SECURITATEA SISTEMELOR DE COMUNICAȚII ȘI INFORMATICĂ ALE ALIANȚEI NORD-ATLANTICE ÎN CONTEXTUL AMENINȚĂRILOR HIBRIDE

Colonel prof. univ. dr. ing. Cezar VASILESCU
Departamentul Regional de Studii pentru Managementul Resurselor de Apărare, Brașov
Locotenent-colonel drd. Daniel DOICARIU
Universitatea Națională de Apărare „Carol I”
10.55535/GMR.2023.3.7

În articol sunt prezentate succint câteva argumente privind necesitatea asigurării securității sistemelor de comunicații și informatică la nivelul NATO. Sunt menționate, în acest context, o serie de amenințări, vulnerabilități și riscuri asupra sistemelor de comunicații și informatică, dar și măsuri preventive și indicatori cu privire la acțiunile adversarului.

Pentru asigurarea securității sistemelor de comunicații și informatică, este nevoie de o securitate a „mediului de desfășurare” a informațiilor, adică de o protecție electronică și o securitate a spațiului cibernetic.

Pentru acest demers științific am ales tipul de cercetare descriptivă, cu scopul de documentare și înțelegere a importanței securității sistemelor de comunicații și informatică la nivelul Alianței Nord-Atlantice, prin analiza literaturii de specialitate, pentru problematica ce face obiectul articolului.

Considerăm oportună realizarea acestei lucrări, datorită faptului că sistemele de comunicații și informatică în sprijinul operațiilor militare presupun măsuri de securitate specifice în operațiile cibernetice și de război electronic, în domeniul managementului spectrului radio, asupra echipamentelor/rețelelor de comunicații și informatică proprii etc.

Cuvinte-cheie: alianță, securitate, război hibrid, sisteme de comunicații, informatică.

INTRODUCERE

Amenințările hibride există acolo unde acțiunile asimetrice își fac loc pentru a evita o confruntare directă cu adversarul. *„O amenințare hibridă este combinația diversă și dinamică de forțe regulate, forțe neregulate, teroriști sau elemente criminale care acționează în comun pentru a obține efecte reciproc avantajoase”* (ADP 3.0, 2019, pp. 1-3). Amenințările hibride introduc în luptă elemente noi și complexe, folosind forțe, tehnologii și tehnici atipice, neîntâlnite în cazul războiului clasic. O acțiune hibridă poate pleca de la un atac militar convențional și continuă cu acțiuni de propagandă, de scădere a încrederii în factorul politico-militar, privând populația de servicii de bază, precum cel medical, furnizarea de electricitate, apă, acces la sistemul bancar etc., provocând o criză umanitară. Astfel de acțiuni combinate sunt mai greu de contracarat. Din perspectiva sistemelelor de comunicații și informatică, acestea trebuie să poată acționa, reacționa, adapta, să fie reziliente și robuste pentru a asigura serviciile și facilitățile pe timp de pace, criză sau război.

Amenințările hibride introduc în luptă elemente noi și complexe, folosind forțe, tehnologii și tehnici atipice, neîntâlnite în cazul războiului clasic. O acțiune hibridă poate pleca de la un atac militar convențional și continuă cu acțiuni de propagandă, de scădere a încrederii în factorul politico-militar, privând populația de servicii de bază, precum cel medical, furnizarea de electricitate, apă, acces la sistemul bancar etc., provocând o criză umanitară.

O definiție a securității o găsim la Arnold Wolfers, în articolul *„Securitatea națională ca simbol ambiguu”*: *„Securitatea, în sens obiectiv, înseamnă lipsa amenințărilor la adresa valorilor dobândite, iar în sens subiectiv, absența temerii că aceste valori vor fi atacate”.* (Wolfers, 1952, p. 485). Trebuie subliniat faptul că măsurile proactive și reactive conțin politici, ghiduri și standarde de securitate, aspecte legate de cultura de securitate și aplicarea măsurilor INFOSEC (de securitatea informațiilor). Securitatea informațiilor este necesară protejării numărului tot mai mare de utilizatori, în contextul creșterii amenințărilor din spațiul cibernetic și diversității tehnologiilor emergente și disruptive disponibile din ce în ce mai frecvent pe piața de tehnologia informației (IT).

SECURITATEA SISTEMELOR DE COMUNICAȚII ȘI INFORMATICĂ ÎN NATO

Securitatea sistemelor de comunicații și informatică este definită în AJP 6 ca fiind *„Un element de asigurare a informațiilor și constă în aplicarea măsurilor de securitate pentru protecția comunicațiilor, informaticii și a altor sisteme electronice și informații care sunt stocate, procesate sau transmise în aceste sisteme cu respectarea disponibilității, integrității, autentificării, confidențialității și non-repudierii”.* (AJP-6, 2017, pp. 1-4).

Securitatea sistemelor de comunicații și informatică conține măsuri defensive pentru contracararea atacurilor cibernetice, pentru limitarea efectelor acestora și pentru pregătirea utilizatorilor și administratorilor rețelelor. În scopul asigurării securității sistemelor de comunicații și informatică, criptarea informațiilor este necesară și esențială, iar *„în NATO, criptografia este utilizată la toate nivelurile (de la strategic la tactic, în static și dislocabil) și pentru majoritatea serviciilor de comunicații (de exemplu, voce, videoconferință, date în timp real și non-real)”.* (Ib., p. B-6).

Securitatea sistemelor de comunicații și informatică este integrată pe parcursul planificării și executării tuturor operațiilor militare. De asemenea, activitățile de apărare cibernetică sunt elemente esențiale în asigurarea securității sistemelor de comunicații și informatică, permițând funcționarea serviciilor în contextul acțiunilor ostile ale inamicului în spațiul cibernetic. Informațiile trebuie să fie furnizate și protejate corect, bazându-se pe trei piloni principali și doi secundari: *confidențialitate, integritate, disponibilitate,* precum și *autentificare* și *nerepudiere (figura 1)*, asupra cărora ne vom opri în cele ce urmează.

Securitatea sistemelor de comunicații și informatică conține măsuri defensive pentru contracararea atacurilor cibernetice, pentru limitarea efectelor acestora și pentru pregătirea utilizatorilor și administratorilor rețelelor. În scopul asigurării securității sistemelor de comunicații și informatică, criptarea informațiilor este necesară și esențială, iar „în NATO, criptografia este utilizată la toate nivelurile (de la strategic la tactic, în static și dislocabil) și pentru majoritatea serviciilor de comunicații”.

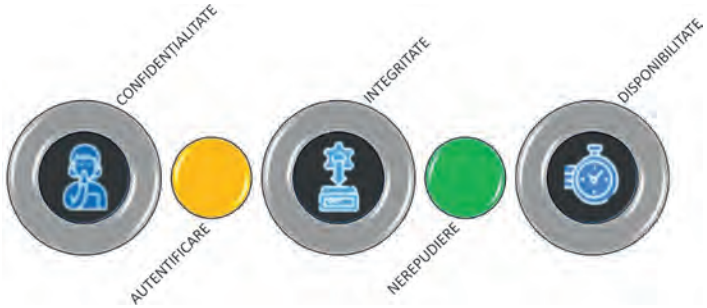

Figura 1: Caracteristicile securității informațiilor (concepția autorilor)

❖ *Confidențialitatea* presupune că informațiile nu sunt puse la dispoziție sau dezvăluite persoanelor, entităților sau proceselor neautorizate. Previne dezvăluirea informațiilor neautorizate.

❖ *Autentificarea* reprezintă actul de verificare a identității revendicate de o entitate.

❖ *Integritatea* informațiilor (inclusiv a datelor) presupune că acestea nu au fost modificate sau distruse în mod neautorizat. Previne manipularea informațiilor prin compromiterea corectitudinii, integrității sau fiabilității acestora.

❖ *Nerepudierea* este o măsură de asigurare pentru destinatar – că informațiile au fost trimise de o anumită persoană sau organizație și pentru expeditor – că informațiile au fost primite de către destinatarii vizați.

❖ *Disponibilitatea* presupune că informațiile sunt accesibile și utilizate la cererea unei persoane sau a unei entități autorizate. Constă în protejarea informațiilor față de încercările intenționate sau accidentale neautorizate, prin refuzul la informații sau sisteme. (Ib., pp. 1-13 _ 1-14).

Pentru sprijinul cu sisteme de comunicații și informatică, în doctrina NATO sunt specificate câteva *caracteristici esențiale.* Una dintre aceste caracteristici esențiale ale sistemelor de comunicații și informatică este **securitatea**, care *„garantează nivelurile necesare de confidențialitate, integritate și disponibilitate pentru servicii, sisteme și informații, proporționale cu cerințele misiunii”* (AJP-6, pp. 1_10).

Relația dintre asigurarea informațiilor și securitatea sistemelor de comunicații și informatică (inclusiv apărarea cibernetică) este strâns legată și cu celelalte medii de securitate, precum cel industrial, fizic și al personalului, conform *figurii 2.*

Securitatea sistemelor de comunicații și informatică presupune asigurarea informațiilor prin aplicarea măsurilor de securitate asupra tehnicii, echipamentelor, rețelelor și a informațiilor transmise sau recepționate. Apărarea cibernetică contracarează atacurile cibernetice sau atenuează efectele acestora prin integrarea eforturilor pentru răspunsuri la incidente, măsuri de prevenire a securității sistemelor de comunicații și informatică, dar și conștientizarea operatorilor privind necesitatea protejării echipamentelor.

Când vorbim de securitatea sistemelor de comunicații și informatică, aceasta include și apărarea cibernetică (conform Allied Joint Publication – AJP-6).

Apărarea cibernetică contracarează atacurile cibernetice sau atenuează efectele acestora prin integrarea eforturilor pentru răspunsuri la incidente, măsuri de prevenire a securității sistemelor de comunicații și informatică, dar și conștientizarea operatorilor privind necesitatea protejării echipamentelor.

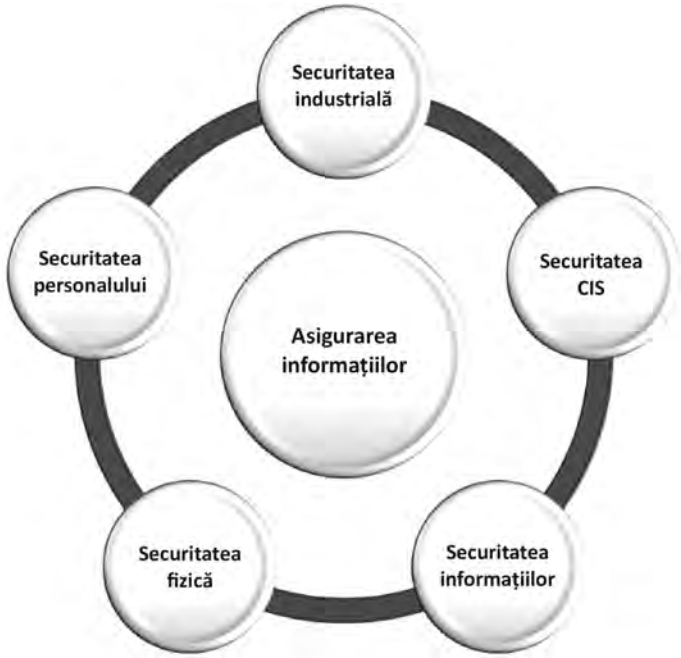

Figura 2: Relația dintre asigurarea informațiilor și securitatea sistemelor de comunicații și informatică (Ib., pp. 1-14, adaptare)

Pentru asigurarea și menținerea unei securități a sistemelor de comunicații și informatică, este nevoie de asigurarea securității spațiului cibernetic, întrucât „acțiunile de securitate cibernetică protejează rețelele și sistemele în toate fazele de planificare și implementare a rețelei”.

Pentru asigurarea și menținerea unei securități a sistemelor de comunicații și informatică, este nevoie de asigurarea securității spațiului cibernetic, întrucât *„acțiunile de securitate cibernetică protejează rețelele și sistemele în toate fazele de planificare și implementare a rețelei. Activitățile de securitate cibernetică includ evaluarea și analiza vulnerabilităților, gestionarea vulnerabilităților, gestionarea incidentelor, monitorizarea continuă, detectarea și restaurarea capabilităților pentru protejarea și păstrarea informațiilor și sistemelor informatice”.* (Wade, 2019, pct. 2_12, lit. E).

Mediul operațional este mult mai mare decât o arie de operații. Acesta cuprinde zonele fizice ale domeniilor terestru, maritim, aerian și spațial, precum și spațiul cibernetic și spectrul electromagnetic. Trebuie avute în vedere condițiile și contextul operațional care pot influența deciziile unui comandant sau capacitatea de a acționa a forțelor și mijloacelor tehnice. Sistemele de comunicații și informatică

pun la dispoziție serviciile și echipamentele în funcție de misiune, pentru susținerea exercitării comenzii și controlului. Amenințările hibride sunt desfășurate cu precădere în mediul informațional, spațiul cibernetic și spectrul electromagnetic fiind componente ale acestuia. În conflictele hibride, controlul mediului informațional este la fel de important ca și controlul domeniilor fizice. Mai mult decât atât, cele două medii sunt integrate și orice activitate care are loc într-unul îl afectează și pe celălalt.

Spațiul cibernetic include *„rețeaua interdependentă de infrastructuri informatice și de date rezidente, inclusiv internetul, rețele de telecomunicații, sisteme informatice și procesoare și controlere încorporate”.* (conform JP 3-12, 2013/8, p. I-1).

Spectrul electromagnetic asigură legătura între spațiul cibernetic și domeniile fizice în care se desfășoară acțiunile militare. Forțele proprii trebuie să asigure securitatea sistemelor de comunicații și informatică proprii în spațiul cibernetic și spectrul electromagnetic și, pe cât posibil, să controleze capacitatea adversarilor în a opera în aceste componente ale mediului informațional.

SECURITATEA INFORMAȚIILOR LA NIVEL NAȚIONAL

În *Strategia Națională de Apărare a Țării pentru perioada 2020-2024 (SNApT)*, unul dintre obiectivele naționale de securitate, din perspectivă internă, vizează *„asigurarea securității și protecției infrastructurilor de comunicații și tehnologia informațiilor cu valențe critice pentru securitatea națională, precum și cunoașterea, prevenirea și contracararea amenințărilor cibernetice derulate asupra acestora de către actori cu motivație strategică, de ideologie extremist-teroristă sau financiară”.* (SNApT, 2020, p. 15). În acest sens, în *Carta albă a apărării*, o prioritate de acțiune este reprezentată de *„derularea unor programe de perfecționare continuă pe linia asigurării securității cibernetice, a sistemelor de comunicații și a combaterii amenințărilor de tip hibrid, în vederea creșterii rezilienței în fața noilor provocări”* (Carta albă, 2021, p. 18). În cele două documente de nivel strategic care reglementează apărarea națională, avem, printre priorități și obiective, securitatea cibernetică și pe cea a sistemului de comunicații și informatică, care necesită a fi implementate prin directive de planificare și programe majore de înzestrare. De asemenea, în SNApT se regăsesc câteva dintre amenințările, riscurile și vulnerabilitățile ce vizează domeniul

În Strategia Națională de Apărare a Țării pentru perioada 2020-2024, unul dintre obiectivele naționale de securitate, din perspectivă internă, vizează „asigurarea securității și protecției infrastructurilor de comunicații și tehnologia informațiilor cu valențe critice pentru securitatea națională, precum și cunoașterea, prevenirea și contracararea amenințărilor cibernetice derulate asupra acestora de către actori cu motivație strategică, de ideologie extremist-teroristă sau financiară”.

comunicații și informatică la nivel național, așa după cum se poate observa în *tabelul 1*.

Tabelul 1: Amenințări, riscuri și vulnerabilități în domeniul comunicații și informatică (extras din SNApT, pp. 25-29)

Amenințări	*- „**Acțiuni ostile de influență derulate în spațiul public**, având ca scop schimbarea de percepții și influențarea comportamentului societății civile, constituie o amenințare constantă la adresa securității sociale, având potențialul de a se amplifica pe fondul diversificării mijloacelor de comunicare în mediul online.* *- **Atacurile cibernetice** lansate de entități statale și non-statale (grupări de criminalitate cibernetică, grupări de hackeri cu sau fără motivație ideologică, politică sau extremist-teroristă) asupra infrastructurilor informatice și de comunicații cu valențe critice.* *- **Integrarea tehnologiilor emergente și disruptive** în instrumentarul ofensiv al entităților cibernetice multiplică exponențial sursele de amenințare și potențează soluțiile de disimulare a operațiunilor cibernetice în vederea creării aparenței unei apartenențe false.* *- **Criminalitatea informatică** se situează pe o tendință ascendentă, tot mai multe grupări autohtone specializându-se în activități ilicite din această sferă (compromitere de ATM-uri și POS-uri; clonări de carduri; acces neautorizat în sisteme informatice, interceptarea ilegală de date informatice, postare de anunțuri fictive pe site-uri de comerț intens accesate, infectarea sistemelor informatice cu ransomware, preluarea sub control de resurse informatice pentru minarea de monede virtuale, dar și utilizarea sau exploatarea criptomonedelor pentru derularea de operațiuni ilicite din zona economică).*
Riscuri	*- Utilizarea **noilor tehnologii** de către entități ale criminalității organizate și infracționalității cibernetice, grupări și organizații cu profil terorist sau extremist și actori interesați să dezvolte acțiuni ofensive **se va situa pe un trend ascendent**.* *- Dependența serviciilor de comunicații de un **număr restrâns de furnizori de tehnologie** sau existența unor **fluxuri nesecurizate de achiziții de tehnologii** utilizate în furnizarea de servicii esențiale sau critice reprezintă un fenoment cu impact asupra disponibilității și integrității rețelelor de comunicații.*

Integrarea tehnologiilor emergente și disruptive în instrumentarul ofensiv al entităților cibernetice multiplică exponențial sursele de amenințare și potențează soluțiile de disimulare a operațiunilor cibernetice în vederea creării aparenței unei apartenențe false.

	*- **Riscul declanșării unui conflict armat interstatal se menține redus**, dar se profilează **riscul adaptării operațiunilor ofensive cu caracter hibrid** la evoluțiile tehnologice, printr-o diversificare continuă a modalităților de acțiune și a resurselor coordonate, în scopul afectării intereselor naționale, inclusiv de securitate.*
Vulnerabilități	*- **Nivelul redus de securitate cibernetică** a infrastructurilor de comunicații și tehnologia informației din domenii strategice (inclusiv ca efect al vulnerabilităților tehnologice și procedurale ale infrastructurilor deținute de operatorii de comunicații) facilitează derularea de atacuri cibernetice de către actori statali sau non-statali.* *- **Acutizarea decalajului tehnologic** și valorificarea insuficientă a beneficiilor conferite de utilizarea noilor tehnologii în marea majoritate a domeniilor de activitate pot genera un impact negativ în planul dezvoltării și competitivității economice, pe linie de cercetare-dezvoltare-inovare și, pe termen mediu și lung, în asigurarea securității naționale.* *- **Nivelul scăzut al culturii de securitate** la nivelul societății civile și al aparatului decizional poate fi exploatat de entitățile informative ostile în scopul obținerii de informații sau desfășurării acțiunilor de influență”.*

În viitoarele conflicte militare, așa după cum susțin specialiști în domeniu, *„cu cât mai mare va fi avantajul obținut din tehnologia informației și a comunicațiilor, cu atât va crește și vulnerabilitatea sa potențială”* (Boaru, Iorga, 2018, p. 31). În acest context, putem menționa înființarea Directoratului Național de Securitate Cibernetică (DNSC), care a înlocuit Centrul Național de Răspuns la Incidente de Securitate Cibernetică (CERT-RO), fapt materializat prin Ordonanța de Urgență nr. 104 (22 septembrie 2021). Dintre obiectivele activității DNSC evidențiem câteva:

- *„asigurarea securității, confidențialității, integrității, disponibilității, rezilienței elementelor din spațiul cibernetic național civil, în cooperare cu instituțiile care au competențe și atribuții în domeniu;*
- *asigurarea cadrului de strategii, politici și reglementări care să susțină implementarea viziunii naționale în domeniul securității cibernetice;*

GÂNDIREA MILITARĂ ROMÂNEASCĂ

Acutizarea decalajului tehnologic și valorificarea insuficientă a beneficiilor conferite de utilizarea noilor tehnologii în marea majoritate a domeniilor de activitate pot genera un impact negativ în planul dezvoltării și competitivității economice, pe linie de cercetare-dezvoltare-inovare și, pe termen mediu și lung, în asigurarea securității naționale.

- *crearea cadrului național de cooperare între instituții din domeniul public, privat, de educație și cercetare, pentru asigurarea unei viziuni și abordări realiste, comune și coerente privitor la securitatea cibernetică a României;*
- *promovarea și susținerea pe plan internațional a strategiei naționale în domeniul securității cibernetice".* (Ordonanța de Urgență nr. 104, art. 4).

De asemenea, conform *Ghidului practic pentru operatorii de servicii esențiale (OSE) – Implementarea măsurilor minime de asigurare a securității rețelelor și sistemelor informatice*, securitatea informațiilor are ca preocupare *„protejarea activelor organizației împotriva amenințărilor interne și externe"* (Munteanu, Păuna, Constantinescu, Măgdălinoiu, Voinea, Găbudeanu & Anghel, 2021, p. 22). Aceste amenințări pot fi clasificate în funcție de daunele pe care le pot provoca activelor protejate. În acest sens, în *figura 3* este redată relația dintre active și vulnerabilități, amenințări și riscuri, conform ISO/IEC 27032 (Information Technology – Security Techniques – Guidelines for Cybersecurity).

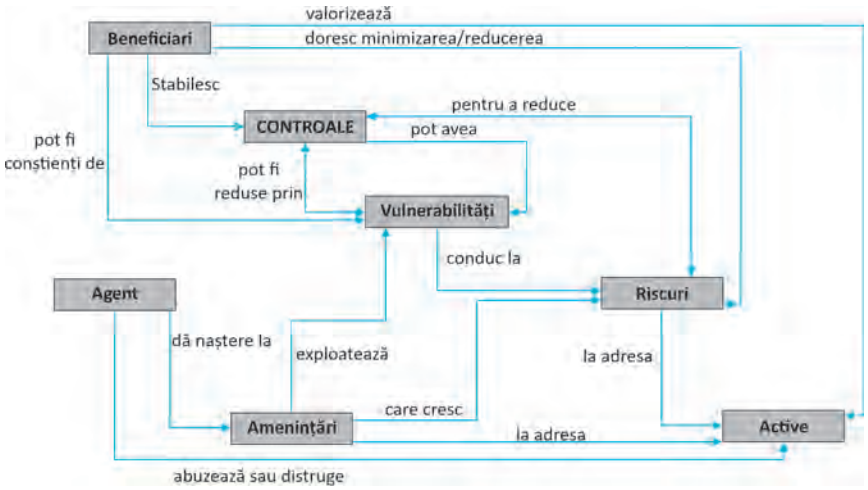

Figura 3: Relația dintre active și vulnerabilități, amenințări și riscuri (Ib., p. 23)

Este evident, astfel, că orice analiză ar trebui să aibă în vedere relația dintre vulnerabilități, amenințări și riscuri. Riscul se raportează la fiecare amenințare și vulnerabilitate în parte. Dacă probabilitatea de apariție a amenințărilor este greu de estimat, atunci reducerea riscurilor se poate realiza prin diminuarea vulnerabilităților.

SECURITATEA SISTEMELOR DE COMUNICAȚII ȘI INFORMATICĂ ÎN SPRIJINUL OPERAȚIILOR

Experiențele militare ale forțelor NATO în Irak și în Afganistan nu mai pot fi luate ca punct de reper în dezvoltarea și consolidarea sistemului de comunicații și informatică. Operațiile militare în cele două țări au fost caracterizate ca misiuni de contrainsurgență, de sprijin și stabilitate. Conflictul din Ucraina însă ne prezintă o altă realitate, în care ritmul operațiilor este accelerat, iar pierderile umane și de echipamente sunt considerabil mai mari. Efectele asupra economiilor țărilor europene, și nu numai, s-au resimțit odată cu începerea acestui conflict.

Gestionarea, diseminarea și controlul informațiilor transmise prin echipamentele de comunicații și informatică sunt esențiale din perspectiva îndeplinirii misiunilor. Potențialii adversari au înțeles acest lucru și, pentru a-și atinge obiectivele, adună informații tehnice și tactice pentru a acționa cu operații specifice războiului electronic. Astfel de elemente presupun:

- bruiajul asupra sistemelor de comuncații care utilizează spectrul de frecvențe radio;
- interceptarea comunicațiilor în rețelele radio/radioreleu/satelitare;
- interferențe cu fluxul de comunicații al adversarului etc.

Planificatorii sistemelor de comunicații și informatică pot lua măsuri pentru a atenua amenințările adversarului în spectrul frecvențelor radio. Dintre măsurile de reducere a semnăturii electromagnetice în punctele de comandă și în centrele de comunicații, elocvente sunt cele specificate în FM 6.02 (2019, p. A-1), precum:

- selectarea atentă a locației pentru echipamentele de comunicații;
- utilizarea antenelor direcționale;
- operații care utilizează cea mai mică putere necesară;
- limitarea transmisiilor radio;

Experiențele militare ale forțelor NATO în Irak și în Afganistan nu mai pot fi luate ca punct de reper în dezvoltarea și consolidarea sistemului de comunicații și informatică. Operațiile militare în cele două țări au fost caracterizate ca misiuni de contrainsurgență, de sprijin și stabilitate. Conflictul din Ucraina însă ne prezintă o altă realitate, în care ritmul operațiilor este accelerat, iar pierderile umane și de echipamente sunt considerabil mai mari. Efectele asupra economiilor țărilor europene, și nu numai, s-au resimțit odată cu începerea acestui conflict.

- utilizarea transmisiilor în rafală pentru a minimiza timpul de transmitere;
- folosirea unui program aleator de ritm de luptă.

De asemenea, pot fi luate diverse măsuri de mascare radio, de valorificare a terenului, măsuri de protecție electronică etc. Aceste măsuri sunt aplicabile în condiții optime, pentru perioade reduse de timp. Fără comunicații asigurate în mod continuu, comanda și controlul forțelor au de suferit și pot determina pierderea inițiativei: *„Un inamic poate folosi echipamente de identificare a unei direcții de frecvență radio pentru a localiza orice emițător de frecvență, cum ar fi o stație radio, un terminal de comunicații prin satelit, un sistem împotriva dispozitivelor explozive improvizate, un radar sau telefon mobil. Odată ce a determinat o locație precisă, inamicul poate direcționa focuri letale pentru a distruge capabilitățile”* (ATP 6-02.71, 2019, p. 3-20). Oricare situație dintre cele menționate este posibilă dacă nu sunt respectate măsurile de securitate în mediul electromagnetic.

Sprijinul sistemelor de comunicații și informatică reprezintă mult mai mult decât transmiterea de informații în cadrul unei operații militare, acesta constituind legătura dintre informații și decizie, precum și dintre decizie și acțiune. De aceea, există o preocupare asupra securității comunicațiilor și informaticii de a proteja conținutul informațiilor proprii față de adversar.

Sprijinul sistemelor de comunicații și informatică reprezintă mult mai mult decât transmiterea de informații în cadrul unei operații militare, acesta constituind legătura dintre informații și decizie, precum și dintre decizie și acțiune. De aceea, există o preocupare asupra securității comunicațiilor și informaticii de a proteja conținutul informațiilor proprii față de adversar. Sistemele criptografice permit protejarea informațiilor vehiculate de utilizatori: *„Includerea managementului de chei al COMSEC în planificarea operațiilor este esențială pentru a asigura comunicații sigure”* (FM 6.02, pp. 2-38), așa după cum se arată în *Signal Support to Operations*, manual de luptă american. Securitatea comunicațiilor presupune acțiuni care au rolul de a *„împiedica accesul persoanelor neautorizate la informații de valoare prin protejarea accesului la echipamente, material și documente sau observarea acestora cu privire la deținerea și studiul telecomunicațiilor sau pentru a induce în eroare intenționat persoanele neautorizate în interpretarea rezultatelor acestor deținere și studii”* (JP 6-0, 2019, p. GL-4). Aceste tehnici de protecție electronică sprijină securitatea comunicațiilor prin neidentificarea de către inamic a semnăturii electromagnetice. Existența unui *ofițer CEMA (cyber and electromagnetic activities)* poate juca un rol esențial în planificarea protecției electronice.

Operatorii radio ar trebui să recunoască și să reacționeze atunci când identifică acțiuni de bruiaj electromagnetic, în contextul în care bruiajul inamic și interferențele electromagnetice proprii sunt dificil de diferențiat, îngreunând sarcinile acestora. De exemplu, interferențele pot fi provocate neintenționat de alte stații radio – proprii sau ale adversarului –, de echipamente electrice și electronice din împrejurimi, de condițiile atmosferice sau defecțiunile echipamentelor proprii etc.

Generalul-locotenent Ben Hodges, comandant al Forțelor Terestre ale SUA în Europa, menționa, într-un interviu acordat în anul 2015, lipsurile din zona *„tehnologiei informaționale”*, subliniind următoarele aspecte:

❖ *„Securizarea stațiile radio FM, astfel încât trupele americane să poată comunica în siguranță și cu aliații, fără a fi bruiați.*

❖ *Partajarea datelor care permit trupelor să vadă o imagine operațională comună (COP), astfel încât comandanții SUA și cei aliați să vadă aceeași situație pe monitoarele lor.*

❖ *Securizarea rețelelor digitale pentru a apela la focul artileriei, conectând observatorii și radarele cu armele în sine”.* (Freedberg Jr., 2015).

Utilizarea tehnologiilor specifice sistemelor de comunicații și informatică poate fi îngreunată de diferite aspecte, precum protocoalele, măsurile de securitate, lățimea de bandă și interoperabilitatea echipamentelor, astfel că *„un corp trebuie să fie sprijinit, în orice moment, de o brigadă de comunicații, cu elemente multinaționale atașate să lucreze cu provocările de interoperabilitate (…). Pe măsură ce arhitecturile de comunicații continuă să se dezvolte în ritm alert, merită, de asemenea, reiterat faptul că cele mai eficiente capabilități ale multor state membre vor depinde de sisteme care, din motive de securitate, nu pot fi aliniate cu STANAG-urile NATO”.* (Watling, Farland, 2021, p. 2). Acordurile de standardizare și interoperabilitate, se arată în aceeași lucrare, presupun numeroase *„eforturi de integrare și protecție a rețelei, care sunt posibile numai cu participarea activă a tuturor membrilor cheie ai echipei corpului”* (Ib.).

Utilizarea tehnologiilor specifice sistemelor de comunicații și informatică poate fi îngreunată de diferite aspecte, precum protocoalele, măsurile de securitate, lățimea de bandă și interoperabilitatea echipamentelor, astfel că „un corp trebuie să fie sprijinit, în orice moment, de o brigadă de comunicații, cu elemente multinaționale atașate să lucreze cu provocările de interoperabilitate.”.

Cele mai importante atacuri care pot fi executate asupra sistemelor de comunicații și informatică sunt:

- *atacuri COMPUSEC*, care pot duce la: indisponibilitatea unor servicii; accesul neautorizat la informații clasificate stocate,

procesate și transmise prin SIC; accesul neautorizat la informațiile de management; copierea și sustragerea/furtul unor informații senzitive; blocarea completă a unor centre de comunicații și informatică;

- *atacuri COMSEC*, materializate prin acțiuni de criptanaliză sau atacuri *TEMPEST* (Turcu, 2014, pp. 17-18).

Componentele COMSEC din *figura 4* presupun:

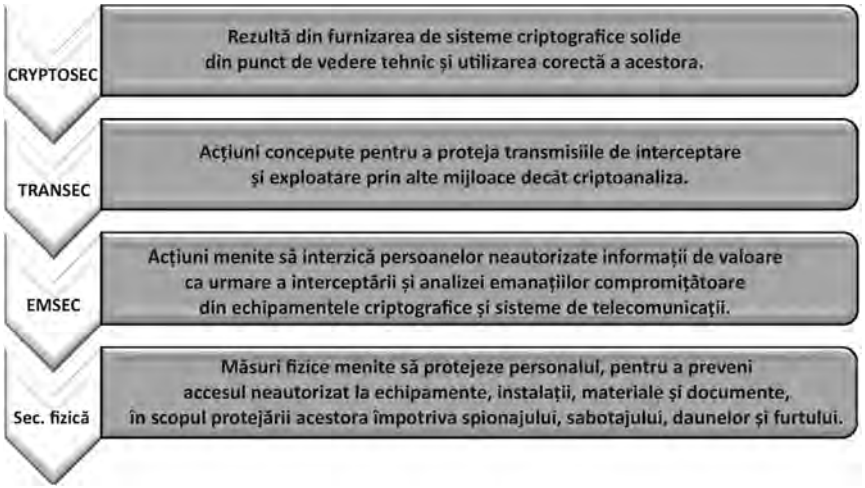

Figura 4: Componentele COMSEC (ATP 6-02.75, 2020, p. 1_1)

Securitatea calculatoarelor – COMPUSEC presupune aplicarea unor măsuri de securitate hardware, software și firmware pentru a preveni divulgarea, modificarea sau ștergerea neautorizată a informațiilor sau invalidarea neautorizată a unor funcțiuni din rețelele de calculatoare. COMPUSEC cuprinde *„ansamblul de măsuri și controale care asigură autenticitatea, confidențialitatea, integritatea, disponibilitatea și nerepudierea informației procesate și memorate în calculatoare (servere și stații de lucru)”* (Alexandrescu, C., Alexandrescu, G., Boaru, 2010, p. 256). Informațiile transmise prin sisteme de comunicații și/sau informatică sunt vulnerabile la interceptări și exploatări tehnice ale adversarului. De asemenea, *„comunicațiile sunt o componentă deosebit de importantă a sistemului*

informațional militar și, implicit, securitatea acestora are importanță funcțională de excepție, prin urmare măsurile de protecție trebuie să fie adecvate, oportune și eficiente și cu mare valoare informațională” (Boaru, Iorga, p. 77). Contracararea acțiunilor adversarului necesită protejarea informațiilor pe timpul transmiterii și recepționării acestora. Transmiterea informațiilor la nivelul marilor unități și unități tactice se realizează prin infrastructura sistemelor de comunicații și informatică. NATO, pentru nivelul unui corp/divizie, are nevoie de sprijinul unei brigăzi/batalion de comunicații și informatică, alcătuit din elemente de la mai multe forțe aliate. În acest sens, considerăm că trebuie acordată o atenție specială aspectelor referitoare la interoperabilitate, standardizare și securitate. Informațiile trebuie să circule fără întreruperi și în siguranță, pe orizontală și verticală, iar eforturile de integrare și securitate a rețelelor sunt posibile numai cu participarea activă a tuturor membrilor Alianței Nord-Atlantice.

CONCLUZII

După Războiul Rece, conflictele care au avut loc nu au pus în dificultate comunicațiile HF, VHF și UHF ale Alianței Nord-Atlantice. Activitățile de război electronic au fost reduse sau nu au existat deloc, însă aceste condiții se schimbă într-un conflict potențial ce opune forțe aproximativ egale. În aceste condiții, războiul electronic va avea un rol mult mai mare, iar comunicațiile militare vor fi nesigure sau chiar întrerupte.

În funcție de teren, starea vremii, adversar etc., sistemele de comunicații și informatică proprii trebuie să fie redundante și reziliente, pentru a asigura securitatea informațiilor. Chiar dacă sistemele de comunicații prin satelit oferă suportul esențial în punctele de comandă, comandanții trebuie să fie pregătiți să conducă operațiile militare și prin comunicații radio sau fir, la nevoie.

Pregătirea utilizatorilor, antrenamentul, cultura de securitate, respectarea măsurilor de securitate sunt necesare în securitatea sistemelor de comunicații și informatice. De asemenea, redundanța este o măsură de rezolvare a unor situații privind COMSEC (atunci când situația o impune), iar gestionarea spectrului de frecvențe este esențială în asigurarea securității comunicațiilor.

În funcție de teren, starea vremii, adversar etc., sistemele de comunicații și informatică proprii trebuie să fie redundante și reziliente, pentru a asigura securitatea informațiilor. Chiar dacă sistemele de comunicații prin satelit oferă suportul esențial în punctele de comandă, comandanții trebuie să fie pregătiți să conducă operațiile militare și prin comunicații radio sau fir, la nevoie.

Pentru o interoperabilitate eficientă în sistemele de comunicații și informatică, ideal ar fi, în opinia noastră, să existe o singură autoritate centrală în NATO, care să permită aplicarea comună a algoritmilor și a cheilor de criptare. Această soluție ar putea asigura comanda și controlul la nivelul Alianței Nord-Atlantice, însă ar reprezenta, totodată, o provocare pentru implementarea și asigurarea securității în sistemele naționale de comunicații și informatică.

BIBLIOGRAFIE:

1. ADP 3.0 – *OPERATIONS* (31 iulie 2019). Department of the Army. Washington, D.C.
2. AJP-6, *Allied Joint Doctrine for Communication and Information Systems* (februarie 2017). Edition A, Version 1.
3. Alexandrescu, C., Alexandrescu, G., Boaru, G. (2010). *Sisteme informaționale militare – servicii și tehnologie.* București: Editura Universității Naționale de Apărare *„Carol I”*.
4. ATP 6-02.75 (mai 2020). *Techniques for communications security*. Headquarters. Departament of the Army. Washington.
5. ATP 6-02.71 (aprilie 2019) *Techniques for department of defense information network operations*. Department of the Army. Washington, D.C.
6. Boaru, Gh., Iorga, I.M. (2018). *Securitatea sistemelor informaționale militare*. București: Editura Universității Naționale de Apărare *„Carol I”*.
7. *Carta albă a apărării* (2021). București: Ministerul Apărării Naționale.
8. FM 6.02 (septembrie 2019). *Signal Support to Operations*. Department of the Army. Washington, D.C.
9. JP 6-0 (octombrie 2019). *Joint Communications System*.
10. JP 3-12 (2018). *Cyberspace Operations*.
11. Munteanu, A., Păuna, A., Constantinescu, C., Măgdălinoiu, G., Voinea, I., Găbudeanu, L., Anghel, T. (2021). *Ghidul practic pentru OSE – Implementarea măsurilor minime de asigurare a securității rețelelor și sistemelor informatice*. Editura Sitech.
12. Ordonanța de Urgență nr. 104 din 22 septembrie 2021, publicată în *Monitorul Oficial* nr. 918 din 24 septembrie 2021.
13. SNApT/*Strategia Națională de Apărare a Țării pentru perioada 2020-2024 – „Împreună, pentru o Românie sigură și prosperă într-o lume marcată de noi provocări”* (2020). București: Administrația prezidențială.
14. Turcu, D. (2014). *Securitarea Informațiilor*. București: Editura Universității Naționale de Apărare *„Carol I”*.
15. Wade, N.M. 2019). CYBER 1 – *The Cyberspace Operations & Electronic Warfare SMART book*. SUA: FL, The Lightning Press, Lakeland.

16. Watling, J., Macfarland, S. (ianuarie 2021). *The Future of the NATO Corps*. Royal United Services Institute for Defence and Security Studies (RUSI).
17. Wolfers, A. (decembrie 1952). *National Security as an Ambiguous Symbol*, p. 485, în *Political Science Quarterly*, vol. 67, nr. 4.
18. https://breakingdefense.com/2015/09/upgraded-radios-networks-needed-for-russian-challenge-troops-fine-lt-gen-hodges/, accesat la 17 iunie 2023.
19. https://sgg.gov.ro/1/wp-content/uploads/2021/03/CARTA-ALBA-A-APARARII-.pdf, accesat la 21 mai 2023.