

REVISTA COMUNICAȚIILOR ȘI INFORMATICII



**70 DE ANI DE LA ÎNFIINȚAREA
CENTRULUI 89 STRATEGIC DE
COMUNICAȚII ȘI INFORMATICĂ**



Nr. 2/2018

REVISTA
COMUNICAȚIILOR ȘI INFORMATICII
fondată sub denumirea
BULETINUL TRANSMISIUNILOR

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

sub îndrumarea
Direcției Comunicații și Tehnologia Informației
și a
Comandamentului Comunicațiilor și Informaticii

Coordonatori științifici:

Gl. mr. dr. Valentin BECHERU
Gl. bg. ing. Nicolae MARIA-ZAMFIRESCU

Redactor-șef:

Mr. Vasile-Cosmin GROZA

Redactori:

Mr. Nuțu-Marius MACHEK
Mr. Ionel BOUARIU
Lt. Iulian-Alexandru PÎRLOG
Plt. Florin-Marian ȘEICĂRIN

Procesare text și fotografii:

P.c.c. Karin TIUCĂ-LEUTSCHAFT

ADRESA REDACȚIEI:

SIBIU, Bd. V. Milea, nr. 3-5, jud. Sibiu
Telefoane: 0269233930
int. 436, 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

Ordinul șefului Statului Major al Apărării privind aniversarea a 70 de ani de la înființarea Centrului 89 Strategic de Comunicații și Informatică	3
- General Nicolae-Ionel CIUCĂ	
Ordinul comandantului Comandamentului Comunicațiilor și Informaticii	5
- General-maior Valentin Becheru	
Centrul 89 Strategic de Comunicații și Informatică - scurt istoric	6
- Colonel Adrian VĂTAFU	
Ordinul Marelui Stat Major nr. 45270 din 25 septembrie 1948, Secția I-a	11
Centrul de Comunicații Principal – evoluție, realizări și perspective în cadrul Centrului 89 Strategic de Comunicații și Informatică	13
- Locotenent-colonel Cristinel OLARU	
Dimensiunea multidisciplinară a apărării cibernetice. Implicații pentru securitatea națională în context euroatlantic.....	16
- Colonel dr. Dan ȚIGĂNUȘ	
Învățământul distribuit la distanță - o formă modernă și eficientă pentru formarea profesională continuă a specialiștilor din domeniile comunicații, tehnologia informație și apărarea cibernetică din Armata României	22
- Locotenent-colonel Laurențiu IRIMIA	
Centrul 89 Strategic de Comunicații și Informatică în pas sau în „conflict” cu evoluția tehnologiei informației?	28
- Locotenent-colonel Florin NICU-TONCEAN	
Cloud computing - o descoperire utilă sau un motiv de îngrijorare pentru securitatea informațiilor.....	30
- Locotenent-colonel Cristinel OLARU	
- Locotenent Cătălin MÂRZA	
Îmbunătățirea navigației prin satelit utilizând sistemul EGNOS (European Geostationary Navigation Overlay Service)	34
- Maior Vasile VLAD	
- Locotenent Teodor MITREA	
Sisteme de management al documentelor: rol și criterii de evaluare în perspectiva implementării în mediul militar.....	39
- Maior Nuțu-Marius MACHEK	
Corectitudinea, transparența și șansele egale de evoluție în cariera militară.....	47
- Maior Bogdan BURLOI	
Proiect privind interconectarea centrelor din RTP/RMNC la infrastructura VoIP	49
- Căpitan Daniel CALCIU	

S3 și provocările începutului	53
- Locotenent Niculina FULGER	
Provocările începutului de carieră	55
- Locotenent Alexandra BARBU	
Tineretea în S4 - Logistică	57
- Locotenent Mădălina CRAIOVEANU	
Dronele – istoria unei revoluții tehnologice.....	59
- Locotenent Mădălina CRAIOVEANU	
Tehnologia WiMax	62
- Locotenent Mihai LUCACIU	
Conceptul FMN	64
- Sublocotenent Adrian CARPIUC	
Repetoare hibride în gama microundelor (SHF).....	66
- Plutonier-adjutant Cristian DANALACHE	
O problemă majoră: securitatea IT	68
- Plutonier Cornel-Cristian CIOBOTEA	
Protecția datelor și a informațiilor personale	70
- Caporal clasa a II-a Nicolae INDRIE	
Primit în marea familie a transmisioniștilor militari.....	73
- Psiholog Robert TUDOROIU	
Consilierea juridică a personalului unității: prezent și perspectivă	75
- P.c.c. Mariana NEAGU	
Impactul și modul de manifestare a factorilor de risc asupra calității muncii personalului	77
- Responsabil SSM Florina CEACȘÎRU	
Balanța și sabia cu două tăișuri	79
- P.c.c. Mariana NEAGU	
Integramă „La ordin”	83
- Claudiu SOFRONE	
Cuvinte încrucișate „Arma noastră”	84
- Claudiu SOFRONE	
NOSTALGIE	85
- Caporal clasa a III-a Victoraș COSMESCU	
Dezlegarea integralei „La ordin”	86
Dezlegarea cuvintelor încrucișate „Arma noastră”	87

ORDINUL ŞEFULUI STATULUI MAJOR AL APĂRĂRII PRIVIND ANIVERSAREA A 70 DE ANI DE LA ÎNFIINŢAREA CENTRULUI 89 STRATEGIC DE COMUNICAŢII ŞI INFORMATICĂ



Sărbătorim, la 1 octombrie 2018, a 70-a aniversare a Centrului 89 Strategic de Comunicații și Informatică, purtătorul și continuatorul tradițiilor militare ale Batalionului Transmisiuni M.A.N., înființat pentru a asigura exploatarea rețelelor de comandament, telefonică, telegrafică și radio, precum și poșta militară pe întreg teritoriul țării.

În cele șapte decenii de existență, unitatea a cunoscut transformări succesive ale cadrului de organizare și a denumirii, toate acestea contribuind la crearea unui corp de cadre foarte bine pregătit, îmbunătățirea asigurării cu tehnică de comunicații și informatică modernă, fiabilă, conform standardelor NATO, adaptându-se astfel evoluțiilor din domeniul comunicațiilor și a tehnologiei informației.

Implicat în majoritatea activităților din domeniul de responsabilitate cu caracter de noutate, atât la nivel național, cât și internațional, Centrul a reușit să-și îndeplinească misiunile de fiecare dată în termenele ordonate și la un nivel calitativ foarte ridicat, asigurând sprijinul de comunicații și informatică atât de necesar conducerii la nivel strategic și operativ a Armatei României.

În prezent, în contextul apariției spațiului cibernetic ca mediu operațional, Centrul 89 Strategic de Comunicații și Informatică se află în plin proces de modernizare structurală în vederea adaptării la cerințele de asigurare a sprijinului de comunicații și informatică necesar exercitării comenzii și controlului pentru desfășurarea acțiunilor de luptă la nivel NATO.

Dragi camarazi,

Aniversarea acestui moment important din istoria centrului are loc într-o perioadă în care Armata României depune eforturi consistente în vederea reorganizării și adaptării structurilor de forțe, pentru atingerea și menținerea unui nivel ridicat al capacității de luptă necesar pentru a putea răspunde în cel mai scurt timp și adecvat riscurilor și amenințărilor tot mai complexe.

Achiziția de tehnică modernă, dar și programele de înzestrare presupun, în continuare, un efort uriaș din partea fiecăruia, pe care trebuie să ni-l asumăm cu responsabilitate și profesionalism. Pentru a putea opera cu noile tehnologii trebuie ca modul de gândire să fie unul flexibil și să rămânem permanent conectați la noutățile din domeniul nostru de activitate.

Ținând cont de evoluția constantă a acestei prestigioase unități, sunt încrezător în capacitatea și determinarea dumneavoastră de a continua în aceeași linie de conduită, bazată pe responsabilitate și spirit

inovator și că veți fi în măsură să asigurați în continuare toate elementele de comunicații și informatică, adoptând cele mai moderne soluții în domeniu.

Sunteți un colectiv deosebit, format din oameni hotărâți, buni camarazi, cu un evident potențial de a duce mai departe, cu succes, bogatele tradiții ale structurii din care faceți parte.

Cu prilejul aniversării a 70 de ani de activitate și în contextul aniversării Centenarului Marii Uniri, vă felicit și aduc mulțumiri întregului personal activ, în rezervă și în retragere pentru rezultatele obținute.

Vă adresez urări de sănătate, realizări profesionale și personale dumneavoastră și celor dragi și succes în îndeplinirea misiunilor care vă sunt încredințate.

La mulți ani!

ȘEFUL STATULUI MAJOR AL APĂRĂRII

General

Nicolae-Ionel CIUCĂ

ANIVERSAREA CENTRULUI 89 STRATEGIC DE COMUNICAȚII ȘI INFORMATICĂ

„Informatica fără comunicații nu poate fi, cum nici comunicațiile nu pot exista fără informatică”.



Ziua de 1 octombrie reprezintă, în istoria armei comunicații și informatică, un reper deosebit de important – constituirea, prin Ordinul Marelui Stat Major nr. 45270 din septembrie 1948, a Batalionului de Transmisiuni al Ministerului Apărării Naționale, în subordinea Comandamentului Geniului, ale cărui tradiții le continuă, astăzi, Centrul 89 Strategic de Comunicații și Informatică.

Multiplele transformări de-a lungul celor 70 de ani de existență, participarea cu personal și tehnică la diferite misiuni, atât la nivel național, cât și internațional, au permis ca astăzi să ne mândrim cu performanțele militarilor noștri transmisioniști, distanța dintre prima legătură radio Somalia – România, de 6.000 km, organizată de către unitatea dumneavoastră și prezent constituie puntea către recunoașterea profesionalismului de care ați dat și dați dovadă.

70 de ani în arma comunicații și informatică înseamnă foarte mult, ritmul rapid în evoluția tehnologiei din domeniu precum și volumul tot mai mare de informație necesar actului de comandă-control au făcut ca evoluția comunicațiilor să fie una spectaculoasă, iar rolul dumneavoastră să fie unul definitoriu.

Faceți parte din una dintre cele mai importante unități de comunicații și informatică din Armata României, ale cărei tradiții glorioase le duceți mai departe cu cinste și devotament.

Ați demonstrat permanent că aveți o mare capacitate de adaptare la noile tehnologii din domeniul comunicațiilor și informaticii, precum și la noile cerințe de compatibilitate și interoperabilitate cu structurile similare ale NATO și statelor membre, ceea ce ne asigură garanția că veți participa cu succes la realizarea, exploatarea și mentenanța sistemului strategic de comunicații și informatică.

La ceas aniversar, în anul centenar al Marii Uniri, doresc să vă felicit pentru realizările remarcabile obținute de-a lungul timpului și să vă adresez cele mai calde și sincere urări de succes în activitate, împliniri profesionale și satisfacții personale, multă sănătate și bucurii!

La mulți ani!

**COMANDANTUL COMANDAMENTULUI COMUNICAȚIILOR
ȘI INFORMATICII (ȘI LOCTIITOR AL ȘEFULUI STATULUI
MAJOR AL APĂRĂRII PENTRU TEHNOLOGIA INFORMAȚIEI)**

General-maior

Valentin BECHERU

CENTRUL 89 STRATEGIC DE COMUNICAȚII ȘI INFORMATICĂ ~ SCURT ISTORIC ~

Colonel Adrian VĂTAFU

Centrul 89 Strategic de Comunicații și Informatică



Data de 01 octombrie 1948 marchează, așa cum este consfințit fără urmă de îndoială în documentele de arhivă, înființarea Batalionul de Transmisiuni M.A.N.

În urmă cu 70 de ani, la 25 septembrie 1948, generalul maior IACOB TELCU, în numele șefului Marelui Stat Major, semna Ordinul cu numărul nr. 45270 emis de Secția I-a a Marelui Stat Major, prin care, din ordinul Ministrului Apărării Naționale, „la data de 1 Octombrie 1948 se înființează Batalionul Transmisiuni M.A.N.”.

Ordinul de înființare a Batalionului consemnează astfel ziua de naștere a unității noastre.

Ca aproape în orice început, pașii au fost mici, dificili, cu multe neajunsuri, însă încet, încet, unitatea și-a câpătat rolul, locul și importanța în cadrul sistemului de comunicații al Ministerului Apărării Naționale.

Necesitatea înființării unității este consemnată chiar în ordinul de înființare: „exploatarea rețelelor de comandament: telefon, telegraf și radio, precum și poșta militară de **pe întreg teritoriul țării noastre**”. Această hotărâre a fost luată pentru a concentra și îngloba toate centrele, centralele telefonice, posturile radio și oficiile poștale militare de pe întreg teritoriul țării într-o singură unitate, acestea funcționând până la data de 01 octombrie 1948 pe principiul teritorialității, fiind asigurate la nivelul fiecărei garnizoane care dispunea de un centru de transmisiuni propriu. Necesitatea acestei decizii era motivată de faptul că se dorea exercitarea unei conduceri unice la nivelul Ministerului Apărării Naționale a tuturor elementelor și structurilor de transmisiuni în scopul realizării „... securității depline a transmisiunilor telefonice, telegrafice, radio și poștale”.

Dacă inițial unitatea urma să fie subordonată Serviciului de Informații al Armatei/S.I.A., ulterior s-a luat hotărârea că Batalionul va fi organizat și va intra în subordonarea Comandamentului Geniului prin Brigada Transmisiuni „... din toate punctele de vedere, mai puțin exploatarea rețelei, contrainformativ și al încadrării și selecționării personalului pentru care batalionul va depinde de M.A.N., Serviciului de Informații al Armatei”.

Este de remarcat faptul că unitatea avea responsabilitate pe întreg teritoriul țării, cu o organigramă ce însuma 959 militari și 47 civili și funcționa în 71 localități, fiecare microstructură fiind însă în subzistența unei unități militare din zonă.

Acest proiect de concentrare a tuturor elementelor esențiale ale sistemului de transmisiuni din acea perioadă într-o singură unitate dispusă în București și menită să conducă și să supravegheze elementele de execuție din teritoriu au condus la data de 20 iunie 1949, la desființarea Batalionului Transmisiuni M.A.N., iar conducerea și organizarea legăturilor de garnizoană revenea la forma avută anterior. Totuși, elementele dispuse în București care deserveau structurile centrale (centrele de transmisiuni și centralele telefonice ale M.A.N., M.St.M., D.S.P.A., S.I.A., și ale Comandamentelor de armă) erau reorganizate într-o singură subunitate și se constituia Compania de Transmisiuni din compunerea Batalionului 320 Gardă. Astfel, în numai nouă luni de la înființare, batalionul cu organigramă de nivel regiment și responsabilități la nivel național se transformă într-o companie în cadrul unui batalion de infanterie.

Parafrazându-l pe Octavian Paler, „*Tot ceea ce se întâmplă se întâmplă fiindcă așa trebuia să se întâmple*”¹, la 01 octombrie 1952, se reînființează unitatea care avea să deservească din punct de vedere al asigurării legăturilor Ministerului Forțelor Armate și organele sale de conducere dispuse în București, sub denumirea de „Batalionul 923 Transmisiuni M.F.A.”.

În anii ce au urmat au avut loc transformări și reorganizări specifice întregului organism militar, dar unitatea nu a mai cunoscut schimbări radicale așa cum au fost cele de început.

Misiunea unității a rămas în esență neschimbată, ea fiind doar adaptată noilor concepte sau structuri conform doctrinelor și concepțiilor ce au stat și stau la baza asigurării sprijinului de CIS în Armata României.

Dintre toate aceste schimbări și transformări, unele dintre ele trebuie subliniate și amintite:

23 februarie 1959	BATALIONUL 923 de TRANSMISIUNI și-a schimbat denumirea în BATALIONUL 89 TRANSMISIUNI al MINISTERULUI FORTELOR ARMATE, iar indicativul numeric U.M. 03489 se transformă în U.M. 01681.
15 mai 1960	BATALIONUL 89 TRANSMISIUNI și-a schimbat indicativul numeric în U.M. 01704, indicativ pe care îl are și astăzi.
25 octombrie 1962	Unității i-a fost înmănat DRAPELUL DE LUPTĂ de către general-maior Păucă Costache, comandantul Trupelor de Transmisiuni.
15 aprilie 1969	Unitatea s-a mutat din localul de pe strada Drumul Taberei în localul pe care îl ocupă și în prezent, Șoseaua București – Măgurele, numărul 33.
1970	Se înființează Centrul de Transmisiuni al M.Ap.N., ca subunitate distinctă, organizat pe elemente: centrul de emisie radio, centrul de control radio, centrul telefon-telegraf, registratura.
22 decembrie 1972	Drapelul de Luptă al unității a fost decorat cu ORDINUL “APĂRAREA PATRIEI”, clasa a doua.

¹ Paler Octavian „Deșertul pentru totdeauna”

15 aprilie 1980	BATALIONUL 89 TRANSMISIUNI trece la o nouă organizare la pace și război, mai complexă, dar mai suplă, pe baza nevoilor operative de asigurare a legăturilor.
1 octombrie 1990	BATALIONUL 89 TRANSMISIUNI se transformă în CENTRUL 89 PRINCIPAL DE TRANSMISIUNI, un nume care exprimă locul și rolul acestei structuri în sistemul de transmisiuni al armatei, cu o nouă organizare la pace, corespunzător noilor cerințe de conducere a armatei.
1 mai 1992	CENTRUL 89 PRINCIPAL DE TRANSMISIUNI trece la un nou stat de organizare la pace și la război.
07 iulie 1993	În cadrul primei misiuni de menținere a păcii, militarii din unitatea noastră au luat legătura prin stația radio R-140 cu Spitalul Militar de Campanie din Somalia, în cadrul misiunii UNSOM II, realizând legătura la aproximativ 6000 de km între două continente, ceea ce a constituit o premieră absolută pentru armata română.
1 iulie 1995	Unitatea parcurge procesul de restructurare a armatei române, trecând la o nouă structură de pace și război, conformă noilor sale misiuni.
14 iulie 1996	Cu ocazia sărbătoririi Zilei transmisioniștilor militari, CENTRULUI 89 PRINCIPAL DE TRANSMISIUNI i s-a înmănat noul DRAPEL DE LUPTĂ.
1 iulie 2002	Cu numărul S/B5/2168/2002, STATUL MAJOR GENERAL a aprobat noul stat de organizare al unității.
1 octombrie 2003	CENTRULUI 89 PRINCIPAL DE TRANSMISIUNI i s-a conferit ORDINUL VIRTUTEA MILITARĂ în GRAD DE CAVALER, cu însemn pentru militari.
19 aprilie 2003	Începând cu această dată, unitatea a asigurat legăturile radio cu unitățile românești dislocate în Teatrul de Operații din Irak.
28 iulie 2004	Începând cu această dată, unitatea a asigurat legăturile radio cu structurile românești dislocate în Teatrul de Operații din Afganistan. În noiembrie 2004 a intrat în funcțiune Modulul de comunicații și informatică dislocat în Kandahar. Legătura a fost realizată prin sistemul satelitar dispus în Centrul 1E, locația M-100, asigurându-se servicii de videoconferință, date și voce.
1 aprilie 2006	CENTRUL 89 PRINCIPAL DE TRANSMISIUNI trece la un nou stat de organizare sub denumirea de CENTRUL 89 PRINCIPAL PENTRU COMUNICAȚII ȘI INFORMATICĂ.

2-4 aprilie 2008	CENTRUL 89 PRINCIPAL PENTRU COMUNICAȚII ȘI INFORMATICĂ participă cu forțe și mijloace tehnice la exploatarea și mentenanța echipamentelor de comunicații pe timpul operației de securitate a SUMMIT – ului NATO de la București.
28 august 2008	CENTRUL 89 PRINCIPAL PENTRU COMUNICAȚII ȘI INFORMATICĂ trece la un nou stat de organizare, păstrându-și denumirea.
1 octombrie 2008	Cu ocazia aniversării a 60 de ani de la înființare, unității i se conferă „Emblema de Onoare a STATULUI MAJOR GENERAL” și „Emblema de Onoare a COMANDAMENTULUI COMUNICAȚIILOR ȘI INFORMATICII”, în semn de recunoaștere a rezultatelor obținute în exploatarea și mentenanța echipamentelor de comunicații pe timpul operației de securitate a SUMMIT – ului NATO, dar și a aplicațiilor desfășurate de categoriile de forțe ale armatei și conduse de S.M.G.
14 iulie 2013	Cu ocazia aniversării a 140 ani de la înființarea armei Comunicații și Informatică, se conferă Centrului 89 Principal pentru Comunicații și Informatică „ <i>Emblema de Onoare a Armatei României, cu însemn de pace.</i> ”
01 octombrie 2013	La data de 01.10.2013 cu ocazia aniversării a 65 de ani de la înființarea Centrul 89 Principal pentru Comunicații și Informatică, Drapelul de luptă al unității a fost decorat cu „ <i>Ordinul Virtutea Militară, în grad de ofițer cu însemn pentru militari, de pace</i> ”, pentru întreaga activitate desfășurată.
01 decembrie 2014	CENTRUL 89 PRINCIPAL DE COMUNICAȚII ȘI INFORMATICĂ trece la un nou stat de organizare sub denumirea de CENTRUL 89 STRATEGIC DE COMUNICAȚII ȘI INFORMATICĂ.
07 septembrie 2015	În perioada 07.09-18.09.2015, C.89 SCI a participat alături de unitățile sistemului de comunicații și informatică la exercițiul HISTRIA 2015 pentru a realiza sprijinul C2 prin îndeplinirea cerințelor de schimb informațional necesare asigurării capacității operaționale inițiale a CFI și validării „Concepției privind conducerea instruirii de forțe a armatei române” la nivel strategic, operativ și tactic.



Sunt pe deplin convins de faptul că realizările și succesele Centrului 89 Strategic de Comunicații și Informatică în cei 70 de ani de istorie se datorează în totalitate și în egală măsură întregului personal al unității care, în toți acești ani, a trudit cu profesionalism, dăruire și modestie pentru îndeplinirea misiunilor și pentru creșterea prestigiului acestei unități.

Este o fericită coincidență că în acest an când arma sărbătorește 140 ani de la înființare și țara sărbătorește Centenarul Marii Uniri, Centrul 89 Strategic de Comunicații și Informatică poate să raporteze cu mândrie: „MISIUNE ÎNDEPLINITĂ”.

Se cuvine, cred, ca în aceste clipe de sărbătoare, gândul nostru, al tuturor, să se îndrepte spre cei care timp de 70 de ani au slujit cu pasiune, devotament și sacrificiu în această unitate. Pentru că ei sunt, stimați cititori, cei care cu modestia, abnegația și îndârjirea caracteristică tuturor transmisioniștilor au pus piatra de temelie a acestei construcții care astăzi se cheamă Centrul 89 Strategic de Comunicații și Informatică și au făcut, astfel, posibilă această sărbătoare!

La mulți ani, dragi camarazi!



**ORDINUL MARELUI STAT MAJOR
NR. 45270 DIN 25 SEPTEMBRIE 1948, SECȚIA I-A**

În conformitate cu ordinul Domnului Ministru al Apărării Naționale, la data de 1 Octombrie 1948 se înființează Batalionul Transmisiuni M.A.N.

Acest batalion va asigura exploatarea rețelelor de comandament: telefonică, telegrafică și radio, precum și poșta militară pe întreg teritoriul țării.

În acest scop se dispune următoarele:

1 - Toate centrele de transmisiuni, centralele telefonice, posturile radio și oficiile poștale militare trecute în alăturatele tabele întră cu începere de la 1 Octombrie 1948 în compunerea Batalionului Transmisiuni M.A.N. cu întreg personalul ce-l au în prezent.

2.- Batalionul va fi organizat de Comandamentul Geniului (Brigada Transmisiuni) în conformitate cu tabela de organizare anexată, mai puțin Compania de instrucție care va lua ființă ulterior.

Grafice de organizare și tabele recapitulative au fost trimise și M.A.N. Dir. Sup. Politică, Dir. Super. a Personalului, S.I.A. și Regiunei a 2-a Militară.

3.- Efectivele trupă necesare pentru organizarea centrelor de transmisiuni, a centralelor telefonice și a posturilor radio conform tablei de organizare anexate, vor fi luate dela regimentele de transmisiuni după dispozițiunile Comandamentului Geniului, din excedentul rămas.

Ofițerii, subofițerii și maiștrii ce mai lipsesc vor fi ceruți M.A.N. Dir. Sup. a Pers.

Personalul civil P.T.T. deficit se va cere dela M. St. M. Secția 3-a.

4.- Batalionul va fi subordonat Comandam. Geniului prin Brigada de Transmisiuni din toate punctele de vedere, mai puțin exploatarea rețelei, contrainformativ și al încadrării și selecționării personalului pentru care batalionul va depinde de M.A.N. Serv. Inform. al Armatei.

5.- Comanda batalionului va fi cazată în BUCUREȘTI în cazarma fostă a Centr. Instr. Transmisiuni. Subunitățile și subîmpărțirile batalionului dislocate pe teritoriu vor fi cazate prin grija Comandamentelor și a unităților pe lângă care ele funcționează.

6.- Dotarea cu armament, mijloace de transport, materiale, etc. se va face de M.A.N. Secret. G-ral ptr. Inzestr. și Adm. după tabela de dotare întocmită de M. St. M. Secția IV-a.

7.- Efectivele centrelor de transmisiuni, a centrelor telefonice, a posturilor radio și a oficiilor poștale militare din compunerea Btl. Transm. M.A.N. vor rămâne în subzistența Comandamentelor, unităților și formațiunilor pe lângă care ele funcționează.

8.- Comandamentele, unitățile și formațiunile armatei unde am contat până acum oamenii care încadrează centralele de transmisiuni, centralele telefonice, posturile radio și oficiile poștale militare care

intră în compunerea Btl. Transm. M.A.N., vor trimite acestuia formele de vărsare până cel mai târziu la 1 Nov. 1948.

9.- Cu începere de la 1 Noembrie 1948 toate efectivele Btl. Transm. M.A.N.(de la sediu și după teritoriu) vor fi raportate pe situația 9700 - întocmită de batalion.

10.- Centralele telefonice interioare ale unităților, posturilor de radio ale unităților și oficiile poștale militare categ. 4-a nu intră în compunerea organică a Btl. Transm. M.A.N. Ele vor funcționa totuși după instrucțiunile date de S.I.A.

11.- M.A.N. Direcția Super. A Personalului este insistent rugată a realiza cât mai grabnic încadrarea cu ofițeri, subofițeri și maștri acestui batalion, cu personalul indicat de S.I.A.

Rog dați ordine de urmare.

/ ȘEFUL MARELUI STAT MAJOR
GENERAL MAIOR,

IACOB TECLU

Șeful secției I-a
Colonel,

Gh. Olteanu

Secția I-a
Nr. 45.270 din 25. Sept 1948
odtre

Copie

In conformitate cu ordinul Domnului Ministru al Aparării Naționale, pe data de 1 Octombrie 1948 se înființează Batalionul Transmisiuni M.A.N.
Acest batalion va asigura exploatarea rețelilor de comandament telefonice, telegrafice și radio precum și poșta militară pe întreg teritoriul țării.

In acest scop se dispune următoarele:

- 1.-Toate centrele de transmisiuni, Centralele telefonice, posturile radio și oficiile poștale militare trecute în alăturatele tabele intră cu începere de la 1 Octombrie 1948 în compunerea Batal. Transmisiuni M.A.N. cu întreg personalul și materialul ce-l au în prezent.
- 2.-Batalionul va fi organizat de Comandamentul Geniului (Brig. Transmisiuni) în conformitate cu tabela de organizare anexată, mai puțin Compania de instrucție care va lua ființă ulterior.
Grădile de organizare și tabele recapitulative au fost trimise și M.A.N. Dir. Sup. Politică, Dir. Super. a Personalului, S.I.A. și Regiunii 2-a Militară.
- 3.-Efectivele trupă necesare pentru organizarea centrelor de transmisiuni, a centrelor telefonice și a posturilor radio conform tabelii de organizare anexate, vor fi luate dela regimentele de transmisiuni după dispozițiunile Comand. Geniului, din excedentul rămas.
Ofițerii, subofițerii și maștrii vor fi ceruți M.A.N. Dir. Sup. a Pers.
Personalul civil P.I.R. deficit se va cere dela M. St. M. Secția 3-a.
- 4.-Batalionul va fi subordonat Comand. Geniului prin Brigada de Transmisiuni din toate punctele de vedere, mai puțin exploatarea rețelii, contrainformativ și al selecționării personalului pentru oare batalionul va depinde de M.A.N. Serv. Inform. al Armatei.
- 5.-Comanda batalionului va fi cazată în BUCUREȘTI în cazarma fostă a Centr. Instr. Transmisiuni. Subunitățile și subpartiturile batalionului dislocate pe teritoriu vor fi cazate prin grija Comandamentelor și a unităților pe lângă care ele funcționează.

.../..

6.-Dotarea cu armament, mijloace de transport, materiale, etc. se va face de M.A.N. Secret. G-ral ptr. Inzestr. și Adm. după tabela de dotare întocmită de M. St. M. Secția 17-a.

7.-Efectivele centrelor de transmisiuni, a centrelor telefonice, a posturilor radio și a oficiilor poștale militare din compunerea Btl. Transm. M.A.N. rămân în subzistența Comandamentelor, unităților și formațiunilor pe lângă care ele funcționează.

8.-Comandamentele, unitățile și formațiunile armatei unde au contat până acum oamenii care încadrează centrele de transmisiuni, centralele telefonice, posturile radio și oficiile poștale militare care intră în compunerea Btl. Transm. M.A.N., vor trimite așezându-se formele de vărsare până cel mai târziu la 1 Nov. 1948.

9.-Cu începere de la 1 Noembrie 1948 toate efectivele Btl. Transm. M.A.N. (dela sediu și după teritoriu) vor fi raportate pe situația 9700 - întocmită de batalion.

10.-Centralele telefonice interioare ale unităților, posturile de radio ale unităților și oficiile poștale militare categ. 4-a nu intră în compunerea organică a Btl. Transm. M.A.N. Ele vor funcționa totuși după instrucțiunile date de S.I.A.

11.-M.A.N. Direcția Super. a Personalului este insistent rugată a realiza cât mai grabnic încadrarea cu ofițeri, subofițeri și maștri acestui batalion, cu personalul indicat de S.I.A.

Rog dați ordine de urmare.

/ ȘEFUL MARELUI STAT MAJOR
GENERAL MAIOR,
IACOB TECLU

Șeful Secției I-a
Colonel,
Gh. Olteanu

COMUNICAT:
M.A.N. Cabinet
M.A.N. Secret. G-rale
M.A.N. Dir. Sup. Pol., Dir. Pers., S.I.A.
Regiunile 1-3 Militare
Com. Geniu, Aero, Maritim, Caval., Art.
M. I. V., M. C. G., 2, 4, 6 și 18 Inf.
M. I. V. 1 P. A. și 2 P. A.
Regiunea 1-2 Artilerie
Regiunea 1-2 Cavalerie
M. M. Sec. 1-a Dir. 1, 2 și 4.
M. M. Sec. 2-a și 3-a, Sec. Adjut.
M. M. Sec. 5-a și 6-a, Sec. Adjut.
M. M. Sec. 7-a și 8-a, Sec. Adjut.
M. M. Sec. 9-a și 10-a, Sec. Adjut.
M. M. Sec. 11-a și 12-a, Sec. Adjut.
M. M. Sec. 13-a și 14-a, Sec. Adjut.
M. M. Sec. 15-a și 16-a, Sec. Adjut.
M. M. Sec. 17-a și 18-a, Sec. Adjut.
M. M. Sec. 19-a și 20-a, Sec. Adjut.
M. M. Sec. 21-a și 22-a, Sec. Adjut.
M. M. Sec. 23-a și 24-a, Sec. Adjut.
M. M. Sec. 25-a și 26-a, Sec. Adjut.
M. M. Sec. 27-a și 28-a, Sec. Adjut.
M. M. Sec. 29-a și 30-a, Sec. Adjut.
M. M. Sec. 31-a și 32-a, Sec. Adjut.
M. M. Sec. 33-a și 34-a, Sec. Adjut.
M. M. Sec. 35-a și 36-a, Sec. Adjut.
M. M. Sec. 37-a și 38-a, Sec. Adjut.
M. M. Sec. 39-a și 40-a, Sec. Adjut.
M. M. Sec. 41-a și 42-a, Sec. Adjut.
M. M. Sec. 43-a și 44-a, Sec. Adjut.
M. M. Sec. 45-a și 46-a, Sec. Adjut.
M. M. Sec. 47-a și 48-a, Sec. Adjut.
M. M. Sec. 49-a și 50-a, Sec. Adjut.
M. M. Sec. 51-a și 52-a, Sec. Adjut.
M. M. Sec. 53-a și 54-a, Sec. Adjut.
M. M. Sec. 55-a și 56-a, Sec. Adjut.
M. M. Sec. 57-a și 58-a, Sec. Adjut.
M. M. Sec. 59-a și 60-a, Sec. Adjut.
M. M. Sec. 61-a și 62-a, Sec. Adjut.
M. M. Sec. 63-a și 64-a, Sec. Adjut.
M. M. Sec. 65-a și 66-a, Sec. Adjut.
M. M. Sec. 67-a și 68-a, Sec. Adjut.
M. M. Sec. 69-a și 70-a, Sec. Adjut.
M. M. Sec. 71-a și 72-a, Sec. Adjut.
M. M. Sec. 73-a și 74-a, Sec. Adjut.
M. M. Sec. 75-a și 76-a, Sec. Adjut.
M. M. Sec. 77-a și 78-a, Sec. Adjut.
M. M. Sec. 79-a și 80-a, Sec. Adjut.
M. M. Sec. 81-a și 82-a, Sec. Adjut.
M. M. Sec. 83-a și 84-a, Sec. Adjut.
M. M. Sec. 85-a și 86-a, Sec. Adjut.
M. M. Sec. 87-a și 88-a, Sec. Adjut.
M. M. Sec. 89-a și 90-a, Sec. Adjut.
M. M. Sec. 91-a și 92-a, Sec. Adjut.
M. M. Sec. 93-a și 94-a, Sec. Adjut.
M. M. Sec. 95-a și 96-a, Sec. Adjut.
M. M. Sec. 97-a și 98-a, Sec. Adjut.
M. M. Sec. 99-a și 100-a, Sec. Adjut.

CENTRUL DE COMUNICAȚII PRINCIPAL – EVOLUȚIE, REALIZĂRI ȘI PERSPECTIVE ÎN CADRUL CENTRULUI 89 STRATEGIC DE COMUNICAȚII ȘI INFORMATICĂ

Locotenent-colonel Cristinel OLARU

Centrul 89 Strategic de Comunicații și Informatică

„Învingătorii nu renunță, iar cei care renunță nu ajung învingători.”



Drumul
parcurs de
Centrul de
comunicații de-
a lungul celor
șapte decenii de
existență a fost
la fel ca al

unității și al armei comunicații și informatică – deloc neted, cu ascensiuni, dar și cu momente dificile, marcat de evenimentele ce au avut impact și asupra societății civile.

Pentru a fi mai exact, istoria Centrului de comunicații, ca structură distinctă în cadrul unității, începe în 1964 când, sub denumirea „Nodul de transmisiuni al Marelui Stat Major”, sunt reunite:

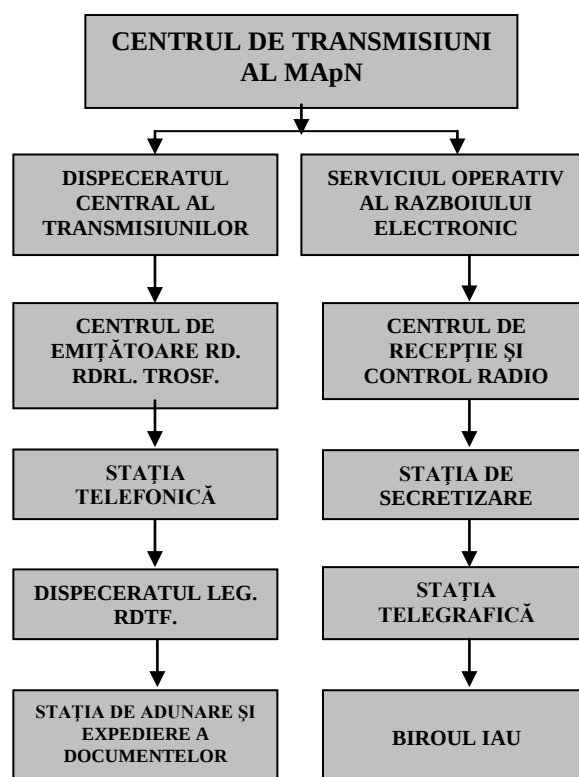
- compania exploatare telefon-telegraf;
- compania exploatare radio;
- punctul adunare corespondență;
- autostații radio R-110.

Anul 1970 aduce o nouă organizare, sub denumirea de „Centrul de transmisiuni al MApN”, care cuprindea:

- centrul emisie radio;
- centrul recepție radio;
- centrul control radio;
- centrul telefon-telegraf;
- registratura.

În 1980, registratura devine Punctul adunare documente, celelalte elemente păstrându-și denumirea.

O importantă transformare are loc odată cu 1 octombrie 1990, când Centrul de transmisiuni al MApN primește noi misiuni și este organizat pe elemente:



La 01.07.2002, Centrul de transmisiuni primește o nouă organizare conform misiunilor repartizate:

- asigurarea sistemului de comunicații pentru realizarea legăturilor interne și internaționale de conducere și cooperare ale MApN, SMG și ale celorlalte structuri centrale ale

armatei pe timp de pace, în situații de criză și de război;

- realizarea și exploatarea legăturilor cu forțele care desfășoară activități în afara teritoriului național sub egida NATO/PfP, UE, ONU, OSCE, la exerciții și misiuni de menținere a păcii sau operații multinaționale.

Următoarele modificări structurale au loc la 01.04.2006, 01.10.2008 și 01.12.2014, când subunitatea primește denumirea de Centrul de comunicații principal.

Încredințarea celor mai complexe misiuni și înzestrarea cu cele mai noi tipuri de tehnică au solicitat ca nivelul de pregătire al personalului să fie permanent la cote ridicate. Totul s-a realizat cu multă muncă, dăruire, ambiție și devotament față de unitate și însemnele ei concentrate pe însemnul heraldic: antena satelit, unda radio, calculatorul și plicul, toate acestea regăsindu-se în activitatea zilnică a personalului din elementele Centrului de comunicații principal.

Această activitate s-a concretizat în participarea la exerciții de interoperabilitate (COMBINED ENDEAVOUR 1998-2006, HERALD HERMES 1998-2006, BLUE ROAD 2004, ROMEX '05 și '06, GATEX'06, ROSOFEX '06, la exerciții tehnice de specialitate, misiuni de asigurare a sprijinului de comunicații și informatică pentru alte structuri, organizarea de expoziții de tehnică cu prilejul vizitelor delegațiilor militare ale unor state membre NATO, participarea cu personal și tehnică de comunicații la zilele porților deschise organizate la MAPN, la aniversarea zilei Armatei României - 25 Octombrie, a zilei NATO.

Realizarea în premieră a legăturii radio cu o stație R-140 la 6000 km (iulie 1993 - misiunea UNOSOM II – Spitalul 50 de Campanie – Somalia) apoi la peste 8000 km cu Batalionul 2 Infanterie „Călugăreni” (august 1995 – misiunea UNAVEM III – Angola) au constituit adevărate repere în istoria unității și armei noastre.... și reperele au continuat – 19 aprilie 2003 Irak, 28 iulie 2004 Afganistan – detașamentele românești dislocate în teatrele de operații au beneficiat, pentru prima dată de legături pe calea undelor cu țara în „era digitală”, legături realizate cu stații radio cu salt de frecvență.

Asigurarea legăturilor radio în cadrul sistemului de comunicații și informatică la Reuniunea Informală a Miniștrilor Apărării din țările membre NATO, Brașov (RIMAp 2004) a constituit o premieră prin complexitatea activităților desfășurate de specialiștii noștri.

Experiența astfel acumulată a fost valorificată prin participarea la realizarea sistemului de comunicații și informatică cu ocazia summitului NATO de la Palatul Parlamentului (2 - 4 aprilie 2008).

Participarea cu personal și tehnică la expoziția internațională dedicată apărării, siguranței naționale și industriei aeronautice Black See Defence Aerospace – complexul ROMAERO Băneasa (15 - 18 mai 2012) constituie încă o piesă de rezistență a „palmaresului” Centrului de comunicații.

Din anul 2011, la fiecare început de decembrie, instalăm un centru de comunicații pentru asigurarea suportului de comandă-control necesar conducerii forțelor și mijloacelor

participante la Parada Națională. La această importantă activitate suntem reprezentați din anul 2014 cu câte două echipaje cu autostații radio FALCON în cadrul blocului de defilare cu tehnică.

Anii trec ... oamenii vin și pleacă, tehnica veche este înlocuită de cea nouă care, peste câțiva ani, are aceeași soartă... căci anii trec!

„Modernizare” a fost înlocuit cu „upgrade” și „update”, totul evoluează într-un ritm amețitor, viitorul de ieri, astăzi este prezent, iar mâine deja este trecut!

Generațiile actuale de stații radio cu salt de frecvență au dimensiuni mult reduse și performanțe net superioare stațiilor analogice utilizate până acum 20 - 25 ani.

Echipamentele radioreleu au urmat aceeași traiectorie evolutivă ... de la 4 - 8 canale obținute cu echipamente care ocupau un șasiu de ZIL, KAMAZ, SR, DAC am ajuns la sute de canale realizate cu un echipament cât „trusa transmisionistului” de odinioară!

Liniile din cablu ușor, greu sau liniile permanente aeriene au fost înlocuite cu UTP, FTP, STP, fibră optică.

Planșele cu scheme tehnice de ieri acum sunt display-uri.

Centralele și aparatele telefonice de campanie au devenit comutatoare și terminale VoIP.

Panourile de linii și abonați se numesc astăzi switch-uri, routere, interfețe, servere.

Documentele trimise odată prin poștă sunt înlocuite acum de schimbul de informații „on-

line” și prin sistemul de videoteleconferință.

Centrul de transmisiuni tip armată (un colos cu zeci de autospeciale și sute de oameni) este înlocuit acum de modulul IT operat de doar câțiva specialiști.

Bătăliile au început pe uscat, s-au extins pe mări și oceane, apoi în spațiul aerian. În cele din urmă, spațiul cosmic a „găzduit” confruntările „războiului rece”.

Acum suntem la a cincea dimensiune – spațiul cibernetic. O nouă provocare pentru transmisioniști, indiferent dacă acum ne numim „comunicații și informatică”, iar în viitor „comunicații și tehnologia informației”!

Din dorința de a nu fi părtinitor am evitat să dau nume, dar amintind faptele (aici cu siguranță am omis câte ceva) sunt convins că cititorii acestor rânduri își vor regăsi strădaniile și eforturile amintite făcând conexiunea cu unele sau altele din aceste realizări. Pentru că nimic nu se face fără oameni, ci cu oameni și pentru oameni.

Perseverență, dăruire, abnegație, profesionalism sunt coordonatele la care întâlnim acești oameni: militari și civili, uneori soți și soții, alteori părinți și copii, cu toții membrii ai marii familii numită Centrul 89 Strategic de Comunicații și Informatică.

La ceas aniversar le urez tuturor celor care au trudit în „1704” și încă o mai fac (dar și celor care au fost alături de noi, la bine și la greu) să fie sănătoși și să continue ceea ce noi am realizat până acum.

LA MULȚI ANI!

DIMENSIUNEA MULTIDISCIPLINARĂ A APĂRĂRII CIBERNETICE. IMPLICAȚII PENTRU SECURITATEA NAȚIONALĂ ÎN CONTEXT EUROATLANTIC

Colonel dr. Dan ȚIGĂNUȘ

Direcția comunicații și tehnologia informației



Rezumat: Prin caracterul de tip comprehensiv, inter-agenții și multinațional al apărării cibernetice se creează premisele unei conlucrări substanțiale, pragmatice și eficiente între instituțiile statului, cu evitarea duplicării eforturilor și a unor tendințe concurențiale la nivel interinstituțional, se deschid oportunități de cooperare internațională în cadrul aliat și euroatlantic, cu scopul unic declarat de întărire a rezilienței infrastructurilor, sistemelor și serviciilor din spațiul cibernetic și pe cale de consecință, de creștere a capacității de apărare a țării în condițiile mediului de securitate actual complex, dinamic și în continuă transformare.

Cuvinte cheie: apărare cibernetică, imaginea operațională cibernetică, informații, supraveghere, achiziția țintelor, cercetare

I. Introducere

Rolul în creștere a spațiului cibernetic deschide calea unor noi amenințări, dar dezvăluie și o serie de oportunități pe care suntem obligați să le aprofundăm în scopul de a face față noilor provocări generate de dezvoltarea tehnologică accelerată în condițiile globalizării și dezvoltării societății informaționale.

Amenințările și atacurile cibernetice devin din ce în ce mai comune, sofisticate și devastatoare într-un mediu de evoluție complex și dinamic pentru securitatea națională. România abordează securitatea cibernetică ca o componentă a securității naționale și din această perspectivă decurge importanța și relevanța aspectelor de ordin operațional, multidisciplinar, a cadrului interinstituțional și a dimensiunii multinaționale a apărării cibernetice ca formă a acțiunilor de luptă.

Diseminarea responsabilităților la nivel național și în cadrul multinațional euroatlantic, în funcție de competențele atribuite strict în baza legislației în domeniu, în contextul nevoii de

creare a unor capacități robuste, coerente și care să rezulte în infrastructuri, sisteme și servicii sigure pentru apărare în spațiul cibernetic poate uneori afecta însăși dezvoltarea acestor capacități dacă nu există un cadru de lucru formal, multidisciplinar, inter-agenții, cu legături puternice în grupurile de lucru consacrate la nivelul NATO și UE, cu implicarea tuturor actorilor în țară din domeniul apărării, ordinii publice și siguranței naționale, incluzând aici mediile de cercetare academice și reprezentanții unei elite a industriei de apărare din sectorul cibernetic.

II. Apărarea cibernetică în context euroatlantic

Dimensiunea aliată. Abordarea proiectelor „smart defence” în cadrul Alianței Nord-Atlantice în domeniul apărării cibernetice impune, în prezent, reconsiderarea acestora cel puțin din punct de vedere cultural, al resurselor și serviciilor vizate, precum și al actorilor implicați, fiind necesară o aprofundare inovativă pentru atingerea

obiectivelor de întărire a capacităților militare naționale și ale NATO în cadrul procesului de dezvoltare integrată a acestora.

În acest sens, proiectele relaționate apărării cibernetice de interes pentru țara noastră¹ sunt: dezvoltarea unei capacități multinaționale de apărare cibernetică/ *Multinational Cyber Defence Capability Development/MNCD2*, pregătire și instruire multinațională în domeniul apărării cibernetice/*NATO Multinational Cyber Defence Education and Training/MNCDE&T*, aprobarea participării României ca națiune sponsor la Centrul NATO de Excelență pentru Apărarea Cibernetică prin Cooperare/Cooperative Cyber Defence Centre of Excellence (CCDCOE) de la Tallinn (Estonia), lansarea parteneriatului NATO cu industria din sfera cibernetică, precum și participarea la proiectul Platforma de distribuție a informațiilor despre aplicații software nocive/*Malware Information Sharing Platform (MISP)*.

Dimensiunea apărării cibernetice în contextul integrării în Uniunea Europeană. Dezvoltarea și utilizarea în comun a capacităților de tip *Pooling and Sharing* are în atenție pe domeniul apărării cibernetice proiecte pe care România și le-a asumat cu scopul de a le implementa în capacitățile proprii de apărare, aliniate în cadrul recenteii inițiative la care țara noastră a aderat² prin hotărârea Consiliului Suprem de Apărare a Țării începând cu luna

octombrie 2017 - *Cooperarea structurată permanentă/PESCO*. Un astfel de proiect prevede constituirea de laboratoare întrunite, dislocabile, de analiză și exploatare a evenimentelor DEI (*Joint Deployable Exploitation and Analysis Laboratory – JDEAL*).

Aceste proiecte nu pot fi dezvoltate pe ***dimensiunea națională*** decât într-un parteneriat puternic, coerent și consolidat cu mediul academic și cu industria de profil din țara noastră într-un efort comun pe baze multianuale cu obiective de etapă aliniate la inițiativele din Alianța Nord-Atlantică din care fac parte și cu construirea acelor interfețe între elementele naționale specifice și cele NATO.

Obiectivele de atins, în opinia autorului, pe acest domeniu sensibil, dar care prin atribuirea dimensiunii operaționale a apărării cibernetice ca nouă formă a acțiunilor de luptă³ a căpătat importanță și un caracter de iminență foarte ridicat, sunt:

- dezvoltarea sinergiei și stimularea cooperării între toți factorii la nivelul statului care acționează pentru apărarea spațiului cibernetic în interesul protecției infrastructurilor critice cibernetice naționale – *dimensiunea interinstituțională*;

- corelarea proiectelor de dezvoltare a capacităților de apărare cibernetică între cei trei lideri de domenii militare întrunite asociate – *dimensiunea multidisciplinară*:

- comunicații și tehnologia informației/J6, pentru protecția, monitorizarea funcționării și asigurarea continuității în serviciu a

¹ Intenția participării României la Centrul NATO de Excelență pentru Apărarea Cibernetică prin Cooperare (Cooperative Cyber Defence Centre of Excellence/CCDCOE) de la Tallinn (Estonia), site internet www.dcnews.ro

² Comunicat de presă preluat de pe adresa de internet <https://www.agerpres.ro>

³ NATO Cyber Defence, <https://www.nato.int>

infrastructurilor, sistemelor și serviciilor de comandă, control, comunicații, computere, informații, supraveghere și cercetare/C4ISR cu componenta ISTAR/informații, supraveghere, achiziția țintelor și cercetare, la nivel tactic;

- informații pentru apărare/*Intelligence/J2* pentru identificarea riscurilor, amenințărilor la adresa securității cibernetice, dezvoltarea capabilităților CyberINT, a celor dedicate preluării informațiilor, analizei și diseminării acestora de la senzori/ISR, precum și pentru preluarea informațiilor relevante și în timp real de avertizare timpurie, de la alte structuri ale statului cu competențe în domeniu: Serviciul Român de Informații, Centrul Național de Răspuns la Incidente de Securitate Cibernetică (CNRISC) – CERT-RO⁴ ca autoritate competentă la nivel național etc.;

- operații/J3, pentru stabilirea și conducerea măsurilor de prevenție și reacție la atacurile cibernetice în infrastructurile critice militare, stabilirea măsurilor de manevră pentru izolarea și neutralizarea atacurilor cibernetice, revederea planurilor de operații pentru creșterea rezilienței etc.;

- dezvoltarea unui cadru de lucru adecvat și eficient cu mediul academic și industria națională de profil pentru inițierea unor proiecte cu relevanță și aplicabilitate, eficiență economică și continuitate multianuală din perspectiva alocării resurselor în implementare la nivel național, acces la resurse și contribuție la implementarea unor proiecte asigurate din fonduri comune la nivelul

NATO, precum și prin contribuții colective ale statelor membre UE – *dimensiunea multinațională*;

- realizarea unui forum adecvat la nivel executiv care să definească pe baza competențelor și aptitudinilor necesare domeniului apărării cibernetice, care sunt nevoile de organizare, educație și instruire multidisciplinară la toate nivelurile de aplicare – *dimensiune interinstituțională și comprehensivă*;

- dezvoltarea cadrului de cooperare internațională pe baza inițiativelor la care România și-a declarat interesul, participare în comun cu reprezentanți de la MAPN și SRI la Grupurile de lucru din cadrul Comitetului NATO pentru consultare comandă și control/C3 Board pentru evitarea duplicării de efort și asigurarea sinergiei și convergenței angajării resurselor pe plan național;

- crearea unui forum academic militar permanent pentru promovarea ideilor, soluțiilor și tehnicilor adecvate în scopul protecției infrastructurilor naționale, NATO și UE din spațiul cibernetic aflat în administrare, precum și promovarea și dezvoltarea unei înalte culturi de securitate cibernetică.

III. Dimensiunea operațională a apărării cibernetice ca formă a acțiunilor de luptă

Cerințele de apărare cibernetică pentru *Sistemul C4ISR* constituie provocări multiple și sunt derivate din:

- nevoia de interoperabilitate a sistemelor de comandă și control și a celor informaționale; implementarea rezultatelor cercetării în domeniul securității sistemelor de comunicații și

⁴ Proiect de *Lege privind asigurarea unui nivel comun de securitate a rețelelor și sistemelor informatice*, lansat în dezbatere publică la 3.10.2017, MCSI, <https://juridice.ro>.

informatică, precum și a celor de arme; dezvoltarea și implementarea capabilităților federalizate în rețea prin aplicarea specificațiilor conceptului *Federated Mission Networking*; utilizarea mijloacelor și serviciilor de comunicații și informatice moderne (stații radio bazate pe software și cognitive, terminale de satelit, interfețe de schimb informațional de abonat și între sisteme, soluții comune de criptare, managementul spectrului electromagnetic, utilizarea la maximum și sigură a internetului, software general și specializat modern, servicii de utilizator diversificate și eficiente); capacitatea de a funcționa în mediul cibernetic modern;

- necesitatea imperioasă de introducere a tehnologiilor digitale în comunicațiile militare ca element fundamental pentru realizarea capabilităților de rețea, creșterea nivelului calității serviciilor, asigurarea comunicațiilor de date cu factor critic de timp (voce și video peste IP), servicii internet (e-mail, transfer de fișiere, acces la baze de date, servicii web etc.);

Sub aspect operativ, pe baza conceptului de operare/CONOPS, a cerințelor de schimb de informații la diferite eșaloane și cu elementele de dispozitiv în contextul unei operații de coaliție sau aliate și plecând de la produsele de schimb operațional, inclusiv cele care concură la realizarea imaginii operaționale cibernetică - *Cyber Common Operational Picture/CyberCOP*, apărarea cibernetică trebuie să ia în calcul următoarele cerințe:

- solicitările determinate de factorii operaționali: concepția operației de management al crizei; structura și manevra sistemului de

comandă și control; structura forței participante la misiune; nevoile de cooperare, colaborare și avertizare-înștiințare; constituirea rețelelor locale și extinse de calculatoare; condițiile de propagare a undelor radio; dotarea și nivelul de pregătire a forțelor neconvenționale; condițiile geografice și climaterice din zona de conflict; constituirea și dispunerea rezervei de comunicații; structura și capacitatea sistemului logistic etc.;

- cerințele de schimb informațional: identificarea și validarea eficientă a acestora; asigurarea unui cadru realist și suportabil de finanțare a infrastructurii informaționale; soluții de implementare pe baza unei arhitecturi de referință conform unui pachet de capabilități; stabilirea unei națiuni gazdă care să aibă responsabilitatea legală pentru dezvoltarea și implementarea unui asemenea pachet; asigurarea funcțiilor privind operarea, întreținerea, managementul și securitatea sistemului;

- cerințele determinate de structura dispozitivului de luptă: elemente fixe (staționare), pentru supraveghere și avertizare timpurie, componente dislocabile și mobile, structuri naționale; combinarea eficientă a infrastructurii de rețea cu echipamentele tehnice și componentele software;

- condițiile operative și tehnice, experiența și lecțiile învățate, numărul de utilizatori și nivelurile de pregătire, numărul și dispunerea în teren a elementelor de dispozitiv, volumul traficului informațional estimat, cerințele de interconectare cu alte sisteme, posibilitățile de utilizare a internetului;

- serviciile de bază ce trebuie asigurate: de

rețea; pentru interoperabilitatea datelor; de securitate; pentru managementul configurației; de comunicații și informatice pentru toate zonele funcționale (interfață cu utilizatorii și alte sisteme, conferință audio și video, acoperire radio zonală, înștiințare și avertizare); asigurarea informațională; comutația de circuite și pachete; transportul informației și managementul capacității de transfer; comunicațiile exterioare; serviciile informatice pentru sprijinul deciziei și specializate (domenii); interconectarea tuturor elementelor forței; asigurarea infrastructurii ambientale;

- categoriile de mijloace de comunicații și informatice utilizate: satisfacerea cerințelor de sprijin informațional (stații radio definite prin software și cognitive, terminale de satelit fixe, mobile și portabile, fibră optică, comutatoare, secretizoare, interfețe, terminale de abonat, calculatoare diverse cu software aferent, terminale de acces la internet); de management, mentenanță și rezervă; module pentru extensia sistemului când situația o impune; terminale comerciale pentru transmiterea informațiilor neclasificate personale; mijloace pentru controlul accesului, semnalizarea accesului neautorizat și izolarea zonelor de sistem penetrate; componente software de sprijin decizional, specializat și pentru asigurarea securității sistemului, inclusiv din punct de vedere cibernetic etc.;

- sistemele de comunicații și informatice care asigură conexiuni pe categorii: interioare (între structurile aceluiasi comandament); exterioare (între utilizatorii interiori și cei aflați la distanță sau în deplasare, între entitățile militare și

civile care acționează în cadrul aceleiași operații de management al crizei); la internet, influențate considerabil de calitatea serviciilor oferite de furnizorii din acest domeniu și care solicită măsuri de securitate severe; de extensie a sistemului prin centrele de comunicații dislocabile și mobile; de partajare a serviciilor de utilizator în funcție de nivelul de clasificare al informațiilor;

- operațiile în spațiul cibernetic (operații defensive, ofensive și de exploatare în rețelele de calculatoare, operații informaționale); pregătirea resurselor umane în domeniile informațional, tehnologic și legal;

- misiunile sistemelor de comunicații și informatice în condițiile implementării rețelelor dislocabile federalizate: servicii de bază (mesagerie, e-mail, chat operativ); managementul distribuit al informației (publicare, retragere, arhivare, modificare, semnalizarea modificărilor în înregistrări); motoare de căutare a informației; autentificare și certificare; accesul și utilizarea informațiilor publice din internet; sprijin al deciziei (acces la documente formalizate stocate electronic, desfășurarea rapidă a proceselor de elaborare a deciziilor, instruirea adecvată a personalului, armonizarea doctrinelor, procedurilor și vocabularului operațional).

Ca cerințe pe linie de *asigurare informativă/Intelligence* acțiunile pentru apărare cibernetică concură la:

- identificarea amenințărilor și vulnerabilităților în spațiul cibernetic, dimensiunea acestora, actorii implicați natura lor statală, individuală sau aparținând organizațiilor teroriste;

- caracteristica atacurilor cibernetice, a instrumentelor și mijloacelor tehnice utilizate;

- angajarea resurselor statice și dislocabile proprii, hardware, software sau prin alte mijloace de luptă convenționale sau asimetrice adecvate ca tip de răspuns la atacurile cibernetice.

Imaginea operațională cibernetică – CyberCOP rezultă din concentrarea acțiunilor ca răspuns la cerințele enumerate mai sus pe trei componente interdependente, dar care se generează în medii de planificare și execuție distincte, astfel:

a) componenta de operații și evenimente semnificative, aparținând J3/Operații care contribuie la integrarea Cyber COP cu elemente din: evenimente generate de ritmul ducerii acțiunilor de luptă/Battle Rhythm; operații curente și operații viitoare; comandă și control; protecția forței; management informațional;

b) componenta de comunicații și tehnologia informației prin: monitorizarea funcționalității și evaluarea nivelului de performanță a sistemului; evaluarea activității la nivelul interfețelor de acces și a log-urilor în rețele; monitorizarea traficului și evaluarea capacității de transport a sistemului, informarea asupra rapoartelor CERT, capacitatea de preluare și integrare a serviciilor generate de senzori etc.;

c) componenta de informații: identificarea, analiza și măsuri proprii anticipative la amenințări; estimarea vulnerabilităților propriului sistem; preluarea, analiza și diseminarea informațiilor relevante obținute în comunitatea de

informații; schimb de informații adecvat în cadrul proceselor de tip *Enterprise* și *Business* în care sunt implicații pe timpul efortului de apărare, actori din societatea civilă, industrie, organizații non guvernamentale, structuri operaționale aparținând celorlalte componente ale Sistemului național de apărare, ordine publică și siguranță națională, gestionarea alertelor CERT etc.

VI. Concluzii

În acest spațiu limitat, abordarea teoretică a unui domeniu atât de complex cum este apărarea cibernetică ca și componentă operațională în sfera cibernetică, definit ca domeniu al acțiunilor de luptă, am adus în atenție acele elemente caracteristice de multidimensionalitate ale acestuia, care să contribuie ca idei de început pentru abordări aprofundate ulterioare.

Credem, cu această ocazie, că prin caracterul de tip comprehensiv, inter-agenții și multinațional al apărării cibernetice se creează premisele unei conlucrări substanțiale, pragmatice și eficiente între instituțiile statului, cu evitarea duplicării eforturilor și a unor tendințe concurențiale la nivel interinstituțional, se deschid oportunități de cooperare internațională în cadrul aliat și euroatlantic, cu scopul unic declarat de întărire a rezilienței infrastructurilor, sistemelor și serviciilor din spațiul cibernetic și pe cale de consecință, de creștere a capacității de apărare a țării în condițiile mediului de securitate actual complex, dinamic și în continuă transformare.

ÎNVĂȚĂMÂNTUL DISTRIBUIT LA DISTANȚĂ, O FORMĂ MODERNĂ ȘI EFICIENTĂ PENTRU FORMAREA PROFESIONALĂ CONTINUĂ A SPECIALIȘTILOR DIN DOMENIILE COMUNICAȚII, TEHNOLOGIA INFORMAȚIE ȘI APĂRAREA CIBERNETICĂ DIN ARMATA ROMÂNIEI

Locotenent-colonel Laurențiu IRIMIA

Centrul de Instruire pentru Comunicații și Informatică „Decebal”



Învățământul la distanță este o formă modernă de pregătire, care se utilizează atât la nivel universitar, cât și la cursurile de formare continuă. Este folosit de milioane de studenți

din întreaga lume și, de câțiva ani, este prezent și în universitățile românești. Această formă de organizare a procesului didactic nu presupune prezența zilnică a studentului la cursuri, însă implică participarea la activitățile tutoriale și asistate, precum și efectuarea temelor de control.

Necesitatea implementării unui astfel de tip de învățământ nu mai constituie în secolul 21 un simplu deziderat, ci un element esențial care trebuie să facă parte în mod indubitabil din strategia de pregătire continuă a personalului MAPN¹. De altfel, strategia NATO pe linia pregătirii și instruirii continue a personalului pune un accent evident pe această formă de pregătire².

Învățământul la distanță reprezintă un proces de învățământ flexibil care permite

instruirea în condiții optime a unor largi categorii de beneficiari cu un consum redus de resurse materiale și umane. Învățământul la distanță, bazat pe forme și metode moderne, transformă și îmbunătățește experiența de predare și învățare prin utilizarea de grafică, video și animație, realitate virtuală, chestionare și evaluări, precum și lucru colaborativ între cursanți, cu sau fără participarea instructorilor. Furnizarea materialelor de învățare pe orice dispozitiv, oriunde, oricând, prin utilizarea unor metode moderne de instruire, precum și a celor mai recente tehnologii în domeniul comunicațiilor și tehnologiei informației, determină îmbunătățirea eficacității instruirii.

Modernizarea domeniului comunicațiilor și tehnologiei informației reprezintă un proces complex și continuu pentru Armata României și reprezintă o condiție esențială pentru realizarea interoperabilității în cadrul operațiilor multinaționale și naționale. Acest fapt presupune achiziția și dotarea cu tehnică de ultimă generație de comunicații și tehnologia informației, care să corespundă cerințelor și standardelor asumate de Armata Română. Formarea profesională inițială și continuă a personalului din arma comunicații și informatică în vederea asigurării sprijinului CIS presupune acumularea de cunoștințe noi, precum

¹ Luminița Giurgiu, Ghiță Bârsan, Dănuț Moșneanu, Aspects of e-Learning and Knowledge Management Convergence in Knowledge-Based Society, International Conference on Applied Social Science 2011, Changsha, China

² NATO e-Learning Concept, 2014

și formarea și dezvoltarea de deprinderi, care sunt într-un volum din ce în ce mai mare și de un înalt grad de tehnologizare. Astfel, într-un mediu în continuă schimbare și foarte tehnologizat, procesul de instruire trebuie să progreseze, să se adapteze noilor cerințe. Sistemul de învățământ la distanță poate fi o variantă prin care personalul din arma comunicații și informatică poate să-și formeze deprinderile pentru a face față noilor cerințe ale războiului modern.

Conform portalului e-learning NATO, învățământul la distanță, care utilizează tehnologii pentru a furniza sau a îmbunătăți metodele tradiționale de învățământ, este una dintre zonele cu cea mai rapidă creștere a capacităților de educație și formare a NATO. Învățarea electronică (e-Learning) este un instrument important prin care se formează și se perfecționează într-un mod performant personalul din NATO și țările partenere, într-un mod eficient din punct de vedere al costurilor. Capacitățile sale pot oferi unui număr nelimitat de forțe o educație și o formare profesională de înaltă calitate, pentru a spori pregătirea misiunii³.

Avantajele oferite de învățământul la distanță sunt:

- Oferă posibilitatea învățării continue și dezvoltarea profesională;
- Schema de învățământ este flexibilă, ceea ce permite îmbunătățirea calității învățării, având ca rezultat utilizarea mai eficientă a resurselor umane existente;
- Contribuie la dezvoltarea unor abilități de

autoinstruire într-o atmosferă relaxantă atât pentru cursant, cât și pentru tutori sau profesori;

- Cursanții învață în mod independent, în ritmul lor, în locul și timpul pe care ei îl aleg. De asemenea, cursanții pot să se concentreze pe zonele sau temele care sunt cele mai dificile sau, dacă este necesar, pot relua unele segmente ori de câte ori este nevoie;

- Învățământul la distanță oferă flexibilitate cursanților datorită accesibilității sale 24 ore din 24, 7 zile din 7. Acesta oferă o disponibilitate a cursurilor, care permit cursanților să le parcurgă oricând doresc sau timpul le permite;

- Auto-organizarea timpului de studiu (motivație crescută, planificarea timpului și capacitatea de analiză și sinteză a conținuturilor predate);

- Învățământul la distanță răspunde nevoilor unui public dispersat geografic. Din cauza lipsei de constrângeri privind locația, se poate oferi acces la instruire și educație într-o mai mare măsură decât prin metodele tradiționale. Cursanții au nevoie de acces la un calculator cu o conexiune la rețeaua INTERNET sau INTRAMAN. Alternativ, cursanții pot descărca lecțiile și apoi să le utilizeze atunci când au timp disponibil sau după terminarea cursului;

- Locul de învățare este liber ales - depinde de mijlocul utilizat pentru distribuirea materialelor de învățat (învățarea la locul de muncă, acasă);

- Alegerea modalității de învățare – învățarea activă sau pasivă, niveluri diferite de interacțiune: „clasice” materiale scrise pe lângă notițele proprii, simulări interactive, discuții cu

³ www.act.nato.int/elearning

alți cursanți (e-mail, forum, chat), mai multe componente multimedia - grafică, animații, sunet;

- Încercarea practică a diferitelor tehnologii – se pot dobândi nu numai informații despre ceea ce se învață, ci și cunoștințe suplimentare și abilități legate de utilizarea diferitelor tehnologii;

- Învățământul la distanță oferă posibilitatea de a pune în aplicare instrumente de învățare prin colaborare prin forumuri de discuții sau de a vorbi cu colegii de clasă și instructorii de la distanță prin chat, fără limitări de timp și de locație;

- Costul total redus este probabil factorul cel mai influent pentru utilizarea învățământului la distanță. Deși inițial este costisitor prin necesitatea de a produce material educațional, ulterior sunt economii de costuri deoarece poate suporta un număr nelimitat de cursanți. De asemenea, apar economii privind reducerea costurilor legate de cazarea și deplasarea cursanților;

- Posibilitatea de a lucra în timpul desfășurării cursurilor.

Învățământul la distanță poate fi folosit într-o varietate de forme și condiții: ca metodă unică de pregătire, ca metodă de a oferi diverse cursuri de perfecționare, care ajută la menținerea unor abilități, precum și prin metoda blended learning. Potrivit conceptului NATO de e-Learning, acesta cuprinde: ADL – Advanced Distributed Learning, CBT – Computer Based Training, Immersive Learning, m-Learning și Collaborative Learning. ADL – Advanced Distributed Learning este forma comună de învățământ la distanță prin care se

oferă cursuri de instruire sau de formare profesională care sunt furnizate printr-o rețea de calculatoare folosind un browser standard (rețelele folosite pot fi INTERNET sau INTRAMAN). CBT – Computer Based Training oferă cursuri folosind CD-uri sau alte forme de stocare. Această metodă nu folosește rețelele de calculatoare pentru difuzarea informațiilor și, din motivul că informația nu mai poate fi actualizată, nu prea se mai folosește. Immersive Learning folosește un mediu simulat pe calculator care reproduce o realitate 3D. Prin simulări interactive, un cursant sau echipe de cursanți pot să dobândească sau să-și dezvolte abilități printr-o gamă largă de activități educaționale. Astfel, conceptul de gaming poate fi folosit pentru a instrui și educa. M-Learning folosește dispozitivele informatice portabile conectate wireless la rețea. Acest fapt aduce noi oportunități de interacțiune și noi provocări pentru mediul de instruire. Folosind capacitățile GPS ale dispozitivelor mobile se pot oferi materiale de învățare dinamice și ghida cursanții în timpul antrenamentelor; de asemenea, se poate furniza acces imediat și particularizat pentru fiecare cursant. Collaborative Learning oferă forma de învățământ la distanță colaborativ prin forumuri de discuții, webminarii și webcast-uri. Acesta permite schimbul activ de discuții și idei, atât între tutore și cursanți, cât și între mai mulți cursanți. Acest schimb activ de discuții și idei promovează gândirea critică, precum și dezvoltă capacitatea de lucru în echipă.

Blended learning îmbină metoda de învățământ la distanță cu metoda de învățământ clasică, într-o clasă tradițională, față în față.

Această metodă combină cele mai bune caracteristici ale învățământului la distanță (accesibilitate, disponibilitate, costuri reduse) cu cele oferite de învățământul în clasă (interacțiune socială). Această metodă oferă posibilitatea de a combina implementarea de strategii de învățare sincronă, specifică cursurilor în clasă, cu strategii de învățare asincronă, prin beneficiul adus de învățarea în ritmul propriu. Cursanții primesc și învață noțiunile teoretice prin intermediul învățământului la distanță și astfel aceștia vor ajunge mai bine pregătiți la instruirea în clasă. În acest mod, instruirea la clasă se poate desfășura preponderent prin activități practice. Prin folosirea diverselor metode de simulare on-line a unor echipamente de comunicații și tehnologia informației, anumite deprinderi practice se pot dobândi și prin învățământ la distanță, iar activitățile în clasă vor cuprinde atunci doar acele practice complexe, care presupun efectiv existența unor echipamente care nu pot fi simulate sau care necesită un grad ridicat de interacțiune cu tehnica militară.

Programele de formare și educație trebuie definite, proiectat, dezvoltate, livrate, evaluate, validate și gestionate după anumite standarde și modele recunoscute. Modelul ADDIE a fost creat pentru a gestiona procesul de instruire. Acesta cuprinde următoarele etape: analiza, proiectarea, dezvoltarea, implementarea și evaluarea. Prin folosirea acestui model se asigură că toate programele de formare se concentrează pe competențele și cunoștințele esențiale care satisfac operațional nevoile specifice. Prin forma sa iterativă a pașilor se confirmă faptul că cerința

de instruire a fost îndeplinită. De asemenea, programele sunt adaptate la nevoile și caracteristicile de învățare ale beneficiarilor și astfel educația se desfășoară într-un mod care previne sau elimină efortul inutil. În faza de analiză se definesc obiectivele instructive plecând de la o înțelegere clară a rezultatului dorit, a nevoilor de instruire, dar și a cunoștințelor și abilităților actuale ale cursanților. Astfel se stabilesc obiective, mediul de învățare, opțiuni de livrare a informațiilor, precum și timpul avut la dispoziție. Faza de proiectare este procesul prin care se planifică designul cursului: conținutul temei, metoda de instruire, exercițiile, conținutul cursurilor și criteriile de evaluare. În faza de dezvoltare sunt produse și asamblate materialele care au fost dezvoltate în faza anterioară. În această fază, materialele ce curs audio și video sunt create, colectate și pregătite pentru a fi testate. Faza de implementare este momentul în care cursul dezvoltat este pus în practică și este prezentat ca un produs prototip publicului țintă. În faza de evaluare se recepționează feedback-ul de la cursanți pentru identificarea eficacității și calității conținutului educațional și pentru a regla programul. În această fază se determină dacă materialele de instruire au eficacitate și dacă obiectivele au fost îndeplinite.

Prin folosirea unui sistem adaptiv de învățământ la distanță se asigură difuzarea către fiecare cursant a unui parcurs și conținut pedagogic particularizat pentru fiecare individ. Sistemul adaptiv de învățământ la distanță este un sistem orientat spre cursant și oferă posibilitatea de învățare individualizată oferind o experiență

personală și unică, cu scopul final de a maximiza performanța acestuia. Sistemul adaptiv de învățământ la distanță este definit ca un: „...sistem interactiv care personalizează ... [care] adaptează conținutul prezentat pe e-Learning, metodele pedagogice și interacțiunile dintre participanții la mediu pentru a satisface nevoile și preferințele individuale ale utilizatorilor atunci când apar”⁴. De asemenea, sistemul adaptiv de învățământ la distanță a mai fost definit ca: „o metodă de a crea experiență de învățare a elevului, dar și tutorelui, bazată pe configurația unui set de elemente într-o anumită perioadă având ca scop creșterea performanței unui criteriu predefinit”⁵. Aceste criterii ar putea fi nivelul de cunoștințe pe care cursantul le deține în momentul începerii unei forme de pregătire, formele și metodele de învățământ care au o mai mare eficiență în formarea competențelor și deprinderilor individuale sau feedback-ul utilizatorilor.

Învățământul la distanță reprezintă un proces de învățământ flexibil care permite instruirea în condiții optime a unor categorii largi de beneficiari cu un consum redus de resurse materiale și umane.

Implementarea propriei platforme de învățământ la distanță, optimizată pentru instruirea de comunicații și informatică, reprezintă una din preocupările permanente ale

Centrului de Instruire pentru Comunicații și Informatică de a veni în întâmpinarea nevoii crescute și din ce în ce mai diversificate de instruire. Preocupările pe această direcție fac parte din însăși natura existenței sale, și anume creșterea calității actului educațional prin folosirea unor metode și mijloace moderne, care să permită facilitarea asimilării conținutului informațional. Fiind singura instituție din cadrul MApN a cărei menire este instruirea cu caracter preponderent practic pe linie de comunicații și informatică, Centrul de Instruire pentru Comunicații și Informatică Sibiu își propune, prin desfășurarea unei astfel de forme de învățământ, să marcheze o nouă etapă în evoluția învățământului militar de specialitate.

Principalele domenii de acțiune în cadrul sistemului de învățământ la distanță destinat formării profesionale continue a specialiștilor din domeniile comunicații, tehnologia informație și apărarea cibernetică din Armata României sunt: specializarea și perfecționarea în domeniul comunicațiilor și tehnologiei informației prin utilizarea unui sistem de învățământ centrat pe cursant, optimizarea procesului de instruire prin oferirea de material pedagogic particularizat pentru fiecare cursant, utilizarea tehnicilor de virtualizare pentru aplicații sau simulatoare de planificare și programare a echipamentelor de comunicații și informatică, micșorarea timpului destinat realizării instruirii, precum și utilizarea mult mai eficientă a tehnologiilor avute la dispoziție.

⁴S. Stoyanov, P. Kirschner, Expert Concept Mapping Method for Defining the Characteristics of Adaptive E-Learning: ALFANET Project Case, Educational Technology, Research & Development, 2004

⁵D. Burgos, T. Tattersall, R. Koper, Representing Adaptive E-learning Strategies in IMS Learning Design, TENCompetence Conference, 2004, Sofia, Bulgaria

Bibliografie:

- **** NATO e-Learning Concept, 2014;
- Luminița Giurgiu, Ghiță Bârsan, Dănuț Moșneanu, Aspects of e-Learning and Knowledge Management Convergence in Knowledge-Based Society, International Conference on Applied Social Science 2011, Changsha, China
- Diane Elkins, Desiree Pinder, E-learning Fundamentals, 2015

Pagini web:

- www.act.nato.int/elearning
- <https://jatl.act.nato.int>
- www.elearninglearning.com
- <https://elearningindustry.com>

CENTRUL 89 STRATEGIC DE COMUNICAȚII ȘI INFORMATICĂ ÎN PAS SAU ÎN „CONFLICT” CU EVOLUȚIA TEHNOLOGIEI INFORMAȚIEI?

Locotenent-colonel Florin NICU-TONCEAN

Centrul 89 Strategic de Comunicații și Informatică



La ceas aniversar, rememorez momentul în care, în mai 2017, am reușit să devin membru al „familiei” Centrului 89 Strategic de Comunicații și Informatică. Spun

familie și nu mai pun ghilimele pentru că, din toate impresiile și concluziile pe care le-am tras de-a lungul timpului despre unitate, atât în urma activității pe care am desfășurat-o în Centrul de Management General de Bază al RTP (denumirea de atunci a Centrului Operațional de Rețea de Bază), cât și a activităților ulterioare executate din postura de membru în diferite comisii ale Direcției Comunicații și Tehnologia Informației și Comandamentului Comunicațiilor și Informaticii, cel mai puternic m-au impresionat spiritul de echipă și înțelegerea mutuală care defineau oamenii de aici. Din postura de membru al familiei, am realizat în timp scurt că amintirile și impresiile proprii referitoare la unitate erau confirmate din multe puncte de vedere dar, [bineînțeles că există întotdeauna un „dar”] am înțeles și faptul că totul este într-o continuă schimbare. Astfel, am descoperit faptul că și în Centrul 89 Strategic de Comunicații și Informatică procesul de transformare a Armatei României și-a pus pe deplin amprenta. Mulți dintre cei cu care am lucrat

împreună în urmă cu 10-15 ani au plecat din unitate, iar cei care au rămas erau parcă mai distanți, mai încruntați. Am sperat un timp că este vorba despre perioada de „citire” și adaptare la cerințele și conduita impuse de noua echipă de comandă investită în vara anului 2017, dar nu acesta era motivul.

Reorganizarea sistemului militar și evoluția tehnologică rapidă au generat modificări structurale semnificative și au impus o adaptare dinamică a unității pentru a putea acoperi un set de domenii de activitate care din străine trebuiau să ne devină prietene. Coloana vertebrală a unității, constituită din „cătanele bătrâne”, cărora calculatorul nu a reușit să le întrerupă cursul carierei militare, susținea cu oarece dificultate povara noilor provocări tehnologice. Sentimentul responsabilității, al demnității și al datoriei față de haina militară și față de unitate nu puteau fi umbrite de utilizarea unor jumătăți de măsură în rezolvarea noilor sarcini. Multă tehnică nouă, diferită de ce au avut până atunci în dotare, concepte și principii noi...

Am simțit acea perioadă ca pe o perioadă de cotitură în viața unității. Aveam nevoie de ajutor. Așa cum familiile întemeiate pe dragoste, încredere și respect rezistă oricărei încercări, am strâns rândurile și am încercat să găsim soluțiile și căile de urmat pentru a face față acestor provocări.

Oare câți dintre noi nu am cumpărat un „device” nou și am deschis din prima manualul de

operare pentru a citi instrucțiunile de utilizare, în timp ce copiii noștri au luat echipamentul, l-au pornit și au început să-l utilizeze de parcă ar fi fost proiectat de ei? Probabil vă imaginați că am avut parte de această surpriză atunci când am fost solicitați să ne asumăm responsabilități în domeniul telefoniei mobile criptate, apărării cibernetice sau rețelelor de misiune. Nu a fost vorba de surprindere! Poate am avut nevoie de un moment pentru regroupare. Mai mulți „copii” din familie au realizat că au învățat, fie pe băncile școlii, fie din pasiune, „segmente” din lucrul cu echipamentele sau din noile concepte în curs de implementare. De aici până la nominalizarea responsabililor de proiecte și constituirea echipelor de lucru nu a mai fost decât un pas. Și ce mare a fost acest pas! Personal l-am perceput ca pe un moment al confirmării maturizării tinerilor camarazi, de câștigare a respectului, de responsabilizare a acestora, dar, ca să respect cele afirmate mai sus, a fost un moment de consolidare a coloanei vertebrale a unității. A fost clipa în care

am înțeles că orice obstacol ar fi pus în fața minunatei noastre familii, ar fi prea mic să ne oprească din drum și că putem onora realizările trecutului cu reușitele viitorului. Printr-o metamorfoză extraordinară impusă de caracterul și educația oamenilor din „Schalke 04”, timiditatea a devenit ambiție, suficiența a devenit orgoliu și sete de cunoaștere. Și nu vorbesc de schimb de generații! Vorbesc de promovarea, integrarea și, cât de curând, consacrarea tinerei generații în rândul specialiștilor în armă.

Am certitudinea că, indiferent cât de rapid se va dezvolta tehnologia, vom găsi resursa umană și viteza în plus care să ne permită să împlânzim și să stăpânim tehnica.

Împlinirea a 70 de ani de existență a unității din care, simt nevoia să mărturisesc cu mândrie, fac și eu parte, îmi oferă prilejul să urez celor care au muncit și muncesc în această unitate și tuturor celor dragi acestora, multă sănătate, împliniri familiale și profesionale și LA MULȚI ANI!



CLOUD COMPUTING - O DESCOPERIRE UTILĂ SAU UN MOTIV DE ÎNGRIJORARE PENTRU SECURITATEA INFORMAȚIILOR

Locotenent-colonel Cristinel OLARU

Locotenent Cătălin MÂRZA

Centrul 89 Strategic de Comunicații și Informatică



Rezumat:

Scopul acestui material este de a explora conceptul de „cloud computing”, de a analiza dacă acest nou concept este un plus sau un minus pentru evoluția tehnologiei și de a oferi informațiile necesare care ar putea ajuta o organizație pentru a lua o decizie pro sau contra privind implementarea noului concept. Acesta presupune externalizarea infrastructurii

de rețea, găzduirea informațiilor și a aplicațiilor de către un furnizor specializat, care să ofere întregul suport în ceea ce privește stocarea și rularea aplicațiilor necesare organizației.

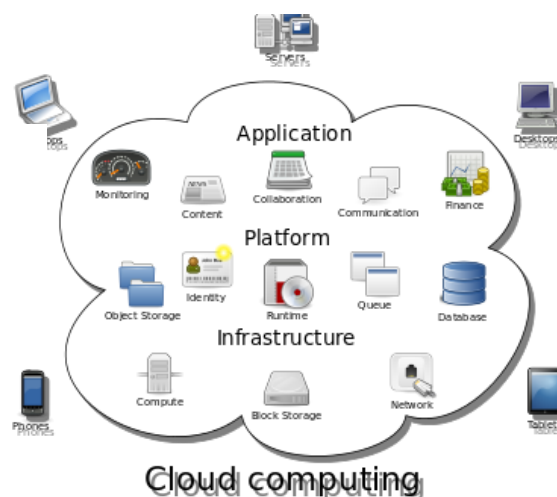
CE ESTE CLOUD COMPUTING?

„Cloud computing” este conceptul prin care descriem diferite situații în care resursele de calcul sau de operațiuni sunt livrate ca un serviciu printr-o conexiune de rețea. Conceptul reprezintă ansamblul distribuit de servicii de calcul, aplicații, acces la informații și stocare de date, fără ca utilizatorul să fie nevoit să cunoască amplasarea și configurația fizică a sistemelor care furnizează aceste servicii.

Dacă privim doar din perspectiva produsului livrat, „cloud computing” se poate împărți în trei categorii: Software as a Service - Software ca Serviciu (SaaS), Platform as a Service - Platformă ca Serviciu (PaaS) și Infrastructure as a Service - Infrastructură ca Serviciu (IaaS).

Cel mai comun și cel mai des folosit este SaaS. Se referă la un model de produs în care

aplicațiile sunt găzduite de un provider și sunt disponibile prin intermediul unei infrastructuri private, cu ajutorul unei conexiuni la internet. Multe persoane folosesc un SaaS fără să-și dea seama că aplicațiile web prin care o fac sunt livrate în acest mod cum ar fi: Gmail, Facebook și Twitter sau este foarte probabil ca factura pe care o primim în urma cumpărăturilor online să fie livrată printr-un sistem SaaS.



PaaS este o categorie diferită și se adresează mai ales dezvoltatorilor. Serviciile PaaS sunt de obicei livrate către dezvoltatori care au nevoie de un mediu în care să-și construiască aplicațiile. Din punct de vedere al flexibilității, acest tip de client știe de ce componente, sisteme de operare sau programe terțe are nevoie și caută un provider „cloud” care îi poate îndeplini cerințele. Este important factorul sau puterea de replicare a acestui serviciu, nu de puține ori fiind nevoie de adăugarea altor medii de dezvoltare într-un timp scurt.

IaaS, prin definiția termenului, se referă la infrastructură. Este gândit ca o suită de resurse virtualizate, adunate sub un serviciu printr-o conexiune de internet. IaaS include resurse ca spațiu pe disk virtualizat, spațiu de stocare flexibil cu accesibilitate foarte mare, conexiuni diferite și multiple, adrese de IP cu destinație specială sau alte caracteristici speciale.

Serviciile „cloud” pot fi împărțite în următoarele două categorii: private și publice.

Un „cloud” public se referă la acel sistem în care serviciile și infrastructura sunt oferite de un terț. Serviciile sunt accesate printr-o rețea de internet publică. Acest tip de cloud este cel mai avantajos din punct de vedere economic și al scalabilității. Dezavantajul este constituit de vulnerabilitatea la atacurile cibernetice datorită nivelului mare de accesibilitate.

„Cloud-ul” privat însă se găsește într-o rețea privată, administrată de o echipă sau un expert în securitate, având o platformă de servicii și o infrastructură accesibilă unui client sau a unui număr strict limitat de clienți.

Cloud computing se bazează pe partajarea resurselor software și a informațiilor în internet care sunt folosite de utilizator și găzduite pe un server virtual.

Cu toate că mai mult de 80% din datele stocate la nivel mondial se preconizează că se vor muta în „cloud” în următorii 5 - 10 ani, există o serie de întrebări fără răspuns deocamdată, care vor decide cât de repede va avea loc dezvoltarea în această zonă. Este un nou concept în domeniul tehnologiei informației care încearcă să fie acceptat, unde serviciile tehnice și aplicațiile să fie furnizate de o terță parte.

AVANTAJELE IMPLEMENTĂRII CONCEPTULUI CLOUD COMPUTING

Sunt o serie de factori pozitivi ce atrag atenția asupra noului concept, cum ar fi:

- **Flexibilitatea.** Tehnologiile „cloud” permit ajustarea cantității de resurse alocate, în mod automat, în funcție de necesități. Nivelul resurselor alocate trebuie să fie doar puțin mai ridicat față de nivelul resurselor consumate. Organizațiile nu mai sunt nevoite să investească sume mari în produsele hardware pentru scalabilitate.

- **Creșterea eficienței și controlul costului.** Întregul cost pentru stocarea informațiilor în „cloud” este mult mai redus față de modul tradițional. În cadrul organizației militare, acest cost privind rularea sistemelor IT poate fi văzut ca un cost operațional.

- **Reducerea semnificativă a investițiilor** în ceea ce privește achiziția de hardware și software, deoarece aceasta se face central, la furnizor;

- **Eliminarea problemelor în ceea ce privește durata de viață** a resurselor hardware/software și **a costurilor cu mentenanța.**

- **Posibilitatea utilizării doar a aplicațiilor necesare,** nefiind obligatorie achitarea întregului cost pentru pachetul software.

- **Dinamicitatea resurselor** adiționale de tehnică de calcul nu provoacă nicio întrerupere în funcționarea rețelei datorită tehnologiei de virtualizare. Odată ce avem un sistem funcțional în „cloud”, el poate fi replicat sau dublat foarte rapid.

- **Accesarea integrală a informațiilor de oriunde** folosind browser-ul PC-ului. Tot ceea ce avem nevoie este doar un PC și o conexiune la internet, „cloud-ul” funcționând prin împărțirea informației pe mai multe servere, dar fără a crea dependență tehnică fixă între ele. În orice moment, dacă un server devine inutilizabil sau întâmpină probleme de funcționare, din orice motive, restul sistemelor pot suplini lipsa lui.

DEZAVANTAJELE IMPLEMENTĂRII CONCEPTULUI CLOUD COMPUTING

Având în vedere că orice lucru are și părțile lui negative, în ceea ce privește „cloud computing” identificăm câteva dezavantaje care trebuie luate în considerare, cum ar fi:

- Centralizarea datelor în afara controlului organizației. Dacă vorbim de organizația militară, atunci rezultă o problemă majoră în ceea ce privește securitatea informațiilor, căci datele sensibile vor fi de acum sub controlul furnizorului de servicii.

- Aplicația fiind furnizată ca un serviciu și

folosită de un client diferit, personalizarea pare a fi limitată.

- Având în vedere că totul va fi accesibil prin intermediul internetului, acest lucru va face ca structura să devină dependentă de rețea și de infrastructura de service a furnizorului. Structura nu va putea desfășura nicio activitate dacă nu există legătură la internet.

- Dacă, din diferite motive, apar nemulțumiri față de furnizorul de servicii, schimbarea acestuia înseamnă reformatarea datelor și convertirea lor, ceea ce presupune timp suplimentar și un cost adițional privind transferul.

CONCLUZIE

Având în vedere avantajele și dezavantajele menționate, considerăm că nu deținem încă un răspuns concret în favoarea sau defavoarea acestui concept. În ceea ce privește organizația militară, până când preocupările legate de confidențialitatea informațiilor vor fi soluționate pentru „cloud computing”, aplicațiile și informațiile critice sau sensibile ar trebui să fie vehiculate în continuare pe modelul tradițional. Între timp, aplicațiile simple vor deveni din ce în ce mai populare în spațiul „cloud”. Conceptul și tehnologia sunt aici pentru a rămâne, sunt în faza incipientă, dar avem de parcurs un drum lung înainte de a ajunge la maturitate.

Cloud-ul a devenit și va fi pentru multă vreme o soluție eficientă pentru asigurarea serviciilor de comunicații. „Cloud computing” prezintă deci o serie de avantaje, dar și dezavantaje, iar decizia de a implementa conceptul ar trebui să se bazeze pe nevoile organizației.

BIBLIOGRAFIE:

- Brandel, M. (2009). The Trouble with Cloud Vendor Lock in. Retrieved from [http://www.cio.com/article/488478/](http://www.cio.com/article/488478/The-Trouble-with-Cloud-Vendor-Lock-in) The Trouble with Cloud Vendor Lock in.
- Cunningham, P. & Wilkins, J. (2009). A Walk in the Cloud. Information Management (15352897), 43(1), pp.22-30. Retrieved from Computers & Applied Sciences Complete database.
- Erdogmus, H. (2009). Cloud Computing: Does Nirvana Hide behind the Nebula?
- Nelson, M. (2009). The Cloud, the Crowd, and Public Policy. Issues in Science & Technology, 25(4), pp.71-76. Retrieved from Computers & Applied Sciences Complete database.
- Zhong, L., Wo, T., Li, J. & Li, B. (2010). A Virtualization - based SaaS Enabling Architecture for Cloud Computing. 2010 Sixth International Conference on Autonomic and Autonomous Systems. pp.144-149.

ÎMBUNĂTĂȚIREA NAVIGAȚIEI PRIN SATELIT UTILIZÂND SISTEMUL EGNOS (EUROPEAN GEOSTATIONARY NAVIGATION OVERLAY SERVICE)

Maior Vasile VLAD

Locotenent Teodor MITREA

Centrul de Instruire pentru Comunicații și Informatică „Decebal”



1. Introducere

Un sistem global de navigație prin satelit (GNSS – Global Navigation Satellite System) reprezintă un sistem care calculează poziția geospațială a obiectelor de pe pământ sau din spațiu cu ajutorul semnalelor recepționate de la sateliții de navigație.

Navigationa cu ajutorul sateliților este o tehnică prin care un utilizator își poate determina poziția bazându-se pe măsurarea distanței între sateliții care orbitează în jurul Pământului și receiverul sistemului său de navigație. Fiecare satelit transmite așa-numitele efemeride - informații despre propria poziție la orice moment dat în timp, cât și semnale periodice care sunt folosite pentru determinarea timpului de propagare a semnalului de la satelit la receiver. Acest timp poate fi convertit în distanță prin aproximarea faptului că viteza semnalului este constantă.

Cunoscând poziția sateliților și distanța până la aceștia, prin folosirea principiului triangulației,

echipamentul de navigație își poate calcula poziția. Teoretic, această poziție poate fi determinată utilizând datele de la trei sateliți, dar, în practică, este nevoie de un al patrulea satelit pentru a estima o a patra necunoscută (în afară de cele trei coordonate spațiale) - eroarea de timp a sistemului de navigație, deoarece ceasul receptorului nu are acuratețea de timp pe care o au ceasurile de la bordul sateliților. Evident, cu cât mai mulți sateliți se află în aria de vizibilitate, cu atât estimarea poziției devine mai exactă.

Cel mai cunoscut sistem de navigație este GPS (Global Positioning System), un sistem de navigație global folosit de utilizatori din întreaga lume, dar care aparține armatei Statelor Unite ale Americii. Însă GPS nu este singurul sistem de acest tip. GLONASS (GLOBAL NAVIGATION Satellite System/Global'naya Navigatsionnaya Sputnikovaya Sistema) este sistemul global de navigație prin satelit care aparține Federației Ruse, având performanțe similare cu sistemul american.

În ceea ce privește sistemele de navigație încorporate în telefoanele mobile, aproape toate cele de ultimă generație suportă funcția A-GPS (Assisted GPS) care permite atât scăderea timpului necesar pentru localizare, cât și îmbunătățirea preciziei prin utilizarea informațiilor geografice ale hot-spoturilor Wi-Fi și ale antenelor celulare din apropiere. Această funcție este utilă în principal în aglomerările

urbane, unde clădirile înalte blochează de multe ori vizibilitatea directă la sateliții de navigație, iar hot-spoturile Wi-Fi și antenele celulare sunt mult mai dese.

Mai mult, dacă până acum câțiva ani aproape toate sistemele de navigație prin satelit se bazau pe GPS, sistemele de navigație moderne (inclusiv cele încorporate în telefoanele mobile) folosesc multiple sisteme de poziționare, crescând astfel precizia de localizare.

2. Sisteme complementare de îmbunătățire a navigației prin satelit

Un GNSS (cum este GPS) poate deveni chiar mai precis cu ajutorul sistemelor complementare de îmbunătățire a navigației prin satelit (SBAS – Satellite Based Augmentation Systems). Aceste sisteme iau în calcul factori de mediu cum ar fi erorile provocate de traversarea ionosferei sau exploziile solare pentru a îmbunătăți datele furnizate de GNSS.

Un exemplu de SBAS este EGNOS (European Geostationary Navigation Overlay Service), sistem care reprezintă prima contribuție a Europei la navigația prin satelit, îmbunătățind precizia sistemului american de navigație cu ajutorul unor sateliți geostaționari. Acest sistem este considerat a fi predecesorul lui Galileo, sistemul european de navigație prin satelit aflat în dezvoltare în acest moment, un produs al colaborării dintre ESA (European Space Agency) și EC (European Commission). Primii sateliți au fost lansați în 2011, la sfârșitul lui 2016 au fost furnizate primele servicii, iar în timp vor fi testate și puse la dispoziție servicii noi, finalizarea sistemului fiind estimată pentru 2020 și prevăzând

o constelație formată din 30 de sateliți.

EGNOS nu este singurul sistem de acest tip. Statele Unite ale Americii au WAAS (Wide Area Augmentation System), Japonia are MSAS (Multi-functional Satellite Augmentation System), iar India deține sistemul GAGAN (GPS and GEO Augmented Navigation). De asemenea, Federația Rusă își modernizează sistemul GLONASS prin propriul SBAS - SDCM (System for Differential Corrections and Monitoring); similar, China își modernizează sistemul de navigație denumit BEIDOU.

Principala diferență între SDCM și celelalte SBAS este că acesta este conceput ca un sistem de îmbunătățire a navigației ce folosește atât semnalele furnizate de sateliții GPS, cât și cele furnizate de cei ai GLONASS, în timp ce celelalte SBAS furnizează corecții și mesaje de integritate bazate doar pe sateliții GPS.

3. Îmbunătățirea navigației utilizând sistemul EGNOS

În ceea ce privește EGNOS, cele mai importante componente ale acestui sistem sunt:

- componenta terestră formată din stații de referință care monitorizează sateliții - RIMS (Ranging & Integrity Monitoring Stations), centre de control - MCC (Mission Control Centres) și stații de up-link - NLES (Navigation Land Earth Stations);
- componenta spațială formată din sateliții geostaționari.

La momentul actual, componenta terestră este formată din peste 40 de site-uri, din care 34 stații de referință, 2 centre de control și 6 stații de up-link.

Fiecare stație de monitorizare, a cărei locație este cunoscută foarte exact, colectează date brute de la sateliți, transmițând erorile detectate la centrele de control. La acestea din urmă se realizează o prelucrare a datelor în timp real, efectuându-se corecții diferențiale care se transmit prin intermediul stațiilor de up-link către sateliții geostaționari fiind difuzate apoi către utilizatori, în aria de acoperire. Astfel, precizia actualelor semnale GPS este îmbunătățită la mai puțin de 2 m, având o disponibilitate de peste 99%. Mai mult, sistemul furnizează un mesaj de integritate referitor la continuitatea și disponibilitatea semnalului, cât și un semnal de timp universal extrem de exact.

EGNOS este esențial pentru aplicații în care precizia și integritatea sunt critice. În 2011 EGNOS a fost certificat pentru aviația civilă, satisfăcând standardele ICAO (International Civil Aviation Organization). Pe lângă acest sector, de acest sistem beneficiază numeroase alte domenii, cum ar fi transporturile, navigația maritimă, supravegherea și cartografierea.

Aria de acoperire a EGNOS cuprinde majoritatea Europei, aceasta depinzând de dispunerea stațiilor de monitorizare, iar România se află la granița acestei zone, beneficiind doar parțial de serviciile acestui sistem. În prezent, sunt în derulare câteva proiecte pentru extinderea EGNOS. Monitorizarea performanței sistemului în zonele de frontieră este fundamentală pentru acest proces de extindere, România fiind o locație ideală pentru realizarea de măsurători.

Studii recente au demonstrat că în țările aflate la granița ariei de acoperire estimările cu

privire la performanțele sistemului sunt optimiste, semnalul suferind o degradare semnificativă în zonele cu vizibilitate redusă (de exemplu, în zonele împădurite) sau în zonele urbane ^{[5],[6]}.

În cazul Finlandei - o altă țară care se află la limita zonelor de acoperire a sistemului european (EGNOS) și a celui rusesc (SDCM) - studii efectuate de Institutul Finlandez de Cercetări Geospațiale au demonstrat că, în anumite situații, sistemul rusesc oferă o precizie mai bună decât cel european^[6].

Cea mai plauzibilă explicație pentru acest rezultat ar fi faptul că sistemul rusesc utilizează atât semnalele furnizate de sateliții GPS, cât și pe cele furnizate de cei ai GLONASS, în timp ce EGNOS furnizează corecții și mesaje de integritate bazate doar pe sateliții GPS.

Întrucât România se află la granița ariei de acoperire, studierea modului în care s-ar putea îmbunătăți performanțele sistemului de navigație prin implementarea unor stații de monitorizare pe teritoriul României și beneficiile pe care le-ar aduce în diverse domenii prezintă un real interes.

Parametrul care măsoară acuratețea semnalului de navigație este denumit Navigation System Error (NSE) – eroarea sistemului de navigație, fiind definit ca diferența maximă ce poate apărea între poziția reală și poziția estimată de către echipamentul de navigație. Acesta, la rândul său, are două componente: Horizontal Navigation System Error (HNSE) și Vertical Navigation System Error (VNSE).

Pentru a evidenția diferențele de acuratețe în estimarea poziției în situația implementării unor stații de monitorizare pe teritoriul țării noastre, s-

au realizat câteva simulări. Astfel, în figurile 1 și 2 sunt prezentate două simulări ce compară valorile HNSE în două cazuri: situația actuală a acurateței semnalului de navigație pe suprafața României și situația ipotetică în care la Sibiu s-ar afla încă o stație de monitorizare.

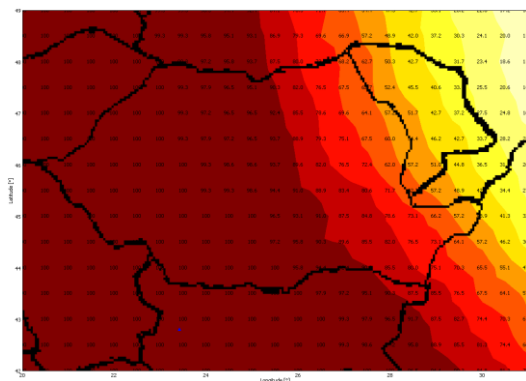


Figura 1 – HNSE EGNOS în situația actuală

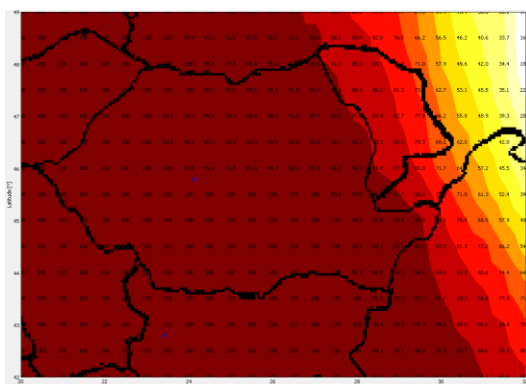


Figura 2 – HNSE EGNOS cu stație de monitorizare la Sibiu

Rezultatele obținute ilustrează acuratețea sistemului în fiecare caz în parte, mai exact, procentele de timp în care valorile HNSE se situează sub o anumită limită impusă.

Se poate observa din aceste simulări că dezvoltarea rețelei prin construirea unei astfel de locații ar fi suficientă pentru ca serviciile EGNOS să acopere toată suprafața țării noastre.

În cazul în care se impun limite mai stricte pentru valorile HNSE (8 metri), așa cum este necesar în cazul aplicațiilor în care precizia devine critică, implementarea unei stații de monitorizare

la Sibiu, chiar dacă duce la îmbunătățirea performanței sistemului, așa cum reiese din figurile 3 și 4, nu este suficientă.

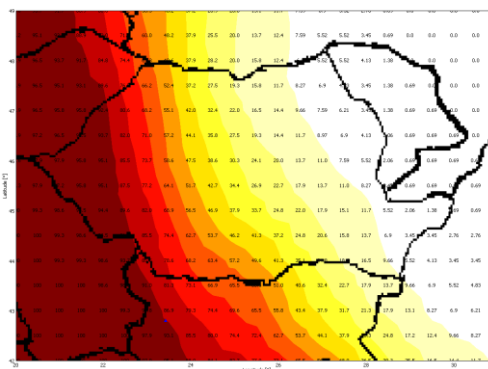


Figura 3 – HNSE EGNOS (8 m)

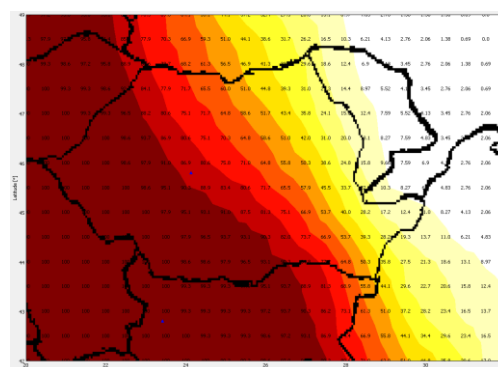


Figura 4 – HNSE EGNOS cu stație de monitorizare la Sibiu (8 m)

Pe de altă parte, dezvoltarea rețelei prin implementarea mai multor stații de monitorizare (Sibiu, Iași și Constanța) ar duce la o creștere semnificativă a performanțelor sistemului, în special în partea estică a României, lucru ilustrat în figura 5.

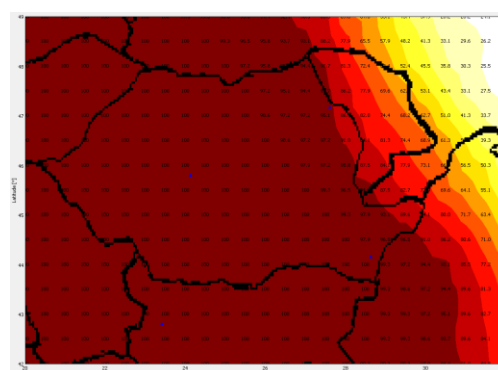


Figura 5 – HNSE EGNOS cu 3 stații de monitorizare în România (8 m)

4. Concluzii

Pentru România, EGNOS reprezintă o oportunitate pentru îmbunătățirea siguranței și eficienței aviației, pentru agricultură, transportul la sol, telecomunicații și informatică, cartografiere și alte aplicații.

Prin simulările efectuate s-a evidențiat modul în care s-ar putea îmbunătăți performanțele

sistemului de navigație pe teritoriul României prin implementarea unor noi stații de monitorizare. S-au făcut simulări folosind două scenarii, unul în care s-a adăugat o stație de monitorizare la Sibiu și unul în care s-au adăugat trei stații de monitorizare (Sibiu, Iași și Constanța), ambele având ca rezultat o modificare pozitivă a performanțelor sistemului.

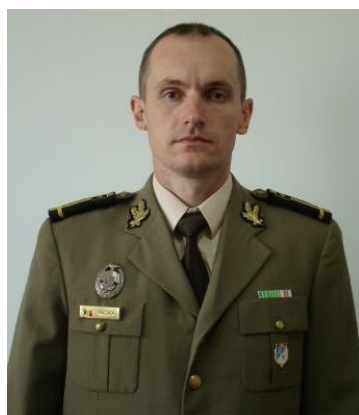
Bibliografie:

1. European GNSS Agency, EGNOS Safety of Life (SoL) Service Definition Document, ISBN 978-92-9206-028-2, 2016;
2. European GNSS Agency, EGNOS Open Service (OS) Service Definition Document, ISBN 978-92-9206-018-3, 2015;
3. https://en.wikipedia.org/wiki/European_Geostationary_Navigation_Overlay_Service;
4. https://egnos-user-support.essp-sas.eu/new_egnos_ops/egnos-system/about-egnos;
5. Mohammad Zahidul H. Bhuiyan, Heidi Kuusniemi, Auryn Soderini, Salomon Honkala and Simo Marila, „Performance of EGNOS in North-East European Latitudes”, Conference Paper, January 2017;
6. Simo Marila, Mohammad Zahidul H. Bhuiyan, Jaakko Kuokkanen, Hannu Koivula, Heidi Kuusniemi, „Performance Comparison of Differential GNSS, EGNOS and SDCM in Different User Scenarios in Finland”, Conference Paper, May 2016.

SISTEME DE MANAGEMENT AL DOCUMENTELOR: ROL ȘI CRITERII DE EVALUARE ÎN PERSPECTIVA IMPLEMENTĂRII ÎN MEDIUL MILITAR

Maior Nuțu-Marius MACHEK

Centrul de Instruire pentru Comunicații și Informatică „Decebal”



Introducere

Importanța managementului informațional pentru eficientizarea conducerii curente, luarea deciziilor operaționale și administrative și obținerea superiorității informaționale reprezintă un stimulent pentru modernizarea sistemelor informatice ale unităților militare din Armata României prin adoptarea unor tehnologii moderne de management al documentelor, similar cu NATO și statele aliate. Sistemele de management al documentelor (SMD) pot contribui la crearea condițiilor pentru optimizarea fluxurilor și proceselor informaționale, precum și a metodelor de management al informațiilor, conform concepției de modernizare și optimizare a sistemului de comunicații și informatică al Armatei României. Cu siguranță, progresele realizate în ultimii ani prin implementarea unor tehnologii care și-au dovedit beneficiile, cum sunt migrarea în mediul electronic a corespondenței între unitățile subordonate Statului Major al Apărării, semnătura electronică și portalurile web, pot fi valorificate mai bine prin utilizarea SMD.

În general, managementul documentelor este cunoscut în ultimii ani sub denumirea de

managementul conținutului în întreprindere (Enterprise Content Management - ECM) și se referă la informațiile nestructurate, fără o schemă sau mod de organizare predefinit, spre deosebire de cele structurate, care pot fi gestionate cu ajutorul bazelor de date și al aplicațiilor specializate. Una din cele mai populare definiții a fost publicată de Asociația Internațională pentru Managementul Informațiilor și Imaginilor, o organizație profesională non-profit fondată în 1943 în Statele Unite, conform căreia ECM este o combinație de strategii, metode și instrumente folosite pentru a colecta, administra, stoca, păstra și furniza informațiile care sprijină procesele organizaționale pe toată durata ciclului de viață¹. În mediul militar, sistemul de management al documentelor sau conținutului ar fi o componentă de bază a sistemului informatic care, conform Doctrinei managementului informațional în Armata României [1], are un rol foarte asemănător: să faciliteze operațiile de culegere, diseminare, stocare, prelucrare și protecție a datelor și informațiilor. Indiferent de denumire, practic toate informațiile sunt conținute în documente și managementul eficient al acestora depinde de utilizarea unor mijloace performante de tehnologia informațiilor.

¹ <http://www.aiim.org/What-is-ECM-Enterprise-Content-Management>, accesat 29.03.2018

Conceptele de „document” sau „document în formă electronică” au mai multe semnificații. În sensul prezentului articol, prin document se înțelege o reprezentare codificată a unor texte, imagini și/sau sunete cu caracter unitar, scrisă de regulă într-un singur fișier pe un mediu de stocare, care poate fi citită cu aplicația software care a generat-o sau cu o aplicație echivalentă.

Rolul SMD în ciclul de viață al informațiilor

Un model al ciclului de viață realizat prin separarea etapelor de culegere, administrarea, stocare, păstrare și furnizare, la care am adăugat principalele fluxuri informaționale existente în unități militare, este reprezentat în figura 1.

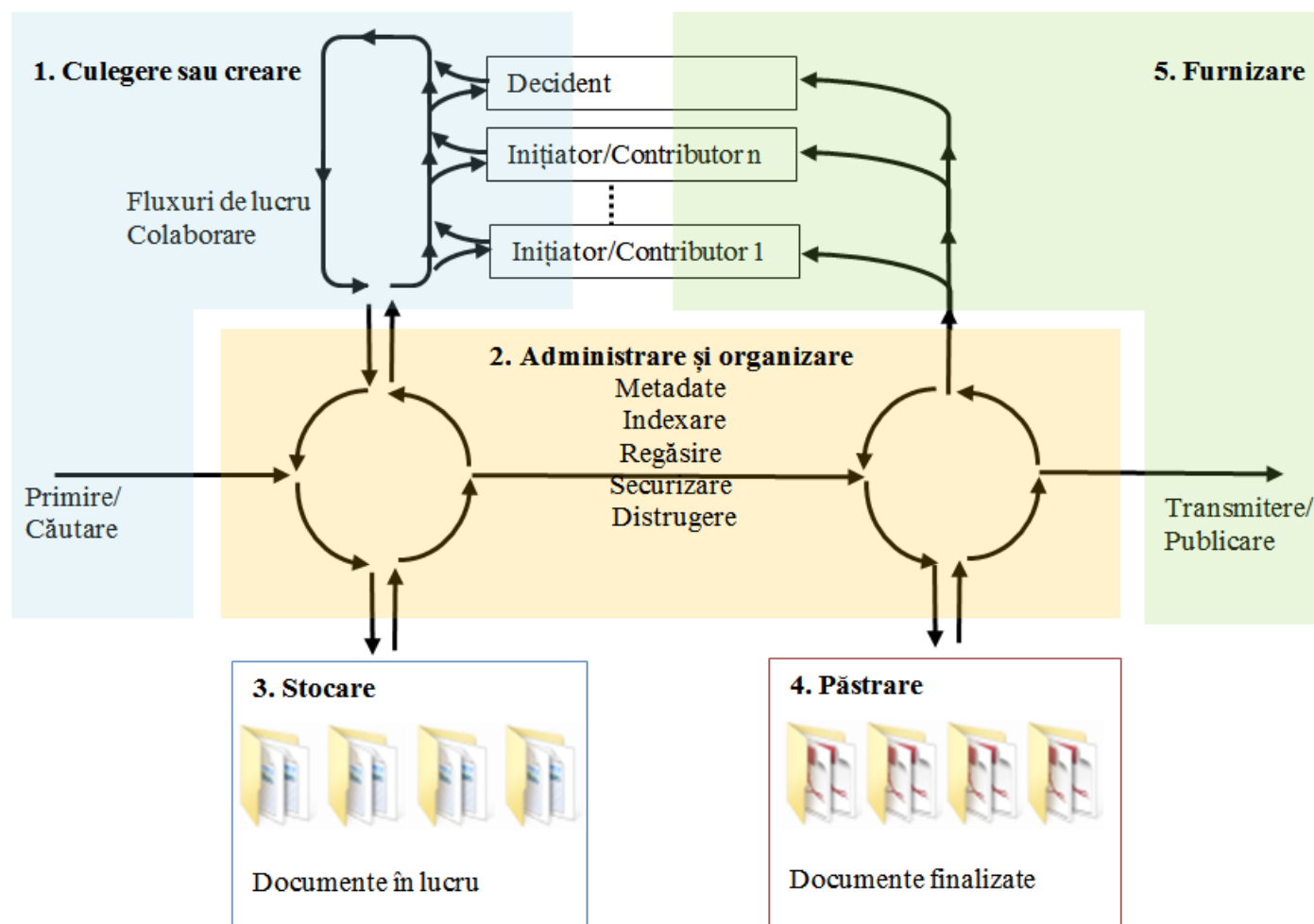


Fig. 1 Etapele ciclului de viață al informațiilor și principalele fluxuri informaționale

Ciclul de viață al informațiilor depinde de traseele de obicei non-lineare și iterative pe care acestea sunt vehiculate în organizații de la creare/primire până la distrugere. Modelul este aplicabil tuturor organizațiilor, inclusiv în mediul militar. De exemplu, dacă o unitate primește un ordin din partea eșalonului superior (etapa 1), documentul circulă mai întâi la comandant, apoi

este păstrat o perioadă de timp determinată (etapa 5), pe durată căreia se asigură accesul la el conform principiului „necesitatea de a cunoaște”, înainte de a fi distrus. Ordinul împreună cu hotărârea comandantului este adus la cunoștința structurilor responsabile de execuția lui (etapa 4), iar una dintre ele inițiază elaborarea unui nou document – raport, plan, studiu etc., care este

stocat temporar într-un spațiu partajat (etapa 3). După modificări succesive și la nevoie repetate (etapa 1), documentul este aprobat și circulă în spațiul de păstrare (etapa 4), de unde poate fi diseminat către beneficiari interni sau transmis către structuri externe (etapa 5). La sfârșitul perioadei de retenție, documentul este distrus. Toate documentele trec prin zona de administrare (etapa 2), în care sunt luate în evidență, clasificate, etichetate etc.

Fluxurile informaționale nu depind de tipul documentelor sau de tehnologia folosită și aparent nu este nevoie de un sistem specializat de management al documentelor. Practic, toate organizațiile își administrează documentele cumva, iar în mod normal cele mici își pot desfășura activitatea la un nivel acceptabil prin utilizarea unui server, a facilităților sistemelor de operare și a serviciului de e-mail. Pe măsură ce fluxul de documente crește, apar o serie de probleme care au fost evidențiate în literatura de specialitate cu mult timp în urmă. Astfel, unii autori au remarcat că volumul mare al documentelor produse și distribuite prin e-mail a agravat problemele privind securitatea, controlul, urmărirea și regăsire documentelor¹. Managementul tradițional sau pasiv al documentelor și-a demonstrat limitările datorită tendinței utilizatorilor de a acumula informațiile odată ce le-au găsit în structuri de directoare, fără garanția că le vor regăsi în viitor.

SMD are un rol cu atât mai important cu cât cerințele ciclului de viață al informațiilor nu pot fi

îndeplinite de sistemele de operare ale serverelor de fișiere sau stațiilor de lucru.

În etapa culegerii sau creării informațiilor. Din perspectiva organizațiilor, informațiile încep să existe din momentul în care au fost create sau primite din exterior. Culegerea trebuie să se poată realiza activ, de la unitățile partenere în schimbul informațional, prin interogarea motoarelor de căutare a bibliotecilor de documente sau a portalurilor web. Documentele printate primite prin poștă sau fax trebuie de regulă scanate cu utilizarea aplicațiilor de recunoaștere a caracterelor (Optical Character Recognition), astfel încât conținutul de tip text să poată fi editat, indexat și regăsit cu ușurință. SMD este capabil să capteze automat toate tipurile de fișiere, inclusiv mesaje de e-mail, să realizeze conversia documentelor scanate sau a celor în format electronic needitabil în documente editabile, și să le ruteze spre o locație în structura de directoare pe baza conținutului scanat. Pentru documentele nou create, se pot automatiza fluxurile de lucru de elaborare și aprobare, facilitând astfel aprobarea la timp a tuturor documentelor planificate și adăugarea completă a metadatelor. SMD facilitează și căutarea activă a informațiilor publicate în folosul altor structuri externe datorită motorului de căutare disponibil pentru toți utilizatorii.

În etapa organizării și administrării informațiilor. Fiecărui document care intră în organizație trebuie să i se atribuie un identificator unic, care să rămână neschimbat până la distrugere. SMD atribuie automat un identificator universal unic în lungime de 128 de biți a cărui

¹ Michael J.D. Sutton, Document Management for the Enterprise: principles, techniques and applications, New York, 1996

probabilitate de a fi duplicat tinde spre zero. Pentru a ușura citirea lui de către oameni, un număr de înregistrare mai simplu poate fi generat tot automat, conform unor reguli prestabilite, și inclus în metadata.

Toate informațiile trebuie să aibă un proprietar, care răspunde de actualizarea, partajarea și etichetarea corectă. În mod obișnuit, proprietarul este inițiatorul sau autorul documentului și este inclus în conținutul acestuia, dar acest fapt nu facilitează regăsirea ulterioară. SMD include proprietarul în metadata și facilitează înlocuirea la nevoie, de exemplu când persoana respectivă părăsește organizația și altcineva îi preia atribuțiile.

Etichetarea informațiilor este o cerință esențială pentru regăsirea lor ușoară și se realizează cu ajutorul metadatelor. Metadatale sunt „date despre date” și pot conține orice cuvinte care ar putea fi folosite drept criterii de căutare. De obicei, cuvintele se aleg dintr-un vocabular predefinit, denumit taxonomie, care definește și relațiile dintre termeni. Metadatale de fapt pot fi considerate fundamentul arhitecturii informaționale a organizației. Pe lângă attributele intrinseci ale fișierelor, cum sunt data creării și tipul, există două tipuri de metadata:

- descriptive: se referă la subiect, cuvinte cheie relevante, nivel de clasificare, categorii aplicabile, domeniu etc.
- administrative: se referă la starea

documentului – în lucru sau finalizat, autor, structura inițiatore, procesul sau activitatea unde este necesar etc.

SMD permite definirea metadatelor, precum și adaptarea la cerințe noi prin redenumire, contopire, mutare sau depreciere. Astfel, chiar dacă nu se proiectează de la început schema perfectă, oricând se pot face ajustări ca răspuns la schimbările din organizație și descoperirea de informații noi. În plus, pentru a evita neglijența utilizatorilor, completarea metadatelor poate fi configurată ca obligatorie la crearea documentului sau pe parcursul unui flux de lucru.

Informațiile trebuie structurate în directoare, cu respectarea modelului tradițional, în care un document fizic pe suport hârtie poate exista într-o singură locație fizică. Structura de directoare este unidimensională și nu ar trebui să depășească trei niveluri în adâncime, în timp ce etichetarea cu metadata este multidimensională și permite localizarea unui document în mai multe containere logice, care formează o taxonomie virtuală. Prin analogie cu o carte, majoritatea informațiilor despre un anumit subiect sunt conținute într-un singur capitol, dar de regulă este nevoie să fie menționate în mai multe contexte; de aceea, cărțile tehnice au pe lângă cuprinsul de la început și un index al cuvintelor relevante la sfârșit. Diferența dintre o structură ierarhică unidimensională și o taxonomie multidimensională este reprezentată în figura 2.

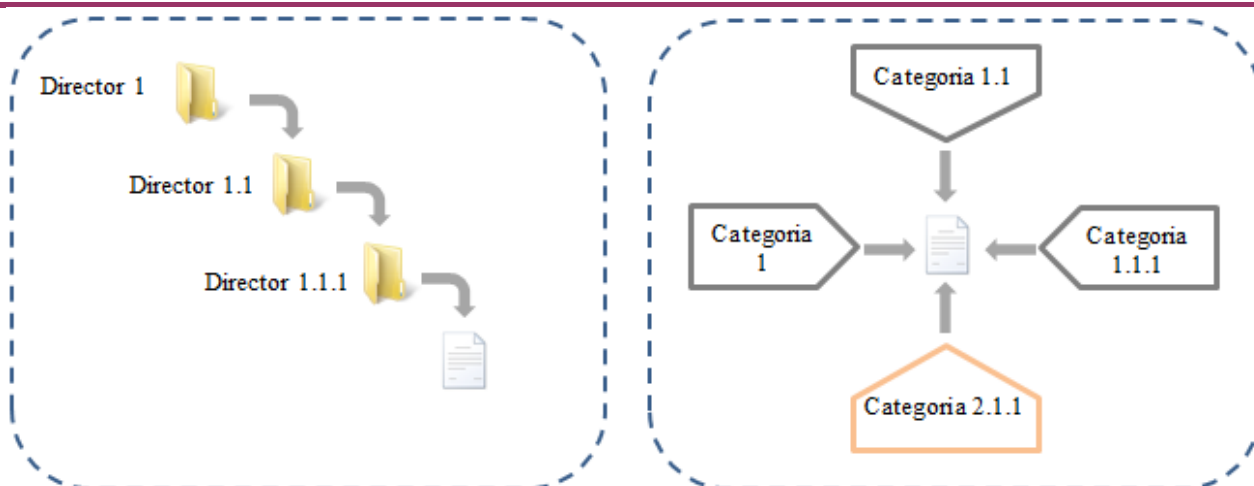


Fig. 2 Exemple de structură unidimensională de directoare și clasificare multidimensională cu ajutorul metadatelor

Administrarea informațiilor presupune și protejarea spațiilor de stocare și păstrare împotriva accesului neautorizat și jurnalizarea operațiunilor efectuate asupra documentelor. În cazul scurgerii sau alterării unor informații este necesară auditarea activității utilizatorilor în perioada respectivă. SMD facilitează controlul accesului mai bine decât sistemul de operare și permite auditarea tuturor operațiunilor relevante din punct de vedere al securității: modificare sau ștergere, descărcare sau printare în scopul distribuirii neautorizate.

Distrugerea informațiilor stocate în zona de lucru sau păstrate în arhivă trebuie să se realizeze doar cu acordul proprietarului, care este titularul dreptului de dispoziție. SMD facilitează distrugerea prin ștergere a informațiilor pentru care a expirat perioada de retenție, automat sau manual, în urma unei notificări trimise proprietarului.

În etapa de stocare a informațiilor. Toate documentele din organizație, indiferent de modalitatea de culegere sau creare, trebuie stocate temporar într-o zonă de lucru. Această zonă are o

parte privată pentru fiecare utilizator și o parte partajată de diferite grupuri. Aceste grupuri sunt formate de regulă în funcție de apartenența la o anumită structură organizațională sau în folosul echipelor de lucru colaborativ pentru rezolvarea unor sarcini specifice, permanente sau temporare. Responsabilitatea de a partaja este un principiu la fel de important ca necesitatea de a cunoaște.

Facilitățile sistemului de operare a serverului de fișiere și schimbul de mesaje prin e-mail permit colaborarea în mediul electronic, dar într-o manieră inefficientă. Pe măsură ce numărul de documente crește, devine tot mai dificil de găsit versiunea corectă. Utilizatorii sunt forțați să includă versiunea în denumirea fișierelor, astfel încât să limiteze confuzia pentru alți colaboratori. Chiar dacă neconcordanțele între versiuni sunt sesizate, este dificil să fie comparate, fuzionate și eliminate versiunile incomplete. O problemă și mai complicată apare când două persoane revizuiesc simultan același document. Să presupunem că, pornind de la documentul inițial, contributorul 1 creează versiunea 1, iar contributorul 2 creează versiunea 2 fără a lua în

considerare versiunea 1. Acest scenariu poate deveni repede complicat și cineva trebuie să coordoneze manual modificările.

SMD oferă o soluție eficientă la aceste probleme. În primul rând, prin controlul versiunilor, colaboratorii pot vedea într-o formă consolidată tot istoricul documentului, ce modificări au fost făcute și de cine, împreună cu comentariile acestora. Prin definirea fluxurilor de lucru se asigură desfășurarea colaborării într-o anumită ordine, ca rezultat al notificării utilizatorilor la momentul potrivit și eventual după desfășurarea unor activități. Și în ceea ce privește configurarea mediului partajat destinat echipelor pentru lucrul colaborativ SMD are un avantaj, întrucât administratorul SMD va acționa mai repede și mai bine pentru acordarea permisiunilor decât administratorul de sistem al serverului de fișiere.

În etapa de păstrare a informațiilor. Organizațiile identifică după criterii de selecție clar definite anumite informații care sunt păstrate sau arhivate conform reglementărilor în vigoare. Arhiva electronică trebuie să permită păstrarea informațiilor pe perioade determinate de timp, cu asigurarea integrității și autenticității acestora, căutarea după diverse criterii și cuvinte cheie și reutilizarea conținutului pentru informare sau crearea altor informații. SMD sunt indispensabile pentru arhivarea electronică având în vedere că sunt dezvoltate de obicei pe baza specificațiilor actelor normative aplicabile la nivel european sau național.

În etapa furnizării informațiilor. Exploatarea optimă a informațiilor presupune

regăsirea acestora la momentul potrivit de către persoanele care au nevoie de ele. În cel mai bun caz, utilizatorii își amintesc exact locația în structura de directoare unde documentul este stocat sau păstrat sau găsesc pe cineva mai experimentat să îi ajute. Inevitabil se ajunge la căutarea informațiilor utile în întreg volumul de documente sau în toate documentele dintr-un director. Spre deosebire de sistemul de operare care efectuează căutarea citind succesiv toate documentele, SMD este capabil de căutări tip full-text, asemănător cu motorul de căutare Google, sau căutări avansate, bazate în principal pe metadata. SMD citește doar indexul conținutului tip text sau al metadatelor, ceea ce face căutarea mult mai rapidă. Pentru informațiile greu de găsit se poate combina o căutare full-text cu o căutare după metadata, de exemplu atunci când trebuie găsit un anumit tip de raport care conține un anumit cuvânt.

Pentru exploatarea informațiilor de multe ori este necesară diseminarea acestora și confirmarea primirii de către destinatar. În mod obișnuit, diseminarea se realizează prin e-mail cu fișiere atașate sau legături către locația de stocare sau prin publicare pe portaluri web, urmată de notificarea destinatarilor. Diseminarea se poate realiza în cadrul SMD prin fluxuri de lucru, care au avantajul că furnizează la momentul optim informațiile împreună cu sarcina care trebuie executată și confirmă finalizarea activității.

Criterii de evaluare a SMD

Există pe piață numeroase soluții sau aplicații de management al documentelor disponibile cu licență comercială sau open source,

mai simple sau mai complexe și foarte diferite din punctul de vedere al tehnologiilor folosite și al costurilor de achiziție, instalare și operare. Dintre acestea, cele mai cunoscute sunt Microsoft Sharepoint, Alfresco, Nuxeo, LogicalDoc, M-Files, OpenKM, etc. Din fundamentarea deciziei de achiziție a unui anumit sistem trebuie să rezulte care sistem care corespunde cel mai bine criteriilor de evaluare proprii și poate fi adaptat cel cu costuri minime la specificul organizației. În acest scop este recomandat ca evaluarea să ia în considerare următoarele aspecte:

- Capacitatea de a satisface cerințele funcționale descrise mai sus, specifice rolului îndeplinit pe durata ciclului de viață al informațiilor, și de a oferi beneficiarului instrumente avansate de configurare sau dezvoltare pe cont propriu a unor funcționalități noi.

- Maturitatea aplicației. Evaluarea trebuie să determine de cât timp a fost lansată pe piață și în ce măsură o versiune nouă a fost implementată de comunitățile de utilizatori. În mod obișnuit, toate aplicațiile sunt îmbunătățite continuu pentru a oferi noi facilități, a elimina erorile de programare și a se conforma noilor standarde și recomandări în domeniul managementului informațional.

- Disponibilitatea și calitatea documentației sistemului, inclusiv sistemul de ajutor integrat în aplicație.

- Securitatea sistemului. Caracteristicile de securitate ale SMD trebuie să corespundă obligatoriu politicilor și reglementărilor organizației și să existe compatibilitate cu setările

de securitate ale sistemelor de operare.

- Nivelul suportului tehnic pe durata instalării, configurării și testării inițiale, precum și ulterior, pe durata exploatării. Notificarea incidentelor se poate face prin e-mail, pe un portal specializat sau telefonic, de regulă în timpul programului normal de lucru al furnizorului, iar suportul tehnic este asigurat de la distanță sau local, pe diferite niveluri de competență pentru remedierea disfuncționalităților. Comunitatea activă de utilizatori este de asemenea importantă și poate fi evaluată prin analizarea postărilor pe forumuri de suport tehnic și a timpului de răspuns la acestea.

- Scalabilitatea aplicației. Dacă se optează pentru furnizarea serviciului de management al documentelor în cloud pentru mai multe unități beneficiare, arhitectura SMD și relațiile existente între componentele acestuia trebuie să permită adăugarea de noi resurse hardware și software în cazul creșterii numărului de utilizatori.

- Disponibilitatea sistemului, care depinde de numărul de puncte sau componente vulnerabile care ar putea cauza o întrerupere totală a funcționării și de timpul necesar pentru dezvoltarea unui patch de remediere a unei disfuncționalități grave.

- Costul total de exploatare. Pe lângă costul de achiziție, trebuie determinate costurile de administrare curentă și pentru menținerea unui mediu de testare și dezvoltare, precum și costurile pentru instruirea administratorilor și utilizatorilor.

- Indicatorii de performanță de referință, preferabil obținuți de la un sistem asemănător în funcțiune, facilitează evaluarea capacității SMD

privit ca o soluție unitară hardware și software de a face față solicitărilor în condiții de încărcare maximă.

Concluzii

Managementul documentelor cu ajutorul mijloacelor moderne de tehnologia informației presupune un efort suplimentar relativ mic, dar poate crește considerabil eficiența sprijinului cu informații în luarea deciziilor și execuția sarcinilor. Pentru a obține un avantaj competitiv în mediul economic sau superioritatea

informațională în mediul militar, organizațiile trebuie să recunoască rolul important al SMD și să aloce resursele necesare pentru implementarea unui astfel de sistem. Criteriile de evaluare pentru fundamentarea deciziei de procurare a SMD sunt relevante în primul rând pentru structurile de comunicații și informatică care trebuie să asigure planificarea, instalarea, configurarea și mentenanța sistemului, dar și pentru managerul de informații, în calitate de beneficiar.

Bibliografie:

*** *Doctrina managementului informațional în Armata României*, București, 2013.

Michael J.D. Sutton, *Document Management for the Enterprise: principles, techniques and applications*, New York, 1996

Pagini publicate pe internet:

<http://www.aiim.org/What-is-ECM-Enterprise-Content-Management>, accesat 29.03. 2018

CORECTITUDINEA, TRANSPARENȚA ȘI ȘANSELE EGALE DE EVOLUȚIE ÎN CARIERA MILITARĂ

Maior Bogdan BURLOI

Centrul 89 Strategic de Comunicații și Informatică



De calitatea cadrelor va depinde întotdeauna calitatea armatei și, ca urmare, efectul produs de ea”
(*Mareșal Alexandru Averescu*)

Corectitudinea, transparența și șansele egale de evoluție în cariera militară constituie principiile de bază pe care se articulează normele legale, regulamentele și instrucțiunile interne aferente domeniului resurselor umane, în Armata României.

Într-o abordare tehnică, evoluția în carieră a personalului militar presupune parcurgerea succesivă a stagiilor în grade și funcții, conferind, în principiu, tuturor posibilitatea atingerii celor mai înalte trepte ale ierarhiei militare. Profesiei militare îi este asociată o pregătire profesională temeinică, precum și dobândirea competențelor și experienței asociate posturilor ierarhice specifice carierei militare, din momentul acordării primului grad și încadrării în prima funcție.

Structura de resurse umane este un departament funcțional cu o importanță deosebită în cadrul Centrului 89 Strategic de Comunicații și Informatică. Personalul răspunde de cunoașterea și aplicarea legislației specifice domeniului de activitate.

În centrul atenției sunt oamenii care din

1948 și până în prezent au împletit spiritul riguros, temperamentul dinamic și sacrificiul cu satisfacția și bucuria de a asigura rețele, servicii și echipamente de comunicații electronice structurilor centrale din Ministerul Apărării Naționale și pentru care structura de personal este și va fi mereu în „slujba lor”.

Aniversarea a 70 de ani a Centrului 89 Strategic de Comunicații și Informatică este reprezentată înaintea de toate de personalul unității - ofițerii, maiștri militari, subofițerii, soldații și gradații profesioniști și, nu în ultimul rând, personalul civil contractual.

Ofițerii reprezintă corpul de elită al Centrului 89 Strategic de Comunicații și Informatică. Ei au capacitatea de a planifica, organiza, de a lua decizii juste și la momentul potrivit, de a-și asuma răspunderea propriilor decizii, de a motiva și coordona oamenii din subordine. Aceștia trebuie să fie întotdeauna apropiați de subordonați și îndeplinesc funcții de comandă/conducere și de execuție.

Maiștrii militari și subofițerii sunt coloana vertebrală a unității, ei sunt specialiștii și luptătorii care ocupă funcții de comandanți/șefi de grupe, centre de comunicații, registraturi, depozite de tehnică sau materiale.

Formarea lor profesională urmărește dezvoltarea competențelor în domeniul comunicațiilor, informaticii și apărării cibernetice,

precum și de utilizare, administrare, întreținere și reparare a tehnicii de comunicații și informatică în vederea asigurării operativității acesteia. În aceeași măsură, maiștrii militari și subofițerii se specializează în activitatea de stat major și de management executiv al activităților din armele, serviciile și domeniile funcționale ale armatei.

Soldații și gradații profesioniști constituie cel mai numeros corp de personal, fiind destinat îndeplinirii misiunilor de execuție specifice luptătorilor și specialiștilor militari în cadrul microstructurilor de tip echipă, post de luptă sau grupă de întreținere tehnică de comunicații.

Soldații și gradații profesioniști participă nemijlocit la procesul de instrucție individuală și colectivă, asigură exploatarea și întreținerea tehnicii de comunicații și informatică din dotare și execută paza și apărarea unității.

Personalul civil contractual din Centrul 89 Strategic de Comunicații și Informatică asigură stabilitatea microstructurilor în care își desfășoară activitatea, ei sunt acei „militari” care poartă haine civile la serviciu. Aceștia au putut adera la disciplină totală, la rigorile specifice organismului militar, sunt cei care s-au angajat să răspundă

„prezent” acolo unde este nevoie de competența lor profesională ca inginer, tehnician, electromecanic sau centralist, dar și de psiholog, jurist, referent, economist, asistent medical sau muncitor calificat.



Consider că perioadele petrecute la diferite compartimente din statul major, cât și cea desfășurată ca șef al structurii de personal, sunt deosebit de importante și frumoase deoarece, alături de oamenii cu care lucrez, camarazii mei, fie ofițeri sau soldați gradați, mai experimentați sau la început de drum, am sentimentul datoriei împlinite și al satisfacției profesionale. De aceea, nu doar colegilor mei, ci tuturor celor care fac parte sau au făcut parte din marea familie a Centrului 89 Strategic de Comunicații și Informatică le urez:

LA MULȚI ANI!

PROIECT PRIVIND INTERCONECTAREA CENTRELOR DIN RTP/RMNC LA INFRASTRUCTURA VoIP

Căpitan Daniel CALCIU
Centrul 105 Comunicații RMNC



Tehnologia VoIP permite efectuarea convorbirilor telefonice peste o rețea bazată pe protocolul IP, reușind în același timp să asigure o anumită calitate a serviciului (QoS) cu un raport preț/calitate superior telefoniei clasice.

1. Introducere: Scurtă descriere a conceptelor folosite

În cadrul tehnologiei VoIP, standardele H.323 și SIP facilitează interoperabilitatea dintre diferite aplicații și dezvoltarea de noi aplicații, astfel:

- H.323 cuprinde un set de specificații majore date de ITU-T, specificații ce se referă atât la partea de control al apelului, cât și la managementul multimedia sau al ratei de transfer. H323 utilizează codec-uri pentru compresia și decompresia semnalelor, cum ar fi codec-uri audio: G.711, G.729 sau codec-urile H.261, H.263, H.264 pentru video.

- 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.

- Quality of Service QoS (calitatea serviciului) în rețelele de comunicație orientate pe pachete se referă la aspectul că rețeaua de comunicații dată trebuie să se încadreze în anumiți parametri de calitate; în cele mai multe situații este vorba ca un pachet să reușească să tranziteze rețeaua între două puncte ale sale.

- Centrala telefonică IP-PBX reușește să îmbine cu succes funcționalitățile standard ale centrelor telefonice clasice de tip PABX cu avantajele și beneficiile tehnologiei VoIP. Centrala IP-PBX comută apeluri dinspre și înspre orice rețea de voce existentă: PSTN (de exemplu rețeaua TELEKOM), GSM și internet (inclusiv în rețelele publice gratuite, precum Skype).

2. Diagrama de principiu este ilustrată în figura nr. 1.

Construirea unui sistem de telefonie IP end-to-end necesită o infrastructură IP bazată pe Layer 2 și Layer 3 - switch-uri și routere.

Designerii de rețea trebuie să se asigure că sunt conectate punctele finale la porturile Ethernet, după cum este ilustrat în figura nr. 2.

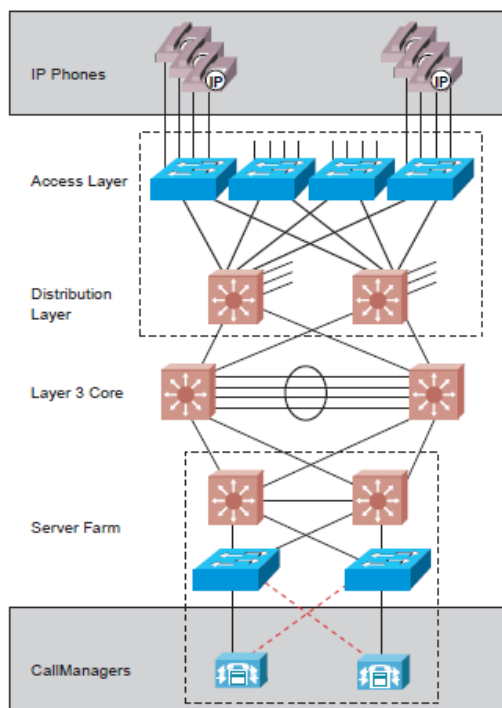


Figura nr. 1

Terminalul VoIP este conectat la echipamentul CERAGON instalat într-un centru cu management local la portul Ethernet al acestuia, iar printr-un canal VPN este realizată legătura direct cu centrul de management regional din aria de responsabilitate.

Terminalele VoIP asigură interoperabilitatea dintre centrele de comunicații

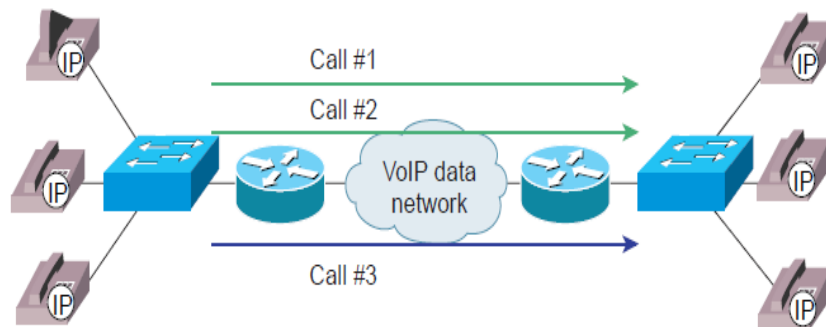


Figura nr. 2

izolate și factorii de conducere, asigurând posibilitatea convorbirilor video-telefonice prin infrastructura de radiorelee CERAGON.

Centrul de management regional face legătura cu centrul de management (Call Manager) principal prin magistrala de radiorelee CERAGON.

Centrul de management (Call Manager) principal

Centrul de management (Call Manager) secundar

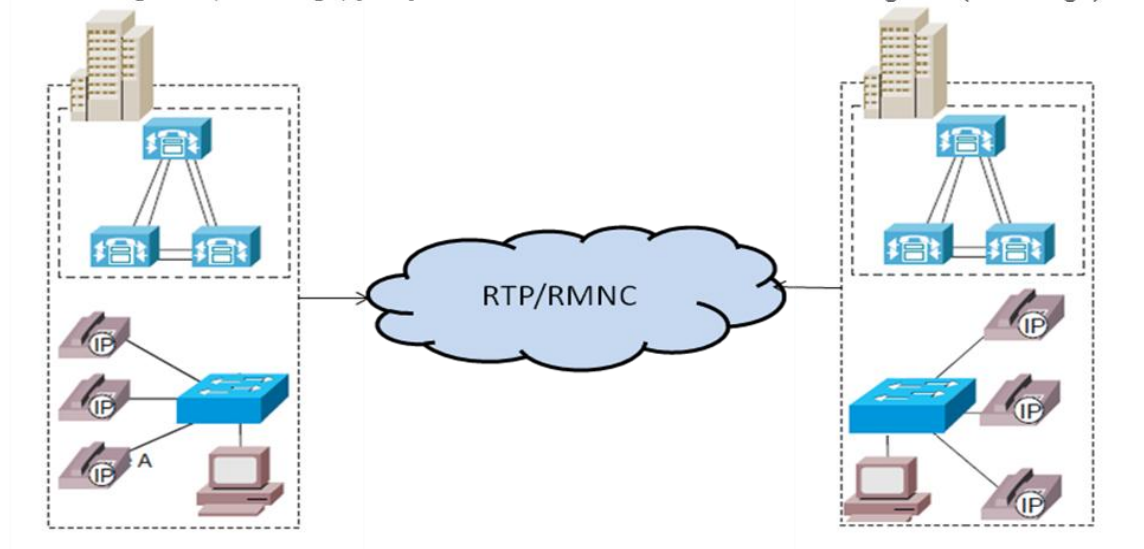


Figura nr. 3

Toate setările de configurare și adresare IP a rețelei de VoIP sunt executate de către centrul de management (Call Manager) principal.

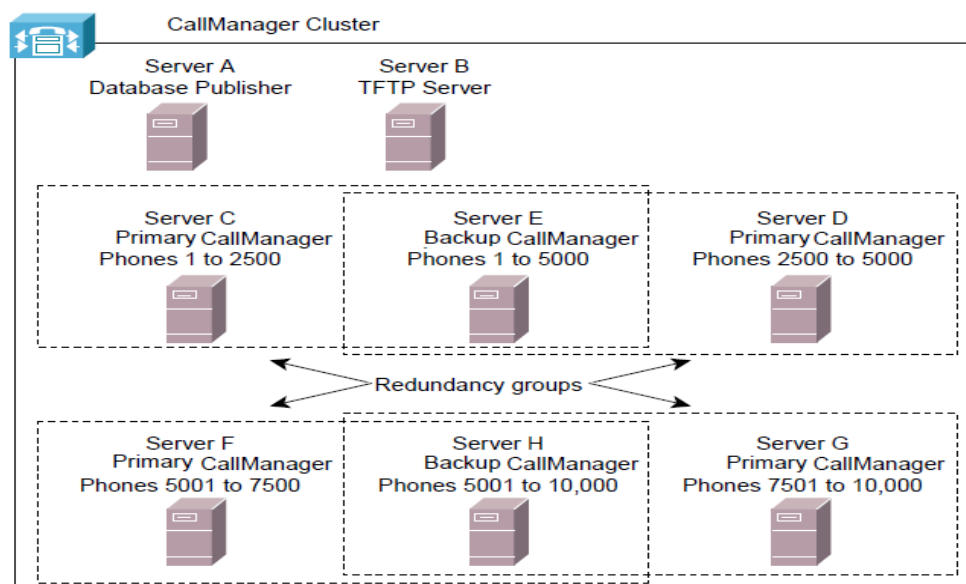


Figura nr. 4

Un singur CallManager are următoarele caracteristici de proiectare:

- maximum de 10.000 de utilizatori per grup;
- maximum 8 servere dintr-un cluster CallManager (patru servere pentru procesarea apelurilor primare, două pentru procesarea apelurilor de rezervă, o bază de date și un server TFTP);
- cel mult 2.500 de utilizatori înregistrați cu un CallManager în orice moment;
- PSTN pentru toate apelurile externe;
- resurse pentru procesoare de semnal digital (DSP) pentru conferințe;
- mesaje vocale și componente de mesagerie unificată;
- codec G.711 pentru toate apelurile telefonice IP (80 kbps de lățime de bandă pe IP, necomprimat).

3. Schema de ansamblu a rețelei de telefonie VoIP propuse

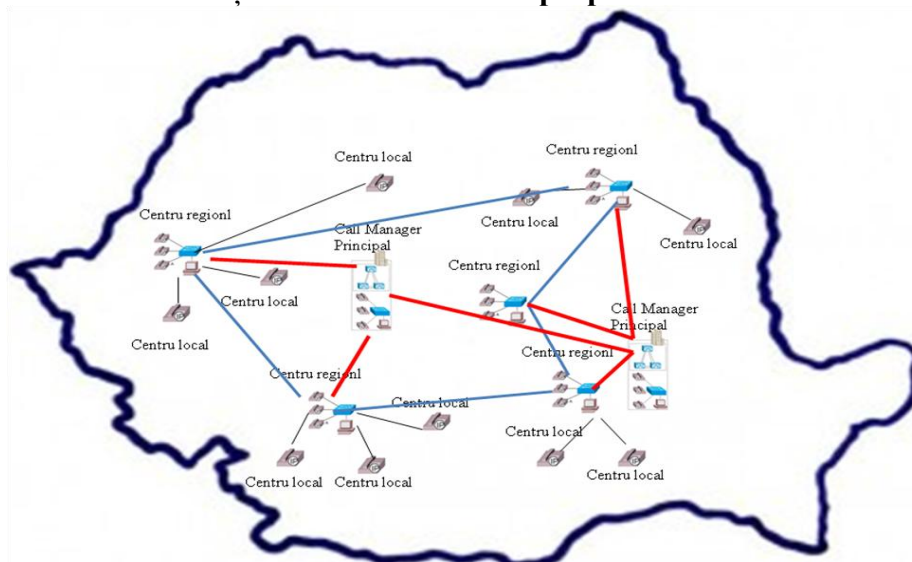


Figura nr. 5

4. Schema de interconectare a rețelei VoIP neclasificate la nivelul C 105 COM. RMNC propusă

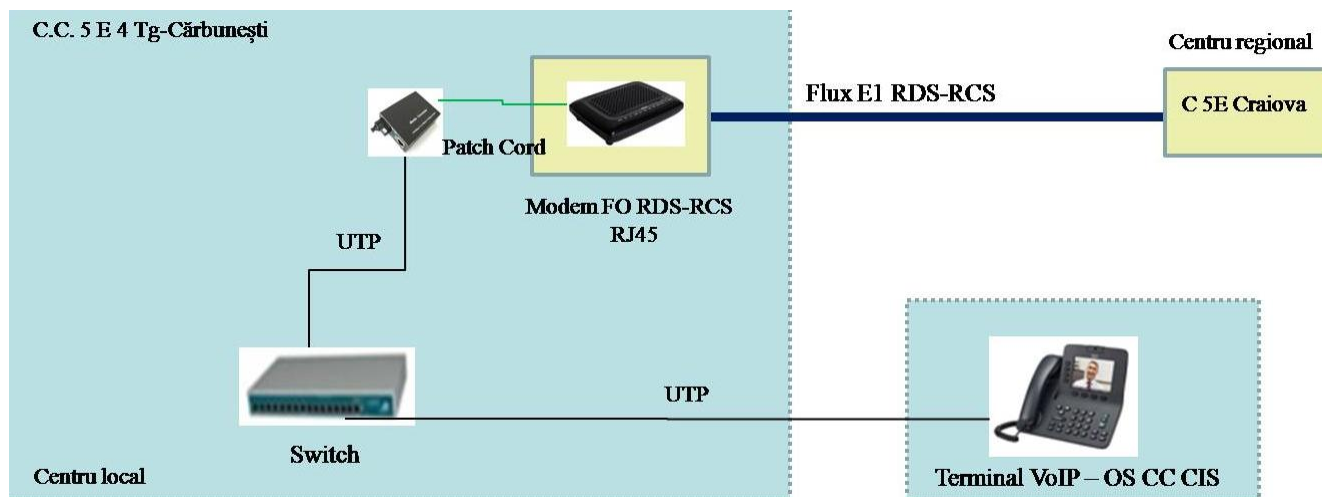


Figura nr. 6

S3 ȘI PROVOCĂRILE ÎNCEPUTULUI

Locotenent Niculina FULGER

Centrul 89 Strategic de Comunicații și Informatică

„Nu-ți fie teamă că înaintezi prea încet. Teme-te dacă te oprești!”

Sun Tzu



Am venit în
Centrul 89 Strategic
de Comunicații și
Informatică la
începutul anului
2016, când mi-am
luat repartiția din
școală. Îmi amintesc
cu drag și nostalgie

ziua în care, după 3 ani de academie, a venit, în sfârșit, ziua cea mare, ziua repartiției. Era ziua pe care o așteptam încă de la absolvirea liceului militar pentru că, gândeam eu atunci, avea să fie ziua în care voi scăpa de grija școlii, școală pe care știm cu toții cum o percepeam pe vremea când eram copii.

Așadar, fiind pusă în fața faptului împlinit, m-am dus cu emoție să citesc lista funcțiilor din care aveam de ales. După o singură privire mi-au atras atenția funcțiile Centrului 89 Strategic de Comunicații și informatică. Astfel, am început să întreb „în stânga și în dreapta”, profesori, cadre militare și colegi mai mari dacă au auzit despre această unitate, precum și păreri sau recomandări. Nu mare mi-a fost mirarea când din gura tuturor auzeam cuvinte de laudă, cuvinte care m-au convins că 1704 este o unitate de elită în domeniul comunicațiilor și informaticii și că merită să fac primii pași ai carierei mele de ofițer în această unitate. De atunci, U.M. 01704 a fost pentru mine,

sublocotenent Fulger Niculina, o continuare a școlii. Spun asta pentru că, în tot acest timp, nu a trecut o zi în care să nu pot spune că am mai învățat ceva nou, că m-am dezvoltat ca ofițer și ca om.

Primele mele zile în această unitate au stat la baza a ceea ce urma să fac în următorii ani. Atunci am aflat că funcția pe care eram încadrată urmează să fie desființată și că va trebui să mă reorientez. Din îndrumările celor care formau comanda unității am ajuns să lucrez în compartimentul S3 - Operații și instrucție, îndeplinind funcția de ofițer de stat major. Începutul a fost promițător, eram înconjurată de șefi și colegi foarte cumsecade, binevoitori și veseli. Ca bonus o aveam lângă mine și pe colega și prietena mea cea mai bună, Alexandra, iar lucrurile mergeau de minune. Timp de un an am fost cea mai tânără din birou, am fost mereu îndrumată de șefi și colegi cu experiență, bine pregătiți, care s-au oferit să-mi împărtășească din experiențele și cunoștințele lor. Așa am ajuns să iau contact cu documentele de planificare ale instrucției, exercițiilor și activităților care se desfășoară zilnic în unitatea noastră.

În tot acest timp, Centrul 89 a fost afectat de fluctuația de personal din Armata României, iar personalul cu experiență a fost înlocuit cu personal tânăr din cadrul unității sau cu absolvenți ai instituțiilor de învățământ. Pentru mine,

adevărata provocare a venit atunci când, rămasă singurul ofițer din cadrul compartimentului, a trebuit să iau în primire documentele operative și atribuțiile modului S3. Am acceptat cu ambiție și optimism această provocare, deși nu cunoșteam pe deplin „secretele” acestui domeniu atât de larg.

A fost o decizie care mi-a schimbat în mare măsură percepția asupra rolului statului major în viața unității. Am ajuns la concluzia că regulamentele militare nu reflectă tocmai fidel sarcinile S3 și că de multe ori ești pus în ipostaze dificile la care nu găsești răspunsurile în „cărți”. Tot aici mi-am dat seama de importanța relaționării atât cu colegii din unitate, cât și cu celelalte module S3 din cadrul Comandamentului Comunicațiilor și Informaticii. Mi s-a dovedit din nou că *unde sunt mulți puterea crește* și că, în ciuda deficitului de personal trebuie să lucrăm în echipă pentru a identifica soluțiile optime de rezolvare a sarcinilor și misiunilor. Am înțeles că drumul către succes este presărat cu provocări și

piedici, iar unele dintre ele pot părea, la un moment dat, de netrecut. Este esențial să nu cedezi atunci și să-ți continui drumul, chiar dacă, pentru moment, pașii sunt mai mici și înaintezi mai greu. Important este să nu stai pe loc și să nu dai înapoi.

În prezent, pot spune că, în ciuda dificultăților întâmpinate zilnic în cadrul acestui compartiment, nu regret această experiență pentru că, în primul rând, mă ajută să mă dezvolt și să înțeleg, „din inima statului major”, viața armatei și a unității.

Acum, la ceas de sărbătoare, când unitatea împlinește 70 de ani de existență, nu-mi rămâne decât să mulțumesc tuturor colegilor și foștilor colegi pentru sprijinul acordat în tot acest timp, sperând ca pe viitor familia Centrului 89 Strategic de Comunicații și Informatică să rămână la fel de unită, indiferent de greutățile și încercările la care vom fi supuși. LA MULȚI ANI!

PROVOCĂRILE ÎNCEPUTULUI DE CARIERĂ

Locotenent Alexandra BARBU

Centrul 89 Strategic de Comunicații și Informatică



Centrul 89
Strategic de
Comunicații și
Informatică, ce frumos
sună!! La asta m-am
gândit și eu, la
sfârșitul anului 3 de
academie, când, cu

emoție, mi-am ales prima funcție din cariera militară, și anume funcția de șef tură în cadrul acestei unități. Cu emoția începutului, am pășit prima dată în curtea unității și am realizat că în această unitate este un altfel de colectiv față de cum eram eu obișnuită din academie. Cu timiditate am început să mă acomodez noului statut, noii schimbări din viața mea, și anume trecerea de la student la ofițer, și am pășit cu mândrie, cu brațele deschise spre prima mea funcție. Din păcate, funcția mea urma să se desființeze și conducerea unității a luat decizia ca, până la reorganizare, să îmi desfășor activitatea la S3 - operații și instrucție.

Speriată, puțin dezamăgită, cu gânduri de regret față de alegerea făcută, am început o etapă destul de importantă pentru consolidarea carierei mele. Activitatea desfășurată în cadrul S3 mi-a creat o imagine de ansamblu asupra unității și a specificului acesteia. Pe vremea aceea, la S3 era mult personal, care avea răbdarea necesară pentru a explica unor tineri ofițeri cu ce se ocupă compartimentul și unitatea. Ușor, ușor am

acumulat informații, care astăzi stau la baza pregătirii mele ca ofițer.

Lipsa personalului din Armata României a dus la migrarea personalului spre funcții mai mari și astfel, la S3 nu a mai rămas niciun ofițer cu grad superior de la care să avem ce învăța. După 1 an și 6 luni de activitate în cadrul compartimentului S3, m-am orientat spre subunitate, unde aveam acces la tehnica de comunicații. Trecerea de la comandament la subunitate a fost o nouă provocare. Am privit din nou, cu aceeași timiditate spre o nouă etapă din cariera mea.

Într-adevăr, în cadrul Centrului Operațional de Rețea de Bază am avut multe lucruri de învățat, pot spune că sunt multe lucruri despre care nici nu am avut timpul necesar să citesc, am încercat să mă implic în toate activitățile subunității, să creez legături cu oamenii de acolo și, în același timp, „să fur” informații de la ei. Am trecut de la „șef” la subordonat, de la oameni pe care îi cunoșteam, la un nou început. Așa am descoperit ceea ce trebuia să descopăr încă de la început: lucrul cu omul. Cine zice că lucrul cu omul, cu subordonatul, este cel mai complicat, are dreptate, însă adevărata satisfacție vine atunci când realizezi că micul colectiv devine, de fapt, mica familie.

Evoluția comunicațiilor și a tehnicii de calcul și-a pus amprenta și asupra mediului militar prin introducerea modulelor IT. Modulul IT este

format din echipamente de ultimă generație și reprezintă saltul de la tehnica de comunicații (stații radio, echipamente MPS, comutatoare digitale, multiplexoare) la informatică (IP, routere, switch-uri). Acest salt uriaș presupune adoptarea unor tehnici diferite, studierea îndelungată a echipamentelor, configurarea acestora și, bineînțeles, specialiști în domeniu. Fiind un „concept” nou implementat, specialiștii militari în acest domeniu sunt încă în curs de specializare.

Modulul IT nu prezintă un interes foarte mare pentru personalul militar datorită faptului că implică multă muncă, atât psihică, cât și fizică, atât cunoștințe, cât și seriozitate, iar pe lângă toate acestea mai trebuie să fie îndeplinite și sarcinile de zi cu zi de la birou. Pe mine m-a atras datorită faptului că este tehnică nouă, de viitor și care implică multe alte responsabilități. Ca în orice alt domeniu, la început tot timpul este mai greu (după cum spuneam anterior), însă răbdarea, ambiția, încăpățânarea m-au făcut să îmi doresc să știu cât mai multe, să îmi însușesc lucruri noi și să ajung să configurez echipamente.

Nu pot să spun că am reușit de prima dată să fac totul așa cum trebuie, dar vorba aceea: repetiția este mama învățării.

Consider că prin participarea la cursuri de specializare în domeniul informatică și apărare cibernetică se evidențiază nevoia armatei de specialiști și totodată importanța acordată acestui domeniu care este într-un vast proces de dezvoltare.

În încheiere, aș vrea să mulțumesc personalului unității pentru modul în care am colaborat și vreau să le urez tuturor un călduros

„LA MULȚI ANI!”



TINEREȚEA ÎN S4 - LOGISTICĂ

Locotenent Mădălina CRAIOVEANU

Centrul 89 Strategic de Comunicații și Informatică



Un articol despre logistică și ce reprezintă ea pentru mine și colegii mei ... cam așa suna subiectul articolului pe care trebuia să îl redactăm noi, personalul logisticii

din Centrul 89 Strategic de Comunicații și Informatică, sarcină ce într-un final avea să îmi revină mie. Inițial, am fost sceptică cu privire la concretizarea acestui articol. Nu știam exact de unde să încep și unde voi ajunge.

Ușor ușor, am început să aștern pe hârtie idei, opinii, gânduri și sentimente despre ceea ce numim „cea mai frumoasă armă”, logistica. Dincolo de clasicul „fără logistică nimic nu ar fi posibil în armată”, pot spune că logistica nu înseamnă doar un domeniu de activitate în armată, ea este pretutindeni, acasă, la magazinul din colțul blocului, în marile magazine din mall-uri, în restaurant etc.

Logistica înseamnă organizare, coordonare, colaborare cu toate celelalte compartimente, astfel încât să nu existe impedimente în desfășurarea activităților curente.

Aici, în 17, cum spunem noi, logistica începe cu stabilirea necesarului: de tehnică armament, muniții, echipament, combustibili etc.

și continuă cu demersurile necesare pentru asigurarea acestor bunuri materiale. Solicităm, ni se asigură sau nu, recepționăm, distribuim mai departe, luăm măsurile necesare să fie suficient pentru toată unitatea, dar în același timp păstrăm rezerve pentru „zile negre”, că doar așa suntem noi, logisticienii, „avem mereu ceva pus deoparte”.

Primii mei pași în această unitate au fost timizi, iar mintea îmi era invadată de zeci de întrebări ... „Oare cum sunt oamenii?”, „Dar dacă nu mă vor primi frumos?”, „Mă voi descurca pe această funcție?” etc. Nu știam dacă mutarea în Centrul 89 Strategic de Comunicații și Informatică urma să fie ceea ce căutam la acel moment ori un real eșec.

În ciuda îndoielilor, am hotărât să fac acest pas; astfel, m-am găsit la porțile unității într-o ploioasă zi de 22 mai. Am fost întâmpinată de cei ce urmau să îmi devină colegi de muncă, șefi, prieteni. În scurt timp m-am integrat, cu ușurință, în colectivul logisticii, am ajuns să îi cunosc, să îi apreciez și să mă simt apropiată lor. Cu toții sunt oameni calzi și prietenoși.

Ei sunt colegii de la S4: Cristi, colegul binevoitor ce vrea mereu să te ajute și care are zâmbetul pe buze chiar și în cele mai proaste zile ale lui; maiorul, sau Fery pentru ceilalți, omul care nu știe să se enerveze și cel care stă 3 ore să îmi explice cum să completez o fișă de echipare fără

să îşi piardă răbdarea cu mine; Moise, căpitanul MENTEC, acel ofiţer de la care am învăţat să îmi asum responsabilitatea pentru documentele întocmite şi pentru deciziile luate, indiferent de corectitudinea acestora; Ovidiu, o persoană foarte calculată şi ancorată în realitate, este omul care a reuşit să calmeze multe din ieşirile mele nervoase printr-un sfat de viaţă şi un zâmbet liniştitor; doamna Aranghel, o femeie caldă şi sufletistă ce ştia când şi cum să îmi spună o vorbă bună; Diana, blonda, o tânără energică, plină de viaţă, ambiţioasă şi cu aspiraţii înalte.

Concluzionând, pot spune că S4 este un colectiv tânăr, cu putere şi dorinţă de muncă. Zi de zi cu toţii ne străduim să facem lucrurile cum putem noi mai bine, astfel încât activitatea unităţii să nu fie compromisă de lipsa bunurilor materiale.

Tinereţea noastră vine la pachet cu dorinţa unei schimbări de ritm în ceea ce priveşte activitatea logisticii. Avem idei, unele mai bune, altele mai puţin bune, căutăm sprijin în rândul

celor cu o experienţă mai vastă decât a noastră, greşim, ne asumăm greşelile şi căutăm soluţii, facem tot ce considerăm de cuviinţă, astfel încât „S4 de mâine să fie mai eficient decât S4 de azi”.

Pentru câţiva dintre noi, Centrul 89 Strategic de Comunicaţii şi Informatică a reprezentat prima unitate în care am poposit în urma finalizării pregătirii în domeniul logistic, iar pentru ceilalţi a fost unitatea în care s-au regăsit pe ei înşişi, din punct de vedere profesional, cum este şi cazul meu. Aici simt că lucrez cu oameni valoroşi, că am de la cine să învăţ lucruri noi şi că sunt apreciată pentru tot ceea ce reprezintă, atât ca om, cât şi ca ofiţer.

Ca o concluzie, aş adăuga faptul că indiferent de situaţia care ne-a adus pe fiecare dintre noi în modulul logistic al acestei unităţi, este un semn de bun augur faptul că ne-am întâlnit, că avem acelaşi scop – de a aduce un plus în materie de activitate logistică şi că formăm o echipă unită şi cu perspective.

DRONELE – ISTORIA UNEI REVOLUȚII TEHNOLOGICE

Locotenent Mădălina CRAIOVEANU

Centrul 89 Strategic de Comunicații și Informatică



Lumea actuală, caracterizată de schimbare și adaptare la nou, se confruntă cu probleme dintre cele mai variate și complexe în ceea ce privește securitatea și pacea internațională.

Fenomenul globalizării, grăbit de revoluțiile tehnologice, de progresul tehnico-științific, de dezvoltarea comunicațiilor și de economiile tot mai interdependente, poate fi perceput drept un real avantaj pentru societatea modernă. Sfârșitul secolului XX - începutul secolului XXI este puternic marcat de construcția unei noi arhitecturi de securitate și stabilitate, determinată de apariția unor noi riscuri, amenințări și conflicte latente.

Pe fondul unei societăți destabilizate de multitudinea conflictelor și intereselor contradictorii ale marilor puteri economice ale momentului, putem discuta despre inovația tehnologică a secolului XX, și anume apariția dronelor. Drona este ceea ce cunoaștem sub denumirea de UAV (abreviere din englezescul *unmanned aerial vehicle*), mai concret un vehicul aerian fără un pilot propriu-zis, care are capacitatea de a zbura pilotat de la distanță de către un om sau nepilotat, prin intermediul unui

sistem autonom de direcționare¹.

Primele informații cu privire la drone le înfățișează pe acestea în mediul militar, mai exact în mijlocul derulării acțiunilor militare pe câmpul tactic. Conform istoricilor, ideea realizării unei aeronave nepilotate, idee născută cu mult înainte de izbucnirea Primului Război Mondial, aparține austriecilor², însă materializarea ei a fost realizată de englezi în perioada interbelică.

Balonul austriac, 1849

Un tânăr locotenent austriac, Franz von Uchatius, a dat formă ideii „bombardării din aer” creând *bomba-balon*. Baloanele cu aer cald erau realizate din hârtie și puteau transporta în jur de 15 kg de exploziv alcătuit dintr-un proiectil de artilerie încărcat cu șrapnel (gloanțe) și dotat cu focos reglabil/siguranță (ca o presupunere, se pare că siguranțele erau activate electric printr-un fir de cupru legat la o baterie galvanică aflată pe sol). Explozibilul detona la aproximativ 30 de minute de la lansarea balonului. Aceste baloane (fig. nr. 1) au fost lansate de pe nava cu zbatouri „Vulcano” (Clasa Vulcano, lansată în 1845 la Arsenalul din Veneția, scoasă din înzestrare în 1889), însă rezultatele au fost mediocre.

¹ ICAO's circular 328 AN/190: Unmanned Aircraft Systems

² nepilotate, încărcate cu explozivi împotriva Veneției. La 22 august 1849, Austria, imperiu ce controla mare parte din Italia, a lansat aproximativ 200 de baloane cu aer cald.



Fig. nr. 1 - Baloane austriece deasupra Veneției

Queen Bee (Regina Albinelor), 1935

Dacă lansarea baloanelor cu aer cald deasupra Veneției constituie, potrivit specialiștilor în domeniu, primul bombardament aerian înregistrat, despre biplanul De Havilland Queen Bee (Regina Albinelor), prima aeronavă radio-controlată intrată în producție de serie se spune că ar fi „mama tuturor dronelor”. Aceasta a fost o aeronavă-țintă nepilotată, de succes, de înaltă tehnologie la acea vreme, fiindu-i recunoscute scopul și misiunea inclusiv de înalți demnitari civili ai momentului respectiv, precum Winston Churchill (fig. nr. 2).

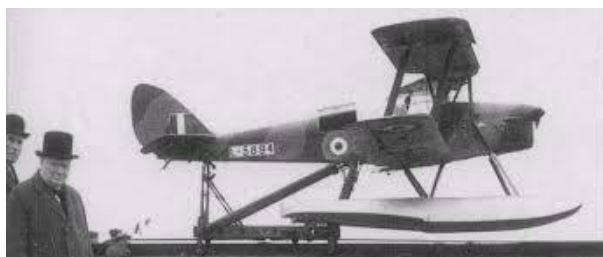


Fig. nr. 2 - Winston Churchill și Queen Bee

Antrenamentele executate de britanici cu Queen Bee au stârnit interesul americanilor. În 1963, amiralul William Harrison Standley, reprezentant al US Navy la Conferința Navală de la Londra și șef al Operațiunilor Navale (ulterior avea să ajungă ambasadorul SUA în URSS, în

perioada 1941 - 1943), a fost martor la un exercițiu de tragere live împotriva unui Queen Bee. Ulterior acestui moment, la întoarcerea în Statele Unite, amiralul a reinițiat cercetarea americană în domeniul aeronavelor nepilotate. Am utilizat termenul *reinițiat* deoarece SUA au avut asemenea preocupări și anterior anului 1963, mai exact la sfârșitul Primului Război Mondial. În acest sens, amintim Kettering „Bug” (1918) și aeronava autopilotată Hewitt-Sperry (septembrie 1917).

Un aspect ce trebuie menționat este acela conform căruia, la acel moment, armata americană prefera soluția autopilotată (*giroscop Sperry*) în detrimentul ghidării radio (considerată nesigură pe motiv că echipamentele radio nu erau de o performanță considerabilă).

Sfârșitul celor două conflagrații mondiale nu a reprezentat și finalizarea cercetărilor în domeniul erei tehnologice, astfel că epoca contemporană este caracterizată de schimbările majore în ceea ce privește utilizarea aeronavelor nepilotate.

Aceste inovații ale domeniului militar au ajuns să reprezinte, în zilele noastre, un centru de atracție pentru multe alte domenii de activitate, precum: jurnalism, serviciul de livrări la domiciliu (o idee de viitor ce aparține site-ului Amazon Prime Air³), urmărirea activității în domeniul agricol (vorbim aici despre monitorizarea aeriană a activității persoanelor ce contractează sume de la fondurile europene în vederea cultivării terenurilor agricole⁴) etc.

³ www.playtech.ro

⁴ www.gazetadeagricultura.ro

Din punct de vedere legislativ, dronele se găsesc încă în zona „gri” a legislației⁵, deoarece, la momentul actual, statutul dronelor nu este foarte clar reglementat, iar utilizarea acestora atât în domeniul militar, cât și în viața civilă, atrage după sine probabilitatea săvârșirii de accidente. Totodată, un subiect amplu dezbătut îl reprezintă faptul că survolarea nestingherită pe spațiul aerian

a acestor aparate de zbor nepilotate va conduce la invadarea intimității personale. Teama populației în acest sens reprezintă un aspect de luat în calcul în ceea ce privește promulgarea de legi care să stipuleze cu exactitate statutul dronelor și modalitatea de utilizare a acestora de către populația civilă.

⁵ www.adevarul.ro

TEHNOLOGIA WiMax

Locotenent Mihai LUCACIU

Centrul 48 Comunicații și Informatică Strategice



Conexiunile fără fir devin tot mai populare, deoarece ele rezolvă probleme ce apar în cazul când avem multe cabluri, conectate la multe dispozitive. WiFi folosește unde radio,

exact ca telefoanele mobile, iar comunicația într-o rețea wireless este foarte asemănătoare cu comunicațiile radio duplex. Un adaptor wireless convertește datele în semnale radio și le transmite folosind o antenă. Un router wireless primește semnalul și îl decodează. Acesta trimite informația către internet folosind o conexiune fizică Ethernet. Procesul lucrează și invers, routerul poate primi informații dinspre internet, pe care le convertește în semnale radio și le trimite către adaptorul wireless al calculatorului.

Chiar dacă atât tehnologia WiMAX cât și WiFi au anumite caracteristici tehnice comune, acestea abordează spațiul radio din perspective total diferite. Deosebirea fundamentală între cele două tehnologii wireless este aceea că sunt destinate unor aplicații total diferite. WiFi este o tehnologie de rețea locală, care aduce mobilitate rețelelor locale cablate; pe de altă parte, WiMAX acoperă arii având raze de aproximativ 50 km pentru stații fixe și raze de 5 - 15 km pentru stații mobile. Principalul scop al accesului wireless de

bandă largă este acela de a asigura un serviciu de acces la internet care este capabil să înlocuiască alte servicii similare prin cablu.

Tehnologie WiMAX are capacitatea de a capta datele de aproximativ șapte ori mai repede și de o mie de ori mai departe decât tehnologia WiFi. WiMAX are un potențial imens în lumea wireless, extinzându-se în utilizare de la fix la portabil și mobil. Pe lângă diferența privind aria de acoperire a transmisiei există o serie de îmbunătățiri ale legăturii radio ce diferențiază WiMAX de WiFi. Standardele de rețea wireless IEEE 802.11 descriu patru interfețe de legătură radio ce operează în benzile radio nelicențiate de 2,4 GHz sau 5 GHz.

Echipamentele WiMAX pot fi utilizate atât în rețele private, cu configurații tipice punct la punct și punct la multipunct, cât și în rețele publice. Rețelele private sunt rețele folosite în mod exclusiv de o singură organizație și oferă legături dedicate de comunicații, folosite pentru transferul de date și/sau de informații video și audio. Rețelele publice oferă resursele de care dispun mai multor utilizatori, care pot fi atât persoane private cât și instituții sau întreprinderi.

Accesul mobil la internet și la alte servicii digitale folosește în multe situații largimi de bandă limitate, atât pentru sensul ascendent (de la utilizator către rețea), cât și pentru cel descendent (de la rețea către utilizator), cu valori de 100 ÷ 300 kbit/s. În situații de deplasare lentă a

echipamentului mobil sau dacă acesta este folosit staționar, vitezele de comunicare pentru ambele sensuri pot crește până la 2 Mbit/s. Deși conexiunile radio mobile conțin în sine un potențial remarcabil, este puțin probabil ca acestea să intre în competiție cu piața de acces fix.

În rețelele constituite WiMAX se pot realiza: servicii de voce și multimedia, accesul la diferiți furnizori de conținut, telefonie mobilă prin VoIP (limitată la zona de acoperire a rețelei), livrarea de servicii IP radiodifuzate sau de tip multicast.

Din punctul de vedere al modului de oferire și al desfășurării serviciilor, WiMAX se caracterizează prin instalare rapidă a echipamentelor. În cazul folosirii benzilor fără licență se evită formalitățile legate de obținerea licenței.

Acoperire rețelei se poate realiza dinamic, pe o arie largă. Acoperirea poate varia în funcție de tipul de modulație folosit. Astfel, dacă se folosește BPSK sau QPSK, aria de acoperire crește, în timp ce, prin folosirea unei modulații de nivel superior, 16-QAM sau 64-QAM, aria de acoperire scade. Acoperirea este favorizată și de posibilitatea de funcționare NLOS. Din punctul de vedere al arhitecturii rețelei WiMAX, aceasta este flexibilă și ușor reconfigurabilă. Se pot configura mai multe tipuri de rețele: punct la punct, punct la multipunct, cu acoperire continuă etc. Prin programarea sloturilor de timp la nivelul MAC se pot realiza mai multe tipuri de acoperire, de exemplu acoperire continuă și de tip punct la punct.

Un alt avantaj îl constituie costul relativ

scăzut pentru echipamente și pentru instalare.

Tehnologia asigură accesul la internet cu o viteză de până la 72 Mbit/s și se bazează pe standardul IEEE 802.16 (numit și acces wireless în bandă largă).

Viteza de transfer la tehnologia WiMax depinde de următoarele 7 componente:

- dimensiunea canalului;
- numărul de sub-purtătoare dintr-un canal;
- sub-purtătoarele folosite ca și canale pilot;
- sub-purtătoarele folosite ca și canale de separație;
- durata simbolului, care include și durata de separare a simbolurilor;
- rata de modulație;
- rata de codare FEC.

Tehnologia WiMax prezintă însă și anumite puncte slabe, care afectează securitatea rețelelor, precum: ascultarea mesajelor de management, mascarada stației de bază sau a stației mobile, modificarea mesajelor de management și respingerea de servicii, bruiajul și modificarea traficului de date (când nu este folosit AES).

Tehnologiile fără fir sunt o soluție cu cost avantajos pentru furnizorii de servicii, fără cerințe de proprietate particulară ori publică. Clădirilor unde utilizarea cablurilor optice este imposibilă din cauza interdicțiilor impuse de proprietăți adiacente, datele pot fi transmise fără fir. Aceasta este soluția recomandată întreprinderilor mici pentru care nu sunt disponibile cabluri optice și alte servicii de bandă largă. Costul scăzut și flexibilitatea WiMax îmbunătățesc eficiența economică a echipamentului de rețea.

CONCEPTUL FMN

Sublocotenent Adrian CARPIUC

Centrul 48 Comunicații și Informatică Strategice



Aliații și-au propus să dezvolte și să mențină întreaga gamă de capacități necesare pentru descurajarea și apărarea împotriva unor potențiali adversari, folosind

abordări multinaționale și soluții inovatoare acolo unde este cazul. Procesul de planificare NATO (NDPP) este principalul mijloc de identificare și prioritizare a capacităților necesare pentru operațiunile cu un spectru larg și de promovare a dezvoltării și furnizării acestora. Poziția modernă de apărare a NATO se bazează pe o combinație eficientă a doi piloni cheie: sisteme și platforme de arme de ultimă generație și forțe antrenate să colaboreze fără probleme. Federated Mission Networking (FMN) reprezintă o contribuție esențială la inițiativa forțelor întrunite (CFÎ), ajutând forțele aliate și ale partenerilor să comunice, să se instruiască și să opereze împreună mai bine. FMN permite o instanțiere rapidă a rețelelor de misiune prin federalizarea organizațiilor NATO, capacităților membrilor NATO și a partenerilor de misiune, sporind astfel interoperabilitatea și schimbul de informații. FMN este un cadru conceptual guvernat, format din oameni, procese și tehnologie și destinat planificării, pregătirii, stabilirii, utilizării și

finalizării rețelelor de misiune în sprijinul operațiunilor federalizate. Rețeaua de misiune federalizată este o capacitate care vizează sprijinirea comenzii și controlului, luarea deciziilor în operațiunile viitoare prin îmbunătățirea schimbului de informații. Oferă agilitatea, flexibilitatea și scalabilitatea necesare gestionării cerințelor emergente ale oricărui mediu de misiune în viitoarele operațiuni NATO. FMN se bazează pe principii care includ eficacitatea costurilor și reutilizarea maximă a standardelor și capacităților existente. FMN-ul este alcătuit din trei elemente: Guvernanța Rețelei de Misiune Federalizată, Cadrul Rețelei de Misiune Federalizată și Rețele de Misiune. FMN-ul este construit pe lecțiile învățate din implementarea rețelei de misiune în Afganistan (AMN) și pe NATO Network Enabled Capability (NNEC). Guvernanța FMN stabilește obiective, definește cadrul de reglementare și mediul (reguli, proceduri, politici, standarde etc.) și ajută la asigurarea unei utilizări responsabile a resurselor și la gestionarea riscurilor.

Executat de Comitetul Militar, nivelul de guvernanță oferă direcții pentru organismele de management de sprijin care execută funcții de management pentru cadrul FMN și pentru fiecare rețea de misiune și pentru cei afiliați la rețeaua de misiune federalizată. Nivelul de management traduce direcția oferită de Comitetul Militar în strategii și planuri care, la rândul lor, sunt

transpuse în acțiuni de către afiliații FMN. Performanța este raportată la nivel de guvernare, care apoi evaluează și o încorporează în ajustarea așteptărilor. Grupurile de lucru constituie sprijin reciproc și complementar pentru activitățile de organizare a rețelelor de misiuni federalizate, abilitate să colaboreze în mod direct cu alte organisme și entități NATO și cu organizațiile native ale partenerilor, după caz. Cadrul FMN este o structură guvernată, gestionată și cuprinzătoare, care oferă o bază continuă permanentă cu procese, planuri, șabloane, arhitecturi, componente și capacități necesare pentru pregătirea (inclusiv planificarea), dezvoltarea, desfășurarea, operarea, evoluția și finalizarea rețelelor de misiune. Rețele de misiune oferă o singură instanță de capacități guvernată, inclusiv sistemele de comunicații și informații, managementul, procesele și procedurile create în scopul unei operațiuni, exercițiu, eveniment de instruire sau a unei activități de verificare a interoperabilității.

Rețelele de misiune sunt stabilite utilizând un set flexibil și adaptat de non-materiale (politici, procese, proceduri și standarde) și materiale (rețele statice și dislocate, servicii, infrastructuri

de sprijin) rezultate prin contribuțiile furnizate de NATO, membrii NATO și non-NATO. Sunt definite niveluri de capacități care oferă opțiuni pentru participarea la evoluția capacității de organizare a rețelelor de misiune federalizate. Elementul de rețea al misiunii (MNE - Mission Network Element) conține infrastructura de rețea și informații și serviciile pentru auto-aprovizionare, inclusiv servicii esențiale de misiune. Un element de extensie al rețelei de misiune (MNX- Mission Network Extension) conține infrastructură și servicii pentru auto-aprovizionare, dar nu poate include servicii esențiale de misiune. Un utilizator găzduit este un participant la rețeaua de misiune care nu este în măsură să furnizeze infrastructură și servicii pentru auto-aprovizionare.

Organizațiile NATO, membrii NATO și non-NATO sunt încurajate să devină afiliați ai FMN, ceea ce implică menținerea și dezvoltarea în continuare a capacităților și principiilor de securitate și interoperabilitate ale sistemelor de comunicații și informații. Asociațiile afiliate cu misiuni federale vor putea să contribuie la o misiune pe termen scurt și cu pregătire minimă.

REPETOARE HIBRIDE ÎN GAMA MICROUNDOR (SHF)

Plutonier-adjutant Cristian DANALACHE

Centrul 42 de Comunicații și Informatică de Sprijin



Comunicațiile radio reprezintă una dintre puținele metode pentru realizarea comunicării instantanee, indiferent de tipul informației transportate. La baza acestora se află undele radio. Acestea sunt radiații electromagnetice utilizate în special pentru transmisii de informații la distanță, cu frecvențe de la câțiva kilohertzi până la câțiva gigahertzi. Undele formate de antene direcționale, care se găsesc la o înălțime mai mare decât lungimea undei și se propagă paralel cu suprafața terestră, se numesc unde directe.

În domeniul comunicațiilor militare, undele directe se folosesc pentru organizarea legăturilor radio, radioreleu, radiolocație și satelitare. Distanța de propagare depinde de relief, înălțimea antenelor și factorii meteorologici.

Directivitatea și focalizarea antenelor este foarte importantă pentru a putea folosi la maximum și cu putere minimă orice tip de repetare a semnalului.

Știut fiind faptul că undele electromagnetice, indiferent de frecvență, pot suferi în urma unor fenomene ca reflexie, refracție, difracție și absorbție, apare ideea de a folosi și exploata aceste caracteristici în favoarea

noastră.

Datorită efectelor difracției și reflecției, comunicarea este posibilă între două puncte de pe pământ, care nu au vizibilitate directă. Curbura pământului, obstacolele naturale (dealuri, munți, vegetație) sau artificiale sunt principalele provocări în obținerea vizibilității directe.

Nevoia de a transmite informații în mod oportun, rapid, pe distanțe mari și cu costuri cât mai mici de exploatare a dus la găsirea unor soluții de compromis și astfel la apariția repetoarelor de semnal. Acestea se împart în două categorii: repetoare de semnal active și pasive.

Repetoarele active funcționează pe principiul recepționării fasciculului de undă, amplificarea acestuia și transmiterea lui mai departe, pe aceeași frecvență și pe altă direcție sau pe altă frecvență și pe aceeași direcție pentru evitarea interferențelor.



Fig. nr. 1 Repetor activ

Avantajele acestui tip de repetor sunt:

- instalare relativ ușoară;
- magistrala poate fi extinsă foarte mult;
- consum redus de energie electrică;

- funcționare cu energie solară;
- autonomie limitată doar de capacitatea acumulatorilor.

Dezavantaje :

- costuri de întreținere mari prin uzura acumulatorilor datorită condițiilor meteorologice;
- panouri solare scumpe și relativ fragile.

Repetoarele pasive (oglinzi radio) se bazează pe reflexia fasciculului de undă, din oglindă în oglindă, schimbându-i acestuia direcția de propagare.



Fig. nr. 2 Repetor pasiv

Avantaje :

- nu necesită alimentare cu energie electrică;
- se pot instala în locuri greu accesibile;
- mentenanță aproape inexistentă dacă sunt montate corect;
- folosirea unui set redus de frecvențe, rezultând degajarea spectrului radio;
- nu necesită infrastructură costisitoare și operatori locali.

Dezavantaje :

- costuri de producție relativ mari, deoarece trebuie să se respecte toleranțe foarte mici față de suprafața plană;
- alinierea perfectă poate fi greoaie;
- poate fi necesară mărirea puterii de

emisie peste anumite limite dorite.

Avantajele folosirii în domeniul militar:



Fig. nr. 3 Câmp de antene

- infrastructură total independentă de alimentarea cu energie electrică;
- interferențe foarte mici față de un punct de retranslație aglomerat de antene;
- instalare rapidă;
- proiectare simplă;
- eliminarea problemelor de compatibilitate între echipamente;
- posibilități de interceptare și bruiaj foarte scăzute;
- amprentă radio și terestră mică;
- nu necesită o infrastructură complexă și costisitoare: piloni, clădiri, drumuri de acces.

Pentru a obține costuri rezonabile, dezvoltatorul rețelei trebuie să găsească soluția cea mai bună, având tot timpul în vedere compromisul dintre calitate și interoperabilitate. Asigurarea interoperabilității între sistemele de comunicații folosite de alte armate partenere va fi punctul cheie în dezvoltarea și perfecționarea rețelelor de transport a informațiilor moderne.

Bibliografie:

<https://www.rumaniamilitary.ro>

<https://ro.wikipedia.org>

O PROBLEMĂ MAJORĂ: SECURITATEA IT

Plutonier Cornel-Cristian CIOBOTEA

Centrul 54 Comunicații RMNC



Specialiștii în cybersecurity afirmă că există două tipuri de organizații: cele care au fost deja victimele unui incident de securitate informatică și cele care urmează să fie. Dincolo de tipologii și încadrări, conștientizarea riscurilor de securitate rămâne o problemă majoră pentru foarte multe organizații din întreaga lume, mai ales din România.

„Cei care lucrăm în domeniul securității IT ne asemănăm, într-un fel, cu doctorii cardiologi. Pacienții noștri știu că sedentarismul și lipsa exercițiilor fizice, alimentația nesănătoasă și fumatul le fac rău. Și, cu toate acestea, continuă să fumeze, să mănânce alimente nepotrivite și să stea pe canapea până fac infarct. Și atunci vor o pilulă magică, cu ajutorul căreia să se facă bine dintr-o dată, fără niciun efort. Și susțin sus și tare că nu e vina lor: vinovate sunt companiile de tutun, lanțurile de fast-food, genetica și, evident, noi, pentru că nu am avut grijă de ei și nu i-am tratat cu o mai mare atenție“. Aceasta este metafora medicală a profesorului Gene Spafford, redactor-șef al „Computers & Security“ și unul dintre cei mai cunoscuți și apreciați specialiști în domeniul securității IT. Ea a fost făcută în 2000. Adică acum 18 ani, timp în care volumul, diversitatea și

complexitatea amenințărilor informatice au crescut exponențial, dar abordarea securității IT în cadrul organizațiilor nu s-a schimbat major.

Ultima amenințare majoră a fost campania ransomware WannaCry.

Global Risks Report	
The 5 risks most likely to happen in the next 10 years	
	rank
Extreme weather events	1
Natural disasters	2
Cyber attacks	3
Data fraud or theft	4
Failure of climate change mitigation & adaptation	5
Source: Executive Opinion Survey 2017, World Economic Forum	
Forumul Economic Mondial de la Davos plasează atacurile informatice pe locul trei în topul celor mai importante amenințări la nivel global.	

Cel mai mare atac informatic la nivel mondial declanșat pe 12 mai 2017 a afectat aproximativ 10.000 de instituții din 150 de țări. România s-a aflat și ea pe lista țărilor afectate. Printre cele mai popularizate cazuri s-au numărat cele ale fabricii Dacia Mioveni, care a fost nevoită să oprească producția pentru a remedia problema, și Spitalul Județean Bacău, care nu și-a mai putut debloca o bază cu date ale 300 de pacienți. După două luni, peste 300.000 de computere din întreaga lume au fost compromise în cadrul celui mai mare atac ransomware la nivel global. Conform datelor CERT-RO, 514 IP-uri proveneau din România.

Un raport anual de securitate dat publicității de către compania Check Point demonstrează că doar 3% dintre companii dețin la momentul actual mijloacele necesare pentru a putea face față unui atac de Generația a V-a. „Cu alte cuvinte, 97% dintre organizații utilizează tehnologii de

securitate depășite, care nu mai reușesc să facă față provocărilor actuale în domeniu“, a subliniat Sebastian Bănică, country manager al companiei Check Point pentru România.

WannaCry utilizează o tehnică de tipul „Divide and conquer” – are nevoie de un singur punct de intrare pentru a infecta întregul sistem și se poate răspândi prin intermediul infrastructurilor Cloud, a echipamentelor de rețea, stațiilor de lucru. Această tactică multi-level a permis atacului ransomware să penetreze cu ușurință arhitecturile de securitate clasice.

În România, alertele de securitate au crescut cu 25%.

Conform „Raportului privind evoluția amenințărilor cibernetice pentru anul 2017”, dat publicității de către CERT-RO în mai a.c., anul trecut au fost colectate și procesate 138.217.026 de alerte de securitate cibernetică, în creștere cu

25% față de 2016.

Analizele alertelor de securitate cibernetică colectate de CERT-RO au arătat că:

- 33,71% (2,89 milioane) din totalul IP-urilor alocate României au fost afectate;
- 83,63% (115,60 milioane) din alertele colectate și procesate au vizat sisteme informatice vulnerabile;
- 10,32% (14,33 milioane) din alertele procesate s-au referit la sisteme informatice compromise (infectate cu diferite forme de malware sau exploatare și utilizate de atacatori în diferite tipuri de atacuri);
- 1.709 de domenii web „.ro” au fost raportate ca fiind compromise.

Raportul CERT-RO a inclus anul acesta și analize ale principalelor campanii ransomware – WannaCry și NotPetya – care au afectat și România.

Surse de informare:

Bitdefender România
www.securityportal.ro
www.marketwatch.ro

PROTECȚIA DATELOR ȘI A INFORMAȚIILOR PERSONALE

Caporal clasa a II-a Nicolae INDRIE
Centrul 54 Comunicații RMNC



Secolul XXI poate fi catalogat ca fiind secolul informației, secolul inteligenței artificiale, secolul vitezei. Niciodată în istoria acestei lumi nu s-a

vehiculat un volum atât de mare de informație, pe distanțe atât de lungi, într-un timp atât de scurt. Nicicând nu a fost atât de ușor ca acum ca un cuvânt rostit la Paris să răsună instantaneu la Beijing sau o fotografie făcută în Australia să poată fi vizualizată instantaneu de aproape jumătate din populația globului, niciodată tranzacțiile bancare nu au fost atât de rapide. Azi informația se transmite la viteze ce ajung la ordinul Gb/s. Volumul informației e de asemenea imens, încât cele mai mici fișiere conțin date de ordinul Mb, mergând până la dimensiuni măsurabile în Tb.

Informația înseamnă bani, timpul înseamnă bani, motiv pentru care accesul la informație nu e doar vital, ci, de cele mai multe ori, imperios necesar. Un lucru esențial și o caracteristică deosebită a informației trebuie să fie securitatea acesteia. Protecția datelor, protecția și securitatea informațională trebuie să joace un rol vital în mediul online.

Cei mai mulți posesori de terminale IT (laptop-uri, notebook-uri, smartphone-uri, routere,

servere) nu conștientizează pericolul la care se expun neprotejându-și aceste dispozitive.

Cei mai mulți oameni, din păcate, gândesc că lor nu li se poate întâmpla ca vreun virus să le fie instalat în calculator sau ca vreun hacker să le fure ceea ce ei dețin pe hard-disk. Din păcate realitatea e cu totul alta. Zilnic au loc milioane de atacuri cibernetice, zilnic sunt furate date personale, bani, identități - și toate acestea au loc în mediul virtual. Au fost semnalate cazuri când întregi rețele fie bancare, medicale sau ale anumitor servicii publice au căzut pentru câteva ore, în urma atacurilor cibernetice. Dar nu doar instituțiile, firmele sau băncile cad pradă acestora, ci mai ales calculatoarele, telefoanele și tabletele personale.

Pentru a nu cădea pradă acestor furturi cibernetice, pentru a nu fi hărțuiți în mediul online, toate dispozitivele inteligente trebuie protejate, securizate și ferite, nu atât de ochiul uman, cât mai ales de algoritmi invazivi ai hackerilor. Protejarea datelor personale implică anumite metode, programe și mai ales o anumită conduită în mediul online.

- Esențială este instalarea unui antivirus cu licență, care să actualizeze zilnic baza de date. Există unele programe antivirus care sunt gratuite, iar unele gratuite doar pentru o anumită perioadă de timp, cele care însă vor oferi o protecție maximă a unui dispozitiv inteligent este antivirusul cu licență. Important este fie ca

antivirusul să facă automat scanări ale sistemului sau, periodic, aceste scanări să se facă manual.

- Programele folosite să fie cele cu licență, deoarece acestea au garanția ultimelor update-uri.

- Sistemele de operare (Windows, Linux s.a.) să fie actualizate.

- Instalarea firewall-urilor, fie că sunt de sine stătătoare, fie că aceste firewall-uri sunt furnizate (incluse în) de către antivirus sau de sistemul de operare.

- Folosirea unui browser ce beneficiază de update-uri (Mozilla, Opera, Chrome). Utilizarea plugin-urilor trebuie făcută doar dacă browser-ul permite acest lucru și mai ales dacă acestea sunt de încredere.

- Accesarea site-urilor care se dovedesc a fi de încredere. Unele plugin-uri sau, mai nou, chiar antivirusul poate să ofere calificativ în ceea ce privește natura site-urilor.

- Folosirea de servicii VPN, în special pentru tranzacții bancare.

- Protejarea sistemelor de tip router și, mai ales, achiziționarea unor dispozitive de acest gen, ce oferă un nivel ridicat de protecție (parole, chei, alerte de intruziune) ASUS, D-LINK, TP LINK, CISCO.

- Accesarea anumitor link-uri poate fi riscantă. Link-urile primite pe adresa de e-mail și care solicită informații personale sau de actualizare a acestora să nu fie accesate. E-mail-ul face parte din categoria acelor servicii nesigure. De asemenea atașamentele unor e-mail-uri provenite din surse necunoscute, cu expeditori necunoscuți, pot fi dăunătoare.

- Instalarea programelor din surse care nu

pot fi verificate pot crea condiții propice pentru invadarea sistemului de către viruși.

- Anonimitatea în mediul online s-a dovedit a fi esențială. Este necesar să nu fie făcute publice informațiile personale, precum nume, adrese, număr de telefon, CNP, parole, numere de cărți de credit.

- Este indicată evitarea rețelelor publice Wi-Fi, pentru comerț online sau afaceri personale.

Pentru a preîntâmpina ca adresa de e-mail sau orice alte conturi online să fie sparte este important ca acestea să fie securizate cu o parolă puternică. Ca o parolă să fie puternică, aceasta trebuie să îndeplinească câteva condiții:

1. Să fie lungă de cel puțin 12 caractere. Cu cât conține mai multe caractere, cu atât mai bine.

2. Să includă numere, simboluri, litere, atât mari, cât și mici.

3. Nu se vor folosi cuvinte din dicționar, de asemenea nici citate sau combinații de cuvinte ușor de ghicit.

4. Pentru ca parola să fie puternică, e bine să existe o combinație de litere mari, litere mici, simboluri, cifre.

Pentru a exista o securitate avansată și o protecție maximă a tuturor conturilor unui utilizator, este important ca fiecare cont să aibă o altă parolă. Pentru a fi mai ușor de reținut aceste parole, pot fi folosite programe de tip manager de parole ca de ex: 1Password sau LastPass.

Securitatea datelor și informațiilor personale nu e doar apanajul instituțiilor și nici obligativitatea providerilor de internet. Acest aspect trebuie să ne preocupe pe fiecare în parte.

În ziua de azi, hoțul sau infractorul nu mai

pătrunde pe ușă și nici prin fereastră, azi toate acestea se întâmplă printr-o conexiune la internet.

Bibliografie:

- Ghid SRI pentru protecția informațiilor în mediul online;
- Cum funcționează un program antivirus: www.scientia.ro;
- How to create a strong password (and remember it): www.howtogeek.

PRIMIT ÎN MAREA FAMILIE A TRANSMISIONIȘTILOR MILITARI

Psiholog Robert TUDOROIU

Centrul 89 Strategic de Comunicații și Informatică



Îmi aduc aminte cu emoție prima zi de lucru în Centrul 89 Strategic de Comunicații și Informatică. Pe atunci nu aveam nicio informație

despre specificul misiunilor pe care îl are unitatea și nici date despre personalul încadrat. Ulterior am aflat că am pășit într-o unitate de elită, ce are ca specific comunicațiile militare, asigurând legături la cel mai înalt nivel de profesionalism celor mai importante structuri din cadrul Ministerului Apărării Naționale.

Am fost plăcut impresionat de modul cum am fost primit de personalul unității, fiind sprijinit încă de la început să-mi desfășor activitatea de asistență psihologică în condiții optime. Însă am constatat că percepția asupra psihologului în unitate a fost influențată de necunoașterea exactă a activităților cu specific psihologic. Asigurarea psihologică a personalului reprezintă o realitate socială importantă, ea nu trebuie privită ca motiv al temerilor, ci mai degrabă ajutorul necesar, aliatul persoanei când cuplul FRICĂ – PANICĂ se interpune între om și provocările pe care și le asumă. Comunicarea cu psihologul este, până la urmă, vorbire despre suflet/psihic (M. Golu, în lucrarea „Fundamentele psihologiei”, arată că

termenul „psihologie” provine din cuvintele grecești psihe = suflet/psihic și logos = vorbire). De asemenea, am adus la cunoștința personalului unității că asistența psihologică nu reprezintă numai evaluare psihologică, ci reprezintă totalitatea acțiunilor, măsurilor și îngrijirilor acordate de o persoană specializată în vederea întăririi, fortificării și însănătoșirii psihice a unei persoane. Consilierea psihologică este acordată atât omului bolnav, care necesită un ajutor terapeutic sau psihoterapeutic, cât și omului sănătos, în scop preventiv, de adaptare psihică. Relaționarea psihologului cu personalul unității presupune disponibilitatea acestuia de a asculta activ, ceea ce asigură, între solicitant și psiholog, o legătură sensibilă, afectivă și intelectuală. Pe parcursul timpului au fost și situații în care angajații unității au fost trimiși la consiliere, dar în aceste cazuri rezultatele au fost limitate sau nu s-a ajuns de fiecare dată la o comunicare reală. Însă persoanele care au participat din proprie inițiativă la ședințele de consiliere psihologică au condus la modificarea modului de percepere a psihologului în unitate, prin schimbări pozitive la nivelul cognitiv și al personalității celui consiliat. Dacă m-aș raporta la propria experiență, aș putea spune că persoanele care au acceptat consilierea psihologică au apreciat indicațiile terapeutice și le-au utilizat într-o direcție favorabilă lor.

Multe cadre militare tratează cu destulă suspiciune și teamă psihologul din unitate, care

însă, pentru a fi eficient, are nevoie tocmai de încredere, comunicare, solicitări concrete, deschise. Sprijinul conducerii pentru desfășurarea în condiții optime a activității este condiția esențială, aproape singura, pentru că apoi celelalte cadre urmează exemplul și, printr-o comunicare adecvată, situațiile solicitante primesc soluții construite de echipa psiholog - persoană/persoane/comandant. Psihologul se așteaptă să fie apreciat în funcție de prestația sa profesională, ca și ceilalți luptători/salariați, ca și comandantul însuși, la rândul său.

Eficiența psihologului depinde de comandant, recunoașterea reală a oportunității de a beneficia de consiliere psihologică și de consiliere în domeniul resurselor umane, atribuțiile sunt decontate în produse ale muncii eficiente/optime. Pentru aceasta, psihologul efectuează cercetări asupra proceselor mentale,

studiază comportamentele umane individuale și colective. Prezența psihologului în unitate este un exemplu valoros al reglării pe baze științifice a relațiilor individuale și de grup în structurile sociale actuale, oferă căi de parcurs pentru viitor, până la anularea fricii cauzate de necunoaștere.

Este relevant faptul că activitatea de asistență psihologică în unitate este utilă atât pentru personalul unității, cât și pentru șefi/comandanți, în sensul unei mai bune cunoașteri a subordonaților.

În încheiere sunt deosebit de onorat că am oportunitatea de a lucra în familia transmisioniștilor militari din Șoseaua Măgurele 33.

În ceas aniversar, urez personalului Centrului 89 Strategic de Comunicații și Informatică un sincer și călduros

LA MULȚI ANI!

CONSILIEREA JURIDICĂ A PERSONALULUI UNITĂȚII: PREZENT ȘI PERSPECTIVĂ

P.c.c. Mariana NEAGU

Centrul 89 Strategic de Comunicații și Informatică

Motto: „Dacă justiția este prima nevoie a unui popor, justiția militară este prima nevoie a unei armate.”



Dreptul este strâns legat de viața socială, iar aceasta are în centrul ei omul.

Justiția este specifică și inseparabilă de natura umană și de organizarea comuni-

tăților umane.

El, omul, ființă socială înzestrată cu rațiune a avut și are nevoie de reguli simple și clare în desfășurarea normală a relațiilor sociale.

Prin excelență, activitatea din armată trebuie să fie caracterizată de lucrul în echipă, conform principiului: „Toți pentru unul și unul pentru toți”.

De aici, și nevoia de a avea un specialist în „reguli”.

Prezența unui consilier juridic în cadrul unității era imperios necesară, în situația creșterii numărului de spețe noi și complexe. Un volum însemnat de documente administrative emise de către comandant și de către șefii structurilor specifice instituției și nevoia avizării acestora din punctul de vedere al legalității și conformității, numărul mic de consilieri juridici la nivel de eșalon, problemele de natura resurselor umane, a achizițiilor publice, precum și a altor situații a

necesitat înființarea unei funcții de consilier juridic.

De-a lungul celor 12 ani de experiență m-am confruntat cu diferite situații juridice, mai mult sau mai puțin complexe. Pentru fiecare situație, cu ajutorul colegilor, am găsit soluția cea mai bună la acel moment; merg, pe principiul că fiecare problemă pe linie personală sau profesională are cel puțin o soluție.

Rolul juristului este acela de avizare și consiliere pe linie de specialitate atât a comandantului, cât și a întregului personal, în conformitate cu reglementările legale în vigoare.

La începutul carierei, am întâmpinat unele probleme privind soluționarea unor situații care aveau mai multe interpretări, situații controversate în literatura și practica judiciară sau administrativă și situații care nu au fost soluționate niciodată în practica judiciară. În această situație, consilierul juridic adoptă un punct de vedere, ce nu poate fi vădit eronat.

Fiind o activitate caracterizată de lucrul în echipă, se lucrează foarte mult cu oamenii.

Munca cu oamenii este cea mai complicată, întrucât fiecare persoană are temperamentul ei, caracterul ei, un grad de cultură diferit, provine dintr-un mediu social diferit și astfel trebuie să știi să comunici cu fiecare dintre ei.

În timp, cunoscându-ne unii pe alții și

căpătând încredere în activitatea de consiliere, personalul a început să-și deschidă „sufletul” în fața juristului și să vină la consiliere atât pe linie personală (moștenire, divorț, proprietate, închiriere etc.), cât și profesională (concedii, sporuri, drepturi salariale, propriiri, contravenții, încetare, suspendare, modificare a contractului individual de muncă etc.).

Oamenii, în general, merg pe ideea de a li se face dreptate, de a primi răspunsul optim la problema lor, indiferent dacă au mai multă sau mai puțină dreptate.

Consilierul juridic trebuie să depună toate diligențele astfel încât să asigure unității și personalului ei un proces corect, echitabil, în urma căruia instituția să primească o soluție echitabilă, legală și temeinică.

Consilierii juridici trebuie să fie mereu oamenii potriviți în locul potrivit pentru menținerea în echilibru a balanței dreptății.

Sunt momente în viață când poți spune foarte multe sau foarte puține.

Majoritatea situațiilor juridice au fost soluționate favorabil, în conformitate cu dispozițiile legale în vigoare. Au fost și situații mai complexe, a căror soluționare a durat în timp, dar au fost rezolvate, din fericire, pe cale amiabilă sau în instanță, tot favorabil unității.

Relațiile profesionale dintre consilierul juridic și personalul unității se bazează pe corectitudine, onestitate, sinceritate, încredere, imparțialitate, confidențialitate și obiectivitate.

Pe viitor doresc scăderea numărului de

proces; creșterea gradului de conștientizare și a nivelului de educație juridică în rândul personalului; o mai bună colaborare atât între consilierul juridic și întregul personal, cât și între angajați; elaborarea și diseminarea de materiale cu caracter informativ privind riscurile și consecințele faptelor ilegale, precum și a nerespectării termenelor; importanța cunoașterii legilor de la data intrării lor în vigoare.

Ce poate fi mai onorant și mai dezirabil pentru un jurist din armată decât să-și fructifice cunoștințele de specialitate direct pe talerul balanței, acolo unde valori precum adevărul sau dreptatea sunt veritabile arme de luptă.

Iar dacă arma juristului este sabia legii, acesta nu uită niciodată tăișul său dublu și sacru.

Cu mentalitate de învingători și sete pentru adevăr, slujitorii ei privesc peste timp cu mândrie, înainte cu încredere, în jos cu înțelegere și în sus cu recunoștința slujitorului nobilei arme a Justiției Militare.

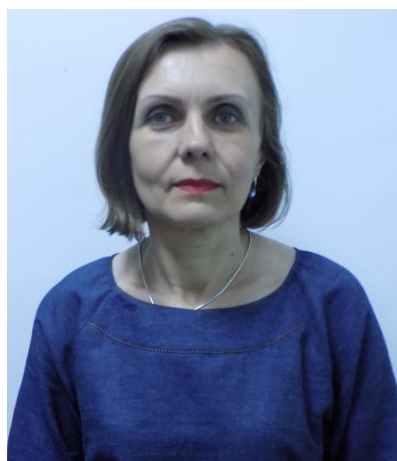
Justiția militară este zeița ce judecă „cu sabia adevărului, ținând cont doar de felul în care se înclină balanța dreptății”.



IMPACTUL ȘI MODUL DE MANIFESTARE A FACTORILOR DE RISC ASUPRA CALITĂȚII MUNCII PERSONALULUI

Responsabil SSM Florina CEACȘÎRU

Centrul 89 Strategic de Comunicații și Informatică



Activitatea umană indiferent de scopul ei, fiind în esență un proces dinamic cu consum de energie, implică pe lângă rezultatele

pozitive și un impact negativ asupra executantului, ceea ce se traduce prin uzura psihică și fizică asupra acestuia.

Această uzură sau acest impact negativ a condus la apariția și dezvoltarea conceptului de securitate și sănătate în muncă, cu rol principal în asigurarea stării de bine a executantului cu beneficii directe, nu numai asupra sa, ci și asupra angajatorului care va beneficia de calitatea muncii executantului.

Odată cu apariția securității și sănătății în muncă s-a dovedit nevoia dezvoltării unor programe coerente, care să garanteze și să consfințească dreptul omului la muncă, la protecție socială, integritate și sănătate.

Una din sursele permanente de pericol pentru om o reprezintă chiar propria-i activitate, fie ea și o simplă deplasare în spațiu.

Fiecare accident înseamnă suferințe fizice și psihice, pierderi de venituri pentru cei implicați (victime, familie, prieteni), pierdere de timp de

muncă pentru unitate și pentru societate.

Accidentele de muncă și bolile profesionale afectează negativ toate elementele sistemului de muncă, mai precis executantul, sarcina de muncă, echipamentele de muncă și mediul de muncă. În cadrul procesului de muncă, omul poate fi considerat în două ipostaze: de ființă umană și de executant al unei sarcini de muncă, fiecare cu valori și caracteristici specifice - viața, sănătatea, integritatea organismului, capacitatea de muncă, aptitudinile și cunoștințele.

Consecințele factorilor de risc se manifestă în multiple planuri: psiho-fiziologic (durere, stres, incapacitate de muncă) și economic (diminuarea productivității și calității muncii).

Consecința directă asupra sarcinii de muncă o constituie neîndeplinirea sarcinii de muncă sau neîndeplinirea ei la timp, mai ales la accidentele de muncă, precum și îndeplinirea necorespunzătoare, la unele boli profesionale, dacă nu se ajunge la incapacitate de muncă.

Asupra mediului social consecințele sunt concretizate mai ales sub forma stresului, suportat de cei aflați la locurile de muncă apropiate de cel al victimei, cu toate manifestările specifice.

Asupra individului, al victimei avem consecințe ca: suferința fizică și psihică datorate agresiunii suportate, incapacitate temporară sau permanentă de muncă, pierderea încrederii în sine privind modul în care fac față sarcinilor de muncă,

cheltuieli medicale, dar și pentru apropiații victimei prin suferință, durere, stres psihic, diminuarea veniturilor familiale.

Pentru angajator privit ca pe o instituție și nu ca persoană, aceste consecințe se pot manifesta prin pierderi de producție, deteriorarea mediului de muncă, cheltuieli de asigurări sociale și asistență medicală.

Un factor de risc prezent permanent în activitatea personalului unității este electrocutarea. Fie că aceasta se produce pentru cei care au ca sarcină activități de mentenanță, întreținere instalații electrice, instalare și exploatare echipamente comunicații, rezultatul ar fi identic.

Acest factor de risc propriu echipamentelor tehnice poate afecta ireversibil personalul, poate produce leziuni grave care duc de regulă la incapacitatea persoanei timp îndelungat. Trebuie să avem în vedere că, totuși, pericolul de electrocutare are în cele mai multe din cazuri legătură directă cu alt factor de risc și anume neutilizarea mijloacelor și echipamentelor de protecție, acesta producându-se prin refuzul lucrătorilor de a folosi echipamentul individual de protecție, deoarece consideră că îi stânjenește în mișcări sau în anumite operațiuni.

Omul (ca executant) își pune amprenta asupra celorlalte trei elemente componente ale sistemului de muncă, pentru că el este cel care

stabilește sarcina de muncă și poate interveni atât asupra mijloacelor de producție, cât și asupra mediului de muncă.

Mediul de muncă este elementul determinant în sănătatea lucrătorilor, motiv pentru care în unitate se efectuează determinări de noxe/analiză bacteriologică și expertizări ale condițiilor de muncă.

Alți factori de risc profesionali prezenți în unitate sunt noxele chimice care se degajă în spațiile de lucru (centrala termică, depozitele de combustibili, depozitul intendență, atelier), respectiv agenții biologici (drojdii și mucegaiuri) ca urmare a manipulării documentelor (arhive, birouri documente clasificate).

Expunerea la noxe poate avea efecte asupra aparatului respirator, nervos, asupra tegumentului, asupra ochilor, asupra aparatului digestiv. Deși la locurile de muncă expertizate, valoarea măsurată a noxei nu a depășit limita admisă (valoarea obligatorie națională), este necesară respectarea cu strictețe a măsurilor de protecție individuală și colectivă, supravegherea atentă a stării de sănătate (control medical periodic).

Acordarea alimentației de protecție, ca măsură individuală de protecție, nu constituie un antidot, ci reprezintă o măsură complementară care poate ajuta organismul să-și întărească mecanismele de apărare.

BALANȚA ȘI SABIA CU DOUĂ TĂIȘURI

P.c.c. Mariana NEAGU

Centrul 89 Strategic de Comunicații și Informatică

*Motto: „Cine nu pedepsește nedreptatea, poruncește ca ea să fie făcută.”
(Leonardo Da Vinci)*



Balanța și sabia
– două simboluri ale
justiției.

Justiția repre-
zintă acea stare
generală ideală a
societății, realizabilă
prin asigurarea pentru
fiecare individ în

parte și pentru toți împreună a satisfacerii
drepturilor și intereselor legitime.

Scurtă istorie a justiției antice

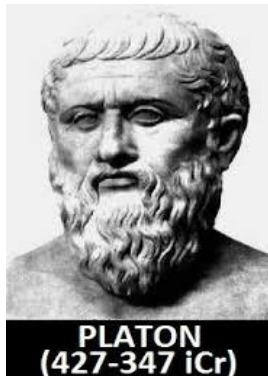


Foto nr. 1 – Platon

În concepția lui Platon (foto nr. 1), justiția se realizează prin îndeplinirea de către fiecare clasă socială a ceea ce îi era destinat prin naștere – să conducă, să muncească, să se lupte; să se supună fără proteste.

Aristotel (foto nr. 2) concepea justiția fie sub forma sa comutativă, care privește raporturile dintre particulari, fie sub forma distributivă, care privește raporturile dintre colectivitate și indivizi;



Foto nr. 2 – Aristotel

iar la greci, echitatea („epieieia”) avea mai mult valoarea unei justiții sociale, al cărei scop era acela de a îndrepta legea acolo unde era deficitară din cauza caracterului său universal. După împărțirea în mod egal a prăzii, grecii strigau: „Dikè” (dreptate), așa cum după izbânda militară strigau: „Nikè” (victorie). Personificată apoi, Dikè, devine zeița armoniei și a păcii civile, iar „Themis” cea care apreciază și judecă, pare a se confunda cu conștiința, întrucât privește viața morală.

La romani, justiția se fonda pe principiiul moral al dreptății, ei așezând la baza justiției acel oneste vivere (a trăi cinstit).

Morala creștină influențează conținutul ideii de justiție. Sfântul Augustin și Toma d’Aquino fac distincție între legea divină, legea naturii și legea omenească. Există o ierarhie a legilor; în vârful piramidei se plasează legile eterne, divine, care dau conținut legilor naturii, la baza piramidei stând legile omenești (dreptul pozitiv). Legea pozitivă are autoritate în măsura în care

corespunde rațiunii.



Foto nr. 3 – Zeița Themis

Zeița Themis (foto nr. 3) reprezintă simbolul antic al justiției, care s-a păstrat până în prezent. În mitologia greacă, Themis semnifică zeița dreptății, fiind echivalentă în mitologia romană cu Justiția, care era considerată personificarea ordinii naturale „Legea Naturii”, stabilite prin legea divină, precum și a dreptății divine. Părinții zeiței sunt Uranus și Gaia, adică Cerul și Pământul, entități cosmologice, dar, în prelungire, sunt și ontologice.

Cuvântul „themis” înseamnă și „obicei” sau „tradiție”, iar termenul mai larg, care le cuprinde pe toate, este „cutuma”.

Zeița are două funcții de bază, una pe verticală și alta pe orizontală. Pe verticală și de Sus în Jos cuprinde următoarele trepte: Legea divină, Legea naturii, Cutuma, care este Legea tradițională, nescrisă. Mișcarea se poate face și de Jos în Sus, această mișcare făcând-o Judecătorul, care, trecător fiind pe Pământ, stă și trebuie să rămână în umbra eternă și protectoare a zeiței. Pe orizontală, adică pe Pământ, zeița face trecerea de la Cutumă la Legea juridică și la Codul Juridic. La romani, popor realist și pragmatic, Themis devine Justiția. O mare parte din Legile Codului roman

sunt valabile și azi, unele dintre ele fiind intangibile. Zeița Themis este reprezentată de o femeie foarte frumoasă, severă, legată la ochi cu o eșarfă, ținând într-o mână o balanță, iar în cealaltă o sabie. Nu este nici oarbă, nici chioară, ci vede chiar foarte bine. Nu este vorba de ochii exteriori, ci de ochiul interior, care vede ceea ce retina nu poate vedea. În acest sens există și o expresie a lui Eminescu: „Fiindcă ochiul, închis afară, înăuntru se deschide”. Eșarfa, care acoperă ochii zeiței, nu acoperă și urechile acesteia, iar mărturia faptelor petrecute, fie ele bune sau rele, o dau ochii, nu urechile. Martorul este chemat în fața Judecătorului ca să spună ce a văzut, nu ce a auzit. Zeița privește de Sus, cu un surâs ironic, așa numitele informații din sursă; aceasta bazându-se pe Ochiul interior, care este Unul.

Balanța din mâna stângă a zeiței sugerează ideea că, judecătorul trebuie să pună pe „cântarul justiției”, toate probele și să lase ca balanța să arate, în condiții de independență și imparțialitate, unde este dreptatea. În examinarea cauzelor, judecătorul trebuie să cântărească drepturile și interesele fiecărei părți, fără să țină seama de considerațiuni străine procesului, oricare ar fi ele. Judecătorul este deasupra părților în cauză, chiar dacă una dintre ele ar fi puterea sau administrația.

Spada – instrumentul Sancțiunii, al pedepsirii celor vinovați. Se observă că spada este ținută cu tăișul în jos, semn că instrumentul Sancțiunii rămâne în stare potențială, sau una virtuală; spada sau sabia cu două tăișuri are o semnificație dublă, și anume: sancțiunea, care trebuie executată, o dată de bună voie, iar în caz contrar, prin punerea în executare (executarea

silită). De asemenea, sabia cu lama îndreptată în Sus reprezintă faptul că sancțiunea dată prin hotărâre trebuie executată numaidecât, imediat; iar sabia cu lama îndreptată în Jos, înseamnă că instrumentul sancțiunii rămâne în stare potențială, sau una virtuală.

De o parte și de alta a Zeiței se află cei doi „matadori” ai procesului: procurorul și avocatul, inculpatului.

Procurorul vede în spadă un instrument bun doar pentru „tăierea capului”, în timp ce Avocatul o vede doar cu tăișul în Jos, un instrument virtual, pasiv. Într-o schemă intuitivă, care pleacă de la Măsura lui Aristotel, Procurorul se află în Stânga, pe poziția lui „prea puțin”, iar Avocatul se află în Dreapta, pe poziția lui „prea mult”. Procurorul spune că, Inculpatul nu are nici cel puțin „o moleculă” de dreptate, pe când Avocatul spune că Inculpatul nu are destulă Dreptate, ci prea multă Dreptate. Spre deosebire de cei doi, Zeița, ca și Măsura lui Aristotel, se mișcă între cele două extreme, evitându-le pe ambele. Ea procedează doar gradual, folosind ambele instrumente, perfect corelate.

Cu Balanța dintr-o mână, ea măsoară gradual Vinovăția, iar cu Spada din cealaltă mână aplică, gradual și proporțional, Sancțiunea meritată de Inculpat. Între echilibru și dezechilibru, Balanța poate avea diverse grade de înclinație, iar Spada poate fi folosită pentru diverse operații de tăiere, de la tăierea unui deget, a unei urechi sau scoaterea unui ochi (pentru minciună), până la „tăierea capului” netrebnic al Inculpatului, care a săvârșit „păcate de moarte”²² !

Mi-aș permite o asociere între Dreptul

Judecător (Dumnezeu) și judecătorii pământenii. Dreptul Judecător niciodată nu va fi părtinitor cu nimeni, niciodată nu va ține cont de rangul social al unei părți implicate în „proces”; legile divine sunt imuabile, absolute și niciodată nu vor putea fi combătute de nimeni și nimic! Să revenim la sabia cu două tăișuri; simbolul sabiei îl mai putem găsi și în religie, simbolizând „cuvântul lui Dumnezeu”. Sfântul Apostol Petru este zugrăvit pe icoane cu sabia în mână.



Foto nr. 4 – Arhanghelul Mihail

Sabia reprezintă cuvântul lui Dumnezeu. De două ori, în scrierile sale, Sf. Ap. Pavel înfățișează cuvântul sub chipul sabiei. În Epistola către Efeseni vorbește despre lupta necontenită care-l aștepta cu căpeteniile, domniile și stăpânirile veacului acestuia și împotriva duhurilor răutății celor de sub cer. Sf. Ap. Pavel, pentru izbânda acestei lupte, dă sfat efesenilor să se îngrijească de armele duhovnicești, în numele cărora arată și sabia duhovnicească, sub care, după cum lămurește el, trebuie înțeles Cuvântul lui Dumnezeu. Acesta lucrează mai puternic, e viu și lucrător și mai ascuțit decât orice sabie cu două tăișuri și pătrunde până la despărțirea sufletului și duhului, dintre încheieturi și măduvă, și destoinic să judece simțirile și cugetările inimii”! (Evrei,

IX.12). Sabia Arhanghelului Mihail (foto nr. 4) este focul purificator al adevărului care învinge forțele răului, ale întunericului, care transformă energiile negative în energii pure, divine aducătoare de viață.

În perioada renașterii, el apare ca un tânăr foarte puternic și frumos, îmbrăcat într-o haină splendidă, purtând sabie, scut și lance, iar în alte reprezentări este cel care ține Balanța Dreptății.

„Spada (sabia) este în primul rând simbolul stării militare și al virtuții sale principale, vitejia, precum și a funcției, a puterii sale”, afirmă Thomas Grison, autorul cărții „Le Symbolisme de l'épée”; de asemenea, afirmă că puterea are un dublu aspect, distrugător și constructiv; asociată cu balanța evocă dreptatea. Spada se regăsește în mitologie, în tradiții religioase, în alchimie, în toate culturile lumii. Apocalipsa descrie o spadă cu două tăișuri ieșind din gura Verbului.

De asemenea, sabia este un simbol al puterii în stare să dea sau să ia viața; simbolizează forța solară și are un înțeles de energie generatoare³.

În istorie, spada reprezintă un simbol al puterii. Spada lui Ștefan cel Mare și Sfânt (foto nr. 5) este o armă cu două tăișuri, folosită de obicei cu ambele mâini, spre deosebire de sabie, cu un

singur tăiș și utilizată doar cu o singură mână. Această spadă (foto nr. 6) se află la Muzeul Topkapî din Turcia, fiind încărcată de legendă, venerată și temută de turci, construită din oțel special la indicațiile personale ale voievodului.



Foto nr. 5 – Ștefan cel Mare și Sfânt



Foto nr. 6 – Spada lui Ștefan cel Mare și Sfânt

Pentru final am ales o maximă antică: „Jus est ars boni et aequi ut eleganter Celsus definit” („Dreptul este arta de a cunoaște ceea ce este bun și just.”) – definiția lui Celsus⁴.

Note:

¹Prof. univ. dr. Nicolae Popa – Teoria generală a dreptului – Editura Actami, București, 1996, pag. 125 și urm.

²Prof. univ. dr. Tudor Catineanu – Balanța Dreptății, vol. 2, 2014.

³Thomas Grison – Les Symbolisme de l'épée, Éditeur Paris, 2017, pag. 118.

⁴Maxime juridice antice, Editura Militară, București, 1992, pag. 1.

LA ORDIN

Claudiu SOFRONE

DĂ ORDINE ÎN ARMATĂ	▼	ȚINE! SCRIS PUȚIN APLECATĂ	▶	▼	UN TIMP DÂNSELE MOȘUL CU SOMNUL	▶		▼	EXPERT ÎN TOATE	▼	GRĂDINĂ DE IARNĂ
		▼			▼		VEDETĂ	▶	▼		▼
							VECHIUL ORAȘ				
NIVEL DE TRAI	▶			E CLAR	▶		▼	ARMĂ VECHE	▶		
FEMEI TRISTE				BRÂNZĂ DULCE				ȚINE O HAINĂ			
				▼		FACE INELE	▶	▼			
						CÂNTATE LA OPERĂ					
BĂRBAT CU PUȘTI	▶				LUATĂ LA TRAGERE	▶	▼			CORP... DE PAZĂ	
APĂ TARE					TRECERE DE NIVEL						
			DĂ ORDINE ÎN ARMATĂ	▶	▼					▼	PUNE O CONDIȚIE
CA O GULIE	▶		▼	ÎN OXID!	▶		GĂSIȚI CU GREUTATE	▶			▼
CĂMAȘĂ CU FLORII				BĂTUT ÎN LEMN			COMPLET				
		LEGALĂ	▶	▼			▼		ÎN VENE!	▶	
		TREABĂ FĂCUTĂ ÎN SILOZ							MARGINI DE TABLOU!		
ZĂPĂCITE	▶	▼				PRIMEȘTE ORDINE ÎN ARMATĂ	▶		▼		
SE ADAUGĂ ÎN SALATA ORIENTALĂ											
▼▶				FACE LINIȘTE	▶	▼		A TERMINA LUCRUL	▶		
				ACORD GLOBAL							
	CONCURS CU CAI NĂRĂVAȘI	▶		▼							
	GINERI										
	▼				ÎNCHIEIE O OPERAȚIE						
▶											
CÂNTEC TURCESC				ESENȚĂ DE ZADA!	▶	▼					
-- PRIMELE LITERE	▶			FINAL DE BILANȚ!							
				▼							
▶											
A CĂUTA DIRECȚIA											
SCUTIT DE PEDEAPSĂ	▶										



ARMA NOASTRĂ

	1	2	3	4	5	6	7	8	9	10	11	12
1	T											
2		R										
3			A									
4				N								
5					S							
6						M						
7							I					
8								S				
9									I			
10										U		
11											N	
12												I

Claudiu SOFRONE

ORIZONTAL:

1) Militari instruiți în manipularea unor aparate de transmisiuni. 2) Primele din armată! – Lupta pentru onoare – Vânător de munte. 3) Articol de bază pentru un roșior – Se ocupă de actele din arhivă – Cântec de greier. 4) Moșul care ne adoarme copiii – Spațiu de expunere la facultate. 5) Tip de comunicare oficială – Întoarcerea rachetei pe teren. 6) Formație din Anglia – Piesă de îmbinare a cablurilor – Răpuse... în război! 7) Final de recul! – A produce un sunet prelung la stația radio – Instalare în centru! 8) Dispersat pe teren – Început și sfârșit de marș! – Învățat să tragă pe teren. 9) Indicația șefului nemijlocit – Predispus la visare. 10) A concentra la unitate – Publicat din toamnă în toamnă 11) Stă în rond cu săbiile scoase – Tipică persoanelor din Ucraina. 12) Vânată într-un safari – Unități scoase în câmp.

VERTICAL:

1) Servește la comanda telegrafistului – Urme de proiectil! 2) Mari diviziuni ale timpului geologic – Neglijență la locul de muncă. 3) A se da în vânt – Instalație de transmitere a sunetelor prin unde electromagnetice. 4) În plin asediu! – Oameni de ordine – Cale de comunicație. 5) Unul care nu stă la discuții – Gazda noastră în expedițiile montane. 6) Lipsită de bunătate – Prezentul la țară – Spațiu de joacă pentru copii. 7) Prima din alfabetul fonetic NATO – A face surprize. 8) Mijloc de ianuarie! 9) Final de compromis... într-o discuție! – Un an din armată – Tragedie în valuri. 10) Surprins în fapt – Aflat la ordinea zilei. 11) Concentrat în timpul luptei – A emite sunete cu tărie – Pusă la zid de fostul soț. 12) A pleca în altă țară – A interpreta un cântec monoton.

NOSTALGIE

Cap. cls. a III-a Victoraș COSMESCU

Centrul 89 Strategic de Comunicații și Informatică

Când eram mic, îmi spunea tata:
Să nu te temi să faci armata,
Că-ți va veni vremea și ție,
Să-ți faci această datorie.

Vedeam ades soldați pe stradă,
Și-n brațe unii mă purtau
Când mă lua tata la paradă,
Precum o vrajă mă uimeau.

Dar timpul iute a zburat
Și mi-a venit vremea și mie,
Și-am devenit și eu bărbat
Mândru să plec la datorie.

Când haina Țării am îmbrăcat
Și-am sărutat Drapelul sfânt,
Cu ochii-n lacrimi am jurat
Să apăr Pacea pe Pământ.

.....

Gândesc adesea cu nostalgie,
La anii din copilărie...
Mă văd micuț, pe-o mare stradă,
Mergând cu tata la paradă!

LA ORDIN

Claudiu SOFRONE

	L		N	A		E	R	A		S	
C	O	L	O	N	E	L		S	T	E	A
	C	A	T		N	E	T		A	R	C
P	O	S	A	C	E		A	U	R	A	R
	T	A	T	A		A	R	M	A		A
J	E	T		S	E	R	G	E	N	T	
	N	A	P		X	I		R	A	R	I
I	E		L	I	C	I	T	A		E	N
	N	A	U	C	E		O	S	T	A	S
O	T	E	T		S	S	T		U	Z	A
U		R	O	D	E	O					
A	M	A	N	A		L					
	I	T	I		A	D					
O	R	I	E	N	T	A					
	I	E	R	T	A	T					

ARMA NOASTRĂ

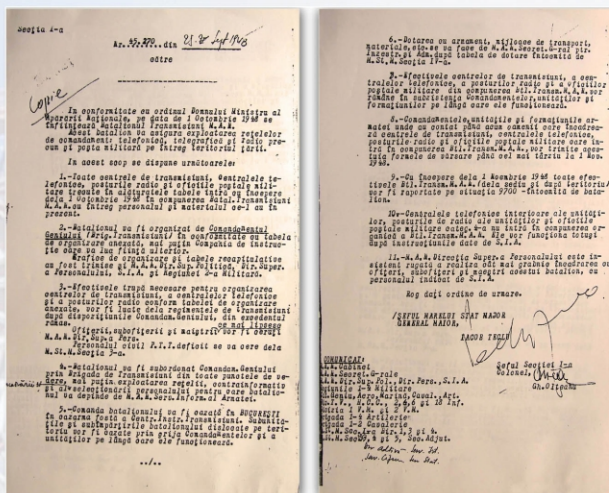
T	E	L	E	G	R	A	F	I	S	T	I
A	R		D	U	E	L		S	O	I	M
S	E	A		R	A	F	T		C	R	I
T		E	N	E		A	U	L	A		G
A	D	R	E	S	A		R	E	T	U	R
T	E	A	M		M	U	F	A		I	A
U	L		T	I	U	I		L	A	T	
R	A	R	I	T		M	S		C	A	L
A	S	A		A	T	I	P	I	T		A
	A	D	U	N	A		A	N	U	A	L
I	R	I	S		R	U	T	E	A	N	A
L	E	O	A	I	C	A		C	L	A	I



CENTRUL 89 STRATEGIC DE COMUNICAȚII ȘI INFORMATICĂ



PRIMIREA PRIMULUI DRAPEL DE LUPĂ AL UNITĂȚII



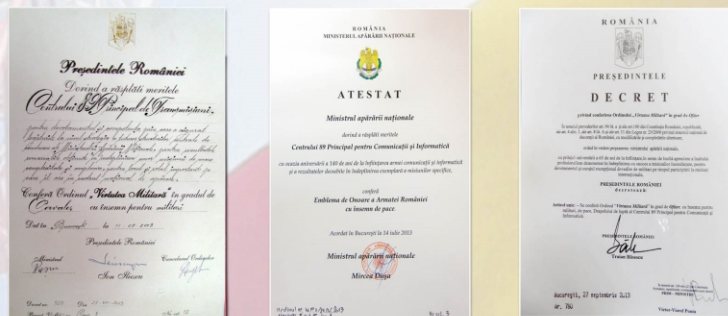
ACTUL DE ÎNFIINȚARE AL UNITĂȚII - 1948



DECORAREA DRAPELULUI DE LUPĂ



ÎNĂMÂNAREA NOULUI DRAPEL
DE LUPĂ-1996



ÎNĂMÂNAREA STEAGULUI
DE IDENTIFICARE-2008



PRIMIREA DRAPELULUI DE LUPĂ
LA SCHIMBAREA COMENZII
Col. Aurel BUCUR-2014



DECORAREA DRAPELULUI DE LUPĂ
-2003-



DECORAREA DRAPELULUI DE LUPĂ
-2012-

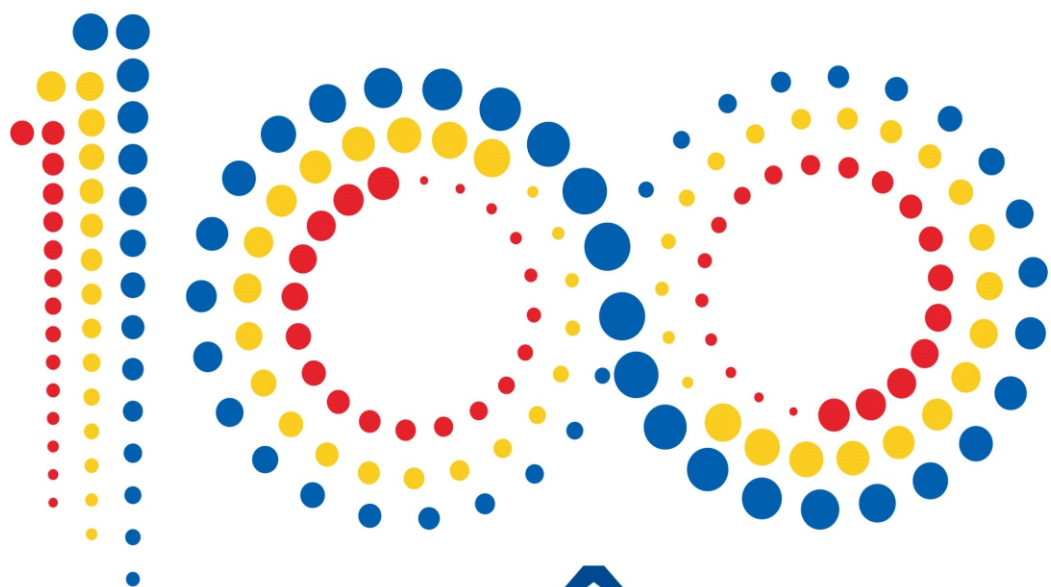


DECORAREA DRAPELULUI DE LUPĂ
-2013-



PRIMIREA DRAPELULUI DE LUPĂ
LA SCHIMBAREA COMENZII
Col. Adrian VĂTAFU-2017





ROMÂNIA

1918-2018 | SĂRBĂTORIM ÎMPREUNĂ

