RISCURI ŞI AMENINŢĂRI LA ADRESA SISTEMELOR C4ISR

RISKS AND THREATS TO C4ISR SYSTEMS

Lt.col.drd. Florin ALEXANDRU*

„Securitatea fiecărei ţări, precum şi a comunităţii internaţionale în ansamblu depinde nu atât de capacitatea de reacţie şi de adaptare cât, mai ales, de capacitatea de anticipare şi de acţiune proactivă. Într-o lume complexă, dinamică şi conflictuală, aflată în plin proces de globalizare, înţelegerea profundă a tendinţelor majore de evoluţie a lumii şi a modului în care fiecare ţară are şansa să devină parte activă a acestui proces este o condiţie esenţială a oricărui progres[1]”.

„The security of every country, as well as the security of the overall international community, is based, not as much on the capacity of reaction and adjustment, but mostly on the capacity to anticipate and act pro-actively. In a complex, dynamic and conflictual world, found in the middle of the globalization process, a profound understanding of the main trends of evolution and the way in which every country has the chance to be actively involved in this process is an essential requirement of progress”.

Cuvinte-cheie: sistem informatic; riscuri; ameninţări; vulnerabilităţi; C4ISR; ISTAR.
Keywords*: info system; risks; threats; vulnerabillities; C4ISR; ISTAR.*

În mediul internaţional contemporan, starea de securitate a devenit dependentă de o multitudine de factori, a căror eterogenitate surprinde neîntrerupt. Acest fapt determină necesitatea obiectivă, de trecere a sistemelor care o asigură din starea de *reactiv* în starea de *anticipativ acţional*, proces dificil, care incumbă dezvoltarea *cunoaşterii*, ca fundament al dezvoltării strategiilor acţionale. Resursa care poate asigura această necesitate este *informaţia* furnizată de sistemele IS(TA)R, aflate în plin proces de dezvoltare, la nivelul strategic (politic şi militar) al tuturor actorilor cărora nu le este indiferentă starea de securitate zonală, regională sau globală.

În acest context, este evident că rolul sistemelor IS(TA)R devine tot mai elocvent.

IS(TA)R înseamnă Informaţii (I), Supraveghere (S), Identificarea, Selectarea şi Combaterea Ţintelor (TA), Cercetare (R) şi reprezintă culegerea, procesarea şi diseminarea coordonată, periodică, precisă, oportună şi sigură a datelor şi a informaţiilor primare/brute *(INFORMATION),* şi a informaţiilor prelucrate *(INTELLIGENCE)*, care sprijină atât planificarea şi conducerea operaţiilor militare curente, cât şi planificarea operaţiilor viitoare, combaterea ţintelor şi evaluarea efectelor la ţintă, în vederea sprijinului pentru îndeplinirea misiunii[2], în operaţiile întrunite.

Pentru o înţelegere exactă a ceea ce se doreşte a fi capacitatea ISR, cele trei componente (*intelligence*, *surveillance* şi *reconnaissance*) nu trebuie privite separat, ci ca un sistem unitar de colectare de date şi de informaţii despre un adversar sau potenţial adversar, care vor fi aduse la cunoştinţa factorului de decizie, militar sau/şi politic, indiferent la ce nivel este situat acesta, iar împreună cu sistemul de C2 vor forma sistemul C4ISR.

Sistemul de comunicaţii reprezintă suportul fizic, necesar schimbului de informaţii dintre toate elementele sistemului C2 şi ISR şi asigură următoarele servicii: comunicaţii de date şi voce, schimb de mesaje, acces transparent la fişiere, suport pentru staţiile de lucru şi securitatea reţelei[3].

Sistemele ISR sunt de tip *complex*, care trebuie să ofere o perspectivă globală asupra ameninţării,

***Universitatea Naţională de Apărare „Carol I”**
e-mail: *florin19al@yahoo.com*

să asigure fuzionarea tuturor tipurilor de informaţii într-o singură imagine, comună completă, să permită accesul la informaţii detaliate despre inamic şi să monitorizeze ţinte specifice, pentru perioade lungi de timp, aducând imputuri în sistemul C2 (comandă şi control).

În fiecare armată, armele cu mare precizie de lovire, care se bazează pe utilizarea inteligenţei artificiale, a ciberneticii şi a tehnologiei informaţiei, care necesită o asigurare informaţională multilaterală, realizată în timp real şi bazată pe mijloace electronice diverse (radare, senzori, GPS, sisteme ISTAR), ocupă un loc principal în armamentul modern, reflectând forţa cibernetică şi transformând calculatoarele în ţinte potenţiale ale primei lovituri[4].

Plecând de la analiza structural-funcţională a domeniilor de desfăşurare a războiului în era informaţională, a ţintelor pentru atacurile în spectrul informaţional, utilizând armele informaţionale sau convenţionale, precum şi de la numeroasele analize ale sistemului C4ISR al unei armate moderne, putem aprecia că principalele ameninţări pot fi împărţite în:

- *ameninţări în domeniul fizic*, care se referă la dezorganizarea sistemului C4ISR, prin lovirea elementelor constitutive cu foc, prin întrebuinţarea armelor clasice, a armelor cu energie dirijată, precum împiedicarea refacerii acestuia în urma atacurilor;
- *ameninţări în domeniul informaţional*, respectiv acţiuni specifice războiului de comandă-control: acţiuni de război electronic, acţiuni de penetrare a sistemului de achiziţie, de centralizare, de procesare, de afişare şi de diseminare a informaţiei despre situaţia aeriană, despre situaţia navală, acţiuni de penetrare a bazelor de date, acţiuni psihologice, acţiuni informaţionale destabilizatoare;
- *ameninţări în domeniul cognitiv (conceptual)*, care se referă la conceptele doctrinare de întrebuinţare, la procesul de reorganizare şi de modernizare a sistemului C4ISR, precum şi la coeziunea elementelor sistemului, la nivelul de instruire şi la asigurarea transferului de experienţă, la schimbarea personalului care încadrează elementele sistemului.

Referitor la domeniul fizic, pentru realizarea scopurilor strategice pe care şi le-ar putea propune un eventual agresor sau adversar, un rol important, uneori chiar hotărâtor, va fi acordat forţelor aeriene militare, deoarece acestea au posibilitatea să lovească simultan trupele şi obiectivele de pe spaţiile extinse şi să producă pierderi şi distrugeri decisive ale sistemului C4ISR de conducere a operaţiilor militare, dar şi capacitatea de apărare a ţării, a populaţiei şi a infrastructurii.

Posibilităţile mari de cercetare şi de lovire, proprii mijloacelor aeriene, fac din ameninţarea aeriană una dintre principalele componente ale ameninţării la adresa securităţii naţionale şi impun o evaluare atentă a modului probabil de întrebuinţare.

Contextul geopolitic şi geostrategic actual a modificat substanţial conţinutul ameninţării aeriene (aerospaţiale) asupra României, astfel riscul de ameninţare aeriană, perceput până în 1991, din direcţiile sud, sud-est, sud-vest şi vest, devenind, practic, unidirecţional (din direcţia est).

Ordinea de importanţă a direcţiilor aeriene operativ-strategice de acţiune, în contextul integrării în NATO, determinată de nivelul ameninţării aeriene, s-a schimbat, pe primul loc situându-se direcţia est – sud-est; timpul de ajungere a mijloacelor aeriene ale unui agresor potenţial la verticala frontierelor naţionale s-a redus, de la 40 - 50 de minute, în anii ’70, ’80, la 5 - 15 minute, ceea ce creează premisa, în caz de conflict, a unui atac aerian masiv sau limitat asupra României, dar selectiv, prin surprindere, din dispozitivul actual (la pace), fără pregătiri şi fără regrupări importante; descoperirea unor eventuale aeronave infractoare/ostile se face mult prea târziu, pentru a se putea riposta eficient, din cauza lipsei unui sistem de cercetare/supraveghere şi de avertizare avansat, precum şi a configuraţiei tehnice a sistemului naţional de supraveghere a spaţiului aerian.

Cunoaşterea dispozitivului operativ, a posibilităţilor de luptă şi a sistemului de lucru al forţelor aeriene proprii (supraveghere aeriană, aviaţie, apărare aeriană cu baza la sol) de către specialiştii militari ai unor state, care pot deveni ostile, precum şi dependenţa de terţi, în domeniul aprovizionării cu piese de schimb şi cu subansamble, necesare mijloacelor de apărare a spaţiului aerian, reprezintă vulnerabilităţi dificil de contracarat.

Deşi unele aspecte ale acestui tip de pericol nu sunt noi, creşterea razei de acţiune, a preciziei şi a vitezei acestor mijloace aeriene şi, mai ales,

creşterea posibilităţii ca astfel de mijloace de atac să fie achiziţionate de organizaţii teroriste sau de reţele de crimă organizată au determinat lărgirea radicală a domeniului reprezentat de pericolele aeriene.

Existenţa tuturor acestor ameninţări şi pericole face necesară elaborarea unor strategii specifice, care să vizeze prevenirea, reducerea şi eliminarea riscurilor, a vulnerabilităţilor şi a ameninţărilor la adresa securităţii naţiunii şi, implicit, a sistemului C4ISR, a unor decizii şi măsuri adecvate pentru diminuarea vulnerabilităţilor de natură militară şi nonmilitară, concomitent cu realizarea capacităţilor de răspuns, corespunzătoare structurilor de gestionare a situaţiilor şi a acţiunilor.

Proiectarea acestui sistem trebuie să răspundă următoarelor cerinţe: condiţii de lucru specifice câmpului tactic, capacitatea conexiunilor, determinată în funcţie de estimările de trafic, utilizarea standardelor internaţionale pentru asigurarea interoperabilităţii (C4I2SR), utilizarea unor dispozitive de reţea care să corespundă cerinţelor de securitate şi standardelor, asigurarea unor rute alternative pentru siguranţa în funcţionare, dispersia geografică, cerinţele de supravieţuire, transmisia sigură şi fără erori a informaţiilor[5]. Toate acestea reduc vulnerabilităţile sistemului.

În funcţie de posibilităţile agresorului sau ale adversarului, ameninţările din aer pot fi diferenţiate de nivelul tehnologiei pe care se bazează, încorporând tehnologii avansate, şi pot fi completate cu acţiuni specifice războiului asimetric. Principalele ameninţări de natură aeriană sunt avioanele, rachetele balistice, elicopterele şi avioanele fără pilot (UAV, drone).

Sistemele de cercetare şi de supraveghere a spaţiului aerian vor trebui să descopere, să identifice şi să urmărească ţintele aeriene, de la o distanţă cel puţin dublă faţă de raza de acţiune a mijloacelor pe care le deservesc, pentru a avea timpul necesar în alegerea sistemului de răspuns, astfel încât sistemele de lovire să poată satisface cererile de combatere a acestora, din ce în ce mai ample, referitoare la:

- posibilitatea combaterii unei game cât mai mari de ţinte aeriene (avioane, elicoptere, avioane fără pilot, rachete balistice de diferite tipuri);
- angajarea luptei într-un interval de înălţimi cuprinse între 200 şi 30.000 m;
- combaterea unor ţinte, a căror viteză, pe timpul apropierii, va fi de până la 3 Mach;
- mobilitatea ridicată a sistemelor de apărare aeriană cu baza la sol şi timpul de reacţie din ce în ce mai mic.

Potrivit scenariilor de desfăşurare a unor conflicte militare recente, într-o eventuală agresiune aeriană asupra României, este de aşteptat să fie lovite, cu prioritate, centrele şi elementele sistemului C4ISR, cu precădere radarele care execută supravegherea şi cercetarea spaţiului aerian, furnizând informaţiile necesare creării imaginii aeriene unice – RAP.

Trebuie subliniată ideea că, anterior sau simultan cu acţiunile la care pot participa forţele aeriene ale unui agresor, atât în timp de pace, cât şi în perioada de tensiune sau în situaţia declanşării unor posibile şi complicate conflicte interetnice, pe teritoriul de operaţii pot avea loc intense acţiuni de război electronic, acţiuni de transport desant şi materiale tehnice, de sprijin logistic, acţiuni demonstrative şi de lovire a unor obiective deosebit de importante.

Este de remarcat şi faptul că acţiunile aeriene şi/sau în spectrul informaţional, desfăşurate de un eventual agresor, în situaţia în care ating un prag limită, pot fi destinate înrăutăţirii şi ruperii relaţiilor politico-diplomatice, creării unor opinii internaţionale defavorabile statului nostru, interpretării voit eronate a răspunsului la provocări şi justificării, în ultimă instanţă, a agresiunii.

Din perspectiva acţiunilor în spectrul informaţional, o ameninţare[6] reprezintă orice entitate străină sau autohtonă, care are atât capacitatea, cât şi intenţia malignă de a exploata vulnerabilităţile unui sistem sau ale unei componente a unui sistem (care are, ca principal scop, tratarea informaţiei, sistemul de comandă-control, implicit, sistemul de cercetare şi de supraveghere a spaţiului aerian).

În mai puţin de un secol, introducerea tehnologiei informaţiei şi a comunicaţiilor, în toate domeniile activităţii sociale, a schimbat semnificativ modul în care oamenii şi organizaţiile obţin sau diseminează informaţii, ori desfăşoară acţiuni, permiţând o mai mare eficienţă, un control operaţional sporit şi un acces rapid la informaţii. Alături de multe beneficii însă, computerele şi interconectarea aduc şi aspecte negative, cum ar fi apariţia unor noi tipuri de infracţiuni, precum şi posibilitatea de comitere a unor infracţiuni clasice, prin intermediul noilor tehnologii.

Proliferarea tehnicii şi a computerelor, din ce în ce mai puternice şi mai disponibile, precum şi dramatica expansiune a interconectivităţii au dat potenţialilor agresori posibilitatea să realizeze atacuri rapide, fără constrângeri geografice, adesea cu consecinţe grave pentru victime şi cu probabilitate mică de detectare şi mai ales de incriminare a acestora.

Deoarece atacurile cibernetice asupra sistemelor informaţionale pot produce o serie de consecinţe negative – strategice, operaţionale, legale sau financiare –, la nivel individual, organizaţional, sau chiar naţional, riscurile de atac cibernetic şi informaţional trebuie bine înţelese, pentru a fi minimizate sau eliminate.

În războiul modern, sistemele C4ISR sunt ţinta unor intense acţiuni destabilizatoare, de natură informaţională şi fizică, cu scopul de a le dezorganiza sau de a le scoate din funcţiune, datorită importanţei deosebite[7]. Principalele categorii de ameninţări sunt: ameninţările intrinseci (erori umane, supraîncărcarea informaţională, defectarea echipamentelor), acţiuni şi ameninţări ale adversarului (acţiuni de distrugere fizică: ale aviaţiei, ale artileriei, ale armelor de nimicire în masă, ale grupurilor de cercetare diversiune; acţiuni de neutralizare/destabilizare: bruiaj radio, viruşi, inducere în eroare, acţiuni psihologice) şi condiţiile de mediu (intemperii, fenomene naturale).

Principalele riscuri informaţionale asupra sistemelor C4ISR, potenţialii atacatori şi motivaţiile acestora, tipurile de ameninţări, de vulnerabilităţi şi de expuneri, precum şi modalităţile de abordare a analizei de risc asupra sistemelor militare C4ISR nu diferă de sistemele civile.

Riscul atacului electronic

Sistemele informaţionale computerizate sunt esenţiale pentru buna desfăşurare a majorităţii activităţilor militare moderne şi, pe cale de consecinţă, securitatea acestora trebuie să fie o preocupare importantă a organizaţiei militare.

O serie de elemente au contribuit la creşterea riscului de atac cibernetic/electronic la adresa sistemelor informaţionale militare, cum ar fi: dificultăţile inerente de securizare, globalizarea crescândă, insuficienta înţelegere de către utilizatorii sistemelor de informaţii militare şi comportamentele care nu respectă procedurile de folosire sau standardele impuse, disponibilitatea privind penetrarea fără autorizare a sistemelor de informaţii militare, reglementările legislative neclare şi anumite dificultăţi jurisdicţionale.

Riscul este, în contextul sistemelor informaţionale computerizate, suma ameninţărilor (evenimentelor care pot cauza disfuncţii şi pagube), a vulnerabilităţilor şi valoarea informaţiilor expuse sau compromise:

$$Risc = Ameninţări + Vulnerabilităţi + Valoarea\ informaţiilor$$

Informaţiile sunt evaluate în raport cu posibilul impact al unui incident care va afecta negativ informaţiile. Ameninţările, vulnerabilităţile şi posibilul impact trebuie combinate pentru a obţine o măsură a riscului la care sunt expuse informaţiile.

Următoarea figură este o schemă sugestivă a conceptelor privind securitatea sistemelor informaţionalizate/ computerizate şi relaţiile dintre acestea, care este descrisă în standardul *Common Criteria for Information Technology Security Evaluation*. Schema arată conexiunea şi legătura dintre riscuri, ameninţări şi vulnerabilităţi, precum şi dintre proprietarul sistemului, atacatori şi informaţiile vehiculate în sistem.

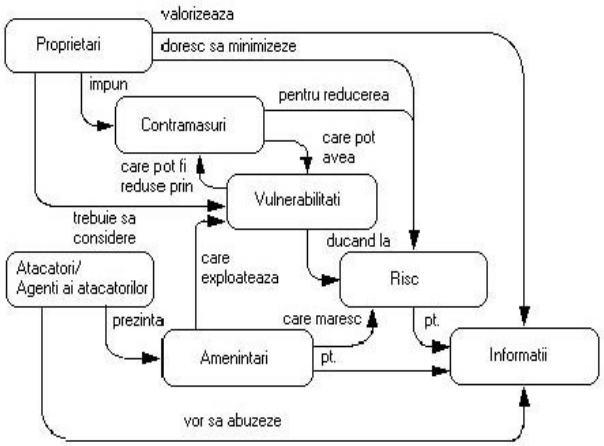

Fig. 1 *Conceptele privind securitatea sistemelor de informaţii şi relaţiile dintre acestea*

Atacatori, vulnerabilităţi şi ameninţări

În lucrarea *Encyclopedia of Computer Science and Technology*[8], autorii consideră că următorii actori pot cauza probleme de securitate a sistemelor informaţionale computerizate:

a. angajaţii – aceştia sunt autorizaţi pentru accesul la sistemele informatice, ceea ce le permite

cunoaşterea slăbiciunilor sistemelor, efectuarea unor operaţiuni, care pot fi în detrimentul organizaţiilor, precum şi ştergerea evidenţelor digitale;

b. consultanţii / personalul de întreţinere – aceste persoane au acces la zonele sensibile ale sistemului informaţional, ceea ce le permite efectuarea unor operaţiuni diverse;

c. furnizorii / clienţii – motivele lor economice nu sunt, în unele cazuri, congruente cu cele ale organizaţiei şi pot efectua anumite acţiuni, care pot prezenta riscuri de securitate;

d. competitorii – actori, care vor avea de câştigat de pe urma pierderilor organizaţiei, cauzate de atacuri asupra sistemului de informaţii;

e. crackerii[9] */ mercenarii informatici / infractorii profesionişti* – persoane care penetrează ilegal sistemele de informaţii şi cauzează intenţionat daune, motivaţiile fiind, în genere, diverse;

f. experţii în spionaj – persoane care sunt specializate în obţinerea unor informaţii, de care vor beneficia alte organizaţii. Aceste persoane au un nivel înalt de cunoştinţe tehnice, sunt bine plătite şi îşi pot realiza acţiunile, fără să fie detectate.

John D. Howard, investitor american, consideră şase categorii de agresori:

- *hackeri* – persoane care invadează sistemele informatice, din provocări intelectuale, pentru obţinerea sau menţinerea unei poziţii în comunitate;
- *spioni* – persoane care pătrund în sistemele informatice de nivel strategic, pentru a obţine informaţii care asigură poziţii favorabile, din perspectivă strategică, politică sau militară;
- *terorişti* – persoane care invadează sistemele informatice, cu scopul de a produce haos şi panică;
- *atacatori cu scop economic* – cei care accesează sistemele informatice, cu scopul de a obţine câştiguri financiare;
- *criminali de profesie* – cei care pătrund în sistemele informatice ale actorilor economici, pentru a obţine câştig financiar, în interes personal sau pentru a face rău intenţionat;
- *vandali* – persoane care pătrund în sistemele informatice, cu scopul de a produce pagube şi de a destabiliza.

Direction de la Surveillance du Territoire din Franţa subliniază diferenţele dintre ameninţările de tip ludic (ale hackerilor), cele care vizează câştiguri financiare, şi cele cu efecte strategice (spionaj militar, spionaj economic etc.).

Autorii americani propun o analiză mai complexă, bazată pe determinantele conduitei criminale, acestea implicând elemente motivaţionale (având caracteristici personale – motive militare, financiare, doctrinare sau psihologice), elemente care ţin de oportunitate (reprezentând caracteristici ale mediului – apartenenţa la grupări criminale, recunoaştere socială, încrederea şi afilierea la un grup), mijloace şi metode.

Accidentele / dezastrele naturale pot cauza distrugerea unor informaţii relevante sau deteriorarea acestora.

Ameninţările sunt specifice pentru fiecare sistem în parte şi reprezintă ceea ce s-ar putea întâmpla nedorit sau ceea ce ar putea destabiliza un sistem. Ameninţările sunt diverse şi obiectivele atacatorilor constau în obţinerea unor avantaje pentru alţii sau pentru sine, ori doar compromiterea şi destabilizarea sistemului informaţional. Ameninţările au fost definite astfel:

- posibil pericol la adresa sistemului informaţional;
- circumstanţa care are potenţialul să cauzeze pierdere organizaţiei/sistemului;
- o circumstanţă sau un eveniment care poate cauza violarea securităţii sistemului.

Vulnerabilităţile se datorează lacunelor sau defectelor de proiectare, de testare, de execuţie şi de implementare, de exploatare sau de mentenanţă a programelor. Acestea fac ca un sistem informaţional să fie mai atrăgător în a fi atacat eficient şi au fost definite după cum urmează:

- puncte ale sistemului susceptibil a fi atacate;
- slăbiciune a sistemului de securitate care poate fi intenţionat folosită pentru a cauza un prejudiciu;
- anumite slăbiciuni ale unui sistem care vor permite violarea securităţii sale.

În conformitate cu *Legea nr. 161/2003*, prin *măsuri de securitate* se înţelege folosirea unor proceduri, dispozitive sau programe informatice specializate, cu ajutorul cărora accesul la un sistem informatic este restricţionat sau interzis pentru anumite categorii de utilizatori[10].

Personalul cu responsabilităţi în asigurarea securităţii trebuie să fie tot timpul în alertă. Niciodată securitatea nu va fi efectivă şi la nivel maxim. Va exista, întotdeauna, o portiţă care să fie folosită pentru lansarea unui atac. Important este ca acel atac să fie descoperit cât mai repede şi să fie

contracarat. Ideal ar fi ca aceste măsuri să ducă la descoperirea şi la pedepsirea vinovatului.

Clasificarea riscurilor şi a ameninţărilor se poate face după mai multe criterii. Voi încerca să analizez câteva dintre acestea.

Pe baza criteriului de acţiune asupra componentelor hardware sau software, se pot identifica:

- interceptarea cablurilor şi a semnalelor emise;
- căutarea prin fişierele şterse;
- hărţuirea;
- mascarea;
- pirateria software;
- copierea neautorizată de date;
- analiza traficului;
- uşile ascunse;
- canalele ascunse;
- viruşii şi viermii;
- deturnarea sesiunilor;
- atacurile temporare;
- caii troieni;
- simularea IP;
- distrugerea datelor;
- interceptarea parolelor;
- privilegiile excesive;
- scanarea.

Pe baza criteriului modului de acces la sistemul informatic, se pot identifica:

- sustragerea de informaţii externe (privitul peste umăr, furtul);
- abuzul extern al componentelor (distrugerea unui hard disk);
- mascarea (înregistrarea şi redarea ulterioară);
- programe dăunătoare (instalarea unui program cu scop distructiv);
- evitarea autentificării sau a autorizării (spargerea parolei);
- abuzul de autoritate (falsificarea înregistrărilor);
- abuzul intenţionat (administrarea intenţionat defectuoasă);
- abuzul indirect (utilizarea unui alt program sau sistem pentru a realiza o acţiune sau un program rău intenţionat).

Clasificarea, conform criteriului acţional, focalizată doar pe informaţia în tranzit, prezintă următoarele patru categorii de atacuri:

- întreruperea – o componentă a sistemului este distrusă sau devine neutilizabilă ori indisponibilă;
- interceptarea – o componentă neautorizată realizează accesul la un bun al sistemului;
- modificarea – o componentă neautorizată nu numai că obţine acces, dar şi realizează modificări;
- falsificarea – o componentă neautorizată introduce obiecte modificate sau contrafăcute în sistemul informatic.

Când datele sau informaţiile sunt citite, folosite sau copiate de cineva neautorizat, rezultatul este cunoscut ca *pierderea confidenţialităţii*. Pentru câteva tipuri de informaţii, confidenţialitatea este un atribut foarte important.

Referindu-ne la sistemele C4ISR, informaţia poate fi alterată, când este disponibilă pe o reţea nesigură. Când informaţia este modificată în moduri neaşteptate, rezultatul este cunoscut drept *pierderea integrităţii*. Aceasta înseamnă că datele suferă modificări neautorizate, fie ca urmare a unei greşeli umane, fie prin modificare intenţionată. Integritatea este importantă în siguranţa infrastructurii critice şi a datelor referitoare la controlul traficului aerian, a cunoaşterii situaţiei aeriene, dar şi navale, terestre şi de mediu.

Informaţia poate lipsi sau poate deveni inaccesibilă, rezultând o *lipsă de disponibilitate*. Aceasta înseamnă că persoanele care sunt autorizate să obţină informaţii nu pot obţine ceea ce doresc, acest lucru afectând desfăşurarea operaţiilor militare conduse cu sisteme C4ISR.

Ca o concluzie, pe măsură ce instituţiile devin tot mai dependente de funcţionarea sistemelor informaţionalizate şi computerizate, problema securităţii acestor sisteme este tot mai relevantă. Doar investind în securitate vom putea avea sisteme C4ISR mai sigure. De multe ori, vom constata că beneficiile vor fi mai mari, iar investiţiile şi eforturile făcute vor fi mai mici, dacă abordăm ansamblul sistemului, decât dacă tratăm problema punctual sau, mai rău, dacă acţionăm pentru a înlătura efectele abia după producerea unui incident de securitate, incident care poate leza securitatea naţională, prin deconspirarea intenţiilor sistemului de comandă-control, a situaţiei şi a poziţiei forţelor adverse şi a celor proprii, din sistemele C4I2SR[11].

NOTE:

1 *** *Strategia de Securitate Naţională a României*, Bucureşti 2007, p. 3.

2 *Necesitatea implementării sistemului ISTAR pentru asigurarea unor capacităţi de informaţii operaţionale şi interoperabile cu structuri similare NATO*, MApN, 2007, p. 5.

3 Cristian Mateescu, *Sisteme de comandă-control*, Editura MatrixRom, Bucureşti, 2004, p. 41.

4 Constantin Alexandrescu, Gelu Alexandrescu, Gheorghe Boaru, *Sisteme informaţionale militare*, Editura UNAp „Carol I”, Bucureşti, 2010, p. 10.

5 Cristian Mateescu, *op.cit.*, p. 42.

6 Vasile Păun, A. Popa, *O provocare strategică – Războiul Informaţional,* Editura UTI, Bucureşti, 2002, p. 62.

7 Cristea Dumitru, *Sisteme C4I*, Editura Militară, Bucureşti, 2005, p. 242.

8 Fred Cohen ş.a., *Encyclopedia of Computer Science and Technology*, 1998.

9 R. Stallman (1984), care se autointitulează hacker, şi recomandă folosirea termenului „cracker” pentru cei care penetrează sistemele de informaţii prin încălcarea măsurilor de securitate.

10 *Legea nr. 161*, *privind unele măsuri pentru asigurarea transparenței în exercitarea demnităților publice, a funcțiilor publice și în mediul de afaceri, prevenirea și sancționarea corupției*, art. 35, alin (1), din 2003.

11 C4I2SR – Comandă, Control, Comunicaţii, Computere, Interoperabilitate, Informaţii, Supraveghere, Cercetare.

BIBLIOGRAFIE

*** *Doctrina Naţională de Informaţii pentru Securitate*, Bucureşti, 2004.

*** *Manualul pentru luptă al unităţilor de cercetare*, Editura Tehnică Militară, Bucureşti, 2005.

*** *Manualul pentru pregătirea informativă a câmpului de luptă*, Editura Tehnică Militară, Bucureşti, 2005.

*** *Legea nr. 161*, *privind unele măsuri pentru asigurarea transparenței în exercitarea demnităților publice, a funcțiilor publice și în mediul de afaceri, prevenirea și sancționarea corupției*, art. 35, alin. (1), din 2003.

Alexandrescu Constantin, Alexandrescu Gelu, Boaru Gheorghe, *Sisteme informaţionale militare, servicii şi tehnologie*, Editura Universității Naționale de Apărare „Carol I”, Bucureşti, 2010.

Dumitru Cristea, *Sisteme C4I*, Editura Militară, Bucureşti, 2005.

Mateescu Cristian, *Sisteme de comandă-control*, Editura MatrixRom, Bucureşti, 2004.

Maxim Gheorghe, *Supravegherea spaţiului aerian al României în condiţii de război informaţional*, Editura Universității Naționale de Apărare „Carol I”, Bucureşti, 2006.

Păun Vasile, Popa A., *O provocare strategică – Războiul Informaţional,* Editura UTI, Bucureşti, 2002.

www.securitatea-iformatica.ro, accesat la 28.04.2017.