# SECURITATEA INFORMAȚIILOR ȘI A SISTEMELOR INFORMAȚIONALE MILITARE

*Colonel (rtr.) prof. univ. dr. Gheorghe BOARU*

*Membru titular al Academiei de Ştiinţe ale Securităţii Naţionale,*
*Membru titular al Academiei Oamenilor de Știință din România*

*Colonel dr. Iulian Marius IORGA*

*Ministerul Apărării Naționale*

*În abordarea domeniului securității informațiilor și a sistemelor informaționale militare s-a plecat de la realitatea faptului că România este membră a NATO și că, în acțiunile militare comune, utilizează sisteme informaționale care trebuie să fie compatibile și interoperabile, dar și protejate.*

*Din punct de vedere informaţional, în acţiunile militare se duce o luptă pentru informaţie, prin intermediul informaţiei și împotriva informaţiei și, de aceea, securitatea acesteia este o activitate specială, îndeosebi privind informaţiile clasificate.*

*Țările membre ale Alianţei, implicit România, trebuie să asigure, individual sau prin acorduri de cooperare bilaterale, resursele informaţionale protejate, atât ca proces, cât și ca sistem, necesare pentru îndeplinirea obiectivelor operaţiilor întrunite sub comandă NATO.*

*Foarte multe dintre ameninţările informaţionale vin prin intermediul spațiului virtual. În acest sens, se consideră că securizarea spaţiului virtual a devenit una dintre provocările de securitate cele mai presante ale secolului al XXI-lea.*

*Cuvinte-cheie: informație, sistem informațional, vulnerabilități, amenințări, securitate cibernetică.*

## INTRODUCERE

Pentru îndeplinirea misiunilor de răspuns la noile provocări ale mediului de securitate, Armata României a fost angajată într-un amplu proces de transformare, care a fost stabilit în *Strategia de transformare a Armatei României*[1].

În acest sens, până în 2025, procesul de transformare a fost planificat a se desfașura parcurgând urmatoarele trei faze[2]:

- cea a **restructurării de bază** (2005-2007);
- cea a **integrării operaționale în NATO și în UE** (2008-2015);
- cea a **integrării tehnice depline în NATO și în UE** (2016-2025).

Cea de-a treia fază va asigura îndeplinirea obiectivelor de transformare pe termen lung: eforturile și resursele financiare și umane vor fi concentrate pentru asigurarea capabilităților asumate și incluse în țintele de capabilități și participarea la NATO și UE – conducerea misiunilor și operațiilor; continuarea activității de îmbunatățire și înzestrare cu echipamente noi și atingerea nivelului de interoperabilitate cu forțele armate ale altor națiuni ale UE și ale NATO etc.

*Obiectivul de bază al procesului de transformare îl constituie ajustarea structurii Forțelor Armate Române la mediul de securitate prezent și viitor, pentru a putea îndeplini angajamentele naționale față de Alianță, în concordanță cu procesele și fenomenele din planul de transformare al NATO.*

În acest context, obiectivul de bază al procesului de transformare îl constituie ajustarea structurii Forțelor Armate Române la mediul de securitate prezent și viitor, pentru a putea îndeplini angajamentele naționale față de Alianță, în concordanță cu procesele și fenomenele din planul de transformare al NATO. Scopul este de a face Forțele Armate Române capabile să participe la întregul spectru de misiuni desfășurate de Alianță și UE.

Considerăm că acesta este contextul legal în care Armata României poate desfăşura acţiuni militare, acțiuni în care procesele de comandă și control au la bază procesele informaționale specifice.

---

[1] *Strategia de transformare a Armatei României*, Bucureşti, 2007.

[2] Vezi https://fcnap.ro/transformarea-fortelor-armate-ale-romaniei-un-raspuns-direct-la-noile-provocari-ale-mediului-de-securitate/, accesat la 20 februarie 2020.

## INFORMAȚIA MILITARA ȘI SECURITATEA ACESTEIA

Este cunoscut faptul că o asigurare informaţională temeinică poate determina un proces de comandă și de control eficient.

În armata noastră, *sprijinul cu informaţii al operaţiilor* este bine reglementat, constituind o *„formă de bază a asigurării acţiunilor și a protecţiei forţelor și reprezintă ansamblul de măsuri și de acțiuni, desfășurate continuu și într-o concepție unitară, de către toate forțele participante și la toate eșaloanele pentru planificarea, obținerea, verificarea, procesarea și valorificarea datelor și a informațiilor referitoare la factorii de situație”*[3].

*În armata noastră, sprijinul cu informaţii al operaţiilor este bine reglementat, constituind o „formă de bază a asigurării acţiunilor și a protecţiei forţelor și reprezintă ansamblul de măsuri și de acţiuni, desfăşurate continuu şi într-o concepţie unitară, de către toate forţele participante și la toate eşaloanele pentru planificarea, obţinerea, verificarea, procesarea şi valorificarea datelor şi a informaţiilor referitoare la factorii de situaţie”.*

În literatura de specialitate, informația este abordată atât ca *„o armă puternică, precum și ca o țintă preferată”*[4] sau se afirmă că *„informația poate fi cea mai de temut armă în cadrul evoluțiilor tehnologice din spațiul de luptă”*[5].

Dacă aceste informații sunt corelate cu alte informații deja cunoscute și dacă sunt analizate în corelație cu experiențe trecute (colaționare și procesare), ele vor da naștere la un nou set de semnificații cu o altă valoare informativă, un proces denumit *„intelligence”.*

Studiind relația dintre date, informații și intelligence, putem concluziona că informațiile procesate sunt transformate în produse de intelligence, care se obțin în urma unui proces structurat, denumit, în doctrinele NATO sau în cele ale unor state aliate, *ciclu de intelligence.*

Apreciem că, în cazul operațiilor întrunite multinaționale desfășurate de NATO, *„intelligence”* nu înseamnă *„informații”,* ci reprezintă un proces complex, prin care se determină intențiile și cursul cel mai probabil de acțiune al inamicului.

În cadrul sistemelor și proceselor de bază implicate în planificarea operației întrunite multinaționale – *intelligence* poate avea atributul de[6]: funcțiune de luptă; capabilitate de luptă; ciclu; proces și sistem.

---

[3] I.P.S.- 3.1, *Manualul privind procedurile de informaţii militare pentru sprijinul operaţiilor*, Statul Major General, București, 2006, p. 14.

[4] *Corner stones of Information Warfare,* Department of the Air Force, Washington D.C., 1995, p. 2.

[5] Peter Grier, *„Information Warfare”*, în *Air Force Magazine*, nr. 3, martie 1995, p. 23.

[6] Colonel (r.) prof. univ. dr. Gheorghe Boaru, colonel drd. Iulian-Marius Iorga, *Ciclul informațional ca proces, procesul și ciclul „intelligence” – în cadrul acțiunilor militare moderne,* în *Revista de Științe Militare*, editată de Academia Oamenilor de Știință din România, nr. 1, 2017, pp. 84-85.

În analiza procesului de intelligence, am luat ca sistem de referință *Doctrina NATO pentru intelligence*[7], pentru că la aceasta au fost raportate aspectele de intelligence analizate din activitatea unor forțe NATO, a unor forțe armate ale unor state aliate, precum și a doctrinelor de intelligence ale acestora[8].

Pentru realizarea cerințelor de intelligence, sunt necesare structuri de intelligence adaptate noilor realități ale mediului operațional, bazate pe o pregătire care să le permită abordarea cu succes a provocărilor legate de aplicarea noilor concepte aliate: *„hybrid operations", „comprehensive approach", „information sharing", „need to know vs. need to share".*

*Pentru realizarea cerințelor de intelligence, sunt necesare structuri de intelligence adaptate noilor realități ale mediului operațional, bazate pe o pregătire care să le permită abordarea cu succes a provocărilor legate de aplicarea noilor concepte aliate: „hybrid operations", „comprehensive approach", „information sharing", „need to know vs. need to share".*

Conform opiniei unor specialiști militari români[9], în armatele statelor membre ale NATO, pentru integrarea activităților de informații/ intelligence sub o denumire unică, este standardizat conceptul ISTAR (**I**ntelligence, **S**upraveghere, **A**chiziția **Ț**intelor și **R**ecunoaștere). Aceiași autori precizează, totodată, că se mai folosesc diferite variante ale acronimului ISTAR, cum ar fi: STAR, RSTA, STA, ISR, numai pentru evidențierea unor activități informaționale parțiale.

În Armata României, conform *Doctrinei pentru Informații, Contrainformații și Securitate a Armatei*, conceptul ISTAR[10] a fost acceptat și integrat, în normele specifice naționale, ca o *„soluție de natură organizatorică, menită să integreze funcțional totalitatea capabilităților de colectare disponibile, definite normativ, în condițiile utilizării unui ansamblu de acțiuni, de procedee, de măsuri și de resurse (tehnice, umane, financiare etc.)"*[11]. Acest concept a fost proiectat normativ pentru a asigura *legătura dintre culegerea, procesarea și diseminarea datelor și informațiilor în vederea sprijinirii comandantului pentru atingerea obiectivelor operaționale din spectrul de conflict*[12].

---

[7] AJP-2, *Doctrina Aliată pentru informații, contrainformații și securitate,* 2003.

[8] Doctrina pentru sprijinul cu informații al operațiilor întrunite (a Forțelor Armate ale României, n.a.), 2003; Doctrina pentru intelligence în operațiile întrunite (a Forțelor Armate ale Canadei, n.a.), 2003; JDP 2-00, Înțelegerea și sprijinul de intelligence în operațiile întrunite (a Forțelor Armate ale Marii Britanii, n.a.), 2011; JP-2, Intelligence în operațiile întrunite (a Forțelor Armate ale Statelor Unite ale Americii, n.a.), 2007.

[9] Constantin Alexandrescu, Gelu Alexandrescu, Gheorghe Boaru, *Sisteme informaționale militare – servicii și tehnologie*, Editura Universității Naționale de Apărare *„Carol I"*, București, 2010, pp. 24-25.

[10] *Ibidem.*

[11] *Doctrina pentru Informații, Contrainformații și Securitate a Armatei*, București, 2005, p. 34.

[12] *Ibidem*, p. 35.

Faptul că există o astfel de capabilitate normativă și de execuție în domeniul informațiilor militare, la nivelul Armatei României, demonstrează faptul că esența concepției de integrare a eforturilor de sprijin informativ este aceea de utilizare, într-un mediu integrat, a tuturor posibilităților oferite pentru acest domeniu, permițând, astfel, integrarea mediului procedural românesc cu cel al altor state membre ale NATO.

În acest context normativ informațional, securitatea informațiilor și a sistemelor informaționale militare este obligatorie, deci necesită cunoaștere și preocupare pentru acest domeniu, precum și stabilirea celor mai eficiente măsuri.

*Armatele moderne acordă problematicii securității informației o atenţie deosebită, considerând-o ca pe un obiectiv primordial pentru câştigarea bătăliei informaţionale, al cărei fundament este reprezentat de introducerea, pe scară extinsă, a tehnologiei informaţiei şi a mijloacelor moderne de comunicaţii şi informatică, pe întregul spaţiu de luptă.*

Din aceste motive, considerăm că este justificată preocuparea ofițerilor de stat major de a cunoaște și de a aborda problematica securității informației, în contextul apartenenței României la NATO și în perspectiva adaptării și transformării unor abordări doctrinare și acționale românești, conform cerințelor Alianței.

Armatele moderne acordă acestei problematici o atenție deosebită, considerând-o ca pe un obiectiv primordial pentru câștigarea bătăliei informaționale, al cărei fundament este reprezentat de introducerea, pe scară extinsă, a tehnologiei informației și a mijloacelor moderne de comunicații și informatică, pe întregul spațiu de luptă.

Apreciem că deosebit de importante sunt și aspectele legate de informațiile clasificate, cele care necesită protecția împotriva dezvăluirii neautorizate și care poartă identificatori specifici în acest sens, precum și informațiile neclasificate care nu sunt destinate publicului și care sunt protejate prin măsuri interne specifice fiecărei organizații, dar și informațiile de interes public, respectiv acele informații care privesc sau rezultă din activitățile unei autorități publice sau instituții publice.

De asemenea, în regulamentele și în manualele militare ale NATO şi ale armatelor aliate sunt prezentate măsurile pentru protecţia informaţiilor împotriva pericolelor și ameninţărilor specifice erei informaţionale.

În concordanţă cu *Legea nr. 182/2002*, a fost elaborată și *Hotărârea de Guvern nr. 585/2002* privind Standardele naţionale de protecţie a informaţiilor clasificate. Totodată, au fost stabilite nivelurile de echivalență a informaţiilor clasificate din România cu cele din NATO și/sau UE, așa după cu se prezintă în *tabelul nr. 1*.

*Tabelul nr. 1*

**Echivalența nivelurilor de clasificare ROMÂNIA – NATO – UE[13]**

| Informații clasificate – România | | Informații clasificate – NATO | Informații clasificate – UE |
|---|---|---|---|
| Secret de stat | Strict secret de importanță deosebită/ SSID | NATO TOP SECRET/ NTS | TRÈS SECRET UE/TSUE |
| | Strict secret/SS | NATO SECRET/NS | SECRET UE/SUE |
| | Secret/S | NATO CONFIDENTIAL/ NC | CONFIDENTIEL UE/ CUE |
| Secret de serviciu/SSv | | NATO RESTRICTED/NR | RESTREINT UE/RUE |

Asigurarea securității informațiilor NATO[14] se realizează conform *Legii nr. 423/2004*, iar prin *Hotărârea de Guvern nr. 353/2002* sunt stabilite Normele privind protecția informațiilor clasificate ale Organizației Tratatului Atlanticului de Nord în România.

În acest context, am considerat că securitatea informației este un domeniu de activitate a cărui importanță este în continuă creștere și care trebuie abordat din toate unghiurile posibile, începând de la concepte, vulnerabilități, riscuri și management.

## SECURITATEA SISTEMELOR INFORMAȚIONALE MILITARE

Organizațiile militare utilizează sisteme informaționale care, cu cât sunt mai complexe, cu atât au nevoie de o cantitate mai mare de informație pentru funcționarea lor. De aceea, componenta informațională a oricărui sistem este în continuă creștere și diversificare, iar lipsa de informații determină însăși dispariția acestuia.

Rezultă așadar că sistemele informaționale trebuie să fie proiectate și realizate, astfel încât să fie eficiente, iar securitatea acestora să fie asigurată în orice situație. Doar în acest fel se pot asigura siguranța, veridicitatea și oportunitatea informațiilor necesare procesului de comandă și de control, ca element fundamental al acțiunilor militare.

*Organizațiile militare utilizează sisteme informaționale care, cu cât sunt mai complexe, cu atât au nevoie de o cantitate mai mare de informație pentru funcționarea lor. De aceea, componenta informațională a oricărui sistem este în continuă creștere și diversificare, iar lipsa de informații determină însăși dispariția acestuia.*

[13] Iulian Marius Iorga, *Securitatea informațiilor în acțiunile militare moderne*, Editura Universității Naționale de Apărare *„Carol I”*, București, 2018, p. 93.

[14] *Legea nr. 423/2004 privind Aderarea României la Acordul dintre părțile la Tratatul Atlanticului de Nord pentru securitatea informațiilor*, adoptată la Bruxelles, la 6 martie 1997.

Ca element specific domeniului militar, importanţa sistemelor informaţionale creşte continuu, ele realizând simbioza cu procesele de comandă și de control, funcţionând integrat şi dând o calitate superioară conducerii acţiunilor organizate şi/sau desfăşurate.

Activităţile de comandă și de control, specifice domeniului militar, dar, în mod special, desfăşurarea efectivă a acţiunilor militare, capacitatea entităţii militare de a efectua cu succes o misiune sunt influenţate de nevoile de date şi de informaţii, precum şi de capabilităţile de obţinere a avantajului informaţional, determinat de capacităţile informaţionale la dispoziţie și de securitatea sistemului informaţional-decizional.

*Ca element specific domeniului militar, importanţa sistemelor informaţionale creşte continuu, ele realizând simbioza cu procesele de comandă și de control, funcționând integrat și dând o calitate superioară conducerii acţiunilor organizate și/sau desfăşurate.*

**Conceptul de sistem informațional** a fost studiat de specialiști din diferite domenii de activitate, atât din punctul de vedere al structurii, cât și al funcționării acestuia, însă nu s-a ajuns la o definiție unică.

Structura sistemului informațional este dependentă de destinația acestuia, de complexitatea și de distribuirea spațială a elementelor structurii de comandă și de control deservite, precum și de obiectivele și de procesele acesteia.

Au fost studiate diferite categorii de sisteme informaționale, cum ar fi cele de securitate și de apărare națională, tehnice, sociale, economice etc., între care există deosebiri importante și care au elemente de structură comune, dar și elemente specifice, care constituie diferența.

Putem considera că structura constituie componenta organizatorică ce definește concepția sistemică și permite configurarea unui sistem informațional din module (subsisteme). Acest lucru se poate face prin identificarea, gruparea, dispunerea și interconectarea optimă a elementelor de infrastructură și de management, ținând cont și de resursele tehnice, de bazele de date, de componentele software și, neapărat, de elementele de securitate.

O temeinică asigurare informațională a structurilor organizatorice, la care comanda și controlul și activitățile operaționale (de execuție) sunt bine conturate, poate constitui o premisă favorabilă pentru succesul misiunii.

În organizația militară, structura sistemului informațional este determinată și depinde esențial de structura sistemului de comandă și de control. Între cele două structuri, există o interdependență reciprocă, biunivocă.

Studiind și analizând mai multe **definiții ale sistemului informațional**[15], prezentate în lucrări de specialitate militare și/sau civile, românești și/sau străine, am constatat că toate au la bază elemente de structură, tehnice, funcționale și de management specific domeniului abordat.

Prezentăm cinci dintre cele mai semnificative definiții menționate în literatura de specialitate, la care am făcut referire mai înainte, în care sistemul informațional:

1. *„este un sistem de persoane, de înregistrări de date și activități privind prelucrarea datelor și a informațiilor în cadrul unei organizații, incluzând procese de prelucrare manuală sau automată a acestora. Tehnologia informației constituie o componentă principală a sistemului informațional”*[16];

2. *„reprezintă ansamblul integrat de componente pentru colectarea, memorarea, prelucrarea și comunicarea informației. Elementele sale principale sunt: calculatoarele (hardware), produsele software, bazele de date, sistemele de comunicații, resursele umane și procedurile”*[17];

3. *„reprezintă un ansamblu de echipamente, de metode și de proceduri și, dacă este necesar, personal, organizat pentru îndeplinirea funcțiilor de prelucrare a informațiilor”*[18];

4. *„cuprinde întreaga infrastructură, circuite și fluxuri informaționale, organizate într-o concepție unitară, personalul, toate componentele care culeg, transmit, stochează, prelucrează, elaborează/procesează informații și asigură afișarea și diseminarea acestora, în vederea valorificării în procesul de conducere (comandă și control) și în desfășurarea acțiunilor militare”*[19];

5. *„cuprinde întreaga infrastructură, organizare, personal și componente destinate culegerii, prelucrării, memorării, transmiterii, afișării, diseminării și acționării asupra informațiilor”*[20].

*Sistemul informaţional „cuprinde întreaga infrastructură, organizare, personal şi componente destinate culegerii, prelucrării, memorării, transmiterii, afişării, diseminării şi acţionării asupra informaţiilor”.*

---

[15] Gheorghe Boaru, Iulian Marius Iorga, *Securitatea sistemelor informaționale militare*, Editura Universității Naționale de Apărare *„Carol I”*, București, 2018.

[16] *Information Systems*, Wikipedia, the free encyclopedia, http:/en.wikipedia.org/wiki/Information Systems, accesat la 12 ianuarie 2020.

[17] *Britannica Encyclopaedia*, http://www.britannica.com/EBchecked/topic/287895/Information Systems, accesat la 12 ianuarie 2020.

[18] AAP6 (2008), *NATO Glossary of Terms and Definitions*, 2008, p. 2-I-4.

[19] FM 101-5-1, *Termeni şi simboluri operaţionale*, Statul Major al Trupelor de Uscat, SUA.

[20] U.S. Army Field Manual 100-6, *Information Operations*, 1996; JP-02, DoD Dictionary Military Terms, 2008, p. 261.

Raportându-se la **sistemul informațional managerial** *(MIS – Management Information System)*, centrat pe obiective manageriale, o abordare interesantă o au și următoarele două definiții:

1. *„sistemul informațional managerial (MIS) este constituit din ansamblul datelor, informațiilor, fluxurilor și circuitelor informaționale, procedurilor și mijloacelor de tratare a informațiilor, menite să contribuie la stabilirea și realizarea obiectivelor organizației”*[21].

2. MIS este definit ca o *„combinație de resurse umane și informatice care urmăresc colectarea, stocarea, organizarea, apelarea, comunicarea, distribuirea și utilizarea datelor și a informațiilor pe care le folosesc managerii în exercitarea funcțiilor de conducere, în scopul realizării unui management eficient. Aceste sisteme oferă acces direct, online la informațiile relevante memorate, interfață prietenoasă, într-un dialog ușor de exploatat”*[22].

*Sistemul informațional managerial este definit ca o „combinație de resurse umane și informatice care urmăresc colectarea, stocarea, organizarea, apelarea, comunicarea, distribuirea și utilizarea datelor și a informațiilor pe care le folosesc managerii în exercitarea funcțiilor de conducere, în scopul realizării unui management eficient”.*

Din analiza acestor definiții, rezultă că sunt evidențiate atât componente esențiale, cât și anumite caracteristici ale sistemului informațional, fiecare dintre acestea necesitând însă, în opinia noastră, anumite adăugări, precizări și actualizări.

Trei specialiști în domeniu, din Universitatea Națională de Apărare *„Carol I”*, ținând seamă de realizările actuale în domeniu și sintetizând opiniile diferiților specialiști, au formulat următoarea definiție generală: *„sistemul informațional reprezintă ansamblul integrat al datelor, al informațiilor și al cunoștințelor necesare organizației, gestionate cu precădere în format electronic, împreună cu infrastructura informațională...”*[23].

În accepțiunea acelorași autori, spre deosebire de alte opinii, în infrastructura informațională sunt incluși, pe lângă *tehnologia informației și a comunicațiilor*, *specialiștii în domeniu*, precum și *structura de management a informațiilor.*

---

[21] Ovidiu Nicolescu şi alţii, *Sistemul informaţional managerial al organizaţiei*, Editura Economică, București, 2001, p. 25.

[22] Club IT&C, *Cum să exploatezi informația în mod intelligent. Management Information Systems*, Club IT&C, Cum să exploatezi informația în mod inteligent-Management Information Systems, [https://www.google.ro/Club+IT%26C, +Cum+s%C4%83+exploatezi+informa%C5%A3ia +%C3%AEn+mod+inteligent-Management+Information+ Systems&tbm...], accesat la 1 februarie 2020.

[23] Constantin Alexandrescu, Gelu Alexandrescu, Gheorghe Boaru, *Sisteme informaționale – fundamente teoretice*, Editura Universităţii Naţionale de Apărare *„Carol I”*, Bucureşti, 2009, pp. 194-195.

În aceeași abordare, se are în vedere ca sistemul informațional să asigure datele și informațiile necesare procesului de comandă și de control, în scopul realizării optime a obiectivului sau a misiunii stabilite și obținerii de *avantaje competitive*[24]. *Avantajul competitiv* constituie o sinteză a masei critice a avantajelor relative din domeniile: informațional, cunoștințelor, înțelegerii și luării deciziilor (comandă și control), incluzând, de asemenea, calitățile morale și de conducere.

Concret, *sistemul informaţional militar*[25] este un sistem mare, dinamic, complex, compus din mai multe sisteme (care, ierarhic, sunt subsisteme) interdependente, care trebuie singularizate, cu grad ridicat de automatizare şi autoreglare, conduse centralizat. Este, de fapt, un supersistem (federaţie de sisteme), care cuprinde un ansamblu omogen de reţele interconectate, împreună cu elementele lor integrate pentru management, având intrările, structura internă și ieşirile necesare, fiind caracterizat printr-un grad mare de autonomie şi eterogenitate.

*Sistemul informaţional militar este un sistem mare, dinamic, complex, compus din mai multe sisteme interdependente, care trebuie singularizate, cu grad ridicat de automatizare şi autoreglare, conduse centralizat.*

Sistemele C4ISR/C5ISR-D presupun furnizarea de informaţii şi cunoştinţe factorilor de decizie politico-militari pentru a asigura o conştientizare situaţională superioară. Având în vedere că operaţiile militare se vor desfăşura cu o mai mare precizie decât oricând, eficacitatea unei misiuni va depinde tot mai mult de sistemele C4ISR/C5ISR-D, care sunt reţele complexe de subsisteme.

Sistemul informaţional militar reprezintă latura dinamică a sistemului de comandă și de control (management) din care face parte, care asigură luarea optimă a deciziei, funcţionarea și coeziunea acestuia, din care cauză, în unele lucrări de specialitate, este denumit sistem informaţional-decizional sau, în literatura occidentală, *sistem informaţional managerial*[26].

*„Sistemul informaţional-decizional reprezintă un sistem cibernetic, organizat piramidal, în fluxuri reciproce, verticale şi orizontale, pe baza unui mecanism unitar de culegere și prelucrare a informaţiilor, de la cel mai mic nivel ierarhic până la cel mai mare, care permite fundamentarea,*

[24] D. Albert, J. Garstka, R. Hayes, D. Signori, *Understanding Information Age Warfare,* Washington DC, CCRP-Data publication, august 2001, p. 41.

[25] W.J. Karplus, *Sisteme de calculatoare cu divizarea timpului*, EdituraTehnică, Bucureşti, 1970, p. 227.

[26] Constantin Alexandrescu, Gelu Alexandrescu, Gheorghe Boaru, *op. cit.,* p. 195.

*adoptarea şi urmărirea îndeplinirii deciziilor. Prin acest sistem se asigură implementarea pachetului de decizii şi urmărirea efectelor aplicării acestuia pentru îndeplinirea obiectivelor organizaţiei"*[27].

Sistemul informaţional nu conţine numai elemente tehnice, ci este constituit ca un ansamblu complex de oameni specializaţi, precum şi activităţi practice, echipamente tehnice de culegere a informaţiilor (inclusiv prin senzori), comunicaţii, memorare, prelucrare și afișare a informaţiilor, software, baze de date şi proceduri, orientate către identificarea necesităţilor de informaţii şi a modalităţilor de satisfacere a lor, pentru asigurarea informaţională a proceselor de conducere (comandă şi control), inclusiv transmiterea deciziilor către nivelurile operaţionale (eşaloanele) subordonate.

*În sistemul informațional intră informațiile de stare provenind de la organele de execuție, surse diferite de informații, sisteme de senzori, elemente cu care se cooperează sau colaborează și ies informațiile de comandă produse de organele de comandă.*

Într-o altă abordare, *„Sistemul informaţional este liantul dintre sistemul de comandă și de control şi sistemul operaţional (de execuţie), care contribuie la simbioza (apropierea) acestora, întărirea disciplinei și creşterea răspunderii asupra activităţilor desfăşurate. El nu trebuie considerat doar o interfaţă între aceste sisteme, ci și un element de legătură între mediul informaţional intern al organizaţiei (structurii militare) și cel extern acesteia prin care se obţine cvasitotalitatea datelor şi a informaţiilor necesare"*[28].

În sistemul informațional intră informațiile de stare (rapoarte, informări, propuneri, sinteze, înștiințări...) provenind de la organele de execuție, surse diferite de informații, sisteme de senzori, elemente cu care se cooperează sau colaborează și ies informațiile de comandă (ordine, dispoziții, comenzi, precizări, indicații, orientări...) produse de organele de comandă.

Privind rolul sistemului informaţional, analizat în strânsă corelaţie cu locul acestuia în cadrul organizaţiei (structurii militare), putem aprecia că acesta constă în:

- determinarea volumelor de date, de informaţii şi de cunoştinţe necesare, astfel încât procesele decizionale și de execuţie ale structurii militare să aibă o desfăşurare optimă;
- să permită stabilirea surselor care pot procura informaţiile;

[27] Ion Ciobanu, Gheorghe Ilie, Aurel Nour, *Confruntarea informaţională şi protecţia informaţiilor*, Editura Detectiv, Bucureşti, 2006, p. 71.

[28] Vasile Dumitru şi alţii, *Sisteme informaţionale militare*, Editura CERES, Bucureşti, 2000, p. 38.

- să se stabilească mijloacele tehnice, care să asigure circulația fluxurilor informaționale și a mijloacelor informatice pentru prelucrarea informațiilor;
- stabilirea resurselor informaţionale (date, informaţii), a circuitelor şi a fluxurilor informaţionale care trebuie asigurate. *Resursele informaţionale* sunt constituite din informaţii împreună cu personalul, echipamentele tehnice și tehnologia informaţiei;
- asigurarea funcţiilor informaţionale specifice (activităţile de culegere, de transmitere, de memorare, de prelucrare și de diseminare a informaţiilor în mod operativ), necesare pentru comanda, controlul (managementul) și execuţia activităţilor;
- asigurarea parametrilor calitativi necesari informaţiei (obiectivitate, oportunitate, precizie, integritate, relevanţă, autenticitate) pentru sistemele de comandă şi de control ale organizaţiei (structurii militare);
- aplicarea eficientă a politicilor de securitate, care vizează atât informațiile, cât și procesele informaţionale.

Funcţionarea sigură şi neîntreruptă a sistemelor informaţionale, care depinde, în totalitate, de măsurile organizatorice, tehnice și funcţionale adoptate, constituie o necesitate pentru oricare organizaţie (structură militară). Afectarea, chiar şi parţială, a lucrului elementelor de structură şi a echipamentelor acestora (hardware, software) aduce prejudicii informaţionale grave, prin întreruperea sau prin întârzierea proceselor de comandă și de control (management) şi a celor operaţionale (de execuţie).

Utilizarea tehnologiei informaţiei și a comunicaţiilor a creat posibilitatea realizării unor sisteme informaţionale moderne, în care reţelele informatice și comunicaţiile au un rol hotărâtor, dar care prezintă şi vulnerabilităţi semnificative. Totodată, acestea sunt supuse și ameninţărilor informaţionale, din cauza acţiunii unor factori interni, dar, mai ales, externi, care urmăresc limitarea sau întreruperea activităţilor de culegere, de transmitere, de prelucrare și de diseminare a informaţiilor, pentru funcţionarea anormală sau chiar blocarea funcţiilor sistemului.

Foarte multe dintre aceste amenințări vin prin intermediul spațiului virtual. În acest sens, se consideră că *„Securizarea spațiului virtual a devenit una dintre provocările de securitate cele mai presante*

GÂNDIREA MILITARĂ ROMÂNEASCĂ

*Funcţionarea sigură şi neîntreruptă a sistemelor informaţionale, care depinde, în totalitate, de măsurile organizatorice, tehnice și funcţionale adoptate, constituie o necesitate pentru oricare organizaţie (structură militară).*

*Afectarea, chiar şi parţială, a lucrului elementelor de structură şi a echipamentelor acestora (hardware, software) aduce prejudicii informaţionale grave, prin întreruperea sau prin întârzierea proceselor de comandă și de control (management) şi a celor operaţionale (de execuţie).*

*ale secolului al XXI-lea, prin importanța sa pentru viața de zi cu zi, pentru guvern, securitate națională, afaceri și deopotrivă pentru cetățeni. Lumea cibernetică și tehnologiile asociate au creat, pe de o parte, mai multe oportunități sociale, culturale, economice și politice pentru toți, iar pe de altă parte, natura sa fără frontiere a adus cu ea amenințări sub formă de atacuri cibernetice și criminalitate informatică"*[29].

*Conexiunea la internet reprezintă o facilitate, dar creează, de cele mai multe ori, mari probleme de securitate pentru aceste reţele, prin formarea unor breşe, care pot fi accesate în mod neautorizat.*

Întrebările esențiale referitoare la securitatea rețelelor informaționale: *„Cine? Când? De unde? Ce? De ce?"* determină împreună o nouă sintagmă, *„a celor cinci W" (5W – Who, When, Where, What, Why?)*. Cine accesează rețeaua? Când și unde se produce accesul? Ce informații sunt accesate și de ce? Aceste aspecte trebuie monitorizate și securizate, în funcție de importanța informațiilor, de caracterul public sau privat al rețelelor de comunicații și informatice, indiferent de terminalul folosit.

Conexiunea la internet reprezintă o facilitate, dar creează, de cele mai multe ori, mari probleme de securitate pentru aceste reţele, prin formarea unor breşe, care pot fi accesate în mod neautorizat. Scopul serviciilor de securitate în domeniul reţelelor de comunicaţii şi informatice vizează, pe de o parte, menţinerea acestora în funcţiune, iar pe de altă parte, asigurarea securităţii aplicaţiilor, precum și a informaţiilor stocate pe suport sau transmise prin reţea.

*Scopul serviciilor de securitate în domeniul reţelelor de comunicaţii şi informatice vizează, pe de o parte, menţinerea acestora în funcţiune, iar pe de altă parte, asigurarea securităţii aplicaţiilor, precum și a informaţiilor stocate pe suport sau transmise prin reţea.*

Securitatea acestor rețele este asigurată, în primul rând, prin reglementări de nivelul strategiilor și doctrinelor, precum și prin dezvoltarea unei culturi de securitate la nivel național și european.

Considerăm că aceste strategii trebuie să fie aplicate atât la nivel european, cât și la nivel național. Astfel, se apreciază că *„Îmbunătățirea modului în care UE asigură securitate cibernetică este esențială pentru a putea continua asigurarea beneficiilor sociale, economice, financiare și culturale pe care cetățenii și afacerile care provin din internet le obțin și, în sens mai larg, evoluţia tehnologiilor pentru comunicaţii şi informaţii. Mai mult decât atât, este esențial pentru UE de a atinge o biectivele pe care le-a stabilit în Agenda digitală pentru Europa (2010) și, la fel de semnificativă, forța motrice a unei astfel de agende – Strategia Europa 2020"*[30].

---

[29] Colonel (ret.) prof. univ. dr. Gheorghe Boaru, *Război și apărare în spațiul virtual,* în *Revista de Științe Militare*, Academia Oamenilor de Știință din România, nr. 2, 2018, p. 51.

[30] Colonel (ret.) prof. univ. dr. Gheorghe Boaru, *Securitatea cibernetică în Uniunea Europeană,* în *Revista Academiei de Științe ale Securității Naționale*, nr. 2, 2017, p. 71.

În deplin acord cu acțiunile europene, la nivel naţional a fost aprobată, în februarie 2015, *Strategia Națională privind Agenda Digitală pentru România 2020*[31].

Această strategie *„definește patru domenii de acțiune, dintre care amintesc doar primul domeniu, care este: e-Guvernare, Interoperabilitate, Securitate Cibernetică, Cloud Computing și Social Media. Acest document a preluat și adaptat la specificul țării noastre elementele Agendei Digitale pentru Europa. Agenda Digitală definește, astfel, rolul major pe care utilizarea TIC trebuie să-l joace în realizarea obiectivelor Europa 2020”*[32].

Sistemele informaționale militare, de tipul C4I (C4I$^2$,C4ISR, C5ISR,...), un concept de actualitate în teoria și în practica militară europeană și euroatlantică, integrează subsistemele de comandă, pe cele informatice, de comunicații și de informații și se bazează pe doctrine și pe proceduri specifice, pe structuri flexibile, pe echipamente de ultimă generație și, în principal, pe un personal înalt profesionalizat.

*Sistemele informaţionale militare, de tipul C4I (C4I$^2$,C4ISR, C5ISR), un concept de actualitate în teoria şi în practica militară europeană şi euroatlantică, integrează subsistemele de comandă, pe cele informatice, de comunicaţii şi de informaţii şi se bazează pe doctrine şi pe proceduri specifice, pe structuri flexibile, pe echipamente de ultimă generaţie şi, în principal, pe un personal înalt profesionalizat.*

În principiu, orice stat sau organizaţie neguvernamentală cu intenţii ostile poate dispune de resursele financiare şi de capacitatea tehnologică de a ameninţa un sistem C4I. Din cauza costului redus al echipamentelor necesare diverselor forme ale atacului informaţional, comparativ cu fondurile necesare realizării unui sistem de tipul C4I, precum și ca urmare a faptului că majoritatea cunoştinţelor solicitate sunt liber răspândite în lume, ameninţările pot surveni inclusiv din partea grupurilor teroriste sau a hackerilor.

Astfel de atacuri se pot desfășura în scopul dezinformării, spionajului electronic pentru obținerea avantajului competitiv global, modificării clandestine a datelor sensibile din cadrul teatrelor de operații sau pentru alterarea sau întreruperea funcționării unor infrastructuri critice naționale, cum ar fi cele de energie, apă, combustibil, comunicații, bancare sau transport, care sunt esențiale pentru funcționarea societății și economiei: *„În plan militar, acestea pot urmări sabotajul, subversiunea, spionajul sau terorismul și sunt concretizate în exploatarea/provocarea de scurgeri de informații,*

[31] *Strategia Națională privind Agenda Digitală pentru România 2020* a fost aprobată prin Hotărârea de Guvern nr. 245/7 aprilie 2015.

[32] Colonel (ret.) prof. univ. dr. Gheorghe Boaru, *Securitatea cibernetică în Uniunea Europeană*, *op. cit.*, p. 72.

*împiedicarea desfășurării misiunilor, provocarea unor anomalii în cursul de desfășurare al operațiilor”*[33].

În România, cadrul general de cooperare care reunește acele autorități și instituții publice cu responsabilități și competențe în domeniul securității cibernetice este reprezentat de Sistemul Național de Securitate Cibernetică (SNSC). Activitatea SNSC este coordonată la nivel strategic de Consiliul Suprem de Apărare a Țării.

*„Caracteristica comună a confruntărilor din spațiul cibernetic este raportul antagonic continuu stabilit între amenințările care se manifestă în spațiul cibernetic – terorism, spionaj, sabotaj, subversiune și crimă organizată, pe de o parte, și securitatea informațională, pe de altă parte. Aceste amenințări se manifestă într-un mediu foarte larg, oferit de războiul informațional, într-o accentuată interferență conceptuală și acțională între războiul electronic, cel al hackerilor, cel psihologic, economic și într-o tipologie complexă a atacurilor informatice”*[34].

*Specificul amenințărilor la adresa securității cibernetice este dat și de faptul că ele nu sunt limitate de frontiere şi înregistrează o creştere permanentă a frecvenţei şi a gradului de sofisticare, dar şi de apartenenţa universală a spaţiului cibernetic.*

În concluzie, în actuala eră a informaţiei, securitatea tehnologică are o importanţă deosebită şi priveşte, în egală măsură, reţelele de calculatoare *(COMPUSEC)* şi reţelele de comunicaţii *(COMSEC)*.

Considerăm că specificul ameninţărilor la adresa securităţii cibernetice, care au devenit din ce în ce mai serioase în ultimii ani, este dat şi de faptul că ele nu sunt limitate de frontiere şi înregistrează o creştere permanentă a frecvenţei şi a gradului de sofisticare, dar şi de apartenenţa universală a spaţiului cibernetic. Riscurile de securitate pe care le implică atacurile cibernetice şi caracterul global al efectelor lor impun eforturi comune de cooperare internaţională pentru asigurarea securităţii sistemelor informaţionale ale statelor membre ale Alianţei.

*Riscurile de securitate pe care le implică atacurile cibernetice și caracterul global al efectelor lor impun eforturi comune de cooperare internațională pentru asigurarea securității sistemelor informaționale ale statelor membre ale Alianței.*

### ❖ Vulnerabilităţi

Ca în orice domeniu de activitate, și în cel privind informațiile și sistemele informaționale există anumite *vulnerabilități*, adică *„părți slabe și slăbiciuni ale sistemului, infrastructurii, mediului de control sau proiectării rețelelor, care nu sunt generate de acțiunile adversarilor, ci de soluțiile proprii adoptate, ce pot fi atacate relativ ușor și exploatate, pentru a deteriora integritatea acelui sistem”*[35].

---

[33] *Idem, Război și apărare în spațiul virtual*, *op. cit.*, p. 54.
[34] *Ibidem,* pp. 54-55.
[35] *Noul dicționar universal al limbii române*, Editura Litera Internațional, București-Chișinău, 2006, p. 1645.

Din punct de vedere tehnic, vulnerabilitatea este prezentată ca o caracteristică a unui sistem, care îi poate provoca acestuia o degradare precisă (incapacitatea de a-și îndeplini funcțiile proiectate), ca rezultat al faptului de a fi fost obiect al unui nivel precis al efectelor, într-un mediu ostil nenatural.

În cadrul operațiilor informaționale, *vulnerabilitatea* este definită ca o slăbiciune în proiectarea sistemului de securitate a informațiilor, a procedurilor, a implementării sau a controlului intern, care poate fi exploatată pentru a obține accesul neautorizat la informații sau la sistemul informațional. În cadrul sistemelor de comunicații și informatice, vulnerabilitatea este reprezentată de un punct în care un sistem este susceptibil de a fi atacat. Orice sistem informatic sau cu un grad semnificativ de informatizare este vulnerabil la atac.

În cadrul sistemelor informaționale militare, se remarcă ponderea mult crescută a celor specifice computerelor și rețelelor de calculatoare. Această pondere se explică atât prin faptul că, în sistemele informaționale actuale, subsistemul de calculatoare are un rol sistemic integrator, cât și prin faptul că subsistemul de comunicații este, la rândul său, în punctele cele mai importante, informatizat.

*Din punct de vedere tehnic, vulnerabilitatea este prezentată ca o caracteristică a unui sistem, care îi poate provoca acestuia o degradare precisă (incapacitatea de a-şi îndeplini funcţiile proiectate), ca rezultat al faptului de a fi fost obiect al unui nivel precis al efectelor, într-un mediu ostil nenatural.*

În acelaşi timp, trebuie subliniat faptul că atât componentele hardware (staţii de lucru, cablaje de reţea etc.), cât şi cele software principale (sisteme de operare) utilizate sunt de origine civilă, fapt care atrage următoarele inconveniente, din punctul de vedere al securităţii:

- multe dintre acestea sunt la dispoziţia publicului larg, deci caracteristicile lor tehnice sunt cunoscute în detaliu de potenţialul adversar;
- componentele produse special pentru sistemul militar, care, deşi sunt proiectate și realizate în condiţiile de securitate stabilite și monitorizate de acesta, pot fi supuse totuşi acţiunilor spionajului industrial, fenomen caracteristic agresivităţii pieţei libere de înaltă tehnologie şi pieţei IT, în particular;
- componentele respective permit o personalizare redusă, deci rezultatele unui studiu de vulnerabilitate asupra sistemelor civile pot fi aplicate, în mare măsură, şi celor militare;
- există, în proporţie covârşitoare, componente de import sau, în cea mai bună situaţie, produse şi verificate în afara sferei militare, intenţionat şi foarte bine camuflat;

- sistemele militare se bazează pe o componentă logică – cea software –, care poate fi atacată tot cu mijloace logice, deci mijloace care nu necesită tehnologii scumpe, gama acestora diversificându-se continuu şi prin contribuţia infractorilor informaţionali.

Aşadar, se urmăreşte ca tehnologia modernă din sistemele informaţionale să fie combătută tot prin tehnologie avansată, confirmându-se concluzia specialiştilor că, şi în conflictele militare viitoare, cu cât mai mare va fi avantajul obţinut din tehnologia informaţiei și a comunicaţiilor, cu atât va creşte și vulnerabilitatea sa potenţială.

*În ceea ce priveşte domeniul sistemelor de comunicaţii şi informatice, vulnerabilitatea este reprezentată de un punct în care un sistem este susceptibil de a fi atacat. Orice sistem informaţional, care are un grad semnificativ de informatizare, este vulnerabil la o diversitate de forme de atac.*

Se poate trage concluzia că obiectivul principal al conflictelor militare contemporane nu trebuie să se concretizeze, cu precădere, în distrugerea totală a tehnicii, a armamentului sau a forţei vii a adversarului, ci, mai ales, în neutralizarea şi în dezintegrarea sistemelor complexe ale acestuia, în principal a sistemelor informaţionale.

În ceea ce priveşte domeniul sistemelor de comunicaţii şi informatice, vulnerabilitatea este reprezentată de un punct în care un sistem este susceptibil de a fi atacat. Orice sistem informaţional, care are un grad semnificativ de informatizare, este vulnerabil la o diversitate de forme de atac.

Pe lângă vulnerabilităţile specifice, externe, interne, nu sunt de neglijat nici cele de tip *„erori umane”.*

Politicile şi produsele de securitate pot reduce posibilităţile şi probabilitatea ca un atac să penetreze sistemul informatic sau, prin arhitectura de securitate adoptată, pot impune agresorului să investească atât de mult timp şi alte resurse, încât atacul să nu mai fie profitabil.

Specialiştii din întreaga lume sunt în unanimitate de acord că nu există sisteme complet securizate, deci vulnerabilităţile sunt prezente chiar și în cazul celor mai perfecţionate sisteme.

### ❖ Ameninţări

O *amenințare* este un posibil pericol pentru sistem. Pericolul poate fi reprezentat de o persoană (un cracker de sistem), un element material (o componentă de echipament tehnic imperfectă, de exemplu) sau de un eveniment (calamități naturale, incendii etc.), care pot exploata o vulnerabilitate a sistemului.

Ameninţările sunt analizate în relaţie cu evenimentele care pot surveni, ca urmare a activităţii acestora, evenimente denumite atacuri, precum și cu vulnerabilităţile care pot fi exploatate de acestea.

Literatura de specialitate clasifică sursele ameninţărilor după mai multe criterii, prezentate în rândurile care urmează.

După modul de manifestare, sursele ameninţărilor pot fi:

- manifeste sau deschise, la vedere, acestea fiind observabile;
- acoperite, mascate sau conspirate;
- accidentale și naturale.

Ameninţările acoperite sunt: spionajul, sabotajul, actele subversive, terorismul, actele care compun criminalitatea specifică.

*Ameninţările acoperite sunt: spionajul, sabotajul, actele subversive, terorismul, actele care compun criminalitatea specifică.*

Ameninţările la vedere sunt: bruiajul radio, radioreleu, de radiolocaţie sau de radionavigaţie; impulsul electromagnetic (EMP); activităţile SIGINT; operaţiile speciale.

Ameninţările accidentale și naturale sunt clasificate astfel:

- cele naturale: fulgere, inundaţii, cutremure, temperaturi extreme, vânt puternic;
- cele accidentale: erori umane, de software, precum și defecţiuni hardware;
- incendii, scurgeri de apă, tensiuni periculoase din reţeaua de alimentare.

După originea lor, sursele ameninţărilor pot fi: din interior, din exterior sau din mediu.

*Ameninţările la vedere sunt: bruiajul radio, radioreleu, de radiolocaţie sau de radionavigaţie; impulsul electromagnetic (EMP); activităţile SIGINT; operaţiile speciale.*

În cadrul agresiunilor informaţionale planificate, ameninţările posibile la adresa sistemelor informaţionale militare provin din toate cele trei tipuri de surse.

Atunci când un mesaj este transmis printr-un canal de comunicaţii, există o multitudine de ameninţări voluntare sau accidentale generale.

### ❖ Riscuri

Ca abordare generală în interiorul domeniului militar[36], *riscul* este definit ca probabilitatea și severitatea unei pierderi, legată de existența unor pericole. În mod distinct, riscul este privit ca o limită, un prag maxim pentru care o contramăsură, stabilită prin norme, a fost demonstrată ca fiind eficientă în eliminarea unei vulnerabilități, în corelație cu un nivel de susceptibilitate și de amenințare dat.

[36] Gheorghe Boaru, Iulian Marius Iorga, *Securitatea sistemelor informaționale militare, op. cit.*, pp. 39-40.

Riscul definește un indicator care reprezintă probabilitatea și ritmul de apariție a unui eveniment sau acțiune care, dacă se produce, cauzează deteriorarea informației în sine sau a suportului material ce susține informația.

Există o relație direct proporțională între vulnerabilitate și risc, în raport cu amenințările[37].

Având în vedere că nu putem influența în niciun fel amenințările, implicit nici probabilitatea de apariție, singura modalitate de reducere a riscurilor este pârghia de acțiune asupra vulnerabilității, respectiv a gradului de vulnerabilitate.

## ATACURI ASUPRA REȚELELOR DE COMUNICAȚII ȘI INFORMATICE

*Riscul defineşte un indicator care reprezintă probabilitatea şi ritmul de apariţie a unui eveniment sau acţiune care, dacă se produce, cauzează deteriorarea informaţiei în sine sau a suportului material ce susţine informaţia.*

Atacurile asupra reţelelor de comunicaţii se pot grupa, în funcţie de anumite criterii. După locul de unde se execută, atacurile pot fi:

- locale (local);
- de la distanţă (remote).

Atacurile locale se materializează prin compromiterea securităţii unei reţele de către un utilizator local.

Riscul de a compromite securitatea unei reţele poate fi tratat (eliminat, diminuat, repartizat) în diferite moduri:

- acordarea de privilegii strict necesare utilizatorilor locali, pentru îndeplinirea atribuţiilor zilnice, conform sarcinilor înscrise în fişele posturilor;
- supravegherea reţelei, pentru a preîntâmpina posibile tentative de încălcare a normelor impuse a se respecta, inclusiv după terminarea orelor de program;
- restricţionarea accesului la echipamentele de reţea importante;
- repartizarea echilibrată a sarcinilor complexe personalului din cadrul organizaţiei militare.

Există însă și posibilitatea nefericită ca aceste măsuri de protecție să fie ineficiente, dacă sunt trădători din interiorul rețelei care contribuie la compromiterea măsurilor de securitate ale sistemului.

De aceea, în vederea acordării unor privilegii de utilizare a resurselor reţelei, utilizatorii trebuie ierarhizaţi pe mai multe niveluri

[37] Gheorghe Boaru, Vasile Păun, Marcel Răducu, *Managementul riscurilor în acțiunile militare,* Editura AÎSM, București, 2003, pp. 17-25.

de încredere, în funcţie de vechimea în reţea, de comportamentul acestora şi de gravitatea unor evenimente de securitate în care au fost implicaţi.

Atacul la distanţă (remote attack) reprezintă o acţiune iniţiată asupra unei reţele de comunicaţii sau asupra unui echipament din reţea, atunci când agresorul nu dispune, iniţial, de niciun control.

Atacul la distanţă se poate realiza în trei etape:

**Prima etapă** este una de informare, în care atacatorul trebuie să descopere informaţii despre:

- administratorul reţelei;
- echipamentele din reţea și funcţiile acestora;
- sisteme de operare folosite;
- puncte de vulnerabilitate;
- topologia reţelei;
- politici de securitate etc.

Această **primă etapă** este asimilată unui atac, denumit **atac de recunoaștere**, și constă în maparea neautorizată a unui sistem informatic, a serviciilor și a vulnerabilităților lui.

**A doua etapă** este una de tatonare și constă în clonarea unei ținte și atacarea acesteia, pentru a se simula modalitatea de răspuns.

**Etapa a treia** constă în lansarea atacului asupra rețelei. Un atac de succes se execută rapid, atunci când rețeaua prezintă vulnerabilități.

Potrivit unei alte clasificări a atacurilor adresate rețelelor de comunicații/informatice, după modul în care se desfășoară acestea, ca destinație și sursă, atacurile pot fi **focalizate** pe o singură țintă (este atacat un anumit server de pe un singur echipament) sau pot fi **distribuite** (inițiate din mai multe locuri sau de către mai multe echipamente concomitent).

După modul de interacțiune a atacatorului cu informația accesată neautorizat, ca rezultat al acțiunii reușite, se disting două categorii de atacuri: **pasive** și **active**.

*Atacurile pasive* sunt acele atacuri în urma cărora atacatorul se limitează la supravegherea modului în care informația circulă prin sistem fără a interveni în acest flux. Tot în categoria atacurilor pasive intră și interceptarea (radio, radioreleu, fir/fibră optică) propriu-zisă și goniometrarea (radio, radioreleu).

*Atacurile pasive sunt acele atacuri în urma cărora atacatorul se limitează la supravegherea modului în care informația circulă prin sistem fără a interveni în acest flux. Tot în categoria atacurilor pasive intră și interceptarea (radio, radioreleu, fir/fibră optică) propriu-zisă și goniometrarea (radio, radioreleu).*

Atacurile pasive pot avea unele caracteristici comune, precum:

- nu creează prejudicii imediate şi care pot fi detectate, deoarece nu şterg şi nu modifică date, nu blochează reţeaua, nu perturbă traficul;
- încalcă regulile de confidenţialitate;
- obiectivul constă în a asculta datele schimbate pe canalele de comunicaţii;
- datele ascultate sunt supuse altor etape de prelucrare, în scopul extragerii informaţiilor utile pentru alte operaţiuni, inclusiv alte atacuri pasive;
- sunt greu, chiar imposibil, de sesizat.

*Atacurile active au ca scop furtul sau falsificarea informaţiilor transmise ori stocate în reţea, reducerea disponibilităţii reţelei, prin supraîncărcarea acesteia cu pachete (flooding), perturbarea sau blocarea comunicaţiilor, prin atac fizic sau logic asupra echipamentelor din reţea şi a căilor de comunicaţii. Aceste atacuri sunt mai periculoase, deoarece modifică starea sistemelor de calcul, de management şi a celor de comutare, precum şi a datelor.*

Aceste atacuri se pot realiza prin diverse metode, cum ar fi: supravegherea convorbirilor telefonice, radio sau radioreleu, exploatarea radiațiilor electromagnetice emise, în scopul transmiterii informațiilor sau a radiațiilor parazite compromițătoare, routarea datelor, prin noduri secundare mai slab protejate.

*Atacurile active* reprezintă acele atacuri prin care atacatorul își materializează acțiunea în distrugerea, în furtul, în modificarea sau în reluarea mesajelor ori în inserarea de mesaje false.

Atacurile active au ca scop furtul sau falsificarea informațiilor transmise ori stocate în rețea, reducerea disponibilității rețelei, prin supraîncărcarea acesteia cu pachete (flooding), perturbarea sau blocarea comunicațiilor, prin atac fizic sau logic asupra echipamentelor din rețea și a căilor de comunicații. Aceste atacuri sunt mai periculoase, deoarece modifică starea sistemelor de calcul, de management și a celor de comutare, precum și a datelor. Există o serie de atacuri active, în cazul acestora impunându-se o nouă analiză, conform criteriului efectului produs de acestea, astfel:

*a. Atacuri care afectează preponderent starea de organizare*

- bruiajul electronic – constă în modificarea semnalelor de recepție;
- dezinformarea – se realizează prin interceptarea și prin modificarea conținutului mesajului, urmate de retransmiterea oportună a comunicării;
- mascarada – este un atac în care o țintă din rețea (utilizator, client, serviciu sau server) indică o altă identitate, pentru a prelua informații confidențiale (parole de acces, date

de identificare, chei de criptare, informații despre cărți de credit și altele);

- reluarea – se produce atunci când un mesaj sau o componentă a acestuia este reluat (repetat), cu intenția de a produce un efect neautorizat;
- modificarea mesajelor – datele mesajului sunt supuse, în mod neautorizat, modificării, inserării sau ștergerii;
- refuzul serviciului *(DoS/Denial of service attack)* – se produce atunci când o entitate autorizată nu izbutește să îndeplinească propria funcție sau când o entitate intrusă desfășoară prin acțiuni, care împiedică o altă entitate în îndeplinirea altor funcții;
- repudierea serviciului – apare atunci când o entitate nu vrea să recunoască un serviciu executat.

*b. Atacuri active cu efect preponderent distructiv* – în sistemele dependente de componentele informatizate, astfel de atacuri se realizează prin intermediul unor programe create în acest scop, care afectează, uneori esențial, securitatea calculatoarelor, inclusiv a serverelor. Aceste atacuri urmăresc citirea neautorizată a informațiilor, dar, cel mai frecvent, distrugerea parțială sau totală a datelor sau chiar a echipamentelor de procesare. Dintre aceste programe distructive, le amintim pe următoarele:

- viruşii sunt reprezentaţi de programe informatice, care se multiplică singure în programele proprii sistemului atacat, utilizând spaţiul rezident din memorie/hard-disk şi blochează computerul sau, după un număr programat de multiplicări, poate produce chiar distrugeri;
- bomba software este o parte de cod sau procedură, inserată într-o aplicaţie necesară, care poate fi lansată de un eveniment programat. Creatorul bombei informează despre acest eveniment, lăsând-o să desfăşoare acţiunile distructive, programate prin efectul *„exploziei”*;
- viermii produc, de cele mai multe ori, efecte distructive, similare cu cele ale bombelor şi ale viruşilor. Diferenţa constă în faptul că viermii nu rezidă la o adresă fixă sau nu se multiplică singuri. În schimb, se mută permanent, ceea ce îi face foarte dificil de detectat;

*Bomba software este o parte de cod sau procedură, inserată într-o aplicaţie necesară, care poate fi lansată de un eveniment programat. Creatorul bombei informează despre acest eveniment, lăsând-o să desfăşoare acţiunile distructive, programate prin efectul „exploziei”.*

- Calul Troian este o aplicaţie care se prezintă sub forma unei funcţii de utilizare cunoscută şi care, în mod disimulat, îndeplineşte şi o altă funcţie.

Există o multitudine de posibilități de atacuri la adresa sistemelor informaționale, care pot exploata vulnerabilitățile acestora.

❖ **Vulnerabilităţi specifice sistemelor informaţionale**

Vulnerabilităţile informaţionale constituie o componentă a vulnerabilităţii de securitate a sistemelor, generată de stări de fapt sau de procese interne ale organizației, care pot duce la reducerea capabilităților de reacție la amenințările posibile, de orice natură, inclusiv informaţionale.

În general, vulnerabilităţile informaţionale sunt cu atât mai mari, cu cât reţelele informaţionale și structura informaţiilor sunt mai complexe, deci mai greu de administrat, fiind mai greu de organizat şi de protejat.

*„Vulnerabilităţile sporesc direct proporţional cu nivelul tehnologic implementat în construcţia şi în funcţionarea echipamentelor sistemelor informaţionale”.*

De asemenea, se consideră că *„vulnerabilităţile sporesc direct proporţional cu nivelul tehnologic implementat în construcţia și în funcţionarea echipamentelor (mai ales digitale) sistemelor informaţionale”*[38].

Cele mai cunoscute vulnerabilităţi, în cazul sistemelor informaţionale militare, sunt:

- erori de proiectare și de funcționare a sistemului;
- posibilitatea defectării unor componente tehnice;
- dificultăți în testarea integrală și integrată a sistemului;
- cantitatea excesivă a informațiilor de analizat;
- dispersarea utilizatorilor și a punctelor de acces, pe o rază geografică întinsă;
- insuficienta pregătire a personalului în domeniul siguranței naționale;
- neexecutarea unei noi acreditări de securitate, după o modificare a sistemului;
- conectarea calculatoarelor din rețele locale neclasificate la alte rețele clasificate;
- adrese routere și firewall greșit configurate/introduse;

[38] Constantin Alexandrescu, Gelu Alexandrescu, Gheorghe Boaru, *op. cit.,* p. 294.

- nerespectarea normelor TEMPEST;
- depășirea termenelor de schimbare a parolelor și a cheilor de secretizare;
- nerestricționarea conexiunilor Dal-in în LAN și nerestricționarea serviciului de poștă electronică;
- folosirea unor canale nesecretizate, pentru transmiterea unor informații clasificate.

Referitor la analiza infrastructurii informaționale, se consideră că principalele vulnerabilități ar putea fi următoarele[39]:

- existenţa posibilităţilor de interceptare a informaţiilor din reţelele de comunicaţii şi de calculatoare atât din interior (de către utilizatori), cât şi din exterior (de către adversari);
- existenţa unui volum foarte mare de informaţii produse, vehiculate și prelucrate în sistemele informaţionale, care pot fi supuse cercetării şi atacului, distruse, falsificate sau sustrase de către adversarii potenţiali;
- îngreunarea managementului infrastructurii informaţionale, din cauza complexităţii acesteia, ceea ce determină imposibilitatea detectării accesului fraudulos la informaţii şi favorizarea atacurilor cibernetice;
- folosirea aceloraşi benzi de frecvenţe atât ale mijloacelor proprii, cât și ale potenţialilor adversari;
- standardizarea echipamentelor tehnice, a componentelor software și a bazelor de date utilizate;
- utilizarea unor elemente comune ale infrastructurii informaţionale naţionale, ceea ce creează condiţii pentru acces fraudulos şi dezinformare;
- posibilitatea ca firmele furnizoare de aparatură să încorporeze din timp, în echipamentele de calcul și de comunicaţii, unele module software maliţioase, care pot fi activate de către adversari, în anumite momente stabilite de aceştia, creând dezordine și haos în reţelele informaţionale și în cele decizionale;

*Una dintre vulnerabilitățile infrastructurii informaționale o reprezintă existenţa unui volum foarte mare de informaţii produse, vehiculate și prelucrate în sistemele informaţionale, care pot fi supuse cercetării şi atacului, distruse, falsificate sau sustrase de către adversarii potenţiali.*

[39] Constantin Alexandrescu, *Amenințări și riscuri electronice privind sistemele informaționale militare moderne în spațiul de luptă*, în volumul Sesiunea de comunicări științifice a U.N.Ap. *„Carol I" – „Sisteme Informaționale SI-2007"*, pp. 107-115.

- vulnerabilităţile la pătrunderi neautorizate (cu rea intenţie sau din neatenţie) din cauza faptului că organizaţiile sunt conectate la internet, intranet sau extranet;
- nerespectarea integrală a cerinţelor şi a standardelor UE și NATO privind compatibilitatea şi interoperabilitatea sistemelor informaţionale, mai ales în ceea ce priveşte schimbul de informaţii (formatul mesajelor), accesul la bazele de date, criptarea automată a comunicărilor și caracteristicile canalelor pentru legătură;
- posibilitatea folosirii de către adversarii potenţiali a războiului electronic împotriva mijloacelor radioelectronice din principalele sisteme informatice și de comunicaţii, cu precădere asupra canalelor care asigură legătura surselor de informaţii cu organele centrale de fuziune și de prelucrare a datelor;
- interceptarea de către adversar (forţele ostile) a comunicărilor transmise prin radio, decriptarea acestora în timp oportun, în cazul folosirii unor sisteme criptografice neperformante şi utilizarea, în scopuri proprii, a acestor informaţii, pentru obţinerea superiorităţii informaţionale;
- mijloacele tehnice actuale ale sistemelor informaţionale nu au asigurată protecţia temeinică împotriva atacului fizic, electromagnetic şi cibernetic, acestea putând fi distruse, deteriorate sau extrasă informaţia stocată;
- dispunerea în locuri necorespunzătoare, din punct de vedere funcţional şi al securităţii fizice și electromagnetice, a echipamentelor tehnice ale sistemelor informaţionale, în principal a mijloacelor de comunicaţii şi de calcul, ceea ce sporeşte vulnerabilitatea de interceptare a informaţiilor şi de atac fizic;
- utilizarea, pentru exploatarea sistemelor informaţionale, a unor persoane insuficient verificate şi neloiale, predispuse a fi racolate de către adversarii potenţiali și determinate să efectueze acţiuni de sabotaj sau să furnizeze acestora informaţii obţinute fraudulos;
- neutralizarea legăturii radio pe unde scurte, mai ales la distanţe mari, bazată pe propagarea undelor electromagnetice, prin ionosferă, prin schimbarea caracteristicilor electrice ale acesteia;

*Dispunerea în locuri necorespunzătoare, din punct de vedere funcţional şi al securităţii fizice și electromagnetice, a echipamentelor tehnice ale sistemelor informaţionale, în principal a mijloacelor de comunicaţii şi de calcul, sporeşte vulnerabilitatea de interceptare a informaţiilor şi de atac fizic.*

- existenţa, la adversarii potenţiali, a armelor electronice cu radiaţii infraacustice, bazate pe propagarea în spaţiu a undelor subsonice, care acţionează asupra personalului, cauzând greţuri grave, vomismente, buimăceală, teamă, depresii etc., determinând inactivarea acestuia, pe anumite perioade de timp şi, implicit, întreruperea funcţionării sistemelor informaţionale;
- instalarea antenelor mijloacelor de comunicaţii, în câmp deschis sau în spaţii fără proprietăţi naturale de protecţie, ceea ce permite scoaterea lor uşoară din funcţiune şi întreruperea legăturilor, mai ales a celor realizate cu staţii radio și/sau radioreleu de putere mare;
- suprimarea accesului la internet al sistemelor informaţionale, pentru izolarea acestora şi împiedicarea folosirii surselor de informaţii deschise ;
- utilizarea internetului pentru acţiuni teroriste, de dezinformare și pentru atac cibernetic asupra infrastructurii informaţionale;
- proiectarea necorespunzătoare a infrastructurii, cu redundanţă informaţională redusă, centralizată excesiv și cu posibilităţi scăzute de replicare a informaţiilor existente în bazele de date;
- preocuparea insuficientă pentru ascunderea şi pentru mascarea elementelor infrastructurii informaţionale, măsuri neadecvate de pază și de apărare a acestora;
- măsurile insuficient studiate de asigurare a securităţii comunicaţiilor (COMSEC – **Com**munications **sec**urity), a calculatoarelor (COMPUSEC – **Compu**ter **sec**urity) şi a echipamentelor electronice în ansamblu prin interzicerea (restricţionarea) interceptării radiaţiilor parazite (protecţia TEMPEST – **T**ransient **E**lectro **M**agnetic **P**ulse **E**manation **St**andard).

*Există numeroase vulnerabilităţi, dar esenţiale sunt cele care privesc: neorganizarea optimă a sistemelor informaţionale, alegerea necorespunzătoare a echipamentelor tehnice utilizate şi a produselor software comerciale, realizarea programelor de aplicaţii şi a bazelor de date, precum și a softwarelor, pentru criptarea automată a informaţiilor în sistemele informaţionale, dar și personalul neloial sau insuficient verificat.*

Din analiza efectuată, rezultă că există numeroase vulnerabilităţi, dar, dintre acestea, esenţiale sunt cele care privesc: neorganizarea optimă a sistemelor informaţionale, alegerea necorespunzătoare a echipamentelor tehnice utilizate şi a produselor software comerciale, realizarea programelor (software) de aplicaţii şi a bazelor de date, precum și a softwarelor pentru criptarea automată a informaţiilor în sistemele informaţionale, dar și personalul neloial sau insuficient verificat.

## CONCLUZII

În noul mediu informaţional global, dezvoltarea tehnologică a adus, odată cu avantajele și facilităţile pe care le oferă, și o serie de ameninţări, de riscuri şi de vulnerabilităţi la adresa securităţii informațiilor și a sistemelor informaţionale.

Preocupările de abordare a ameninţărilor, a vulnerabilităţilor şi a riscurilor, în dinamica specifică ultimelor decenii, cuprind o arie extinsă, eforturi importante fiind concentrate pe domeniul informaţional.

Având în vedere că atacurile informaţionale reprezintă o ameninţare la adresa securităţii sistemelor informaţionale, specialiştii încearcă să implementeze noi metode de luptă împotriva atacurilor informatice și informaţionale, care să vizeze, în principal, protejarea propriilor informaţii şi a sistemelor de informaţii.

*Pentru ca o vulnerabilitate să fie exploatată, trebuie să fie cunoscută sau să poată fi descoperită de o ameninţare. Aceasta face importantă urmărirea aplicării principiului „need to know", cu respectarea măsurilor legate de securitate şi a aplicării lor atât de către personal, cât şi în domeniul tehnologiei.*

Plecând de la faptul că nu se poate face un control absolut, ci doar o limitare a acestora, experţii au declanşat o nouă ofensivă, pentru perfecţionarea legislaţiei, întărirea rolului agenţiilor de profil şi pentru perfecţionarea produselor necesare depistării delictelor informaţionale și a celor informatice.

Pentru ca o vulnerabilitate să fie exploatată, trebuie să fie cunoscută sau să poată fi descoperită de o ameninţare. Aceasta face importantă urmărirea aplicării principiului *„need to know",* cu respectarea măsurilor legate de securitate şi a aplicării lor atât de către personal, cât şi în domeniul tehnologiei. De asemenea, pune accentul pe reacţia corespunzătoare a instituţiei la identificarea oricărei vulnerabilităţi care o poate afecta.

Apreciem că se pot face estimări, cu un anumit nivel de încredere, însă este dificil, din punct de vedere ştiinţific, să se realizeze analize cu exactitate privind ameninţările la adresa sistemelor informaţionale. Aceste estimări sunt dependente, în primul rând, de factorul uman, de gândirea sa, de subiectivismul și de incertitudinea pe care acestea le implică.

Asigurarea securităţii sistemelor informaţionale militare este o activitate complexă şi dificil de realizat, întrucât aceasta se face prin punerea în practică, pe teritoriul naţional, dar şi în afara acestuia, pe baza legislaţiei şi a reglementărilor internaţionale, de alianţă/coaliţie și naţionale, a unor măsuri specifice care, de regulă, sunt: generale, organizatorice, de protecţie fizică, de protecţie a personalului, de protecţie a documentelor, de protecţie juridică și procedurală,

de securitate industrială, precum și a unor măsuri particulare, de securitate a sistemelor informatice și de comunicaţii.

Securitatea sistemului de comunicaţii şi informatic, componentă a sistemului informaţional (C4I), vizează protecţia informaţiilor, componentelor hardware și software, prin măsuri eficiente, de natură să împiedice accesul la informaţii şi intervenţia în procesele informaţionale (colectare, transmitere, stocare, prelucrare, distribuţie, conversie, afişare).

În reţelele locale de calculatoare și în sistemul de comunicaţii, măsurile de securitate trebuie să asigure: autentificarea (verificarea identităţii unei entităţi de comunicare la distanţă); controlul accesului la resurse; confidenţialitatea datelor; integritatea datelor; protecţia fizică a echipamentelor tehnice.

În general, securitatea sistemelor informaţionale reprezintă un domeniu foarte complex, în care este implicat întregul personal şi care, prin restricţiile și algoritmii pe care le adoptă și le impune, generează de multe ori contradicţii şi birocraţii în exces. Cu toate neajunsurile şi inconvenientele pe care le poate genera, este de preferat să se respecte regulile decât să se pună în pericol îndeplinirea misiunii.

Dependenţa din ce în ce mai mare a activităţilor de comandă și control de securitatea sistemele informaţionale conduce la creşterea tipologiei vulnerabilităţilor cărora organizaţiile trebuie să le facă faţă.

Mai mult, problema protecţiei trebuie să aibă în vedere, de multe ori, interconectarea reţelelor private cu serviciile publice. Dacă, la acest aspect, mai adăugăm și problema partajării informaţiilor, se conturează un tablou destul de complicat, în care implementarea unor controale eficiente devine o sarcină dificilă pentru specialistul IT&C.

Considerăm că securitatea informaţiilor nu este doar o problemă tehnică, este, în primul rând, o problemă managerială.

Standardul de securitate ISO/IEC 17799 răspunde nevoilor organizaţiilor de orice tip, publice sau private, printr-o serie de practici de gestiune a securităţii informaţiilor. Standardul poate fi folosit, în funcţie de gradul de expunere a fiecărei organizaţii în parte, pentru a conştientiza, la nivelul conducerii, aspectele legate de securitatea informaţiei sau pentru a crea o cultură organizaţională, în ceea ce priveşte securitatea informaţiilor, sau pentru a obţine certificarea sistemului de securitate.

GÂNDIREA MILITARĂ ROMÂNEASCĂ

*Standardul de securitate ISO/IEC 17799 răspunde nevoilor organizaţiilor de orice tip, publice sau private, printr-o serie de practici de gestiune a securităţii informaţiilor. Standardul poate fi folosit, în funcţie de gradul de expunere a fiecărei organizaţii în parte, pentru a conştientiza, la nivelul conducerii, aspectele legate de securitatea informaţiei sau pentru a crea o cultură organizaţională, în ceea ce priveşte securitatea informaţiilor, sau pentru a obţine certificarea sistemului de securitate.*

Stabilirea cerinţelor de securitate, a măsurilor necesare pentru asigurarea nivelului de control dorit are o componentă deseori subiectivă, fiind dificil de cuantificat, în termeni monetari, pierderea suferită, în cazul unui incident de securitate.

Din studiul acestui domeniu foarte complex al securităţii informaţiilor și a sistemelor informaţionale militare, opinăm pentru câteva măsuri concrete:

- organizarea optimă a sistemelor informaţionale, astfel încât să se asigure condiţia fundamentală pentru funcţionarea eficientă a acestora – reconfigurarea, mobilitatea şi adaptabilitatea lor la mediul de informaţii în continuă dezvoltare;
- să se aibă permanent în vedere condiţiile, restricţiile și standardele care sunt stabilite, ca ţară membră a UE și a NATO. Acestea se impun a fi respectate în totalitate şi aplicate cu fermitate, pentru a se îndeplini criteriile de compatibilitate şi interoperabilitate cu alte organizaţii din ţară şi din exterior;
- informaţiile clasificate vor fi diseminate numai persoanelor care deţin un certificat de securitate corespunzător;
- respectarea reglementărilor NATO[40], prin care aplicarea standardelor minime de asigurare a securităţii informaţiilor este obligatorie pentru tot personalul care accesează sistemul informaţional;
- creşterea responsabilităţii şi a controlului pentru protecţi informaţiilor clasificate de către fiecare persoană care deţine, procesează sau are cunoştinţă de asemenea informaţii;
- executarea periodică a unor analize de risc asupra sistemelor informaţionale și prelucrarea acestora în faţa personalului militar, sub formă de lecţii învăţate;
- achiziţiile de noi tehnologii informaţionale să ţină cont de scopul micşorării vulnerabilităţilor specifice;
- pregătirea profesională a personalului să cuprindă și teme pe domeniul securităţii informaţiei și a sistemelor informaţionale.

*Trebuie respectate reglementările NATO, prin care aplicarea standardelor minime de asigurare a securităţii informaţiilor este obligatorie pentru tot personalul care accesează sistemul informaţional.*

În concluzie, în actuala eră a informaţiei, securitatea tehnologică are o importanţă deosebită și priveşte, în egală măsură, reţelele de calculatoare (*COMPUSEC*) și reţelele de comunicaţii (*COMSEC*).

[40] *AD 70-1, ACO Security Directive*, NATO HQ, Brussels, 2006, p. I-2-4.

Din păcate, nu există un sistem de securitate sigur 100%, dar, prin definirea unei politici de securitate realiste, trebuie găsite permanent cele mai eficiente căi de evitare a riscurilor la care este supusă reţeaua informaţională militară.



## BIBLIOGRAFIE:


1. ***, AAP6 (2008), *NATO Glossary of Terms and Definitions*, 2008.
2. ***, AD 70-1, *ACO Security Directive*, NATO HQ, Brussels, 2006.
3. ***, AJP-3(C), *Allied Joint Doctrine for the conduct of Operations,* NATO, 2019.
4. ***, AJP-2*, Doctrina Aliată pentru informaţii, contrainformaţii şi securitate,* 2003.
5. ***, *Doctrina Armatei României*, București, 2012.
6. ***, *Doctrina pentru intelligence în operațiile întrunite (a Forțelor Armate ale Canadei)*, 2003.
7. ***, *Doctrina pentru Informații, Contrainformații și Securitate a Armatei*, București, 2005.
8. ***, *Doctrina pentru sprijinul cu informații al operațiilor întrunite*, 2003.
9. ***, FM 3-13, *Information Operations*, Washington D.C., December 2016.
10. ***, FM 101-6, *Information Operations*, 1996.
11. ***, *Ghidul Strategiei Naționale de Apărare a Țării pentru perioada 2015-2019*, Administrația Prezidențială, București, 2015.
12. ***, IPS-3, *Doctrina pentru informații, contrainformații și securitate a Armatei*, București, 2005.
13. ***, JP 1-02, *Department of Defense Dictionary of Military and Associated Terms,* 2016.
14. ***, JP-2, *Intelligence în operațiile întrunite* (a Forțelor Armate ale Statelor Unite ale Americii), 2007.
15. ***, *Legea nr. 182/2002 privind protecţia informaţiilor clasificate.*
16. ***, *Normele privind protecția informațiilor clasificate în Ministerul Apărării Naționale*, aprobate de *Ordinul Ministrului Apărării Naționale nr. M.9/2013,* publicat în *Monitorul Oficial al României*, Partea I, nr. 115, din 28 februarie 2013.
17. ***, *Strategia Națională privind Agenda Digitală pentru România 2020,* aprobată prin Hotărârea de Guvern nr. 245/7 aprilie 2015.
18. ***, *Strategia națională de apărare a României*: *„Pentru o Românie care garantează securitatea și prosperitatea generațiilor viitoare”*, București, 2010.
19. ***, *Strategia de securitate națională a României*: *„România Europeană, România Euroatlantică: pentru o viață mai bună într-o țară democratică, mai sigură și prosperă”*, București, 2007.

20. ***, *Strategia de Transformare a Armatei României*, București, 2007.
21. D. Albert, J. Garstka, R. Hayes, D. Signori, *Understanding Information Age Warfare,* Washington D.C., CCRP-Data publication, august 2001.
22. Constantin Alexandrescu, *Amenințări și riscuri electronice privind sistemele informaționale militare moderne în spațiul de luptă*, în volumul Sesiunea de comunicări științifice a U.N.Ap. *„Carol I" – „Sisteme Informaționale SI-2007".*
23. Constantin Alexandrescu, Gelu Alexandrescu, Gheorghe Boaru, *Sisteme informaționale – fundamente teoretice*, Editura Universității Naționale de Apărare *„Carol I"*, București, 2009.
24. Gelu Alexandrescu, Gheorghe Boaru, Constantin Alexandrescu, *Sisteme informaționale pentru management,* Editura Universității Naționale de Apărare *„Carol I"*, București, 2012.
25. Francisco Martínez Álvarez, Alicia Troncoso Lora, José António Sáez Muñoz, Héctor Quintián, Emilio Corchado, *Sinteza Informational Security International Joint Conference: 12th International Conference on Computational Intelligence in Security for Information Systems (CISIS 2019) and 10th International Conference on European Transnational Education (ICEUTE 2019): Seville, Spain, May 13th-15th, 2019 Proceedings,* Series: Advances in Intelligent Systems and Computing 951,Publisher: Springer International Publishing, Year: 2020.
26. Colonel (ret.) prof. univ. dr. Gheorghe Boaru, *Război și apărare în spațiul virtual,* Revista de Științe Militare, Editată de Academia Oamenilor de Știință din România, nr. 2, 2018.
27. Colonel (ret.) prof. univ. dr. Gheorghe Boaru, *Securitatea cibernetică în Uniunea Europeană,* Revista Academiei de Științe ale Securității Naționale, nr. 2, 2017.
28. Colonel (r.) prof. univ. dr. Gheorghe Boaru, colonel drd. Iulian-Marius Iorga, *Ciclul informațional ca proces, procesul și ciclul „intelligence" – în cadrul acțiunilor militare moderne,* Revista de Științe Militare, editată de Academia Oamenilor de Știință din România, nr. 1, 2017.
29. Gheorghe Boaru, Vasile Păun, Marcel Răducu, *Managementul riscurilor în acțiunile militare*, Editura AÎSM, București, 2003.
30. Ion Ciobanu, Gheorghe Ilie, Aurel Nour, *Confruntarea informațională și protecția informațiilor*, Editura Detectiv, București, 2006.
31. Abhishek Chopra, Mukund Chaudhary, *Implementing An Information Security Management System: Security Management Based On ISO 27001 Guidelines,* Publisher: Apress, Year: 2020.
32. Vasile Dumitru și alții, *Sisteme informaționale militare*, Editura CERES, București, 2000.
33. James Dunningan, *O nouă amenințare mondială. Cyber-Terorismul*, Editura Curtea Veche, 2010.
34. Iulian Marius Iorga, *Securitatea informațiilor în acțiunile militare moderne,* Editura Universității Naționale de Apărare *„Carol I"*, București, 2018.

35. W.J. Karplus, *Sisteme de calculatoare cu divizarea timpului*, Editura Tehnică, Bucureşti, 1970.
36. Ovidiu Nicolescu şi alţii, *Sistemul informațional managerial al organizaţiei*, Editura Economică, București, 2001.
37. Ramjee Prasad, Vandana Rohokale, *Cyber Security: The Lifeline of Information and Communication Technology,* Series: Springer Series In Wireless Technology, Publisher: Springer, Year: 2020.
38. *ENISA-Country Reports, 2008*, http://www.enisa.europa.eu.
39. *Information Systems*, Wikipedia, the free encyclopedia, http:/en.wikipedia.org/ wiki/Information Systems.
40. *Information Security*, http:/en.Wikipedia.org/wiki/informationsecurity, 2009.
41. https://*fcnap.ro/transformarea-fortelor-armate-ale-romaniei-un-raspuns-direct-la-noile-provocari-ale-mediului-de-securitate/*.
42. www.dodccrp.org.