelelor de informații, mai ales a internetului. De asemenea, impune un înalt profesionalism și o capacitate deosebită de cunoaștere a evoluției momentelor semnificative ale operației.

Resursa umană specializată în exploatarea sistemelor de comunicații și informatice trebuie

să-și dezvolte continuu pregătirea în instituțiile de învățământ militar, astfel încât să poată asigura funcționarea continuă a acestor sisteme în condiții de securitate. În același timp, trebuie armonizată dinamica pregătirii specialiștilor militari în domeniul comunicațiilor și informaticii cu dinamica introducerii în exploatare a noilor sisteme care vor opera în cadrul conceptului de RBR.

„Evitarea surprinderii în domeniul informațional va fi una din tendințele dominante ale următorilor ani” [3], de aceea militarii specializați în domeniile comunicații și informatică și tehnică de calcul pregătiți în centrele de instruire vor juca un rol foarte

important folosind informația culeasă din spațiul virtual în avantajul trupelor proprii și totodată în menținerea securității sistemelor și rețelelor informatice și de comunicații militare, protejându-le de spionajul electronic și scurgerea de informații.

Esența conceptului de RBR constă în faptul că nu câștigă războiul cel care are cea mai mare cantitate de forțe, ci acela care are cele mai bune informații și comunicații, astfel, fiecare unitate militară trebuie să dispună atât de tehnică performantă, cât și de specialiști care să fie în măsură să exploateze tehnica respectivă la cele mai înalte standarde.

NOTE BIBLIOGRAFICE

1. Constantin ONIȘOR, Constantin MOȘTOFLEI, *Aspecte teoretico-metodologice și modalități practice de aplicare a conceptului "Război bazat pe rețea" în Armata României, corespunzător structurii de forțe 2007*, București, 2003;
2. Constantin TOCILĂ, Octavian ANGHEL, *Războiul bazat pe rețea-componentă activă a conceptului C4I2SR. Aplicații ale acestuia în operațiile speciale*, Buletinul Forțelor Terestre nr.2 din 2010;
3. Vasile PAUL, *Colocviu strategic Nr.6*, București, 2005.
4. http://www.rtf.forter.ro/2010_2_t/02-fm/03.html
5. <http://www.ro.scribd.com/doc/12516360/Referat-Razboiul-bazat-pe-retea#scribd>
6. http://www.cssas.unap.ro/ro/pdf_studii/rbr_in_fizionomia_noilor_conflicte_militare.pdf
7. http://www.cssas.unap.ro/ro/pdf_carti/rbr_si_viitorul_actiunilor_militare.pdf

STANDARDUL IEEE 802.11 ÎN REȚELELE DE COMUNICAȚII WIRELESS

Sublocotenent Daniel RISTEA

Batalionul Instrucție Comunicații și Informatică „Frații Buzești”



Nevoia de comunicare a oamenilor a presupus o permanentă dezvoltare a mediilor de transmitere a informațiilor, pornind de la cabluri și fire până la undele radio.

Mi-am propus prin acest articol să prezint câteva diferențe între rețelele bazate pe fire și rețelele bazate pe unde radio, respectiv implementarea și utilizarea acestora în mediul contemporan.

În prima parte a lucrării am pus în evidență avantajele și dezavantajele folosirii acestor tipuri de rețele, iar în a doua parte am prezentat standardele care au făcut posibilă utilizarea rețelelor wireless la nivel local, precum și evoluția acestora de-a lungul timpului.

O rețea wireless (Wi-Fi) WLAN este o rețea fără fir, locală, extinsă pe arii limitate, în funcție de echipamentele folosite și de puterea acestora, prin care se poate face transfer de date și internet folosind undele radio.

Wi-Fi - reprezintă o categorie de produse compatibile cu standardele WLAN bazate pe protocoale IEEE 802.11.

Noile standarde care au precedat specificațiile 802.11, cum ar fi 802.16 (WiMAX), fac parte din rețelele actuale și oferă multe îmbunătățiri, de la arii mari de acoperire până la viteze mari de transfer.

Diferențele între o rețea terestră și o rețea wireless radio:

1. Spre deosebire de alte sisteme radio, Wi-Fi folosește un spectru de frecvențe radio care nu au nevoie de licență, deci nu necesită aprobare pentru utilizare.

2. Se permite dezvoltarea variată a unei rețele locale WLAN fără utilizarea cablurilor, reducând costurile necesare dezvoltării rețelei și evitând diferite obstacole în implementarea rețelei (locuri inaccesibile, care nu pot fi cablate)

3. Multe rețele Wi-Fi suportă roaming, permițând unui client să se mute dintr-un punct de acces în altul în aceeași clădire sau zonă geografică.

4. Wi-Fi este un standard global, clienții Wi-Fi putând lucra în diferite țări de pe glob.

5. Posibilități variate de conectare a utilizatorului final, prin intermediul plăcilor Wi-Fi PCMCIA, PCI, USB sau a variatelor sisteme Wi-Fi 802.11b sau 802.11g integrate în majoritatea notebook-urilor moderne.

O infrastructură wireless poate fi realizată astăzi cu cheltuieli mult mai mici decât una tradițională pe cablu.

În acest fel, apar premisele realizării accesului ieftin și ușor la internet membrilor comunităților locale, cu toate beneficiile ce rezultă de aici.

Accesul la informația globală constituie o sursă de bogăție la scară locală, prin creșterea productivității muncii bazate pe accesul la cvasitotalitatea informațiilor disponibile în lume în legătură cu activitatea prestată.

Totodată, rețeaua devine mai valoroasă pe măsură ce tot mai mulți oameni se leagă la ea. Comunitățile legate la internet au acces la piața mondială unde au loc tot mai multe tranzacții cu viteza rețelei.

În același timp, accesul la internet le dă oamenilor posibilitatea de a discuta despre problemele lor, despre politică și orice altceva ce-i interesează în modalități pe care telefonul sau televizorul nu le puteau pune la dispoziție.

Chiar și fără accesul la internet, comunitățile legate la rețele wireless se bucură de avantaje:

- pot colabora la diferite proiecte cu întindere geografică mare folosind comunicații vocale;
- e-mail-uri;
- transmisii de date cu costuri foarte mici.

În ultimă instanță, oamenii înțeleg că aceste rețele sunt realizate pentru a intra mai ușor în legătură unii cu alții.

Wireless LAN, cunoscut și sub denumirile de WLAN, 802.11 sau WiFi, deși este cea mai

recentă metodă de conectare, a cunoscut în ultimii ani o creștere fără precedent a popularității.

Această popularitate se datorează chiar principalei sale caracteristici: lipsa cablurilor. Calculatorul se află în rețea fără să aibă nevoie de cabluri sau conectori.

Este un vis devenit realitate pentru cei care folosesc PC-uri mobile (laptop-uri sau PDA-uri) și care obțin o libertate totală de mișcare în interiorul ariei acoperite de rețeaua wireless. Rețeaua wireless are drept componentă principală un echipament care se numește Punct de Acces. El este un releu care emite și receptează unde radio către dispozitive, respectiv de la dispozitivele din raza sa de acțiune.

Există însă și dezavantaje în cazul rețelelor wireless.

- Pe lângă cea mai ușoară utilizare și cea mai mare flexibilitate, o rețea wireless este totodată și cea mai expusă din punct de vedere al vulnerabilității la interceptări neautorizate.

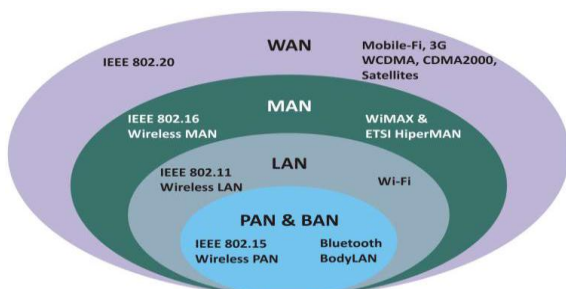
- La nivelul fizic, oricine poate să acceseze o rețea wireless.

- Datele (informațiile) pot trece prin ferestre, la fel de bine cum pot trece și prin pereții subțiri în birourile obișnuite.

- Din fericire, nu este suficient în general, să ai acces la nivelul fizic pentru a obține și accesul efectiv la rețea, deoarece producătorii echipamentelor de comunicații au conceput modalități de criptare a informațiilor care să le facă inaccesibile intrușilor.

- Securitatea rețelelor wireless este un punct de discuție foarte aprins, deoarece, din motive de necunoaștere a utilizatorilor sau de neprofesionalism al administratorilor, ori pentru a permite conectarea ușoară, aceste caracteristici de protecție nu sunt întotdeauna activate.

Standardul WiFi într-o schemă globală a standardelor wireless:



Standardul IEEE 802.11 a fost inițiat în 1990 și finalizat în 1997 pentru a acoperi rețelele

care asigură conexiuni wireless între stații fixe, portabile și în mișcare pe arie locală.

În loc de un singur standard (IEEE 802.11b), există un întreg alfabet de variante wireless din care utilizatorii pot alege: 802.11a, 802.11b, 802.11g și 802.11h concurează pentru preferința userului, ca tehnologii de bază, cu 802.11n așteptând la rând. Iar 802.11c, 802.11d, 802.11e, 802.11f și 802.11i adaugă încă puțină culoare acestui amestec.

IEEE 802.11

Prezentare generală

802.11a	54 Mbps WLAN în banda de 5 GHz
802.11b	11 Mbps WLAN în banda de 2,4 GHz
802.11c	Wireless bridging
802.11d	„World Mode”, adaptare la cerințele regionale
802.11e	QoS și extensii streaming pentru 802.11a/g/h
802.11f	Roaming pentru 802.11 a/g/h (Inter Access Point protocol IAPP)
802.11g	54 Mbps WLAN în banda de 2,4 GHz
802.11h	802.11a cu DFS și TPC, „11a Europe”
802.11i	Autentificare și criptare (AES, 802.1x)
802.11j	802.11a cu canale adiționale peste 4,9 GHz, „11a Japan”
802.11k	Schimb de informații de capabilitate între client și Access Point
802.11l	Nu este utilizat
802.11m	Actualizare - publicarea actualizărilor standardului
802.11n	„Next Generation WLAN” cu cel puțin 100 Mbps
802.11ad	Rată de transfer de până la 7 Gbit/s

Rețelele wireless se împart în două clase importante, factorul decisiv fiind lățimea de bandă utilizată.

Tehnologiile moștenite folosesc banda de 2,4 GHz, în timp ce variantele ulterioare folosesc banda mai lată, de 5 GHz.

1. Prima clasă include standardul IEEE 802.11b (11 Mbps) și succesul său, 802.11g (54 Mbps). Această primă clasă (banda 2,4 GHz) este, în prezent, cea mai frecventă opțiune.

2. Pe de altă parte, 802.11a și 802.11h, ambele putând să obțină o rată nominală de 54 Mbps, operează în banda de 5 GHz.

IEEE 802.11b

- a fost ratificat de IEEE în 16 septembrie 1999 și este, probabil, cel mai popular protocol de rețea wireless utilizat în prezent;

- utilizează tipul de modulație DSSS;

- operează în banda de frecvențe ISM; nu sunt necesare licențe atât timp cât se utilizează aparatură standardizată;

Limitările sunt:

- puterea la ieșire de până la 1 watt;
- modulațiile numai de tipul celor care au dispersia spectrului cuprinsă între 2,412 GHz și 2,484 GHz;
- are o viteză maximă de 11 Mbps cu viteze utilizate în prezent de aproximativ 5 Mbps.

IEEE 802.11g

- a fost ratificat în iunie 2003;
- în ciuda startului întârziat, acest protocol este în prezent protocolul standard în rețelele wireless, deoarece este implementat practic pe toate laptopurile care au placă wireless și pe majoritatea celorlalte dispozitive portabile;
- folosește aceeași subbandă de frecvențe din banda ISM ca și 802.11b, dar folosește tipul de modulație OFDM;
- viteza maximă de transfer a datelor este de 54 Mbps, cu implementări practice la 25 Mbps;
- viteza poate coborî până la 11 Mbps sau chiar la valori mai mici, trecând la tipul de modulație DSSS, pentru a se realiza compatibilitatea cu mult mai popularul protocol 802.11b.

IEEE 802.11a

- a fost ratificat de IEEE în 16 septembrie 1999;
- utilizează tipul de modulație OFDM;
- are o viteză maximă de 54 Mbps cu implementări practice de până la 27 Mbps;
- operează în banda ISM între 5,745 GHz și 5,805 GHz și în banda UNII între 5,170 și 5,320 GHz;
- aceasta îl face incompatibil cu 802.11b sau 802.11g;
- frecvenței utilizate mai mari îi corespunde o bătaie mai mică la aceeași putere de ieșire și, cu toate că în subgamele utilizate spectrul de frecvențe este mai liber în comparație cu cel din jurul frecvenței de 2,4 GHz, în unele zone din lume, folosirea acestor frecvențe nu este legală;
- de aceea, echipamentele cu protocolul 802.11a, cu toate că sunt ieftine, nu sunt nici pe departe la fel de populare ca cele cu 802.11b/g.

IEEE 802.11h

- este numită în SUA o „problemă de compatibilitate în Europa”, este varianta europeană a standardului American;

- cele mai importante funcționalități ale acesteia sunt selectarea dinamică a frecvenței și puterea variabilă a transmițătorului, pe care ETSI o mandatează pentru piața europeană pentru a se asigura că sistemele au o putere a transmițătorului rezonabilă.

IEEE 802.11c

- specifică metodei de wireless bridging, adică metode de conectare a unor tipuri diferite de rețele prin mijloace wireless.

IEEE 802.11d

- este numit și „World Mode”: acest lucru se referă la diferențele regionale din tehnologii, de exemplu cât de multe și care canale sunt disponibile pentru utilizare și în care regiuni ale lumii;

- userul trebuie doar să numească țara în care dorește să folosească placa WLAN și driverul se ocupă de restul.

IEEE 802.11e

- definește Quality-of-Service și extensiile streaming pentru 802.11a/h și g;
- scopul este de a îmbunătăți rețelele de 54 Mbps pentru aplicații multimedia și Voice over IP, adică, telefonie prin rețele IP și internet;
- pentru a fi utilizate cu multimedia și voce, rețeaua trebuie să suporte ratele garantate pentru fiecare serviciu, cu întârzieri minime de propagare.

IEEE 802.11f

- descrie metodele de schimbare a standardului („Roaming”) între access point-uri, iar IAPP se ocupă de detalii.

IEEE 802.11i

- a fost conceput pentru a soluționa problemele de securitate existente în domeniu până în momentul acela. Integrează tot ce poate oferi lumea securității;

- printre principalele funcționalități ale 802.11i se numără autentificarea IEEE 802.1x, cu EAP, RADIUS și Kerberos, precum și criptare bazată pe algoritmul Rijndael AES.

IEEE 802.11n-2009

- folosește frecvența de 2,4 GHz sau 5GHz;
- îmbunătățește semnificativ transferul de date de la (802.11a, 802.11g) - 54 Mbit/s până la 600 Mbit/s => amenințare pentru FastEthernet și o platformă posibilă pentru telefonie și semnale video;

- compatibil cu standardele anterioare.

IEEE 802.11ad – WiGig

- standard anunțat din 2009;

- 2011 – versiunea 1.1;
- folosește banda de 2,4, 5, 50 GHz;
- rata de transfer de până la 7Gbit/s (de 10 ori mai rapid decât rata maximă 802.11n);
- menține compatibilitatea cu standardele existente.

Concluzii

Evoluția standardelor care stau la baza rețelelor wireless este în plină concordanță cu dezvoltarea tehnologiei și a echipamentelor necesare realizării de rețele wireless.

Fiecare nou standard aduce îmbunătățiri, una dintre cele mai importante fiind creșterea ratei

de transmitere a informației, ceea ce presupune acces rapid la informații și nu numai.

În mediul militar, folosirea rețelelor wireless are mare importanță la nivel tactic, ținând cont de faptul că la acest nivel este nevoie de o cunoaștere cât mai detaliată a situației tactice în timp real și a cât mai multor informații care să sprijine luptătorul în îndeplinirea misiunii.

Concluzionez că tehnologia, standardele și tot ce implică acestea țin pasul cu nevoia omului de comunicare și îl sprijină în desfășurarea activităților de zi cu zi.

Abrevieri

IEEE – Institute of Electrical and Electronics Engineers
 Wi-Fi – Wireless Fidelity
 WLAN – Wireless Local Area Networks
 WiMAX – Worldwide Interoperability for Microwave Access
 PCMCIA – Personal Computer Memory Card International Association
 PCI – Peripheral Component Interconnect
 USB – Universal Serial Bus
 PC – Personal Computer
 PDA – Personal Digital Assistant
 QoS – Quality of Service
 IAPP – Inter Access Point Protocol
 DFS – Dynamic Frequency Selection
 TPC – Transmit Power Control
 DSSS – Direct Sequence Spread Spectrum
 ISM – Industrial, Scientific and Medical
 OFDM – Orthogonal Frequency Division Multiplexing
 UNII – Unlicensed National Information Infrastructure
 ETSI – European Telecommunications Standards Institute
 IP – Internet Protocol
 EAP – Extensible Authentication Protocol
 RADIUS – Remote Authentication Dial In User Service
 AES – Advanced Encryption Standard

Bibliografie

- http://ro.wikipedia.org/wiki/Re%C8%9Bea_f%C4%83r%C4%83_fir
- <http://profs.info.uaic.ro/~busaco/teach/courses/net/presentations/net11.pdf>
- <http://ro.wikipedia.org/wiki/Wi-Fi>
- http://www.runceanu.ro/adrian/wp-content/cursuri/retele2013/RC_C10_2013.pdf

RADIORELELE GERMANE DIN CEL DE-AL DOILEA RĂZBOI MONDIAL

Locotenent-colonel Cătălin DASCĂLU

Comandamentul Comunicațiilor și Informaticii

În cel de-al Doilea Război Mondial, în iarna 1942-1943, pe timpul Bătăliei de la Stalingrad, sovieticii au ajuns la concluzia că gruparea germană înconjurată, condusă de generalul Friedrich Paulus, are o conexiune directă cu armata germană din afara încercuirii. În urma controlului radio, executat de Armata Roșie în gama undelor scurte, s-a concluzionat că există o legătură fir îngropată. Astfel, sovieticii au început, în plină iarnă, să sape un șanț în partea de vest a încercuirii în căutarea unui cablu secret.²³

În realitate, germanii utilizau **stații radioreleu pe microunde Michael** în gama undelor decimetrice. Totuși, datorită dimensiunilor mari ale antenelor (catarg telescopic hidraulic cu înălțimea de 30m), ele se puteau utiliza doar e timp de noapte, pentru ca avioanele de vânătoare sovietice să nu le observe.²⁴

Din păcate, referințele găsite nu oferă foarte multe informații despre radiorelele germane pe unde decimetrice din anii 30-40, cele mai multe rezumându-se la denumirea stațiilor și la gama de frecvențe. Totuși, o parte din acestea le voi prezenta mai jos.

În anii 1930, Ministerul german al forțelor aeriene (RLM) a solicitat firmei *Telefunken* realizarea unui sistem de legături radio de încredere („*Richtfunkverkehr*”, abreviat RV).

Prima variantă, fixă, DMG 1G Umbauanlage, opera în gama de frecvențe 500-535,7 MHz și avea emițătorul și receptorul montate direct pe catargul antenei. Stația asigură un canal telefonic ce putea fi multiplexat în trei canale telegrafice. Această versiune a fost testată de armata germană pe timpul manevrelor de toamnă din 1936.

Stațiile fixe au fost ulterior fabricate în variantă mobilă. Acestea lucrau în gama de frecvențe de 555-625 MHz, cu o putere de 200 mW.

O variantă comercială cu numele de *Olympia* (de tip DMG 2G) a fost produsă în anii

1936 și 1937 și a fost folosită pentru asigurarea legăturilor pe timpul Jocurilor Olimpice de la Berlin (1936).

La următoarea variantă îmbunătățită din 1938, *Michael DMG 4K*, emițătorul și receptorul au fost retrase de pe antenă, legătura cu aceasta făcându-se printr-un cablu de radiofrecvență. Aceasta asigură un canal telefonic (cu posibilitatea a fi multiplexat secundar cu trei canale telegrafice) și un canal telegrafic. Gama de frecvențe – 500-560 MHz.

Versiunea *Michael DMG 5K* lucra în gama 502 – 554,2 MHz cu o putere 700 mW. Stațiile au fost instalate pe autocamioane, dintre care unul transporta aparatura propriu-zisă și altul antena. Pentru a funcționa ca stație radioreleu, erau necesare două stații cu două antene.²⁵

Produs în 1943, *DMG 7K Michael/lang* avea gama de frecvențe 442,5 – 497,5 MHz (fig. 1).



Fig.1: Michael DMG 7K

Pe scurt, variantele produse de *Telefunken* au fost cele de mai jos:

- 1936/37 DMG 1G Umbauanlage 1/36;
- 1936 DMG 2G Olympia-Mastanlage;
- 1938 DMG 4K Michael I;
- 1940 DMG 4aK Michael II;
- 1942 DMG 5K Michael IIR;
- 1944 DMG 5aK Michael II aR;

²³<http://russianarms.mybb.ru/viewtopic.php?id=302>

²⁴ Arthur O. Bauer, *Some aspects of military line communication as deployed by the German armed forces prior to 1945*, pe http://www.cdvanndt.org/line_communications.htm

²⁵ *Richtverbindungs-(RV) Geräte von Telefunken*, pe <http://www.geschichtsspuren.de/forum/richtverbindungs-rv-gerate-von-telefunken-t17879.html>

- 1943 DMG 7K Michael/lang;
- 1944 DMG 7aK Michael/lang a.

Principalele caracteristici ale stației radioreleu **DMG 5K Michael IIR** sunt următoarele²⁶:

Destinație: pentru realizarea comunicațiilor fără fir pe o distanță de circa 50-100 km, în funcție de condițiile de vizibilitate directă; în cazul în care receptorul este în afara sectorului de radiație a antenei de emisie se utilizează stații de retranslație.

Gama de frecvențe: 502-554,2MHz (59,76-54,10cm).

Bătaie: 50-100 km, în funcție de vizibilitatea directă.

Canale: două

- canalul I – telefonic pe două sau patru fire (lățime de bandă de 300-5500 Hz) sau multiplexat secundar cu 3 canale telegrafice (pe două tonuri);
 - canalul II - telegrafic pe patru fire cu două tonuri cu frecvențele de 7400 Hz și 8000 Hz.
- Viteză manipulare 120 baud.

Ambele canale operează independent.

Moduri de lucru:

- stație terminală;
- releu. În această situație sunt necesare două baze de operare.

Finisaj: cadru cu cinci sertare extensibile (figura 2):

- I – blocul emițător;
- II – blocul receptor;
- III – blocul canalelor telegrafice;
- IV – blocul de joasă frecvență;
- V – blocul de alimentare.

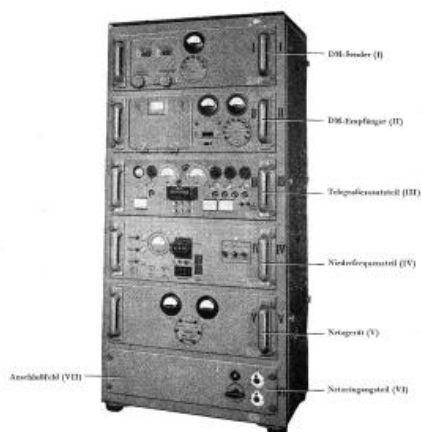


Fig.2: Michael DMG 5K

Pe partea de jos a cadrului sunt rețeaua de intrare (VI) și cutia de borne (VII).

Alimentare: rețea 220V c.a.

Consum de energie: circa 220 de wați.

Dimensiuni: 1170 x 540 x 380 mm.

Greutate: circa 150 kg.

Antene: de bandă largă în cutie din lemn contra intemperiilor (fig. 3).



Fig.3: Antena de bandă largă Michael

În figura 4 este reprezentată harta cu liniile radioreleu realizate cu stații *Michael* în sprijinul Luftwaffe pe timpul celui de-al Doilea Război Mondial. Cu linii punctate sunt reprezentate liniile realizate cu stații mobile. În total, lungimea liniilor instalate măsura peste 50.000 km.²⁷



Fig.4: Rețeaua radioreleu Michael

Între anii 1938-1941, a fost dezvoltată stația multicanal decimetrică *Rudolf DMG*. Stația funcționa în gama 600-652 MHz și asigura 9 canale telefonice sau 27 telegrafice.

Variantele *Rudolf* au fost:

- 1941/42 DMG 3G Rudolf;
- 1943 DMG 3aG Rudolf.

²⁶Dezimetergerät DMG 5K, Der Reichsminister der Luftfahrt und Oberbefehlshaber der Luftwaffe, Berlin, 17 martie 1942

²⁷Kurt Bolliger, *Richtstrahl im Kriege*, Allgemeine schweizerische Militärzeitschrift: ASMZ, vol. 120, 1954, pe http://retro.seals.ch/digbib/browse5_3

Principalele caracteristici ale stației radioreleu **DMG 3G Rudolf**²⁸ sunt următoarele:

Destinație: este utilizat pentru realizarea comunicațiilor fără fir în condiții de vizibilitate directă de până la 100 km, cu ajutorul turnurilor de antenă. Având în vedere că utilizează antene direcționale, interceptarea în afara sectorului de radiații este imposibilă.

Gama de frecvențe: 600-652MHz (50-46 cm).

Canale: nouă canale telefonice, fiecare poate fi multiplexat secundar cu 3 canale telegrafice.

Moduri de lucru:

- stație terminală;
- releu.

Finisaj: cadru cu cinci sertare extensibile (fig. 5):

- I – blocul emițător;
- II – blocul receptor;
- III – unitate de operare;
- III – blocul de alimentare;
- IV – blocul echipamentelor de înaltă tensiune.

Pe partea de jos a cadrului este cutia de borne.

Alimentare: rețea 220V c.a.

Antene: de bandă largă.



Fig.5: Rudolf DMG 3G

Principalele caracteristici ale stației radioreleu **DMG 3aG Rudolf**²⁹ sunt următoarele:

Destinație: este un transmițător/receptor radio în gama undelor decimetrice (46-50 cm), utilizat pentru realizarea legăturilor direcționale.

Gama de frecvențe: 600-652 MHz (50-46cm).

Canale: nouă canale telefonice, fiecare poate fi multiplexat secundar cu 3 canale telegrafice.

Moduri de lucru:

- stație terminală;
- releu.

Finisaj: cadru cu cinci sertare extensibile (fig. 6):

- I – blocul emițător;
- II – blocul receptor;
- III – unitate de operare;
- III – blocul de alimentare pentru receptor;
- IV – blocul de alimentare pentru emițător;
- V – blocul de alimentare.

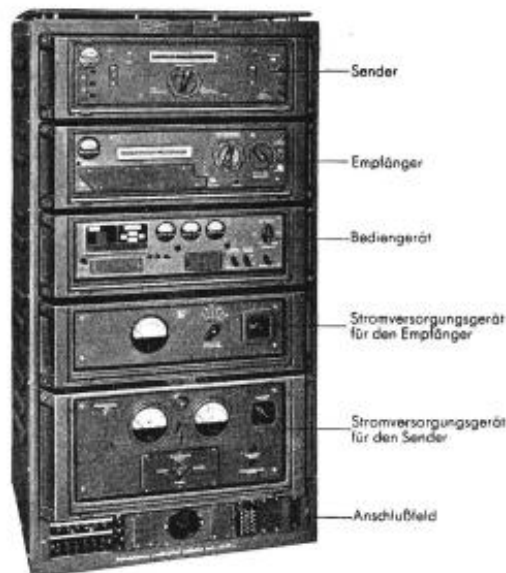


Fig.6: Rudolf DMG 3aG

Pe partea de jos a cadrului este cutia de borne.

Alimentare: rețea 220V c.a.

Dimensiuni: 1075 x 586 x 536 mm.

Greutate: 210 kg, inclusiv suportul gol de 56 kg.

Antene: de bandă largă, fixă BAO3 (Breitbandantenne ortsfest – antenă de bandă largă staționară) – figura 7 și motorizată BAB3 (Breitbandantenne beweglich – antenă de bandă largă mobilă) – figura 8

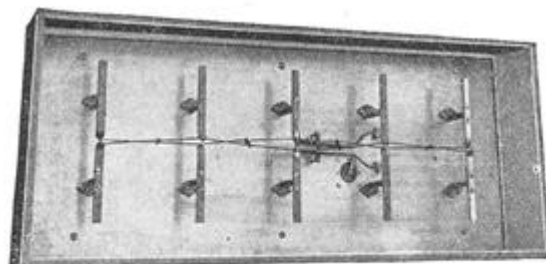


Fig.7: Antena BAO3

²⁸Dezimetergerät DMG 3G, Der Reichsminister der Luftfahrt und Oberbefehlshaber der Luftwaffe, Berlin, 22 iunie 1941

²⁹Dezimetergerät DMG 3aG, Der Reichsminister der Luftfahrt, Berlin, 22 aprilie 1944

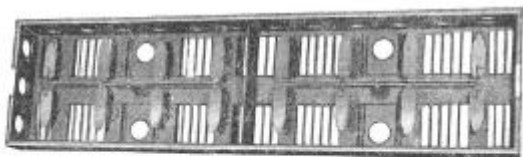


Fig.8: Antena BAB3

Lorentz a produs pentru armata germană două tipuri de echipamente pe microunde.

În 1938, stația de tip *FlorianDMG 3K* ce funcționa în gama 476-529 MHz cu o putere de 50mW și asigură două canale telefonice. De asemenea, a produs și echipamentele *Stuttgart I și II - Fu G 03* cu 10 canale în gama 1250-1400 MHz.³⁰

Varianta modernizată, *Stuttgart III*, a fost produsă după terminarea războiului și cu destinație civilă, cu denumirea de *RVG 901* (figura 9).³¹

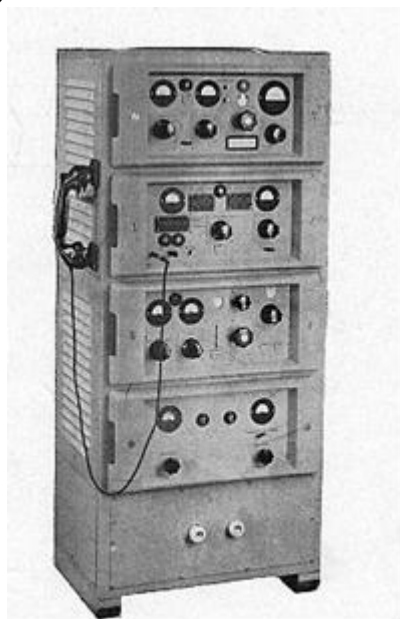


Fig.9: Stuttgart III (RVG 901)

După terminarea războiului și în anii '50, sovieticii au luat, ca despăgubiri din Germania de Est, printre altele, și stații radioreleu civile și militare de diferite tipuri pe care le-au transportat în U.R.S.S.³² Pe baza studiului asupra acestor

stații, în special de tip *Michael* și *Stuttgart*, la începutul anului 1946, au demarat o serie de cercetări pentru realizarea unei stații radioreleu multicanal sovietice. Astfel, începând cu 1950, au început să producă stațiile radioreleu din seria R-400³³, stații ce au fost utilizate și de Armata Română.



Fig.10: Punct de retranslație cu stații Michael

³⁰ Arthur O. Bauer, *Some aspects of military line communication as deployed by the German armed forces prior to 1945*, pe http://www.cdvandt.org/line_communications.htm

³¹ Werner Thote, *Das Sachsenwerk und RAFENA Radeberg 1945 bis 1969*, pe <http://fesararob.de/Publikation/Thote/ferob%20Geschichte3.pdf>

³² Давыдов С.Л., Жеребцов И.П., Лебинзон-Александров Ф.Л., *Радиотехника, Военное Издательство Министерства Обороны СССР*, Moscova, 1963, pe

<http://www.booksshare.net/index.php?id1=4&category=electrotech&author=davidov-sl&book=1963>

³³К. И. Кукк, *Из истории становления отечественной военной радиорелейной и тропосферной связи*, în revista „Электросвязь: история и современность” nr. 1, 2008, pe <http://housea.ru/index.php/computer/50717>

ACORDAREA DISTINCȚIEI MILITARE CU DENUMIREA ONORIFICĂ „OMUL ANULUI 2014”

Centrul 54 Comunicații RMNC Logistică și infrastructură



În cadrul Concursului „Omul Anului-2014” - etapa pe Comandamentul Comunicațiilor și Informaticii, colonelul **GRIGORE MORAR**, comandantul Centrului 54 comunicații RMNC, a obținut locul I la Secțiunea „Logistică și infrastructură”.

Născut la data de 21 iulie 1959 în localitatea Strâmtura, județul Maramureș, ofițerul este absolvent al Școlii Militare de Ofițeri Activi de Transmisiuni, promoția 1981 și al Academiei de Înalte Studii Militare, specialitatea militară transmisiuni, promoția 1991. Și-a perfecționat pregătirea de specialitate prin absolvirea cursurilor de carieră necesare înaintării în gradul următor, precum și prin cursuri de perfecționare.

De-a lungul anilor a îndeplinit cu responsabilitate funcții de comandă succesiv de la comandant pluton și companie până la cea de comandant al Centrului 54 comunicații RMNC și comandant al garnizoanei Oradea.

Nivelul ridicat al cunoștințelor generale, militare și de specialitate, precum și bogata experiență acumulată i-au permis să-și îndeplinească standardele și obiectivele de performanță, să conducă și coordoneze competent unitatea. Ofițerul este integru, sociabil și integrat în societatea civilă din cadrul garnizoanei Oradea.

În domeniul „Logistică și infrastructură”, ofițerul a realizat și menținut o excelență colaborare cu administrația publică locală și cu structurile de apărare, ordine publică și siguranță națională din județul Bihor. A încheiat un protocol cu Primăria Oradea prin care aceasta execută lucrări de reparații și investiții în sprijinul garnizoanei Oradea în sumă de aprox. 2.000.000 lei (sunt finalizate lucrări în valoare de 844.444 lei, în curs de realizare în valoare de 868.425,568 lei și urmează în anul 2015 o lucrare în valoare de

aprox. 300.000 lei) și este singurul invitat care participă, lunar, la ședințele colegiului prefectural.

Ca urmare a măsurilor întreprinse, trei ani consecutivi 2012-2014, Centrul 54 comunicații RMNC s-a clasat pe locul 3 la etapa finală pe M.Ap.N. a Concursului „Cea mai bună bază și activitate sportivă”.

A organizat cu profesionalism și maximă responsabilitate nouă ceremonii militare și religioase cu ocazia sărbătorilor naționale și patru la solicitarea instituțiilor publice locale în Oradea, iar în județul Bihor patru ceremonii militare și religioase, toate reflectate pozitiv în presa locală.

A realizat, din proprie inițiativă, prin Cercul Militar Oradea, protocoale de colaborare cu două instituții culturale de prestigiu, respectiv Ansamblul folcloric Bihorul și Liceul de arte Oradea, acestea reprezentând Cercul Militar Oradea la manifestările organizate pe plan local sau național.

Ca o încununare a modului exemplar în care și-a desfășurat activitatea în anul 2014, colonelul Grigore MORAR a fost desemnat „Omul Anului 2014” în Comandamentul Comunicațiilor și Informaticii la Secțiunea „Logistică și infrastructură”.

În continuare, îi dorim succes și noi realizări în domeniu !

Batalionul Instrucție Comunicații și Informatică „Frații Buzești” Presă, film și literatură



În cadrul concursului „Omul Anului-2014” – etapa pe Comandamentul Comunicațiilor și Informaticii, locotenentul (Com. Infm.) ACSINTE Vasile IULIAN – ALEXANDRU a obținut locul I la secțiunea „Presă, film și literatură”, clasându-se pe același loc și la etapa pe unitate.

Ofițerul s-a născut la data de 03 iulie 1986, în orașul Dorohoi, județul Botoșani, îmbrățișând cariera militară la vârsta de 14 ani.

A absolvit în anul 2005 Colegiul Militar Liceal „Ștefan cel Mare” din Câmpulung **Moldovenesc**, iar în anul 2008 Academia Forțelor Terestre „Nicolae Bălcescu”.

Ofițerul este căsătorit din anul 2012 și are un fiu în vârstă de 2 ani.

A absolvit cursul de bază în arma comunicații și informatică și cursul pentru dezvoltarea pregătirii în armă a comandantului de pluton în anul 2009.

De la terminarea cursului de bază în arma comunicații și informatică a îndeplinit succesiv toate treptele ierarhiei militare:

- 2009 – 2011 – comandat pluton;
- din 2011 – comandant companie.

Întreaga activitate a desfășurat-o în **BATALIONUL INSTRUCȚIE COMUNICAȚII ȘI INFORMATICĂ „FRAȚII BUZEȘTI”**, unitate în care s-a remarcat prin spirit de camaraderie, inițiativă, profesionalism și colegialitate.

De-a lungul activității în unitate, a participat la realizarea unor reportaje despre instruirea soldaților profesioniști, preocupându-se de promovarea imaginii unității.

A organizat și condus permanent activități culturale – educative cu soldații gradații profesioniști care s-au instruit în unitate pentru promovarea tradițiilor armeei și unității.

A organizat prezentări de filme de instrucție și standuri de prezentare a literaturii militare și beletristice din domeniul CIS.

A publicat în Revista comunicațiilor și informaticii- nr. special – nr.1/2014 o lucrare cu titlul „Unele opinii privind apărarea cibernetică la 65 de ani de la constituirea NATO”.

A avut un aport esențial în actualizarea sălii de tradiții a unității și în pregătirea spațiilor de cazare din unitate cu ocazia desfășurării Ceremoniei de încheiere a misiunii Armatei României în Afganistan.

Pentru modul exemplar în care și-a îndeplinit atribuțiile funcționale, în aprecierea de serviciu pentru anul 2014 a fost apreciat cu calificativul „EXCEPȚIONAL”.

Prin întreaga activitate desfășurată, ofițerul a contribuit la crearea și menținerea unei imagini pozitive a unității în rândul populației și instituțiilor din garnizoana Craiova și nu numai.

Batalionul Instrucție Comunicații și Informatică „Frații Buzești” Moral, bunăstare și recreere



În cadrul concursului „Omul Anului-2014” – etapa pe Comandamentul Comunicațiilor și Informaticii, plutonierul major (Com. Infm.) **ION FLOREA GEORGE** a obținut locul I la secțiunea „Moral, bunăstare și recreere”, clasându-se pe același loc și la

etapa pe unitate.

Subofițerul s-a născut la data de 22 iulie 1978, pe meleaguri oltenesti, în orașul Balș, județul Olt, îmbrățișând cariera militară în anul 1996 la vârsta de 18 ani, când a fost declarat ADMIS la Școala Militară de Maiștri Militari și Subofițeri a Trupelor de Uscat, arma transmisiuni.

Doi ani mai târziu, a absolvit cursurile acestei instituții, fiind clasat al 2-lea din 70 de absolvenți și repartizat la Centrul 89 Principal de Transmisiuni.

Subofițerul este căsătorit din anul 2006 și are o fiică în vârstă de 6 ani și jumătate.

A absolvit cursul de comandant pluton în anul 2001, cursul de plutonier major în anul 2006 și cursul de plutonier adjutant în anul 2014. Între cele trei cursuri de carieră, și-a perfecționat pregătirea prin parcurgerea cursului de specializare subofițeri în apărare NBC în anul 2002.

De-a lungul carierei, pentru rezultate remarcabile în procesul de instrucție și pentru îndeplinirea exemplară a atribuțiilor de serviciu, i s-a conferit „Emblema de Onoare a Comunicațiilor și Informaticii” în anul 2008 și a fost recompensat de către comandantul unității cu felicitări în anul 2006 și mulțumiri în anul 2014.

De la terminarea școlii militare a îndeplinit succesiv funcții de operator, comandant grupă, comandant pluton, administrator de subunitate, iar din anul 2008 a fost încadrat subofițer de stat major nivel 2 la S.1 - personal.

Din postura acestei funcții, subofițerul s-a preocupat cu consecvență, conștiinciozitate și responsabilitate de îndeplinirea atribuțiilor funcționale la cele mai înalte standarde, între

acestea cea mai importantă fiind legată de soldații și gradații profesioniști aflați la cursurile de carieră și specializare. A acționat cu profesionalism pentru realizarea unor baze de date veridice, care să ofere permanent informații corecte, s-a implicat în organizarea activităților cultural-educative și sportive pentru menținerea la un nivel înalt a moralului cursanților. De asemenea, a desfășurat activități de consiliere privind formarea inițială și continuă a soldaților și gradaților profesioniști, oferindu-le informații concrete pe linia evoluției în carieră.

A demonstrat în toate împrejurările inițiativă, echilibru, profesionalism și loialitate.

Este un om sincer, cinstit, curajos și demn de încredere pe care orice comandant se poate baza chiar și în cele mai dificile situații.

DCM-E din Batalionul 2 Transmisiuni NATO Soldatul universal



În cadrul Concursului „Omul Anului-2014”-etapa pe Comandamentul Comunicațiilor și Informaticii, căpitanul ECATERINA-CRISTINA DINU a obținut locul I la Secțiunea „Soldatul universal”.

Născută la data de 22 februarie 1986 în municipiul București, ofițerul este absolvent al Academiei Forțelor Terestre „Nicolae Bălcescu”, promoția 2008, și a Cursului de bază-ofițeri, arma comunicații și informatică la Centrul de Instruire pentru Comunicații și Informatică “Decebal”, promoția 2009.

Și-a perfecționat pregătirea militară generală și de specialitate prin studii de master în

științe militare și informații, managementul informațiilor de securitate națională și prin cursuri de perfecționare/specializare: Cursul post-universitar de dezvoltare profesională în cooperare civili-militari, Cursul de politică de securitate și integrare europeană, Cursul de orientare NATO etc.

A ales să înceapă cariera militară la Centrul 48 comunicații și informatică strategice, unitate în care a îndeplinit succesiv funcțiile de comandant pluton, comandant companie și șef de stat major de batalion.

La data de 1 iulie 2014, a fost împuternicită la comanda Modulului NATO de comunicații dislocabil DCM”E”/Batalionului 2 Transmisiuni NATO (2NSB), iar în perioada 08.07.2014-18.01.2015 a participat la misiunea "Resolute Support"-Kabul, Afganistan asigurând cu această structură suportul de comunicații și informatic pentru Comandamentul Forței Internaționale pentru Asistență de Securitate (ISAF).

S-a remarcat prin competență profesională, entuziasm și energie mobilizatoare, curaj și consecvență în îndeplinirea misiunilor încredințate atât în țară, cât și în teatrul de operații Afganistan. În semn de apreciere a calităților sale, i-au fost acordate recompense și însemne onorifice din partea Ministerului Apărării Naționale și din partea NATO.

Seriozitatea, pasiunea și efortul continuu pentru afirmarea calităților profesionale ale militarilor români la nivelul conducerii ISAF și a structurilor de comunicații și informatice ale NATO au stat la baza alegerii sale ca “Soldat universal”.

Generația tânără de cadre militare are în față un model de comandant, luptător, specialist de comunicații și informatică, educator și cetățean demn de urmat în cariera profesională.



OBIECTIVELE FUNDAMENTALE PE ANI DE INSTRUCȚIE:

2008 - INSTRUCȚIE/PREGĂTIRE, OPERAȚIONALIZARE, PROFESIONALIZARE

2009 - INSTRUCȚIE/PREGĂTIRE, EXIGENȚĂ, DISCIPLINĂ, PERFORMANȚĂ

2010 - INSTRUIRE PENTRU MISIUNI, COEZIUNE PENTRU LUPTĂ

2011 - MODERNIZARE STRUCTURALĂ-OPERAȚIONALIZARE ACȚIONALĂ

2012 - OPERAȚIONALIZARE - MODERNIZARE - OPTIMIZARE - DISLOCABILITATE

2013 - CAPABILITĂȚI MAXIME, COSTURI MINIME

2014 - INSTRUIRE LA CELE MAI ÎNALTE STANDARDE PROFESIONALE

ANUL DE INSTRUCȚIE 2015

TRANSFORMARE



OPTIMIZARE



OPERAȚIONALIZARE

