

# REVISTA COMUNICAȚIILOR ȘI INFORMATICII



2017

UN AN ANIVERSAR PENTRU COMANDAMENTUL COMUNICAȚIILOR  
ȘI INFORMATICII ȘI UNITĂȚILE MILITARE SUBORDONATE

Nr. 1/2017

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

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

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

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

**Redactor șef:**  
**Col. dr. Dorin ALEXANDRESCU**

**Redactori:**  
**Lt. col. dr. ing. Mircea BORA**  
**Mr. Ștefan-Florian HOGEA**

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

**ADRESA REDACȚIEI:**

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

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

**ISSN: 1841-0758**

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

## CUPRINS

### **EVENIMENT**

- Mesajul șefului Statului Major General cu prilejul zilei Centrului 48 Comunicații și Informatică Strategice 3  
- General Nicolae-Ionel CIUCĂ
- Mesajul șefului Statului Major General cu prilejul zilei Centrului 115 Comunicații RMNC ..... 5  
- General Nicolae-Ionel CIUCĂ
- Mesajul comandantului Comandamentului Comunicațiilor și Informaticii cu prilejul aniversării a 75 de ani de la înființarea Centrului 48 Comunicații și Informatică Strategice ..... 7  
- General de brigadă Radu-Marius POP
- Mesajul comandantului Comandamentului Comunicațiilor și Informaticii cu prilejul aniversării a 35 de ani de la înființarea Centrului 115 Comunicații RMNC ..... 8  
- General de brigadă Radu-Marius POP

### **ANIVERSARE**

- Centrul 48 Comunicații și Informatică Strategice – 75 de ani de istorie în slujba țării ..... 9  
- Plutonier adjutant principal Titi PIPOS
- Centrul 115 Comunicații RMNC Bacău – repere istorice la ceas de sărbătoare..... 13  
- Maistru militar clasa I Ioan POPA
- La mulți ani C48CIS! ..... 17  
- Locotenent Marius GÂREA  
- Locotenent Adelina APETROAEI

## **ACTUALITATE ȘI PERSPECTIVE**

Implementarea conceptului FMN.....	19
- Colonel dr. Sorin-Silviu BĂLĂȘESCU	
- Locotenent Ilie IULIAN	
Realizări în activitatea de cercetare, dezvoltare și reglementări în armă.....	22
- Colectivul de redacție	
Serviciul de recuperare în caz de dezastre/Disaster Recovery as a Service (DRaaS) .....	26
- Locotenent colonel Cătălin CÎRNU	
Rețele digitale SDH.....	28
- Căpitan Cristian GAFENCU	
Semnătura electronică.....	32
- Căpitan Dorin-Horia ILIEȘ	
Internet of Things – internetul lucrurilor.....	36
- Căpitan Adrian MIHAILEANU	
Rolul rețelelor de misiune MNE, MNX în cadrul FMN.....	39
- Locotenent Cristina CHIRVASE	

## MESAJUL ȘEFULUI STATULUI MAJOR GENERAL CU PRILEJUL ZILEI CENTRULUI 48 COMUNICAȚII ȘI INFORMATICĂ STRATEGICE



La 10 ianuarie se împlinesc 75 de ani de la înființarea Regimentului 4 Transmisiuni, moment care a marcat nașterea și începutul dezvoltării ulterioare a actualului Centru 48 Comunicații și Informatică Strategică.

De la înființare și până astăzi, Centrul 48 Comunicații și Informatică Strategică a cunoscut profunde transformări. Indiferent de denumirea pe care a avut-o de-a lungul celor 75 de ani, centrul s-a modernizat continuu, s-a adaptat misiunilor și cerințelor tehnice, și-a îmbunătățit dotarea specifică, concomitent cu specializarea personalului, ținând pasul cu schimbările produse în ansamblul societății și al instituției militare.

Astfel, Centrul a făcut față cu succes tuturor provocărilor generate în contextul interoperabilității cu NATO și al derulării de acțiuni comune cu Alianța. La data de 01 august 2010, prin ordin al șefului Statului Major General a intrat în vigoare statul de organizare al Modulului NATO de Comunicații și Informatică Dislocabil DCM „E”, parte a batalionului de comunicații al NATO, aflat sub control operațional al SACEUR. Centrului 48 Comunicații și Informatică Strategică îi revine responsabilitatea instruirii militare a personalului și a asigurării suportului logistic necesar pentru misiune.

În perioada 2010-2012, Modulul NATO de Comunicații și Informatică Dislocabil DCM „E” a parcurs programul de operaționalizare, iar în perioada 2012-2016 a participat la diferite exerciții NATO pe întreg continentul Europei, precum și la două misiuni în Teatrul de operații Afganistan.

În acest an, centrul a găzduit cu succes exercițiul NATO „Steadfast Cobalt-16”, desfășurat atât la nivel strategic, cât și operativ și tactic, în mediu static și dislocabil, exercițiul atingându-și obiectivul propus, acela de a testa și evalua interoperabilitatea sistemului de comunicații și informatică în sprijinul structurii de comandă și de forțe ale NATO.

*Dragi camarazi,*

În contextul amplului proces de transformare și modernizare a Armatei României, dumneavoastră, personalului Centrului 48 Comunicații și Informatică Strategică, vă revin responsabilități și misiuni extrem de importante, cu implicații și efecte directe în funcționalitatea organismului militar.

---

Ați demonstrat calități profesionale deosebite și o mare capacitate de adaptare la noile cerințe de compatibilitate și interoperabilitate cu structurile similare ale NATO, iar modul în care ați răspuns cerințelor îmi conferă un sentiment de satisfacție și încredere în potențialul dumneavoastră de a face față cu succes provocărilor viitoare.

La ceas aniversar, vă felicit și aduc mulțumiri întregului personal activ, în rezervă și în retragere, pentru rezultatele remarcabile obținute în cei 75 de ani de activitate.

Vă adresez urări de sănătate, dumneavoastră și familiilor dumneavoastră, și succes în îndeplinirea misiunilor care vă sunt încredințate.

La mulți ani!

**ȘEFUL STATULUI MAJOR GENERAL**

**General**

**Nicolae-Ionel CIUCĂ**

## MESAJUL ȘEFULUI STATULUI MAJOR GENERAL CU PRILEJUL ZILEI CENTRULUI 115 COMUNICAȚII RMNC

La 14 iulie 1873 se înființa, prin decret regal, prima secție de telegrafişti militari, deschizându-se astfel calea către sistemele moderne de comunicații pe care le folosim în zilele noastre în Armata României.

Ca urmare a evoluției și necesităților tot mai mari de comunicare, arma transmisiuni a cunoscut o dezvoltare semnificativă, astfel încât la 28 februarie 1982, în baza ordinului ministrului apărării naționale, se înființa Batalionul 115 Transmisiuni dislocat în garnizoana Bacău, subordonat Comandamentului Trupelor de Transmisiuni, având misiunea de a asigura nevoile de legătură ale acestui eșalon.

Începând cu data de 3 mai 1982, Batalionul 115 Transmisiuni a derulat primul ciclu de instrucție, iar la 9 mai 1983, unității i s-a înmănat primul Drapel de Luptă, simbol al onoarei și, totodată, dovadă de apreciere a capacității unității de a îndeplini, la cel mai înalt nivel, misiunile încredințate.

Începând cu anul 2002, batalionul s-a operaționalizat, primind denumirea de Centrul 115 Transmisiuni de Sprijin, reorganizat ulterior sub denumirea actuală de Centrul 115 Comunicații RMNC.

Misiunea centrului nu a fost deloc ușoară, în noua concepție revenindu-i sarcina de a înființa și exploata, în sistem integrat, noi centre de comunicații în aria sa de responsabilitate. Dovedind deschidere la nou, creativitate și perseverență, centrul a reușit dezvoltarea Sistemului de Telecomunicații al Armatei României (STAR).

Unitatea a făcut permanent proba capacității de a se adapta la standardele moderne, gestionând cu succes activitățile comune în cadrul Alianței Nord-Atlantice, prin realizarea unor legături de calitate, sigure și neîntrerupte, care nu pot fi posibile fără o standardizare și o compatibilitate strictă a tuturor elementelor specifice proiectării, realizării și exploatării sistemelor de comunicații și informatică.

### *Dragi camarazi,*

Pentru armată, dumneavoastră, specialiștii în comunicații, sunteți „nervul central”, cei care faceți posibilă transmiterea ordinelor și informațiile necesare conducerii activităților și acțiunilor militare.

Aniversarea acestui moment important din istoria centrului are loc într-o perioadă în care Armata României se află în plin proces de modernizare și de creștere a capacității de luptă, în cadrul căruia elementele destinate asigurării comenzii și controlului joacă un rol deosebit de important.

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

---

tor și că veți fi în măsură să asigurați infrastructurile de rețea și informațională necesare conducerii la nivel strategic și operativ a Armatei României, adoptând cele mai moderne soluții în domeniu.

Cu prilejul aniversării a 115 ani de activitate, vă felicit și aduc mulțumiri întregului personal activ, în rezervă și în retragere pentru rezultatele obținute.

Vă adresez urări de sănătate, dumneavoastră și familiilor dumneavoastră, și succes în îndeplinirea misiunilor care vă sunt încredințate.

La mulți ani!

**ȘEFUL STATULUI MAJOR GENERAL**

**General**

**Nicolae-Ionel CIUCĂ**



**MESAJUL  
COMANDANTULUI  
COMANDAMENTULUI COMUNICAȚILOR ȘI INFORMATICII  
CU PRILEJUL ANIVERSĂRII A 75 DE ANI DE LA ÎNFIINȚAREA  
CENTRULUI 48 COMUNICAȚII ȘI INFORMATICĂ STRATEGICE**



Îmi revine deosebita onoare de a vă transmite dumneavoastră și valorosului colectiv de cadre, personalului civil contractual, soldaților și gradaților profesioniști acum, la cea de-a 75-a aniversare a înființării Centrului 48 Comunicații și Informatică Strategice, cele mai sincere felicitări și urări de noi succese în noul an de instrucție.

Ați încheiat precedentul an cu unul din cele mai semnificative succese obținute de structurile de comunicații și informatică din Armata României, respectiv Exercițiul NATO de testare a interoperabilității C2/C4ISR/CIS „STEADFAST COBALT 2016”/SFCT 16, experiență unică în istoria armei comunicații și informatică, ce a confirmat încă o dată spiritul de dăruire, camaraderia și înaltul profesionalism al militarilor acestei structuri.

Remarcabilele realizări ale unității dumneavoastră sunt cunoscute și recunoscute la nivelul eşaloanelor superioare. Admirabilele calități ce caracterizează personalul unității au constituit, fără îndoială, factorul determinant al realizărilor deosebite cu care vă prezentați astăzi la sărbătoarea unității.

Pentru toate realizările dumneavoastră, vă rog să-mi permiteți ca în această zi aniversară să vă felicit, să vă adresez cele mai calde urări de sănătate, fericire și reușită în importantele proiecte și întreprinderi profesionale, succese și realizări personale, dorind să vă asigur de cea mai înaltă considerație și prețuire pentru meritoasa și apreciată dumneavoastră activitate!

LA MULȚI ANI Centrului 48 Comunicații și Informatică Strategice!

**COMANDANTUL COMANDAMENTULUI  
COMUNICAȚILOR ȘI INFORMATICII**

**General de brigadă**

**Radu-Marius POP**

**MESAJUL  
COMANDANTULUI  
COMANDAMENTULUI COMUNICAȚIILOR ȘI INFORMATICII  
CU PRILEJUL ANIVERSĂRII A 35 DE ANI DE LA ÎNFIINȚAREA  
CENTRULUI 115 COMUNICAȚII RMNC  
– 28 FEBRUARIE 2017 –**

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

A 35-a aniversare a înființării Centrului 115 Comunicații R.M.N.C., în baza ordinului ministrului apărării naționale nr. O.G. 45 din 08.12.1981, sub denumirea sa inițială de Batalionul 115 Transmisiuni, îmi oferă onorantul prilej de a transmite valorosului colectiv al unității dumneavoastră cele mai sincere felicitări și urări de noi succese în toate domeniile de activitate.

Rezultatele constant foarte bune obținute în toți anii existenței sale constituie un merit al tuturor, de la soldat la comandant, și au contribuit la creșterea continuă a prestigiului unității, la afirmarea dumneavoastră ca adevărați profesioniști, cu o înaltă calificare de specialitate și o solidă pregătire militară generală.

Schimbarea denumirii în Centrul 115 Comunicații R.M.N.C. și intrarea în vigoare a noului stat de organizare, ca urmare a operaționalizării unității la 1 aprilie 2006, au reprezentat începutul unei noi perioade de implementare a cerințelor noilor standarde, pentru asigurarea serviciilor generale și funcționale de comunicații și informatice, precum și pentru managementul, operarea și mentenanța Rețelei Militare Naționale de Comunicații în zona de est a țării.

Remarcabilele realizări ale unității dumneavoastră sunt cunoscute și recunoscute la nivelul eșaloanelor superioare. Admirabilele calități ce caracterizează personalul unității au constituit, fără îndoială, factorul determinant al realizărilor deosebite cu care vă prezentați astăzi la sărbătoarea unității.

Îmi exprim profunda considerație pentru frumoasele dumneavoastră tradiții istorice, precum și pentru remarcabilele realizări ale unității și doresc Centrului 115 Comunicații R.M.N.C. acum, la aniversarea celor 35 de ani de la înființare, mult succes în îndeplinirea misiunii de mare răspundere ce-i revine prin participarea la realizarea sistemului de comunicații și informatică la nivel strategic, operativ și tactic!

*Vă felicit cu prilejul aniversării a 35 de ani de la înființarea unității!*

*La mulți ani Centrului 115 Comunicații RMNC!*

*La mulți ani dumneavoastră tuturor și familiilor dumneavoastră!*

**COMANDANTUL COMANDAMENTULUI  
COMUNICAȚIILOR ȘI INFORMATICII**

**General de brigadă  
Radu-Marius POP**

## CENTRUL 48 COMUNICAȚII ȘI INFORMATICĂ STRATEGICE – 75 DE ANI DE ISTORIE ÎN SLUJBA ȚĂRII

*Plutonier adjutant principal Titi PIPOS*

*Centrul 48 Comunicații și Informatică Strategice*



La **10 ianuarie 2017** se împlinesc șaptezeci și cinci de ani de la înființarea **Centrului 48 Comunicații și Informatică Strategice**, sub denumirile sale

inițiale de *Regimentul 4 Transmisiuni*, *Regimentul 249 Transmisiuni*, respectiv *Regimentul 48 Transmisiuni*.

Aflându-ne în plin război, ca răspuns la nevoile armatei, la *10 ianuarie 1942* se înființează **Regimentul 4 Transmisiuni**. Astfel, având experiența celor trei regimente de transmisiuni existente, se înaintează mareșalului Antonescu, conducătorul statului la momentul respectiv, de către ministrul Apărării Naționale și șeful Marelui Stat Major, *Raportul nr. 18210* înregistrat în *14 ianuarie 1942*, cu propunerea de înființare a celui de-al patrulea regiment de transmisiuni, prin Decretul nr. 199 din 21 ianuarie consființându-se înființarea **Regimentului 4 Transmisiuni** în garnizoana Alexandria.

Sarcinile de înființare le primește Regimentul 1 Transmisiuni, care trimite un ofițer să inspecteze și să ia în primire cazărmile Al. Ghica și tabăra de barcamente germană „Victoria” din

Alexandria. În condiții de iarnă grea, Regimentul 1 Transmisiuni constituie un detașament pentru punerea în funcțiune a celor două cazărmi și primirea efectivelor noului regiment. Prin Ordinul Marelui Stat Major nr. 19230 din 30 ianuarie 1942 i-au fost transmise de la Regimentul 1 Transmisiuni subunitățile: Batalionul 11 Transmisiuni, Batalionul 54 Transmisiuni, Companiile 4, 23, 25 și 32 Transmisiuni, Plutoanele 62 și 64 Transmisiuni Etape și Coloana de Transmisiuni numărul 11 cu următoarele materiale: posturi radio, unul de tip B, două de tip C, șase de tip D, cincisprezece de tip F și opt de tip G, douăzeci și șase de receptoare R.S.1., douăzeci și două de motociclete B.M.W., un grup electrogen de 12 kW.

Primul comandant, colonelul Constantinescu Nicolae, după finalizarea în linii mari a înființării regimentului la ordinul Marelui Stat Major, este numit să îndeplinească funcția de comandant al Transmisiunilor Marelui Cartier General - Eșalonul înaintat, dispus la Rostov, pe Don. Pentru asigurarea conducerii acțiunilor militare în timpul celui de-al Doilea Război Mondial, mai precis în perioada 1942 - 1945, Regimentului 4 Transmisiuni i-au revenit în principal sarcini de mobilizare.

Acesta a concentrat, instruit și trimis pe front 16 unități și subunități de transmisiuni pentru asigurarea legăturilor la diferite eșaloane. La efectivele angajate pe front, de peste 2.500 de oameni, trebuie să adăugăm și efectivele părții sedentare,

dislocate în garnizoana Alexandria, aproximativ 1.000 de militari, care au făcut eforturi considerabile pentru pregătirea rezerviștilor, concomitent cu executarea unor misiuni de asigurare sau refacere a legăturilor în zona interioară, pentru aprovizionarea cu materiale și repararea tehnicii necesare completării pierderilor înregistrate de unitățile și subunitățile care luptau pe front. În cei trei ani și jumătate de campanie, pe ambele fronturi, din est și vest, transmisioniștii Regimentului 4 au înscris fapte nepieritoare de eroism și sacrificii, au fost distinși cu numeroase ordine și medalii românești și străine, au fost citați prin ordine de zi de către comandanții armatelor, corpurilor și diviziilor din care au făcut parte și, nu puțini dintre aceștia, au rămas pentru totdeauna pe câmpurile de luptă, departe de patrie, dându-și jertfa supremă pentru îndeplinirea misiunilor.

Prin pregătirea lor militară și profesională, prin spiritul de jertfă și sacrificiu, transmisioniștii regimentului – ofițeri, maiștri militari, subofițeri, sergenți, caporalii, soldați și civili – au contribuit la acoperirea de glorie a drapelului de luptă ale marilor unități române, sub care au luptat, de la trecerea Prutului și Nistrului, până la Odessa și Cotul Donului, de la eliberarea Capitalei, a sudului țării și Ardealului, la forțarea Mureșului, a Tisei, Hernadului, Hronului, Vahului și Moravei, la eliberarea Reghinului, Clujului, Oradei și Careiului, a Budapestei, Zvolenului și Banska Bistriței, până la cucerirea munților Bük, Hegyalja, Fatra Mare, Fatra Mică și masivului Javorina.

Caz unic în istoria armii transmisiuni, doi ofițeri din aceeași subunitate – Cp. 3 Trs. – au fost decorați (p.m.) cu cea mai înaltă distincție militară

de război – Ordinul „Mihai Viteazul” clasa a III-a, cu spade:

❖ Slt. Milea I. Mihai – „pentru curajul și spiritul de sacrificiu în luptele din Ardeal, la trecerea Tisei și în Cehoslovacia”;

❖ Slt. de rz. Olteanu P. Rizea – „pentru destoinicia și curajul excepțional de care a dat dovadă în realizarea și întreținerea legăturilor telefonice la trecerea Mureșului și Tisei”.

După încetarea războiului, drept recunoștință pentru sacrificiile făcute de militarii săi, **Regimentul 4 Transmisiuni** suferă un șir lung de șicane, mutări și transformări, desființare și iar mutare. În anul 1945 este evacuat din cazărțile pe care le deținea și dispus provizoriu în magaziiile Subdepozitului de Subzistență Alexandria, clădirea morii „Ganovici”, Școala primară nr. 1 și localitățile din apropierea orașului Alexandria, tot în același an, în luna decembrie, fiind dislocat în garnizoana Cluj, în cazărțile „Sf. Gheorghe” și „Principele Nicolae”.

La 01 iulie 1946, în baza Decretului - Lege nr. 1909 din 15.06.1946, Regimentul 4 Transmisiuni se desființează, arhiva, drapelul, gestiunile și o parte din efective fiind predate Regimentului 3 Transmisiuni Deva.

La 01 septembrie 1948, prin Ordinul M.St.M. nr. 45120 din 24.08 1948, se reînființează **Regimentul 4 Transmisiuni** în garnizoana Vaslui, cazarma „Peneș Curcanul”, dintr-un nucleu al Regimentului 2 Transmisiuni.

Prin Decizia nr. M.162 din 07.05.1951, Regimentului 4 Transmisiuni i-a fost acordat un nou Drapel de luptă. La 01 decembrie 1951, prin Ordinele M.St.M. nr. 00319530 și nr. 00319531 din

27.11 1951, se schimbă denumirea Regimentului 4 Transmisiuni în **Regimentul 249 Transmisiuni**. Prin Decretul nr. 350 din 18.08 1954, Regimentului 249 Transmisiuni i-a fost conferit **Ordinul „Steaua Republicii” clasa a IV-a**. În 22 octombrie, Regimentul 249 Transmisiuni este mutat din garnizoana Vaslui în **garnizoana București**, cazarma 1281, Șoseaua București - Măgurele nr. 33. La data de 23 februarie 1959, prin Ordinul M.St.M. nr. C.L.008 din 26.01.1959, Regimentul 249 Transmisiuni își schimbă denumirea în **Regimentul 48 Transmisiuni**.

În 01 aprilie 1964, Regimentul este redislocat în *garnizoana București, cazarma 1147, Șoseaua București - Ploiești km. 12,5* (ocupând până în prezent cazarma istorică - Fortul 3 Otopeni - a Regimentului 2 Pionieri Gardă). Mutarea s-a executat în cursul lunii aprilie 1964, astfel încheindu-se perioada de incertitudine de aproape 10 ani.

La data de 07 mai 1977, prin Decretul Prezidențial nr. 126 din 07.05 1977, Regimentului 48 Transmisiuni i-a fost conferit **Ordinul „Apărarea Patriei” clasa a III-a**. Din luna decembrie 1995, Regimentului i-a fost alocată și cazarma 3270 - Poligonul de tragere „Mogoșoaia” (Fortificațiile Bateriei 1-2 Mogoșoaia). La 27 mai 1996, prin Decretul Prezidențial nr. 141, s-a acordat noul Drapel de luptă Regimentului 48 Transmisiuni cu Brevetul nr. 19/1966 din 17.05 1996.

La 14 iulie 1999 s-a introdus în organizarea regimentului la pace Centrul de Transmisiuni cu Management Regional, transformat în C.T.N. cu management general de rezervă începând cu 01.12 2001.

La 10 ianuarie 2002, prin Decretul Prezidențial nr. 2 din 08.01.2002, Drapelul de luptă al Regi-

mentului 48 Transmisiuni a fost decorat cu **Ordinul Național „Pentru Merit” în grad de Cavaler**.

La 01 iulie 2005, regimentul a fost operaționalizat și a primit denumirea de **Centrul 48 Comunicații și Informatică Strategice**.

La data de 29 iunie 2007, prin Ordinul șefului Statului Major General nr. S.M.G. – 58 din 18.06.2007, Centrului 48 Comunicații și Informatică Strategice i s-a conferit **Emblema de Onoare a Comunicațiilor și Informaticii**.

La 01 octombrie 2008, a intrat în vigoare un **nou stat de organizare** al Centrului 48 Comunicații și Informatică Strategice. Principala diferență față de statul din 2007 a constat în proiectarea Batalionul Centre Comunicații Dislocabile ca structură ce urma a fi pregătită pentru dislocare în afara teritoriului național și includerea acesteia pe termen mediu în pachetul de forțe puse la dispoziția NATO.

În data de 30 septembrie 2009, se constituie **Modulul de comunicații dislocabil (DCM) la dispoziția NATO**. În 01 august 2010, a intrat în vigoare statul de organizare al Modulului NATO de Comunicații și Informatică Dislocabil DCM „E” în cazarma 1147 București, iar necesarul statului **Centrului 48 Comunicații și Informatică Strategice**, la pace, s-a redus. În perioada 2010 – 2012, Modulul NATO de Comunicații și Informatică Dislocabil DCM „E” a **parcurs programul de operaționalizare, iar în perioada 2012 – 2016** a participat la diferite exerciții NATO pe întreg continentul Europei, precum și la 2 misiuni în teatrul de operații AFGANISTAN, dislocând personal pentru a încadra posturile Echipei de Sprijin ISAF la Comandamentul ISAF și posturi

în Comandamentul întrunit ISAF cu durata de 6 luni fiecare, cât și la misiunea „ACTIVE FENCE“, Adana – Turcia. La data de 10 ianuarie 2012, drapelul de luptă al Centrului 48 Comunicații și Informatică Strategice a fost decorat cu **Emblema de Onoare a Statului Major General**.

La data de 14.07.2013, Centrul 48 Comunicații și Informatică Strategice a primit **Emblema de Onoare a Armatei României cu însemn de pace**. La 01 noiembrie 2015, a intrat în vigoare **actualul stat de organizare** al Centrului 48 Comunicații și Informatică Strategice. Principala diferență față de structura anterioară a Centrului 48 Comunicații și Informatică Strategice a constat în modificarea structurii unității în conformitate cu noile misiuni, precum și cu tehnica de comunicații și informatică nou intrată în dotare în cursul anului 2016.

În perioada 18.04. - 10.06.2016, în cazarma 1147 a Centrului 48 Comunicații și Informatică Strategice s-a desfășurat Exercițiul NATO de testare a interoperabilității capabilităților de comunicații „STEADFAST COBALT 2016”/SFCT 16. Exercițiul NATO SFCT 16 s-a desfășurat la nivel strategic, operativ și tactic, în mediu static și dislocabil, și a avut ca scop testarea și evaluarea

interoperabilității sistemului de comunicații și informatică, în sprijinul structurii de comandă și de forțe ale NATO, angajate într-o operație aliată majoră.

Exercițiul SFCT 16 a reprezentat cel mai important exercițiu NATO desfășurat vreodată în România în domeniul comunicațiilor și informaticii. La acesta au participat 12 națiuni NATO, 40 de unități specializate din structura de comandă și de forțe NATO implicate direct sau indirect și peste 1000 de militari NATO.

În ultimii ani, transformările au continuat într-un ritm susținut, tehnica căpătând un rol indispensabil în conducerea acțiunilor militare. În condițiile războiului modern, schimbul de informații depășește cu mult estimările făcute anterior; de aceea, subunitățile de comunicații și informatică trebuie să depună eforturi susținute pentru a-și menține pregătirea la un nivel competitiv. Închei prin a-mi exprima convingerea că militarii din cadrul unității, la ceas aniversar, se gândesc cu mândrie la înaintașii lor știuți și neștiuți, care s-au pregătit neconținut în poligoane, pe câmpurile de instrucție și s-au jertfit în bătălie, scriind cu litere de aur istoria **Centrului 48 Comunicații și Informatică Strategice**.

## CENTRUL 115 COMUNICAȚII RMNC BACĂU – REPERE ISTORICE LA CEAS DE SĂRBĂTOARE

***Mastru militar clasa I Ioan POPA***  
*Centrul 115 Comunicații RMNC*



Comunicațiile militare – cuvinte ca oricare altele, au implicații tot mai adânci și mai percutante în ansamblul de aspirații și nevoi ale societății în care ne-am născut și în care trăim, fără de care lumea modernă, lumea, așa cum o știm noi astăzi, nu ar avea sens – au, în mintea noastră, a celor care lucrăm efectiv cu electronii și cu biții, a celor care apărăm necondiționat și deliberat glia străbună, aceeași semnificație cu cea a aerului, curat de la munte, pe care îl respirăm cu nesaț când mergem în vacanțe.

Cu cât aerul este mai curat și mai tare, cu atât suntem mai performanți și mai energici, iar prin rezonanță, cu cât tehnologia este mai modernă și mai performantă, cu atât este mai sigură și mai limpede comunicarea înlăuntrul granițelor țării, țara din care ne hrănește părinții, fiicele și fiii, și față de care nu trebuie să precupețim niciun efort pentru a o apăra așa cum, cu deosebit respect, am jurat – toți!

Oriunde privim, oriunde mergem vedem acele minuni ale tehnologiei moderne, acele antene de comunicații, adevărate vârfuri de lance ale tehnicii, care ne demonstrează încă o dată,

dacă mai era nevoie, că omul, această ființă universală, indiferent în ce colț de lume trăiește, indiferent în ce limbă se exprimă, omul-profesor, omul-inginer, omul-orice ar fi, dar mai ales omul-militar nu mai poate concepe lumea, nu mai poate viețui fără acest adevărat sistem nervos ce reprezintă comunicațiile moderne.

Istoria telecomunicațiilor își are originea în secolul al XIX-lea odată cu descoperirea „telegrafului electric” care a fost, fără îndoială, cea mai mare descoperire de la inventarea prafului de pușcă, de către chinezi. Drept urmare, în anul 1873, prin înaltul decret din 14 iulie, se înființează prima secție de telegrafiști militari din Armata României.

Ca urmare a evoluției și necesităților tot mai mari de comunicare, arma transmisiunii se dezvoltă și, la 28 februarie 1982, în baza Ordinului General nr. 45 al ministrului apărării naționale, se înființează, în garnizoana Bacău, Batalionul 115 Transmisiuni, sub comanda cpt. (Trs.) Vasile RUSU, unitate subordonată Comandamentului Trupelor de Transmisiuni.

Erau vremuri de restriște, cu multe lipsuri și cu multe nevoi, însă cu multe așteptări din partea tuturor. O mână de oameni, adunați din toate colțurile țării, și-au pus umărul și mintea la treabă, pentru a face din nimic ceea ce este astăzi una din cele mai performante unități de comunicații și informatică.

În data de 2 iunie 1982, comanda a fost preluată de cpt. (Trs.) Gelu Ștefan PRICOPI, iar la data de 9 mai 1983 i s-a înmânat Batalionului 115 Transmisiuni, prin Decretul prezidențial nr. 110/15.04.1983, Drapelul de luptă.

La data de 14 iulie 1996 s-a înmânat Batalionului 115 Transmisiuni, prin Decretul prezidențial nr. 145/27.05.1996, actualul Drapel de luptă.

Începând cu data de 1 iulie 2001, comanda unității a fost preluată de lt. col. (Trs.) Liviu C-tin Pascal MUNTEANU.

Unitatea s-a operaționalizat începând cu data de 2 iulie 2002, primind denumirea de Centrul 115 Transmisiuni de sprijin prin Ordinul Statului Major General Nr. S/B.5/2860 din 17.06.2002, devenind astfel parte integrantă a structurilor moderne ale Armatei României.

Denumirea de Centrul 115 Comunicații R.M.N.C. a fost primită, prin Ordinul Statului Major General nr. B.5/S/205 din 30.01.2006, la data de 1 aprilie 2006.

La data de 28 februarie 2007 – cu ocazia celei de-a 25-a aniversări a înființării, unitatea a fost distinsă de șeful Statului Major General cu „Emblema de onoare a Comunicațiilor și Informaticii”, prima de acest gen oferită unei unități de comunicații din Armata României.

Trebuie amintit faptul că, în toată această perioadă, nu a fost neglijată nici latura spirituală a fenomenului militar; în luna septembrie 2007 a avut loc sfințirea bisericii militare „Sfântul Gheorghe și Eroii Neamului”, ridicată în incinta unității prin truda militarilor Centrului 115

Comunicații R.M.N.C. cu sprijiniul militarilor de toate armele din garnizoană.



Astfel, Armata și Biserica - aceste instituții care la noi, la românii, sunt pilonii de bază ai unității și continuității noastre pe aceste meleaguri - pot aduce, prin colaborarea lor, o contribuție decisivă la progresul moral și spiritual al societății românești.

La data de 31 mai 2010, comanda Centrului 115 Comunicații R.M.N.C. a fost preluată de dl. colonel (com.infm.) Dumitru DONICA, iar cu ocazia celei de-a 30-a aniversări a înființării unității, la data de 28 februarie 2012, unitatea a fost distinsă cu „Emblema de onoare a



Statului Major General”, în baza ordinului șefului Statului Major General nr. SPD-18 din 30.12.2011.

Pentru armată, transmisioniștii sunt „nervul central”, sunt cei care transmit ordinele și informațiile necesare conducerii activităților și



acțiunilor militare, de pregătirea lor de specialitate, de ordinea și disciplina autoimpuse, de caracterul lor depinzând în mare măsură și rezultatul acțiunilor pe câmpul de luptă. Folosirea eficientă și controlul organizării și funcționării sistemelor de comunicații și informatică reprezintă o importantă responsabilitate pentru aceștia, iar Centrul 115 Comunicații R.M.N.C. îndeplinește la cote înalte toate aceste cerințe.

În condițiile în care România este parte a Alianței Nord-Atlantice, realizarea unor legături de calitate, sigure și neîntrerupte între armatele diferitelor țări, ce desfășoară acțiuni militare comune, impune o standardizare și o compatibilitate strictă a tuturor elementelor ce se au în vedere la proiectarea, realizarea și exploatarea sistemelor de comunicații și informatică.

În zona istorică „Moldova”, această misiune este îndeplinită cu succes de Centrul 115 Comunicații R.M.N.C, care poate fi cu ușurință integrat în sistemul de comunicații și informatică al Alianței, personalul și tehnica îndeplinind toate standardele de interoperabilitate cu cele mai moderne armate din NATO.

Dacă la început se avea în vedere asigurarea legăturilor în fonie și telegrafie pe lângă marile unități, astăzi vorbim de transfer de date de mare viteză, pe sute de canale simultan, transmițeri video, satelitare și altele.

Ca urmare a integrării în alianța Nord-Atlantică, în Centrul 115 Comunicații R.M.N.C. s-au pus bazele instrucției de specialitate și a pregătirii la toate nivelurile după standarde NATO, formându-se specialiști în comunicații

militare de nivel internațional, specialiști de care Armata României are nevoie.

Misiunea primită de Centrul 115 Comunicații R.M.N.C. nu a fost deloc ușoară, în noua concepție revenindu-i acestuia sarcina de a înființa și exploata noi centre de comunicații deservite și nedeservite, în toată aria sa de responsabilitate.

Însă, cu multă muncă și inventivitate, s-a reușit punerea pe picioare a acestui sistem de care armata are atâta nevoie, sistemul S.T.A.R.-R.T.P./R.M.N.C.

O altă reușită deosebită o constituie realizarea, prin eforturi proprii, a sălii tradițiilor militare ale unității, sală care oferă ocazia de a cunoaște, în detaliu, aspecte mai puțin cunoscute despre armată, arma „Comunicații și Informatică” și, în special, Centrul 115 Comunicații R.M.N.C.



Sala tradițiilor militare este structurată pe informație științifică și pe un bogat patrimoniu, aici fiind prezentate înființarea și evoluția centrului, momentele importante din activitatea sa, precum și arme și tehnică de comunicații ce au fost folosite de-a lungul timpului.

Am intrat, astfel, în mileniul al treilea cu toată bogăția propriilor tradiții, tot mai cunoscute și apreciate în Europa și în alte părți ale lumii, dar

și cu o deschidere largă și binevoitoare către celelalte tradiții și culturi.

Analizând misiunile deosebit de importante și modul exemplar în care le execută, se poate vorbi despre Centrul 115 Comunicații R.M.N.C. ca despre o unitate de elită a Armatei României, o unitate care a demonstrat de-a lungul timpului că deține un portofoliu bine-definit în structura națională de apărare a țării.



### **Transmisionistul**

Cu ochii spre genune,  
Cu inima-i de leu,  
Mănunchi de raze ține ...  
În brațul de oțel.

Forjând prin biți și unde,  
Speranțe ... înălțând,  
Prin munții sfinți, ai țării ...  
Se-aruncă ... neînfricat.

E transmisionistul,  
Vorbind cu codrii mari,  
Și cu eroii, bravii ...  
Ce mușcă din dușmani.

Și lauri îi înalță,  
Armiei mari, de jderi,  
Iar în vrăjmași împlântă ...  
Și sufletul din el!

## LA MULȚI ANI, C48CIS!

**Locotenent Marius GÂREA**

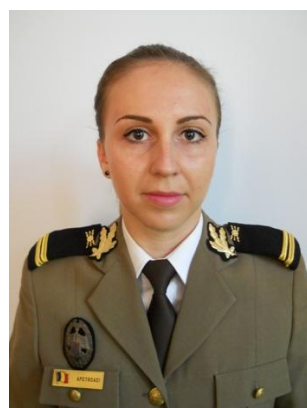
**Locotenent Adelina APETROAEI**

*Centrul 48 Comunicații și Informatică Strategică*



La 10 ianuarie 2017, Centrul 48 Comunicații și Informatică Strategică, aniversează 75 de ani de la înființare. O zi importantă care ne pune pe toți laolaltă, ast-

fel încât să putem face o retrospectivă asupra principalelor evenimente la care Centrul 48 Comunicații și Informatică Strategică a luat parte în ultimul an.



Este important de reamintit că ziua de 10 ianuarie este de mare însemnătate pentru militarii din arma comunicații și informatică, deoarece ea reprezintă un reper important în istoria militară: înființarea, prin Decretul numărul 199 din ianuarie 1942, a Regimentului 4 Transmisiuni.

Regimentul 4 Transmisiuni, acum Centrul 48 Comunicații și Informatică Strategică, a reprezentat o unitate de elită din Armata României, tradițiile acestei unități fiind păstrate și duse mai departe de un personal ce deține experiență și cunoștințe temeinice în domeniul de specialitate, pregătit să răspundă oricând provocărilor profesionale.

De-a lungul anilor, unitatea s-a distins printr-o participare excepțională la numeroase exerciții pe linie de comunicații și informatică atât la nivel național, cât și internațional, precum și în misiuni în teatrul de operații Afganistan, în cadrul cărora a asigurat legături și a oferit servicii (atât radio și radioreleu, cât și informatice) de cea mai bună calitate.

Gândindu-ne doar la anul ce se încheie în curând, putem spune că unitatea a avut parte de evenimente ce au condus la definirea acesteia ca și o unitate de elită în arma comunicații și informatică. Unul din aceste evenimente, a fost exercițiul „Steadfast Cobalt 2016”, un exercițiu multinațional ce a reprezentat o adevărată provocare. Unitatea noastră a avut calitate de gazdă pentru toate unitățile și structurile Alianței Nord-Atlantice participante. Acest exercițiu a avut ca principal obiectiv testarea, dar și evaluarea interoperabilității sistemelor de comunicații și informatică cu structurile celorlalte state membre NATO. La această activitate deosebit de importantă au avut prilejul să participe și militarii ai Centrului 48 Comunicații și Informatică Strategică, care ne-au reprezentat cu succes, cooperând foarte bine cu militarii străini, aceste aspecte fiind apreciate chiar de conducerea exercițiului. Totodată, aceste fapte fac dovada clară că militarii din arma comunicații și informatică se pregătesc în permanență la standardele de performanță impuse de NATO.

O altă activitate importantă la care Centrul 48 Comunicații și Informatică Strategică participă în fiecare an este exercițiul tehnic de specialitate „CETATEA”. Prin intermediul acestui exercițiu, militarii își perfecționează pregătirea în domeniul comunicații și informatică, sunt testate capacitățile tehnicii nou intrate în dotarea subunităților, iar statul major este antrenat să pună în aplicare procedurile naționale și NATO. Practic este exercițiul ce înglobează toată activitatea unității pe parcursul unui an și o certifică prin reușita acestuia. Anul acesta a fost unul mai special pentru că exercițiul

a presupus testarea unei serii întregi de echipamente nou intrate în dotare, iar personalul unității noastre a demonstrat încă odată că este capabil să se adapteze rapid noilor schimbări din domeniu.

Este foarte ușor de observat că această unitate a reușit și reușește în continuare să se dezvolte datorită calității umane pe care o posedă. Devotamentul, spiritul de echipă, priceperea și, nu în ultimul rând, disponibilitatea de care dau dovadă zi de zi militarii din cadrul acestei unități o fac să fie una dintre cele mai bune unități de comunicații din Armata României.



La mulți ani, C48CIS!

## IMPLEMENTAREA CONCEPTULUI FMN

*Colonel dr. Sorin-Silviu BĂLĂȘESCU*

*Locotenent Ilie IULIAN*

*Centrul 42 Comunicații și Informatică de Sprijin*



FMN (Federated Mission Networking) este un cadru conceptual reglementat (fig. 1), format din oameni, procese și tehnologii, creat pentru planificarea, pregătirea, stabilirea, utilizarea și realizarea *Rețelelor de Misiune* necesare eficientizării schimbului de informații pe timpul desfășurării operațiunilor de tip Joint.

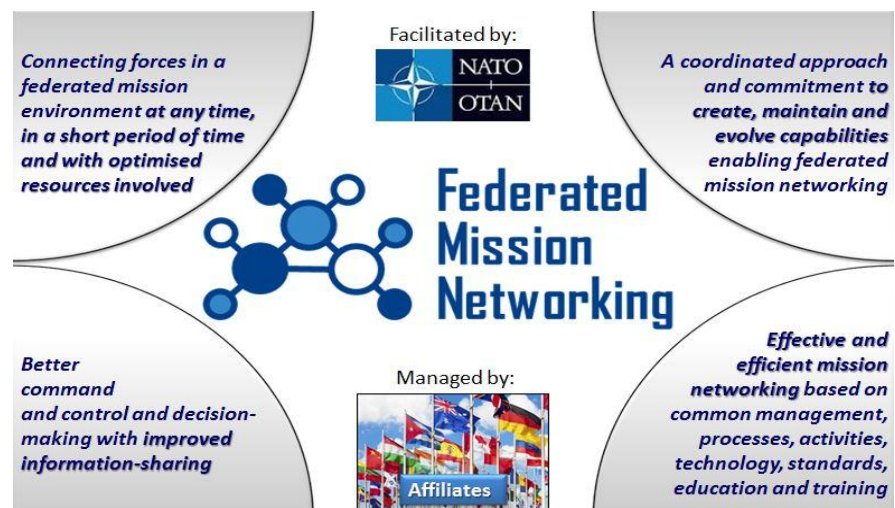


Fig. 1: Conceptul FMN

Coordonarea activității FMN este împărțită pe 2 niveluri (fig. 1): *nivelul de conducere* și *nivelul de management*. Primul nivel este reprezentat de *Comitetul Militar (MC)* care stabilește obiective, reglementează domeniul și asigură utilizarea responsabilă a resurselor. Cel de-al doilea nivel este responsabil cu transformarea obiectivelor stabilite în planuri și strategii, pe care le testează. Rezultatele obținute sunt transmise către nivelul de conducere pentru analiză.

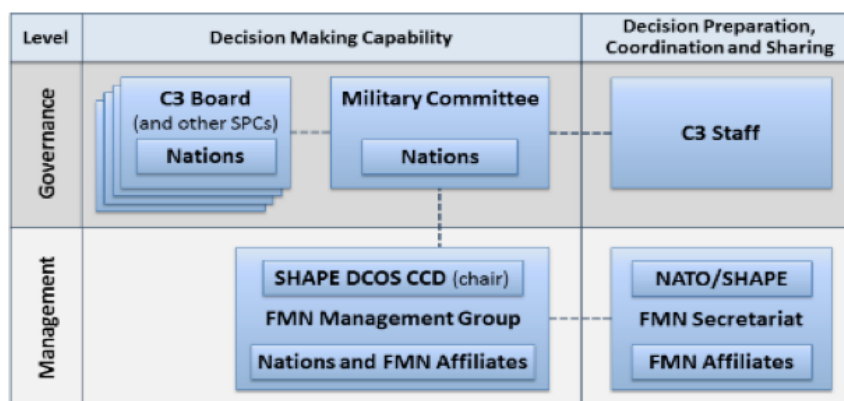
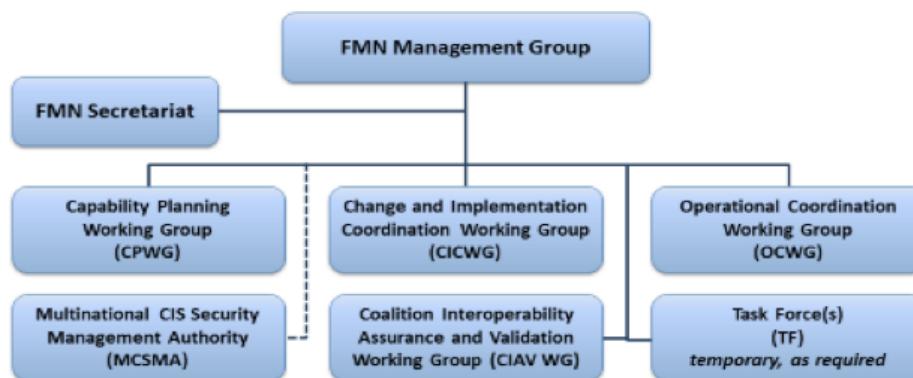


Fig. 2: Conducerea FMN

Pentru operativitate, grupurile de lucru constituite în cadrul nivelului de management (*fig. 2*) relaționează în mod direct cu structuri din cadrul NATO și din cadrul țărilor membre sau partenere.



*Fig. 3: Structura nivelului de management*

Conceptul FMN este primul de acest gen care oferă instrumentele și capacitățile necesare pentru pregătirea, dezvoltarea, dislocarea, operarea și dezvoltarea Rețelelor de Misiune. Acesta include patru procese majore:

- inițierea și integrarea conceptului FMN;
- conducerea și managementul capacităților FMN;
- instruirea continuă a forțelor implicate;
- dezvoltarea conceptului Rețea de Misiune.

Rețelele de misiune asigură una din capacitățile FMN, care include Sistemul de Comunicații și Informatică, procesele și procedurile create pentru o activitate (operațiune, exercițiu, antrenament sau testarea interoperabilității). Acestea se realizează folosind un set special de produse (politici, procese, proceduri și standarde) și materiale (rețele fixe și mobile, servicii, infrastructuri) puse la dispoziție de NATO și de țările membre sau partenere.

Evoluția competențelor FMN în general și a Rețelelor de Misiune în particular se bazează pe patru niveluri de capacități, astfel:

- *Element al Rețelei de Misiune (MNE)*: cuprinde echipamentele și infrastructura care asigură serviciile pentru structura deservită și serviciile esențiale pentru misiune;
- *Extensia Rețelei de Misiune (MNX)*: cuprinde echipamentele și infrastructura care asigură serviciile pentru structura deservită, dar nu oferă serviciile esențiale pentru misiune;
- *Hosted User*: este un participant la Rețeaua de Misiune care nu își poate asigura infrastructura și serviciile de care are nevoie;
- Alte entități care nu sunt parte integrantă a rețelei și nici nu sunt cuprinse în proiectele FMN.

Începând cu anul 2014, conceptul FMN a fost inclus pe agenda CWIX (Coalition Warrior Interoperability eXploration, eXperimentation, eXamination, eXercise) – comunitate care se întrunește anual la Byd-

goszcz, Polonia, pentru a testa și dezvolta interoperabilitatea sistemelor de comunicații și informatică ale țărilor participante (fig. 3).



Fig. 4: Arhitectura FMN testată în cadrul CWIX 2016

În ceea ce privește implicarea țării noastre, România face parte din conceptul FMN, iar dotarea cu echipamente în acest sens a început în cursul anului 2016, când au fost distribuite unităților din cadrul Comandamentului Comunicațiilor și Informaticii, în cadrul *Spiralei 1*, modulele IT care alcătuiesc *Rețeaua de Misiune* a României. În această etapă se urmărește asigurarea următoarelor servicii: legături de voce, videoconferință, web, e-mail și mesagerie. Pentru *Spirala 2* sunt planificate eficientizarea serviciilor din *Spirala 1* și asigurarea unor servicii suplimentare, cum ar fi: vizualizarea forțelor proprii și ale aliaților pe hartă în timp real, accesul la imagini maritime și la hărți actualizate ale reliefului, informații meteorologice și alte detalii, crearea unui spațiu virtual de lucru accesibil pentru utilizatorii rețelelor de misiune.

#### Bibliografie:

- [https://tide.act.nato.int/cwix/index.php/CWIX\\_2016\\_FMN\\_Focus\\_Area\\_Page;](https://tide.act.nato.int/cwix/index.php/CWIX_2016_FMN_Focus_Area_Page;)
- <http://www.act.nato.int/fmn;>
- <http://www.act.nato.int/federated-mission-networking-implementation-seminar;>
- [https://dnbl.ncia.nato.int/FMN/SitePages/Home.aspx.](https://dnbl.ncia.nato.int/FMN/SitePages/Home.aspx)

## REALIZĂRI ÎN ACTIVITATEA DE CERCETARE, DEZVOLTARE ȘI REGLEMENTĂRI ÎN ARMĂ

### *Colectivul de redacție*

*Centrul de Instruire pentru Comunicații și Informatică „Decebal”*

Centrul de Instruire pentru Comunicații și Informatică „Decebal” se înscrie cu succes în rândul instituțiilor de prestigiu ale învățământului militar, cu solide rădăcini în formarea cadrelor de elită ale armatei, prin aportul semnificativ adus la colectarea, producerea, prelucrarea, evaluarea, transmiterea și diseminarea de cunoștințe și repere valorice teoretice și, în principal, cu valențe practice și aplicative.

Obiectivul principal de aliniere a procesului de învățământ în armă la cerințele naționale și internaționale, precum și îmbunătățirea continuă a conținutului informațiilor transmise, reprezintă preocupări constante ale personalului instituției noastre. În acest context se înscriu și contribuțiile la dezvoltarea cunoașterii în domeniul armeei, rezultate din activitatea desfășurată de către Secția cercetare, dezvoltare și reglementări în armă/SCDRA. Specificul acestei activități vizează:

- elaborarea normativelor în armă și manualelor militare într-un cadru armonizat, corelat cu ansamblul celor în vigoare la nivelul armatei, cu tratatele internaționale la care România este parte și cu actele normative similare ale structurilor din cadrul celorlalte state membre NATO;

- realizarea unor produse în domeniul standardizării instrucției compatibile și interoperabile cu cele din Alianță;

- organizarea și desfășurarea, în cadrul unor colective mixte alături de cadre didactice și

cursanți, a cercetării științifice pentru perfecționarea și creșterea eficienței procesului de învățământ;

- participarea la activitățile de acceptare și implementare a documentelor de standardizare NATO/UE;

- valorificarea lecțiilor învățate prin identificarea soluțiilor de corecție necesare și perfecționarea activităților de educație și instruire a forțelor;

- elaborarea de propuneri de înzestrare a armeei cu noi tipuri de tehnică și pentru modernizarea unor sisteme existente în dotare.

Înființată în anul 2002, în statul de funcțiuni al Școlii de aplicație pentru transmisiuni, informatică și război electronic, structura specializată gestionării componentei de cercetare-dezvoltare, SCDRA, a contribuit la susținerea procesului de învățământ în armă prin elaborarea de cursuri și manuale specifice, în special în domeniile noi de specializare ale cursanților și elevilor:

- mijloacele tehnice moderne de comutație, multiplexare, secretizare și transmisie;

- rețele și echipamente radio cu salt de frecvență.

În acest sens poate fi menționată seria completă de instrucțiuni și manuale de operare privind echipamentele din compunerea centrelor de comunicații RTP/RMNC traduse, adaptate și



elaborate în cadrul secției, lucrări care se adresează personalului de serviciu din rețea, precum și personalului care se formează și specializează prin cursuri pentru funcțiile de operatori.

Necesitatea unor manuale militare moderne, compatibile cu cele ale NATO, a determinat începând cu anul 2004 demararea unui proces intens de elaborare a acestora. Prin această activitate extrem de importantă a secției și, implicit, a centrului de instruire, au fost elaborate: *Manualul pentru instrucția soldatului/gradatului transmisionist (2004)*, *Manualul centrelor de transmisiuni din RTP (2005)*, *manualele pentru luptă specifice eșaloanelor batalion, companie și pluton din Forțele Terestre (2005-2007)*, *Manualul instrucției soldatului/gradatului voluntar (2007)* și *manualele de instrucție pentru operatori la stațiile radio cu salt de frecvență VHF și HF (2007-2008)*. Un loc principal în realizările din această perioadă îl ocupă participarea colectivului de membri ai secției și specialiști din statul major al centrului la elaborarea *F.T.–10, Manualul sprijinului de comunicații și informatică în operațiile Forțelor Terestre*, statuându-se astfel cadrul normativ pentru planificarea, organizarea și desfășurarea acțiunilor de luptă ale structurilor de comunicații și informatică.



După revenirea firească a învățământului în armă în subordinea Comandamentului comunicațiilor și informaticii, s-a continuat cu elaborarea unor reglementări adaptate noilor misiuni și obiective: *CI-6.1, Manualul instrucției echipajului autostației radio Panther 2000*, *CI-6.2, Manualul instrucției echipajului autostației radioreleu numerice*, *CI-6.3, Manualul instrucției echipajului autostației radioreleu cu acces radio*, *CI-6.4, Manualul instrucției echipajului autostației de comunicație, multiplexare, supervizare și secretizare*, *CI-6.5, Manualul instrucției echipajului autostației de videoteleconferință*, precum și două acte normative specifice, promovate prin dispoziții ale șefului Statului Major General: *CI-7.1, Proceduri de operare în comunicațiile radio-telefonice militare și Glosar cu termeni și definiții din domeniul comunicațiilor*. Nu în ultimul rând, în cadrul secției s-au elaborat *Programe de Instrucție pentru Misiuni/Individuale* pe categorii de tehnică și tipuri de structuri subordonate CCI și SMFT, urmărind adaptarea instrucției la specificul misiunilor pe care le pot îndeplini și la particularitățile operațiilor în care acționează.

În conținutul tuturor acestor reglementări se regăsesc implementate specificațiile standardelor operaționale, procedurale și tehnice elaborate de NATO și UE (STANAG, MIL-STD, EUROCOM) care reglementează problematica proiectării, realizării, organizării și exploatării sistemelor de comunicații și informatice. De asemenea, s-au implementat prevederi ale unor publicații și proceduri de lucru NATO, asigurându-se astfel interoperabilitatea acțională cu structurile similare din celelalte armate din Alianță. Procedurile

de lucru au fost adaptate – când a fost cazul – la specificul înzestrării armei noastre și asigură deplină concordanță cu manualele structurilor celorlalte arme.

Un rol important îi revine secției în organizarea și conducerea activităților de analiză și formulare a recomandărilor către eșaloanele abilitate privind acceptarea standardelor. Centrul de instruire colaborează cu alte structuri din armă cu responsabilități în domeniul standardizării. Astfel, prin desfășurarea unei ample activități de traducere și adaptare, în cadrul secției s-a constituit și se administrează o importantă bază de date cu standarde militare de comunicații și informatică, publicații NATO, precum și alte documente specifice. Documentele de standardizare implementate contribuie la atingerea nivelurilor de interoperabilitate necesare domeniului comunicațiilor și informaticii pe timpul participării structurilor puse la dispoziția NATO la operațiile întrunite în cadrul forțelor multinaționale prin realizarea următoarelor obiective: instruirea personalului în conformitate cu seturile de proceduri tehnice care asigură capacitatea sistemelor de a se interfața și a se interconecta în cadrul rețelelor ce deservește operații la care participă forțe aliate; utilizarea procedurilor, definițiilor, terminologiei și frazeologiei standard în exploatarea tehnicii; însușirea termenilor și definițiilor care fac parte din fondul terminologic standardizat pe plan mondial.

Totodată, abordarea unor teme de cercetare științifică de actualitate, în pas cu cerințele noi, mereu crescânde, ale evoluției armei comunicații și informatică, s-a concretizat în valorificarea rezultatelor în procesul de elaborare a reglementărilor,

de perfecționare a desfășurării învățământului militar și în comunicări științifice prezentate în Consiliul Științific al SMFT sau sesiuni organizate de instituțiile de învățământ militar. De menționat, în acest context, sunt și contractele încheiate cu Ministerul Educației și Cercetării, atribuite pe bază de competiție națională, cuprinse în programele de grant-uri pentru cercetare științifică din perioada 2004-2007. Fondurile alocate pentru finalizarea contractelor au fost utilizate pentru dezvoltarea bazei materiale proprii pentru cercetare și activități didactice, remunerarea personalului din colectivele de cercetare, participarea la manifestări științifice naționale și internaționale, editarea de lucrări de specialitate, manuale etc. Pentru perfecționarea activității, la nivelul centrului s-a constituit o comisie de cercetare științifică. Pe baza Planului anual de cercetare-dezvoltare, comisia se întrunește în ședințe unde sunt discutate temele realizate și sunt elaborate recomandări de valorificare a acestora.

O altă componentă a activității din cadrul SCDRA este cea a dezvoltării armei, ea reprezentând în perioada 2005-2009 un domeniu fundamental de lucru. În cadrul secției s-au elaborat documentații și puncte de vedere privind proiecția armei în viitor, în raport cu evoluția fenomenului militar. Participarea în cadrul grupurilor de lucru, alături de specialiști din Direcția Comunicații și Informatică, structura G6 a Statului Major al Forțelor Terestre și Agenția de Cercetare pentru Tehnică și Tehnologii Militare, a avut ca rezultat proiectarea și planificarea documentelor fundamentale ale programelor majore de înzestrare – documentele cu nevoile misiunii și documentele cu ce-

rințele operaționale. În componerea echipelor de elaborare a documentației pentru specificațiile de sistem ale programelor punctelor de comandă de divizie/brigadă/batalion din Forțele Terestre, s-au regăsit și foști sau actuali membri ai secției.

Principalele aspecte ale dezvoltării armei s-au concretizat prin lucrări prezentate în cadrul conferințelor doctrinare și prin articole publicate în Revista Comunicațiilor și Informaticii, care este redactată bianual, începând cu anul 2003, de către un colectiv constituit în cadrul SCDRA, și continuatoare a Buletinului Transmisiunilor.



În toată activitatea desfășurată a fost fructificată experiența materializată prin lecții învățate a participanților din centrul de instruire la exercițiile tehnice interne, misiunile din teatrele de operații și la edițiile anuale ale exercițiului tehnic cu participare internațională pentru testarea interoperabilității CIS ale națiunilor membre NATO și PfP „Combined Endeavor”. Experiența acumulată și lecțiile învățate din domeniul comunicațiilor și informaticii sunt valorificate în procesul de învățământ la nivelul centrului de instruire și al batalionului de instrucție, prin implementarea acestora în manuale și programe de instrucție, în documente de conducere, planificare și organizare.

Realizările și implicarea personalului militar și civil al SCDRA în multitudinea de domenii

de responsabilitate demonstrează deschiderea și disponibilitatea acestuia pentru activitățile viitoare. Direcțiile de acțiune pentru perfecționare și eficientizare constau în:

- creșterea calității învățământului, instrucției și educației în cadrul armei comunicații și informatică;
- dezvoltarea relației de colaborare cu mediile implicate în cercetarea științifică și în producerea de tehnică specifică domeniului armei;
- continuarea elaborării manualelor necesare pregătirii și întrebuințării unităților și subunităților de comunicații și informatică;
- actualizarea în vederea reeditării a manualelor deja elaborate, având în vedere caracterul „provizoriu” al acestora (în conformitate cu reglementările NATO, în etapa actuală, „viața” unui manual este mai scurtă, de numai 3-4 ani, față de 10-15 ani cum eram obișnuiți anterior);
- redactarea și editarea în continuare a revistei armei.



– Toate aceste aspecte pun în evidență faptul că activitatea de cercetare, dezvoltare și reglementări în armă constituie un proces complex. Ea este necesară datorită beneficiilor pe care le aduce armei comunicații și informatică pe termen scurt, mediu și lung.

## SERVICIUL DE RECUPERARE ÎN CAZ DE DEZASTRE DISASTER RECOVERY AS A SERVICE (DRaaS)

*Locotenent colonel Cătălin CÎRNU  
Centrul 115 Comunicații RMNC*

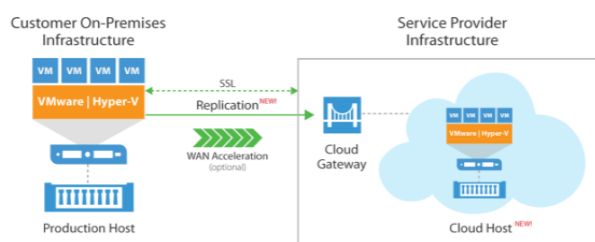


Trăim în era informației, vitezele de calcul depășesc limitele de înțelegere umană, iar capacitățile de stocare și prelucrare a datelor sunt impresionante chiar

și pentru un utilizator casnic. Cu toate că hard discurile zac prin sertarele casei care mai de care plin de Tera și Giga .... oare ne-am gândit vreodată cât poate fi garantată investiția în diversele formate oferite de soluțiile digitale. Ridicând puțin miza, mergem la nivelul unei instituții, mai apoi a unei corporații și vom vedea că valoarea datelor se ridică și pierderea acestora poate duce chiar la blocarea activităților acesteia. Unele date publicate de Disaster Recovery Journal arată că doar 15% din companiile globale au un DRP (Disaster Recovery Plan) complet operațional și un procent de 43% din companiile afectate de un dezastru nu s-au mai deschis, iar 29% și-au întrerupt activitatea în următorii doi ani.

Ultimii ani au deschis o nouă piață în domeniul recuperării datelor după evenimente nedorite și se vehiculează din ce în ce mai des termenul de *Disaster Recovery as a Service (DRaaS)*, în câteva cuvinte fiind vorba despre capabilitatea

oferită de un terț de a asigura continuarea activităților, recuperarea datelor și repornirea aplicațiilor critice specifice unei organizații într-un timp foarte scurt. Soluțiile se referă atât la companii care preferă un provider extern, cât și la instituții sau companii care doresc menținerea controlului fizic asupra rețelelor.



Potrivit companiei americane de consultanță IT Gartner, industria *DRaaS* a avut o creștere rapidă începând cu 2012, estimată la 1,3 miliarde dolari, cu o creștere anuală de aproximativ 30%. Printre principalii ofertanți pe piața mondială de soluții *DRaaS* se numără *Bluelock*, *IBM Cloud Services*, *Sungard Availability Services*, *Acronis Disaster Recovery Service*. Produsele lor oferă posibilitatea recuperării datelor vulnerabile pe mai multe niveluri, în medii de configurare mixte, cu mașini fizice și virtuale cu cerințe complexe de securitate.

Cvadrantul magic, cum este numit de cei de la Gartner, în soluții *DRaaS* a fost actualizat în 2016 și, pe baza criteriilor de evaluare a companiilor ofertante, au fost poziționate în una dintre secțiunile afișate în imagine.



*Cloud Failover Appliance (CFA)* este soluția oferită de cei de la Infrascale și aduce un iz de noutate și inovație prin îmbinarea tehnicilor DR cu tehnologia cloud, cu un accent deosebit pe viteza de restabilire a sistemelor și asigurarea protecției și integrității datelor pe servere fizice și virtuale cu diferite sisteme de operare.



Iată câțiva pași care trebuie urmați pentru construirea unui DRP viabil în viziunea specialiștilor de la Bluelock

**Evaluarea bugetului** – află cât ești capabil să cheltui pe toate aplicațiile și stabilește care abordare a costurilor corespunde scopurilor tale.

**Enumerarea aplicațiilor** – stabilirea locului fiecărei aplicații și gruparea acestora pe niveluri de importanță.

#### Bibliografie:

<https://www.gartner.com>

<http://www.itbusinessedge.com/>

**Efectuarea analizei riscurilor și evaluarea impactului pentru fiecare aplicație** – estimarea timpului cât pot funcționa activitățile instituției fără fiecare aplicație și stabilirea cantității datelor pierdute în cel mai rău scenariu.

**Stabilirea RTO (Recovery time objective) și RPO (recovery Point Objective)** – corelarea bugetului alocat cu cantitățile de date ce se doresc recuperate și încadrarea acestora într-un anumit interval de timp.

**Stabilirea destinației de recuperare** – funcție de poziționarea centrelor de date și importanța fiecărei aplicații se stabilesc pozițiile geografice ale locațiilor favorabile.

**Revederea nevoilor de securitate pentru protejarea datelor vulnerabile** – stabilirea capacităților tehnologice necesare pentru protejarea datelor senzitive.

**Elaborarea procedurii pentru continuarea activităților** – aranjarea procesului de recuperare, pas cu pas, pentru a documenta cât mai bine toate activitățile ce se vor desfășura și păstrarea acestora în zonele specifice de lucru.

**Stabilirea unui program de testare** – se vor efectua periodic teste de recuperare pentru verificarea funcționalității planului.

Asigurarea serviciilor de recuperare în caz de dezastre poate fi o provocare bună și o oportunitate de a spori importanța unităților noastre în arhitectura sistemului de apărare și poate de a crește nivelul de interes în rândul proaspeților absolvenți ai instituțiilor de învățământ prin implicarea acestora în lucrul cu tehnologii de actualitate.

<https://www.infrascale.com/>

<http://go.bluelock.com/>

## REȚELE DIGITALE SDH

*Căpitan Cristian GAFENCU*  
*Centrul 115 Comunicații RMNC*



Legătura dintre echipamentele militare de comunicații existente în Sistemul Național de Apărare și tehnologiile moderne de transport a semnalelor este una cât se poate de strânsă, având în vedere necesitatea armonizării facilităților oferite de infrastructura de transport RTP la ora actuală cu echipamentele periferice existente. Viitorul preconizează integrarea tuturor rețelelor specializate într-o singură rețea, care va permite transmiterea tuturor tipurilor de informații, indiferent de viteză, lățimea de bandă și serviciile oferite, fiind, de asemenea, posibilă și apariția de noi servicii în acord cu cerințele utilizatorilor.

Pentru a face față cererii din ce în ce mai mari de lățime de bandă de către aplicațiile software și tehnologiile de comunicații, a fost dezvoltată o ierarhie multiplex, numită ierarhia digitală plesiocronă (PDH). Gama de debite pentru Europa începe cu 2 Mbit/s, cât are multiplexul primar, și continuă cu multiplexurile de ordin mai înalt: 8, 34 și 140 Mbit/s. În America de Nord și Japonia, multiplexul primar este de 1,5 Mbit/s. Treptele ierarhice următoare sunt de 6 și 44 Mbit/s. Datorită acestor dezvoltări foarte diferite, legăturile din-

tre rețelele celor două ierarhii au fost foarte dificile și costisitor de realizat.

Spre sfârșitul anilor 1980, a fost propusă (de Bellcore în 1985) ierarhia digitală sincronă (SONET) devenită SDH după adoptarea și standardizarea sa de către ITU-T în 1988. Aceasta a deschis drumul spre o structură unificată de rețea la scară mondială, rezultând un management mai economic și mai eficient pentru operatorii de rețea. Rețelele pot fi ușor adaptate pentru a satisface cererea din ce în ce mai mare de lățime de bandă.

SDH oferă următoarele avantaje operatorilor de rețea:

### **1. Rate mari de transmisie**

Sistemele moderne SDH (Synchronous Digital Hierarchy) pot atinge rate de transmisie de până la 40 Gbit/s. SDH este, din acest motiv, cea mai potrivită tehnologie pentru realizarea magistrelor de mare viteză.

### **2. Funcție de inserare și extragere simplificată**

În comparație cu sistemele PDH, în SDH sunt mult mai ușoare operațiile de extragere și inserare de afluenți cu debit scăzut din sau în fluxurile de mare viteză. Nu mai este necesară demultiplexarea și apoi remultiplexarea structurii plesiocrone, o procedură complexă și costisitoare.

### **3. Bandă la cerere; capacitatea rețelei se alocă dinamic**

Cu SDH, operatorii de rețea pot reacționa rapid și ușor la cerințele clienților. Spre exemplu,

liniile închiriate pot fi schimbate în câteva minute. Operatorul de rețea poate folosi elemente de rețea standardizate, care pot fi controlate și monitorizate de la o locație centrală printr-un sistem de management al rețelei de telecomunicații.

#### 4. Fiabilitate

Rețelele moderne SDH conțin diverse mecanisme automate de rezervă și reparare pentru a face față deranjamentelor din sistem. Căderea unei legături sau a unui element de rețea nu conduce la căderea întregii rețele, ceea ce poate fi un dezastru din punct de vedere operațional pentru operatorul rețelei. Aceste circuite de rezervă sunt, la rândul lor, monitorizate de un sistem de management.

#### 5. Platformă deschisă pentru serviciile ce vor apărea în viitor

În acest moment, SDH este platforma ideală pentru servicii începând cu PSTN (Public Switched Telephone Network), ISDN (Integrated Services Digital Network) până la comunicații de date (LAN, WAN etc.) și este capabil să acomodeze și cele mai noi servicii, cum ar fi difuzare video digitală via ATM (Asynchronous Transfer Mode), care devin din ce în ce mai populare.

#### 6. Interconectarea

SDH face mult mai ușoară realizarea de conexiuni între diferiți operatori de rețea și către sistemele SONET (Synchronous Optical Network). Interfețele SDH sunt standardizate global, făcând posibilă combinarea elementelor de rețea de la producători diferiți într-o rețea. Rezultatul este o reducere a costului echipamentelor în comparație cu PDH.

Tendința este evidentă înspre oferirea de rate de bit din ce în ce mai mari, cum ar fi STM-

64 (10 Gb/s) și STM-256 (40 Gb/s). Dificultățile tehnologice și costurile foarte ridicate sunt factori care întârzie introducerea acestor sisteme.

#### Componentele unei rețele sincrone

Rețelele SDH curente sunt, în general, alcătuite din patru tipuri diferite de elemente de rețea. Topologia (inel sau plasă) este dată de cerințele operatorului de rețea.

##### 1. Regeneratoare

Regeneratoarele, după cum le spune și numele, au rolul de a regenera ceasul și forma semnalului de la intrare, care a fost atenuat și distorsionat de dispersie. Acestea își extrag semnalele de ceas din fluxul de date de la intrare. Mesajele sunt recepționate extrăgând diverse canale de 64 kbit/s (de exemplu canalele de serviciu E1 și F1) din RSOH (overhead-ul secțiunii de regenerare). Mesajele pot fi emise folosind tot aceste canale.

##### 2. Multiplexoare terminale

Acestea sunt folosite pentru a combina semnale de intrare plesiocrone și sincrone în semnale STM-N, cu rate de bit mai înalte.

##### 3. Multiplexor cu inserție/extragere (ADM)

Semnalele plesiocrone și cele sincrone cu debite mai mici pot fi extrase din sau inserate în fluxuri SDH de mare viteză folosind ADM-uri. Această caracteristică permite formarea de structuri în inel, care au avantajul unei siguranțe sporite prin comutarea căilor de rezerva în cadrul inelului în cazul unor defecțiuni.

##### 4. Rețea digitală de interconectare (DXC)

Acest element de rețea are cea mai largă varietate de funcții. Permite maparea (asamblarea)

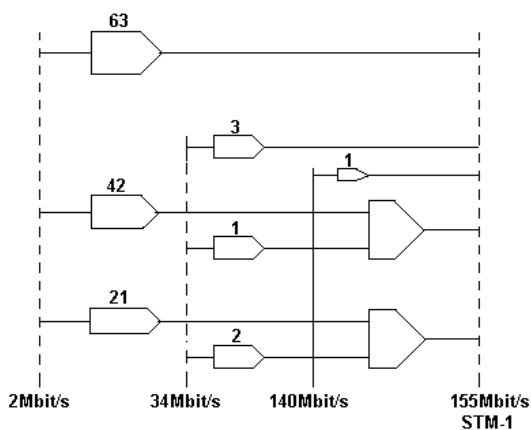
semnalelor tributare PDH în containere virtuale, dar și comutația diverselor containere până la VC-4, inclusiv.

### Unitatea de transmisie elementară

Unitatea elementară de încadrare pentru SDH este STM-1 (Synchronous Transport Module level 1), ce operează la 155,52 Mbps.

Cadrul STM-1 se compune din cadre PDH:

- 63 semnale la 2 Mbit/sec, sau
- 3 semnale la 34 Mbit/sec, sau
- 1 semnal la 140 Mbit/sec, sau
- 42 semnale la 2 Mbit/sec și 1 semnal la 34 Mbit/sec, sau
- 21 semnale la 2 Mbit/sec și 2 semnale la 34 Mbit/sec.



Câteva cadre STM-1 pot fi multiplexate împreună:

- 4 cadre STM-1 = 1 STM - 4 cadre (622 Mbit/s)
- 16 cadre STM-1 = 1 STM - 16 cadre (2,5 Gbit/s)

Cu toate acestea, echipamentul PDH poate fi înlocuit cu ușurință de echipamentul SDH. În plus, ultimul permite o operare mai ușoară și un

management facil în folosirea biților supraîncăcați în cadrul SDH.

### **Transportul semnalelor PDH și ATM folosind SDH**

Natura diversă a rețelelor moderne de telecomunicații a făcut necesar ca toate semnalele PDH și ATM să fie transportate folosind rețeaua SDH. Procesul adaptării diverselor semnale la caracteristicile de transport ale rețelei se numește mapare. Unitatea de bază pentru transportarea semnalelor tributare este containerul.

Pentru fiecare semnal tributar PDH avem la dispoziție câte un container special (C-i).

Aceste containere sunt totdeauna mai mari decât încărcătura care se cere transportată. Capacitatea rămasă liberă este folosită parțial pentru dopare datorită nevoii de egalizare a inacurateții temporale din semnalele PDH. Un container virtual (VC-i) este compus din container și din overhead-ul căii (POH). Acesta este transmis neschimbat pe o cale din interiorul rețelei. Următorul pas spre crearea unui semnal complet STM-N este adăugarea unui pointer ce indică startul POH-ului. Unitatea formată din pointer și containerul virtual se numește unitate administrativă (AU-i) sau unitate tributară (TU-i).

Mai multe TU luate împreună formează un grup de unități tributare (TUG-i). Una sau mai multe AU formează un grup de unități administrative (AUG). În final, un AUG plus overhead-ul secțiunii formează STM-N-ul.

### **Transportul unui semnal E1 într-un STM-1**

Structura de transport SDH destinată transportului semnalului E1 este VC12. Acesta



rezultă prin maparea unor semnale E1 în C12 și adăugarea overhead-ului de cale de ordin inferior POH-VC12. Containerelor VC12 sunt apoi multiplexate în containere de ordin superior VC4, care sunt apoi introduse în module STM-1. Orice container VC12 poate fi inserat/extras în fiecare element de rețea în/din modulele de transport STM-1, dar, ca și în cazurile precedente, el nu va fi dez-asamblat decât în nodul terminator al căii, care va asigura și interfața cu rețeaua PDH.

### **SONET/SDH-ul generației viitoare**

Dezvoltarea SONET/SDH a fost inițial împinsă de necesitatea transportului a multiple semnale PDH, precum DS1, E1, DS3 și E3, împreună cu alte grupuri de trafic de voce de 64 kbps *pulse-code modulated* (PCM), multiplexate. De la început, posibilitatea de a transporta trafic ATM a motivat încă o aplicație. Pentru a susține lărgimi de bandă ATM mari, s-a dezvoltat tehnica de concatenare, prin care containere mai mici de multiplexare (de exemplu STS-1) sunt *invers multiplexate* (*inversely multiplexed*) pentru a forma containere mai mari (de exemplu STS-3c), cu scopul de a susține traficul masiv de date.

O problemă a concatenării tradiționale este inflexibilitatea. În funcție de amestecul de date și voce ce trebuie purtat, poate exista o cantitate mare de bandă nefolosită, din cauza dimensiunilor fixe ale containerelor concatenate. Spre exemplu, potrivirea unei conexiuni de 100 Mbps Fast

Ethernet într-un container de 155 Mbps STS-3c duce la risipe considerabile. Mai importantă este necesitatea ca toate echipamentele de rețea intermediare să susțină mărimile de concatenare nou introduse. Această problemă a fost mai târziu depășită cu introducerea concatenării virtuale (VC – Virtual Concatenation).

Concatenarea virtuală (VCAT) permite o asamblare arbitrară a containerelor multiplexoare de ordin mai mic, construind containerele mai mari cu dimensiuni suficient de puțin constrânse (de exemplu de 100 Mbps) fără a necesita echipamente de rețea intermediare care să susțină această formă specifică de concatenare. Concatenarea virtuală folosește progresiv protocoalele Generic Frame Procedure (GFP) sau X.86 pentru a mapa payload-urile cu lățime de bandă arbitrară în containerul concatenat virtual.

Link Capacity Adjustment Scheme (LCAS) permite schimbarea dinamică a lățimii de bandă prin concatenare virtuală dinamică, multiplexând containerele pe baza necesităților de termen scurt din rețea.

**În concluzie**, tehnologia SDH se va impune în domeniul comunicațiilor digitale de bandă largă într-o configurație mixtă, păstrând investițiile și permițând o introducere graduală. Astfel, noua tehnologie va îmbunătăți protocoalele standard și serviciile implementate.

### **Bibliografie:**

- [1] Eugen Borcoci, „Sisteme de comunicatii digitale”, Editura Vega, Bucuresti, 1994
- [2] William Stallins, „Data & computer communications”, Editura Macmillan Publishing Company, New York
- [3] Raif Onvural, „Asynchronous Transfer Mode Networks “, Artech House, Londra

## SEMNĂTURA ELECTRONICĂ

*Căpitan Dorin-Horia ILIEȘ*  
*Centrul 54 Comunicații RMNC*



Cu toate că reglementarea semnăturii electronice [1], inclusiv a regimului juridic al înscrisurilor în format electronic, are deja o vechime de 15 ani în România, constatăm faptul că acestea sunt utilizate foarte puțin deopotrivă în sistemul public, cât și în cel privat, ignorându-se beneficiile extraordinare pe care le aduc proceselor organizaționale. Eliminarea activităților cu consumuri nervoase, de timp și financiare asociate managementului documentelor tipărite (printare, transmitere, îndosariere, depozitare, recuperare, distrugere) sau rapiditatea transmiterii informațiilor intra- și interorganizaționale sunt doar două beneficii evidente pe care utilizarea înscrisurilor în format electronic, împreună cu certificarea asigurată de semnătura electronică, le aduc organizațiilor, inclusiv celor militare. Printre domeniile care au acceptat și utilizează în mod uzual semnătura electronică se remarcă cel financiar-bancar, energetic și marile corporații internaționale prezente în România [2].

Constatarea existenței unei rețineri în utilizarea acestor instrumente, rețineri cauzate în bună măsură de necunoașterea (neînțelegerea) mecanismelor specifice, precum și convingerea că ex-

tinderea utilizării semnăturii electronice în organizația militară poate aduce beneficii nu doar materiale m-au făcut să abordez în acest articol câteva elemente generale referitoare la mecanismele semnăturii electronice și a certificatului digital. Obiectivul articolului este de a contribui la o mai bună cunoaștere (înțelegere) a problematicii. Abordarea articolului este una generală, constrâns fiind de spațiul și caracteristicile unei reviste, dar consider că reprezintă un bun punct de plecare spre aprofundarea noțiunilor specifice.

Societatea umană a început să transfere pe rețelele de calculatoare o parte din activitățile obișnuite, cărora comunicațiile aproape instantanee între puncte situate geografic la mii de kilometri le conferă valențe superioare. Vorbim astăzi de transferul electronic al documentelor, teleconferințe și grupuri de lucru prin rețele de calculatoare, grupuri de discuții, ca niște veritabile cluburi, profilate pe cele mai variate domenii de interes, ziare distribuite prin rețele, sisteme electronice de plăți prin rețele, sisteme de transfer de fonduri și de comerț prin rețele și altele. Toate aceste servicii au început să fie o realitate a celui mai mare și mai impresionant mediu de comunicații între oameni, reprezentat de rețelele de calculatoare, iar dintre acestea internetul, o lume *în egală măsură bazar și agora, lume totală sau cocon secret, spațiu fără limite și constelație de celule independente, internetul poate face posibilă coabitarea între negustori și militanți, consumatori și*

*cetățeni, mari organizații și eremiți, potrivit unor configurații mobile și logici deseori contradictorii ce pot afecta înseși principiile funcționării sale: valorile fundamentale ce definesc colectivitatea umană, frontieră între spațiul public și spațiul privat, natura apartenenței la o comunitate sau teritoriu [3].*

Nevoia de securitate și de autenticitate apare la toate nivelurile arhitecturale ale rețelelor. La nivel înalt, utilizatorii vor să se asigure, spre exemplu, că poșta electronică sosește chiar de la persoana care pretinde a fi expeditorul. Uneori, utilizatorii, mai ales când acționează în numele unor organizații, doresc asigurarea caracterului confidențial al mesajelor transmise. În tranzacțiile financiare, alături de autenticitate și confidențialitate, un loc de mare importanță are și integritatea mesajelor, ceea ce înseamnă că mesajul recepționat nu a fost alterat în timpul tranziției prin rețea [4]. În fluxurile organizației poate fi foarte important ca, odată recepționată o comunicare, aceasta să fie nu numai autentică, cu conținut nemodificat, dar să nu existe posibilitatea ca expeditorul să nu o mai recunoască, adică să se respecte proprietatea de nerepudiere.

O semnătură electronică reprezintă o informație care îl identifică pe expeditorul unui document. Semnatura digitală este creată prin criptarea conținutului documentului, folosind cheia criptografică a expeditorului. Aceasta face ca semnatura să fie unică atât pentru fișier, cât și pentru deținătorul cheii. Orice modificări aduse documentului afectează semnatura, oferindu-se astfel atât integritate, cât și autentificare.

Semnăturile electronice reprezintă echivalentul electronic al semnăturilor de mână, acest concept fiind introdus ca funcționalitate adițională a criptosistemelor cu cheie publică de către Diffie și Hellman în 1976 [5], în absența unei scheme criptografice pentru acest scop. Obiectivul principal de securitate pe care îl asigură semnăturile digitale îl reprezintă nonrepudierea, și anume faptul că o entitate, odată ce a semnat o informație, nu poate nega că a emis acea informație și orice altă entitate neutră poate verifica acest lucru. Semnăturile electronice reprezintă deci o valoare numerică care leagă conținutul unui mesaj de identitatea unei entități. În principiu, orice algoritm asimetric poate fi utilizat pentru crearea unei semnături digitale prin inversarea rolului cheii publice cu al celei private, iar primele propuneri de semnături digitale se găsesc în lucrările lui Rivest, Rabin și ElGamal [6]. Subliniem că și folosind algoritmi simetrici se pot crea semnături digitale de tip one-time, dar acestea sunt rar utilizate în practică.

O semnătură electronică nu este decât un fișier criptat, care conține în interiorul ei numele, prenumele, email-ul și țara utilizatorului. La cererea utilizatorilor s-au mai introdus încă două câmpuri noi, funcția și societatea. Astfel, fiecare posesor de semnătură electronică poate acționa și ca reprezentant al unei persoane juridice. Semnatura electronică reprezintă informații în format electronic și care sunt atașate sau asociate logic unor documente în formă de asemenea electronică. Semnatura electronică servește ca metodă de identificare a semnatarului și este înmagazinată pe suport magnetic securizat (spre exemplu un stick electronic).

Semnăturile electronice utilizează criptarea asimetrică, în care se folosește o cheie pentru a crea semnătura și o altă cheie, legată de prima, pentru a o verifica. Cheia privată este un cod digital cu caracter de unicitate, generat printr-un dispozitiv hardware și/sau software specializat. Cheia publică este un cod digital, perechea cheii private necesare verificării semnăturii electronice. Cheia privată reprezintă datele de creare a semnăturii electronice, iar cheia publică - datele de verificare ale acesteia. Cheia privată nu poate fi dedusă în niciun fel din cheia sa publică pereche.

Legătura dintre o anumită persoană și o semnătură electronică extinsă/un cod sau o cheie criptografică este confirmată printr-un certificat, eliberat de un furnizor de servicii de certificare. Acesta poate fi o persoană fizică sau juridică, care, deși nu are nevoie de acreditare în mod obligatoriu, are obligația de a notifica autoritatea de reglementare și supraveghere specializată în domeniu. Certificatul digital reprezintă o colecție de date în formă electronică ce atestă legătura dintre datele de verificare a semnăturii electronice și o persoană, confirmând identitatea acelei persoane. Altfel spus, într-un sistem de securitate a cheii publice, toți participanții au nevoie de propria cheie de semnare, sau cheie privată. Cheia publică este răspândită și identificată de către certificatele digitale. Certificatul digital este o *carte de identitate* virtuală, care poate permite crearea de semnătură electronică cu valoare legală, permițând identificarea fără echivoc în mediul electronic.

Cel mai cunoscut sistem cu chei publice este RSA, al cărui nume provine de la cei trei

cercetători de la Massachusetts Institute of Technology care l-au creat - Rivest, Shamir și Adleman. El este un adevărat standard „de facto” în domeniul semnăturilor digitale și al confidențialității cu chei publice. Se bucură de o foarte mare apreciere atât în mediul guvernamental, cât și în cel comercial, fiind susținut prin lucrări și studii de comunitatea academică. Sub diferite forme de implementare, prin programe sau dispozitive hardware speciale, RSA este astăzi recunoscută ca cea mai sigură metodă de cifrare și autentificare disponibilă comercial.

O semnătură digitală pentru documentele electronice este echivalentă cu o semnătură olografă pentru documentele tipărite. Semnătura reprezintă un eșantion de date care demonstrează că o anumită persoană a scris sau a fost de acord cu acel document căruia i s-a atașat semnătura. În fapt, o semnătură digitală furnizează un grad mult mai mare de securizare decât semnătura olografă [7]. Exigența încheierii unui act juridic în formă scrisă, *ad validitatem* sau *ad probationem*, este satisfăcută de înscrisul electronic cu semnătură electronică încorporată, bazată pe un certificat calificat și generată cu ajutorul unui dispozitiv de creare a semnăturii. Nerecunoașterea de către una dintre părți a înscrisului sau a semnăturii va obliga instanța, în fața căreia a fost adus litigiul, să dispună verificarea celor contestate, prin efectuarea unei expertize tehnice de specialitate. Expertul va solicita certificatele calificate, acte de natură să identifice autorul înscrisului, semnatarul sau titularul de certificat.

**Bibliografie:**

- [1] Legea nr. 455/2001 privind semnătura electronică și Hotărârea nr. 1259/2001 privind aprobarea Normelor tehnice și metodologice pentru aplicarea Legii nr. 455/2001
- [2] [www.certsign.ro/certsign/studiu\\_piata\\_2015](http://www.certsign.ro/certsign/studiu_piata_2015)
- [3] Thierry Vedel. 2013. „*The Internet in Campaigns and Elections.*” In *The Oxford Handbook of Internet Studies*, ed. William H Dutton, 401-420. Oxford: Oxford University Press.
- [4] Mircea Băduț. 2003 „*Informatică în management*”, Editura Albastră, Cluj-Napoca
- [5] Whitfield Diffie, Martin E. Hellman. 1976 „*New Directions in Cryptography*” accesat la adresa web: <https://www-ee.stanford.edu/~hellman/publications/24.pdf>
- [6] Comparative analysis of Rivest Shamir Adleman (RSA), Rabin and El Gamal public key cryptosystems by M. S. Olajide, O. S. Adewale, B. K. Alese and A. O. Adetunmbi. Vol.13, accesat la adresa web: <http://e.nampjournals.org/product-info.php?pid740.html>
- [7] Samuel S. Wagstaff, Jr.. 2002. „*Cryptanalysis of Number Theoretic Ciphers*”, accesat la adresa web <https://books.google.ro/books?isbn=8131708322>

## INTERNET OF THINGS – INTERNETUL LUCRURILOR

*Căpitan Adrian MIHAILEANU*  
*Centrul 346 Comunicații RMNC*



**1. Ce este?** Internetul este util și interesant, nu? De fapt, este absolut fantastic! Poate conecta persoane de pe tot globul folosind un standard comun. A

evoluat de la mica rețea între calculatoare la o rețea globală, robustă, tolerantă la erori și creată din subrețele care pot funcționa independent. Și acum evoluează din nou.

Vedem în jurul nostru cum apar o varietate de dispozitive, unele mai „inteligente” decât altele, toate cu posibilitatea de conectare la internet. Ceasuri inteligente, mașini inteligente, case inteligente, capabile să acceseze internetul și să fie accesate via internet, toate au devenit concepte materializate la care acum 10-20 de ani doar visam.

Să ai o interfață web prin care poți accesa aparatura din casă nu este doar interesant, ci este și util pentru a economisi resurse. Atât locuințele proprii, cât și companiile, serviciile medicale, fabricile, serviciile de stat și comunitățile vor avea beneficii de pe urma acestei interconectări. Este vorba atât despre informații de la aparate la oameni, cât și comunicarea independentă între aparate. Astfel, Internetul Lucrurilor (Internet of

Things/IoT) este următorul pas în evoluția internetului, evoluție care deja a început.

IoT este interconectarea prin internet a oricărui dispozitiv fizic, mașină, clădire etc., care, prin intermediul senzorilor, programelor, modulelor electronice etc., are posibilitatea colectării și schimbului de informații. În 2013, organizația Global Standards Initiative on Internet of Things definea IoT ca „infrastructura societății informaționale”.

### **2. Cum funcționează?**

Pentru ca dispozitivele să fie „inteligente” au nevoie de module care să le ajute să comunice cu internetul, să culegă informații/date din mediul înconjurător, sau module cu ajutorul cărora să se autoanalizeze și autoregleze pentru o funcționare optimă. În continuare vom trece în revistă principalele tipuri de module ce asigură interfața între dispozitivele „inteligente” și internet:

#### **RFID**

Radio-frequency identification este o tehnologie care folosește un mic aparat care poate stoca date despre un anumit lucru și care poate fi prins sau atașat de acel lucru și citit sau rescris de câte ori este nevoie. Este deja folosit pentru accesul în clădiri, urmărirea de animale, obiecte, deschiderea de portiere la mașini și în multe alte locuri. Marele avantaj este că aceste dispozitive sunt ușor de produs, implicând și costuri reduse.

Un exemplu interesant de aplicație a acestui aparat în conjunctură cu internetul este siste-

mul pe care funcționează anumite porturi din China, prin care traficul vapoarelor este supervizat automat cu ajutorul RFID-urilor plasate pe ele și a unor cititoare de putere plasate strategic, prin care se autocompletează datele și actele necesare de plecare și intrare în acele porturi. Mai puțină birocrație, un trafic mai fluent, mai mulți oameni fericiți.

### **QR-codes**

Denumit și link de obiect, Quick Response code este un fel de frate mai mare al codurilor de bare pentru că poate stoca mai multe date și poate fi citit de mult mai multe aparate, incluzând și majoritatea smartphone-urilor. Implică mai puține costuri la implementare decât RFID-urile, singurul lor dezavantaj fiind că nu pot fi decât citite și pentru a schimba informația de pe ele este necesar să fie regenerate și reprintrate.

Printre avantajele ar fi că pot stoca atât text, cât și linkuri care sunt interpretate automat de telefon și încărcate în browser. Deja apar pe tot mai multe afișe, produse și obiecte ca și etichete inteligente.

### **Senzori**

În această categorie regăsim majoritatea elementelor care sunt atașate pe diferitele dispozitive pentru a le face „inteligente”. Aceste mici aparate pot măsura caracteristici din jurul nostru și care sunt transmise apoi ca date la aparate mai complexe pentru interpretare. Categoriile mari de senzori ar fi acustici, de vibrație, chimici, electrici, magnetici, radio, de vreme, de umiditate, de curgere, de radiație, de poziție, de unghi, de viteză, de accelerație, optici, de presiune, de forță, de

densitate, de nivel, termici, de prezență, dar și alții.

Folosindu-i putem culege informații din lumea fizică, să le interpretăm și să întreprindem acțiuni în consecință. Smartphone-ul nostru are deja o multitudine de senzori cum ar fi GPS, accelerometru, proximitate, nivel ambiental de lumină și alții în funcție de model, care ne modifică automat anumiți parametri fără a avea nevoie de aprobarea noastră.

### **Microcontrollere mici și ieftine**

Senzorii nu pot încărcă datele direct pe internet, deci este nevoie de niște mici circuite integrate, care pot interpreta aceste date și să le trimită spre internet. Cei doi mari producători de pe piața actuală sunt Atmel AVR și ARM.

Proiectul Arduino este o platformă open source care câștigă teren ca un proiect pentru pasionații de electronică. Bazat pe un microcontroller, Atmel AVR oferă posibilități de primire de date de la diferiți senzori, interpretarea acestora și retrimiteră mai departe. De asemenea, oferă și posibilitatea de a se conecta la calculator pentru a fi programat. Desigur există și alte soluții; spre exemplu, o altă platformă, mai performantă este RaspberryPi bazată pe microcontrollerul ARM, cu sistem de operare Linux și interfață Ethernet, făcând-o perfectă pentru integrarea cu IoT. Momentan, Arduino, având în spate o comunitate mare pe internet și documentație extensivă, a câștigat teren comparativ cu celelate platforme.

### **Module WiFi & Ethernet**

Având datele de la senzori și procesându-le cu un microcontroller, este momentul să le trimitem spre internet. Pentru aceasta avem nevoie

de module Ethernet sau WiFi. Plăcile de rețea pentru PC nu vor funcționa direct cu microcontrollerele; de aceea trebuie să folosim module capabile să funcționeze cu noile platforme apărute (Arduino, RaspberryPi etc.).

### 3. Securitatea IoT

Desigur că, odată cu toate avantajele și posibilitățile noi care ni se deschid prin intermediul IoT, apar și noi vulnerabilități și bineînțeles un număr mult mai mare de potențiale ținte pentru atacuri cibernetice.

Dezvoltarea rapidă a IoT fără o implementare a unor măsuri de securitate adecvate poate avea consecințe mult mai grave decât până acum, deoarece atacurile cibernetice pot avea nu doar efecte în spațiul virtual, ci și în cel fizic.

Ca exemple de posibile atacuri cu posibile efecte grave: în 2008, cercetătorii în domeniul securității au reușit conectarea neautorizată și controlarea de la distanță a unui peacemaker și a unei pompe de insulină. Un alt domeniu care ridică semen de îngrijorare este cel auto, unde a început dezvoltarea mașinilor inteligente, ce permit accesarea neautorizată a anumitor funcții ale mașinii,

cum ar fi sistemul de frânare, direcție sau injecție. Scenarii asemănătoare celor de mai sus sunt posibile în toate domeniile unde dispozitivele inteligente conectate la internet sunt sau vor fi utilizate. Astfel, securitatea datelor prin IoT devine o problemă foarte serioasă, cu implicații cât se poate de grave.

Ca răspuns la această problemă, în 23 septembrie 2015 a fost creată organizația *Fundația pentru securitatea IoT (the Internet of Things Security Foundation)* care are ca scop promovarea cunoașterii IoT și tot ce ține de acesta, precum și „bunele practici” legate de IoT.

Așadar, IoT - Internetul Lucrurilor, și-a făcut încet loc în viețile noastre fără să ne dăm seama și numărul „device-urilor deștepte” din jurul nostru crește. Este o unealtă care ne oferă monitorizarea, controlarea și modificarea (uneori automată - autoreglare) realității prin intermediul mediului virtual de la distanță, teoretic având aplicații și posibilități nelimitate, dar care deschide și o „cutie a Pandorei” cu pericole potențiale la fel de greu de definit.

### Bibliografie:

1. [www.wikipedia.en.org](http://www.wikipedia.en.org)
2. [www.inventeaza.ro](http://www.inventeaza.ro)



## ROLUL REȚELELOR DE MISIUNE MNE, MNX ÎN CADRUL FMN

*Locotenent Cristina CHIRVASE*

*Centrul 48 Comunicații și Informatică Strategice*



Filosofia FMN (Federated Mission Networking) este să asigure un mediu federativ în care Alianții și partenerii să comunice, să se instruiască și să funcționeze eficient împreună. Misiunea FMN este să asigure o instanțiere rapidă a rețelelor de misiune de către organizațiile NATO federative, națiunile NATO și partenerii de misiune, asigurând interoperabilitatea și partajarea informațiilor. Rețeaua de misiune federativă (FMN) este un cadru conceptual reglementat, format din oameni, procese și tehnologii și creat pentru a planifica, pregăti și utiliza rețelele de misiune în sprijinul operațiilor federative. FMN este o capacitate pentru suportul comenzii și controlului (C2) și luării deciziei în operațiile viitoare prin îmbunătățirea schimbului de informații. FMN se bazează pe implementarea lecțiilor învățate din Rețeaua de Misiune din Afganistan (Afganistan Mission Network - AMN).

Rețelele de misiune (MN) oferă o instanță unică de capacitate, inclusiv sistemele SIC (Communication and Information System - CIS), managementul, procesele și procedurile create în scopul unui exercițiu, eveniment de instruire sau

activitate de verificare a interoperabilității. Rețelelor de misiune le sunt asigurate contribuții materiale (rețele statice și dislocabile, servicii, infrastructură) și non-materiale (politici, procese, proceduri, standarde) furnizate de NATO, de aliați sau de parteneri.

Sistemul este alcătuit din mai multe rețele, cu același nivel de clasificare, construite pe un set comun de echipamente, aplicații și servicii standardizate, care sunt disponibile la nivel global, regional sau local, unele dintre ele având mai mulți membri, altele mai puțini, iar altele fiind bilaterale prin natura lor. Standardizarea implementată la nivelul întregului sistem permite aplicarea principiului conectează-te și lucrează în orice nod de acces, oriunde pe glob și în oricare din rețele, cu același tip de nod sau terminal.

În ceea ce privește evoluția capacităților FMN și participarea cu rețele de misiune, sunt definite patru niveluri de capacitate: element al unei rețele de misiune (MNE), extensie a unei rețele de misiune (MNX), utilizator găzduit (HU) și alte entități. Un MNE (Mission Network Element) conține rețele, informații de infrastructură, serviciile necesare funcționării, inclusiv serviciile esențiale pentru misiune. Un MNX (Mission Network Extension) conține infrastructura și serviciile necesare funcționării, dar nu include suficiente servicii esențiale de misiune. Un utilizator găzduit (hosted user) este un participant la rețeaua de misiune care nu își poate asigura infrastructura și

serviciile necesare funcționării. Celelalte entități, care nu fac parte integrantă a rețelei, nu sunt supuse unor cerințe din cadrul FMN. Națiunile sau organizațiile stabilesc nivelul de implicare în fiecare rețea de misiune în funcție de obiectivele propuse.

Pentru a îndeplini serviciile minime din Spirala 1 FMN, un element al rețelei de misiune trebuie să realizeze următoarele servicii: servicii de management a documentelor (Office); servicii

de mesagerie informală (eMail cu atașamente); servicii colaborative bazate pe text (Chat); servicii colaborative bazate pe video (videoteleconferință); servicii colaborative bazate pe voce (Voce peste IP); servicii de platformă web.

În concluzie, orice stat membru sau entitate stabilește, în funcție de capacitățile pe care le deține, nivelul de implicare în rețeaua de misiune.

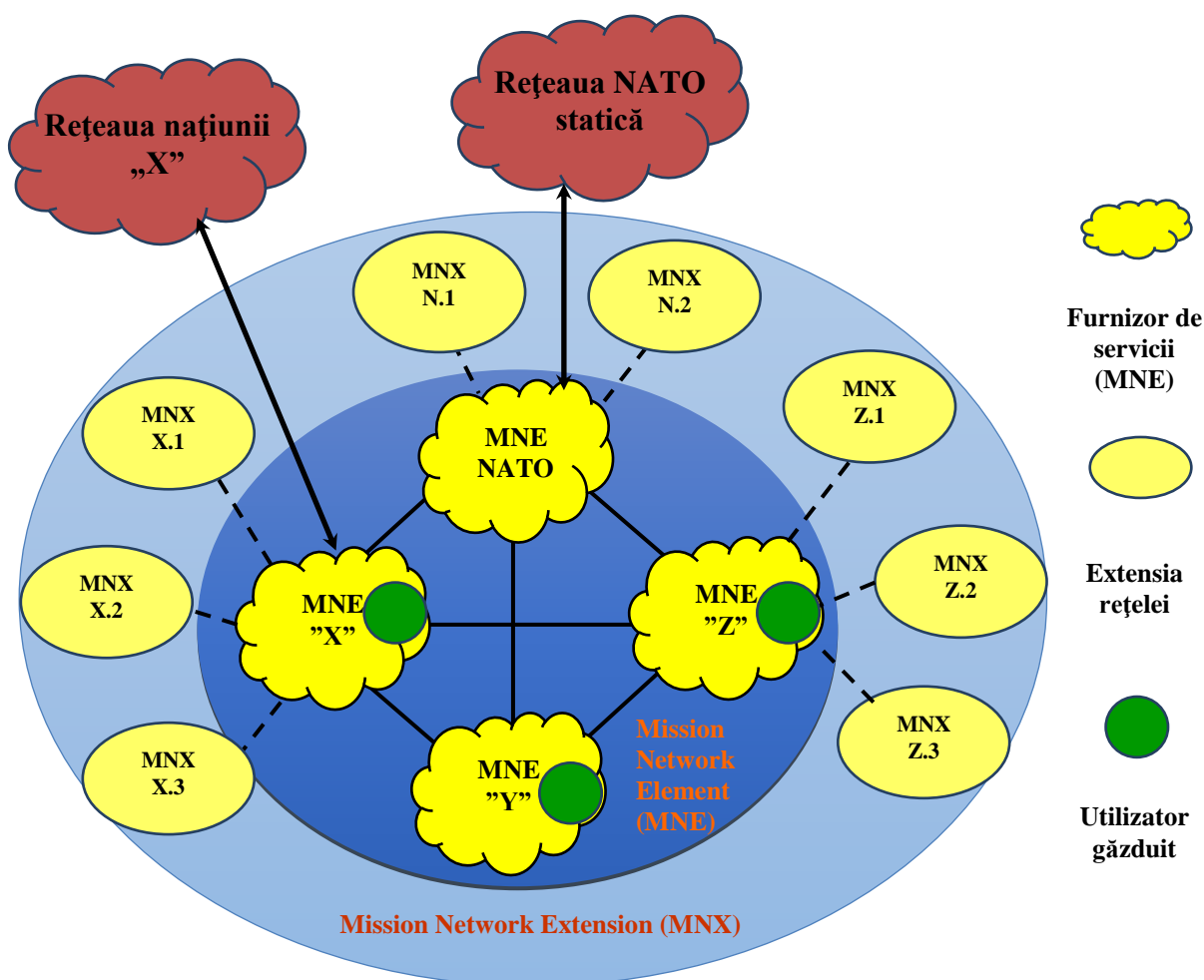


Figura 1 Opțiuni pentru participarea la o rețea de misiune

Sursa: <http://www.act.nato.int/fmn>



## **OBIECTIVELE FUNDAMENTALE PE ANI DE INSTRUCȚIE:**

**2008 - INSTRUCȚIE/PREGĂTIRE, OPERAȚIONALIZARE, PROFESIONALIZARE**

**2009 - INSTRUCȚIE/PREGĂTIRE, EXIGENȚĂ, DISCIPLINĂ, PERFORMANȚĂ**

**2010 - INSTRUIRE PENTRU MISIUNI, COEZIUNE PENTRU LUPTĂ**

**2011 - MODERNIZARE STRUCTURALĂ-OPERAȚIONALIZARE ACȚIONALĂ**

**2012 - OPERAȚIONALIZARE - MODERNIZARE - OPTIMIZARE - DISLOCABILITATE**

**2013 - CAPABILITĂȚI MAXIME, COSTURI MINIME**

**2014 - INSTRUIRE LA CELE MAI ÎNALTE STANDARDE PROFESIONALE**

**2015 - TRANSFORMARE, OPTIMIZARE, OPERAȚIONALIZARE**

**2016 - VALIDAREA STANDARDELOR DE INTEROPERABILITATE**

