PROTECȚIA INFRASTRUCTURILOR CRITICE DIN DOMENIUL COMUNICAȚIILOR ŞI TEHNOLOGIEI INFORMAȚIILOR

CRITICAL INFRASTRUCTURES PROTECTION IN THE COMMUNICATIONS AND INFORMATION TEHNOLOGIES FIELD

Colonel (r) prof. univ. dr. Gheorghe BOARU*
Colonel (r) prof. univ. dr. ing. Eugen SITEANU**

Sunt analizate tehnologia informației, amenințările asupra infrastructurilor critice informaționale şi războiul cybernetic în contextul revoluțiilor în afacerile militare, al protecției şi vulnerabilităților infrastructurilor critice informaționale.

Cuvinte cheie: *tehnologia informației; amenințări; vulnerabilități; infrastructuri critice informaționale; război cibernetic.*

The information technology, the threats to information critical infrastructures, the cyberwar are analyzed in the context of revolutions in military affairs (RMAS) and of information critical infrastructures vulnerabilities and protection.

Keywords*: information tehnology; threats; vulnerabilities; informational critical infrastructures; cyberware.*

În condițiile actuale de dezvoltare a societății, informațiile şi tehnologiile de comunicații, alături de alte sisteme şi rețele importante, constituie *infrastructuri critice*[1], iar metodele de asigurare a securității reprezintă un mijloc de protecție a

* boarugheorghe@yahoo.com
** Profesor univ. dr. ing., Academia Comercială, Satu Mare şi Universitatea Națională de Apărare „Carol I"; membru asociat al AOŞR; e-mail: esiteanu@yahoo.com

[1] *Infrastructura critică* este reprezentată de un element, un sistem sau o componentă a acestuia care este esențial pentru menținerea funcțiilor societale vitale, a sănătății, siguranței, securității, bunăstării sociale sau

datelor şi informaţiilor, a sistemelor informaţionale, aplicaţiilor informatice şi bazelor de date împotriva accesului neautorizat, dezvăluirii, utilizării, modificării sau distrugerii acestora. Scopul măsurilor de securitate constă în asigurarea confidenţialităţii, integrităţii şi disponibilităţii informaţiei, precum şi a operării corecte a sistemelor (reţelelor) de calcul. De asemenea, trebuie să permită, oricărei persoane autorizate, accesibilitatea la resursele de calcul ale reţelei, prin mijloacele hardware şi software ale acesteia.

Tehnologia informaţiei şi comunicaţiilor

Tehnologia informaţiei şi comunicaţiilor constituie o „*locomotivă*" a schimbărilor din lumea contemporană, iar noua putere militară depinde de aceasta. Ea nu este importantă numai din punct de vedere tehnologic, ci şi prin abilitatea sa de a selecta, organiza, analiza şi utiliza efectiv informaţia pentru construirea de cunoştinţe, precum şi prin disponibilitatea sa de a asigura acces la cunoştinţe şi a realiza comunicarea la orice distanţă, aducându-şi contribuţia la dezvoltarea activităţii de creaţie ştiinţifică, educaţie şi management.

Tehnologia informaţiei şi comunicaţiilor este sursă a avantajului competitiv şi a performanţei structurii militare (organizaţiei), asigurând potenţialul necesar pentru multiplicarea letalităţii şi mobilităţii forţelor, îmbunătăţirea eficienţei şi eficacităţii operaţionale. Corelat cu conceptul de infrastructură informaţională, a fost creat un nou mediu de luptă, separat pentru interacţiunea interumană, anume „*ciberspaţiu*" similar cu cele deja cunoscute (aerian, terestru, naval). De aceea, forţele militare ale erei informaţionale evoluează în direcţia utilizării acestei tehnologii în ciberspaţiu, adaptându-şi corespunzător structura organizatorică.

Tehnologia informaţiei şi comunicaţiilor[2] este un termen colectiv pentru diferite tehnici privind procesarea, controlul electronic şi securitatea informaţiei, adică generarea (crearea), manipularea, memorarea, regăsirea, prelucrarea[3] automată, comunicarea, diseminarea şi protecţia datelor şi informaţiilor, incluzând texte, grafică, sunete şi imagini video. Ea se bazează pe convergenţa dintre tehnologia informaţiei şi tehnologia comunicaţiei şi constă în aplicarea comunicaţiilor moderne şi a tehnologiei de calcul pentru

economice a persoanelor şi a căror perturbare sau distrugere ar avea un impact semnificativ ca urmare a incapacităţii de a menţine respectivele funcţii [Directiva 2008/114/ CE a Consiliului din 8 decembrie 2008, p.3]. Infrastructurile critice privind tehnologia informaţiei şi comunicaţiilor cuprind: (1) sistemele şi reţelele de informaţii, (2) sistemele de comandă şi control, automatizare şi instrumentare, (3) serviciile de telecomunicaţii fixe şi mobile, (4) sistemele de radiocomunicaţii şi navigare, (5) serviciile de comunicaţii prin satelit, (6) serviciile de radiodifuziune şi televiziune [Programul European pentru protecţia infrastructurilor critice], 12.12.2006.

[2] Reference Answer, *Information and Communication Technology*, în Wikipedia the Free Encyclopedia 10.08.2010 [http//en. Wikipedia.org/wiki/ information and communication technology].

[3] *Prelucrarea datelor* constă în introducerea, verificarea, organizarea, memorarea, regăsirea, transformarea şi extragerea informaţiei din date. Orice proces de prelucrare a informaţiei (organizarea, manipularea şi diseminarea) se desfăşoară în patru faze: introducerea datelor, procesul de prelucrare, ieşirea informaţiei şi memorarea.

crearea, managementul, utilizarea şi protecţia informaţiei, reflectând rolul important pe care îl au calculatoarele în comunicaţii pentru transmiterea de date, e-mail, web, telefonia mobilă, legătura prin sateliţi etc. Această tehnologie cuprinde: date şi informaţii în format electronic necesare structurii militare (organizaţiei), echipamente de culegere a informaţiilor, de calcul şi de comunicaţii împreună cu aparatura electronică conexă, produsele software de aplicaţie şi securitate, bazele de date şi limbajele de programare aferente, reţele de calculatoare şi comunicaţii (hardware şi software), Internet, robotica, videotext, televiziunea prin cablu, poşta electronică, birotica, echipamente de conversie, afişare şi securitate a informaţiei etc.

Informaţia şi tehnologia informaţională trebuie considerate arme principale în lupta armată pentru realizarea obiectivelor naţionale fundamentale.

În aceste condiţii, vulnerabilitatea informaţiei despre mediul de luptă creşte considerabil, iar durata de viaţă a acesteia scade în raport invers proporţional cu dinamica acţiunilor militare, devenind în timp nerelevantă, ceea ce determină apariţia riscului operaţional[4] şi impune o multiplicare însemnată a surselor de informaţii, integrate în reţele complexe, dispuse în spaţiul de luptă, precum şi crearea condiţiilor pentru ca acestea să transmită în timp real volumul de date cules către centrele de integrare şi fuziune a informaţiilor.

S-a dovedit că şi armele războiului cibernetic au viaţă scurtă, întrucât depind de existenţa erorilor software în reţelele adversarului care sunt permanent descoperite şi corectate.

Vulnerabilităţi şi ameninţări privind sistemele informaţionale

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

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

[4] *Riscul operaţional* reprezintă o reuniune complementară, cu o componentă *energetică* de acoperire, care-l face să aibă consecinţe mai mari sau mai mici în caz de nereuşită, dar şi una *informaţională* bazată pe cunoaştere, evaluare, informare şi dezinformare. Componenta informaţională îi asigură dinamismul necesar aprecierii şi evaluării situaţiei [Gh. Ilie, *Securitatea sistemelor militare*, Editura Militară, 1995, p.89].

Vulnerabilităţi informaţionale

Ca în orice domeniu de activitate, şi în cel privind informaţiile şi sistemele informaţionale, există anumite *vulnerabilităţi*[5], adică părţi slabe şi slăbiciuni ale sistemului, infrastructurii, mediului de control sau proiectării reţelelor care nu sunt generate de acţiunile adversarilor, ci de soluţiile proprii adoptate, ce pot fi atacate relativ uşor şi exploatate pentru a deteriora integritatea acelui sistem.

Vulnerabilităţile informaţionale constituie o componentă a vulnerabilităţii de securitate a sistemelor, generată de stări de fapt, procese sau fenomene din viaţa internă a organizaţiei, care diminuează capacitatea de reacţie la riscurile existente ori potenţiale de orice natură, inclusiv informaţionale sau care favorizează apariţia şi dezvoltarea acestora, cu consecinţe privind îndeplinirea obiectivelor stabilite.

În general, vulnerabilităţile informaţionale sunt cu atât mai mari cu cât reţelele informaţionale şi structura informaţiilor sunt de complexitate mai mare, fiind mai greu de organizat, administrat şi protejat. De asemenea, vulnerabilităţile sporesc direct proporţional cu nivelul tehnologic implementat în construcţia şi funcţionarea echipamentelor (mai ales digitale) sistemelor informaţionale. 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 şi comunicaţiilor cu atât va creşte şi vulnerabilitatea sa potenţială. Rezultă că obiectivul principal al conflictelor militare contemporane nu trebuie să se concretizeze, cu precădere, în distrugerea totală a tehnicii, armamentului sau forţei vii a adversarului, ci mai ales în neutralizarea şi dezintegrarea sistemelor complexe ale acestuia, în principal a sistemelor informaţionale.

Principalele vulnerabilităţi ale infrastructurii informaţionale ar putea fi următoarele:

- posibilităţile de interceptare a informaţiilor din reţelele de comunicaţii şi calculatoare atât de către utilizatori, cât şi de către adversari;

- volumul foarte mare de informaţii produse, vehiculate şi prelucrate în sistemele informaţionale, care pot fi supuse cercetării şi atacului adversarilor potenţiali, distruse, falsificate sau sustrase;

- sofisticarea infrastructurii informaţionale, ceea ce determină complexitatea managementului acesteia, imposibilitatea detectării accesului fraudulos la informaţii şi favorizarea atacurilor cibernetice;

- folosirea aceloraşi benzi de frecvenţe, modulaţii şi regimuri de lucru la echipamentele bazate pe propagarea undelor electromagnetice, atât în reţelele de comunicaţii proprii, cât şi în cele ale adversarilor potenţiali;

[5] *Noul dicţionar universal al limbii române*, Editura Litera Internaţional, Bucureşti-Chişinău, 2006, p. 1645.

- utilizarea de echipamente tehnice, componente software şi baze de date cu structuri şi exploatare standardizate (comerciale) în toate reţelele de calculatoare ale organizaţiilor, eventual şi în reţelele de comunicaţii ale acestora;

- dependenţa infrastructurii sistemelor informaţionale ale organizaţiilor de infrastructura informaţională comercială a ţării, ceea ce creează condiţii pentru acces fraudulos şi dezinformare;

- posibilitatea încorporării (ascunderii) din timp, în echipamentele de calcul şi de comunicaţii, de către firmele furnizoare de aparatură, a unor module software malitioase, care pot fi activate de către adversari la momente hotărâte de aceştia, creând dezordine şi haos în reţelele informaţionale şi cele decizionale;

- prin conectarea la Internet, Intranet sau Extranet, organizaţiile devin vulnerabile la pătrunderi neautorizate (cu rea intenţie sau din neatenţie);

- existenţa unor reţele informaţionale cu număr mare de noduri şi cu o largă interconectivitate, greu de sincronizat şi gestionat, ceea ce permite penetrarea acestora, accesul neautorizat, capturarea fizică a unor echipamente sau a unor noduri (centre de comunicaţii) în totalitate, interceptarea sau întreruperea unor fluxuri de informaţii importante şi/sau introducerea de informaţii false care să afecteze procesele decizionale;

- digitalizarea exhaustivă a structurii informaţionale, care are un impact contradictoriu: pe de o parte omogenizează, sincronizează şi sporeşte gradul de compatibilitate şi interoperabilitate a reţelelor informaţionale, iar pe de altă parte determină stăpânirea cu greutate a complexităţii şi a nivelului deosebit de ridicat de tehnicitate al acestora, oferind condiţii pentru atacul cibernetic de la distanţă sau din interiorul lor;

- nerespectarea integrală a cerinţelor şi a standardelor UE şi NATO privind compatibilitatea şi interoperabilitatea sistemelor informaţionale, mai ales în ceea priveşte schimbul de informaţii (formatul mesajelor), accesul la bazele de date, criptarea automată a comunicărilor şi caracteristicile canalelor pentru legătură;

- posibilitatea folosirii de către adversarii potenţiali a războiului electronic împotriva mijloacelor radioelectronice din principalele sisteme informatice şi de comunicaţii[6], cu precădere asupra canalelor care asigură legătura surselor de informaţii cu organele centrale de fuziune şi 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;

[6] C. Alexandrescu, *Ameninţări şi riscuri electronice privind sistemele informaţionale militare moderne în spaţiul de luptă*, în volumul Sesiunea de comunicări ştiinţifice a UNAp „Carol I", „Sisteme Informaţionale SI-2007" (ISBN 978-973-663-496-3), pp. 107-115.

- mijloacele tehnice actuale ale sistemelor informaţionale nu au asigurată protecţia temeinică împotriva atacului fizic, electromagnetic şi cibernetic, acestea putând fi distruse, deteriorate sau penetrate pentru extragerea informaţiei stocate ;

- dispunerea în locuri necorespunzătoare, din punct de vedere funcţional şi al securităţii fizice şi electromagnetice a echipamentelor tehnice ale sistemelor informaţionale, în principal a mijloacelor de comunicaţii şi de calcul, ceea ce sporeşte vulnerabilitatea la interceptare a informaţiilor şi la atacul fizic;

- utilizarea pentru exploatarea sistemelor informaţionale a unor persoane insuficient verificate şi neloiale, predispuse a fi racolate de către adversarii potenţiali şi determinate să efectueze acţiuni de sabotaj sau să furnizeze acestora informaţii obţinute în mod 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, ceea ce determină atenuarea, modificarea aleatoare a direcţiei de propagare şi reflectarea numai parţială a undelor electromagnetice;

- 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 radiocomunicaţii 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 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 şi atac cibernetic asupra infrastructurii informaţionale;

- proiectarea necorespunzătoare a infrastructurii, cu redundanţă informaţională redusă, centralizată excesiv şi cu posibilităţi scăzute de replicare a informaţiilor existente în bazele de date;

- preocuparea insuficientă pentru ascunderea şi mascarea elementelor infrastructurii informaţionale, măsuri neadecvate de pază şi apărare ale acestora;

- măsurile insuficient studiate de asigurare a securităţii comunicaţiilor (COMSEC), calculatoarelor (COMPUSEC[7]) şi a echipamentelor electronice în ansamblu, prin interzicerea (restricţionarea) interceptării radiaţiilor parazite (protecţia TEMPEST - Transient ElectroMagnetic Pulse Emanation STandard).

Din prezentarea efectuată rezultă că există numeroase vulnerabilităţi, dar dintre acestea esenţiale sunt cele care privesc: neorganizarea optimă a sistemelor informaţionale,

[7] *COMPUSEC* (Computer security) – securitatea calculatoarelor.

alegerea necorespunzătoare a echipamentelor tehnice utilizate şi a produselor software comerciale, realizarea programelor (software) de aplicaţii şi a bazelor de date, precum şi a produselor software pentru criptarea automată a informaţiilor în sistemele informaţionale, sub standardele impuse.

Adaptarea sistemelor la mediul de informaţii impune echiparea acestora cu mijloace tehnice capabile să suporte, în cazuri extreme, fluxuri informaţionale de 2-3 ori mai mari decât în condiţii normale de funcţionare.

Ameninţări informaţionale

Ameninţările privind sistemele informaţionale sunt omniprezente în societatea modernă bazată pe informaţii şi cunoştinţe. Acestea sunt cu atât mai periculoase cu cât necesarul de informaţii reale şi oportune pentru luarea deciziei şi executarea acţiunilor este mai mare şi trebuie asigurat în timp cât mai scurt.

În general, ameninţarea[8] este acel pericol posibil la care este expus un sistem informaţional şi poate consta în acces neautorizat, modificarea sau distrugerea resurselor de date şi informaţii ale unei organizaţii. Pericolul poate fi reprezentat de o persoană (hacker), o componentă a reţelei (echipament deteriorat) sau un accident (foc, inundaţii), care pot exploata vulnerabilităţile sistemului.

Ameninţările sunt generate[9] atât de factori interni unui sistem informaţional, cât şi de factori externi, rezultaţi din acţiunea intenţionată a adversarului contra informaţiilor, bazată pe vulnerabilităţile specifice. Ambele grupe de factori pot avea influenţe destabilizatoare majore asupra capacităţii sistemelor informaţionale de a produce şi de a furniza în timp real informaţiile necesare.

Factorii interni pot fi identificaţi şi înlăturaţi prin observarea sistemelor informaţionale şi prin organizarea, proiectarea corectă, dotarea cu echipamente tehnice performante şi stabilirea precisă a condiţiilor lor de funcţionare, exploatare şi securitate, astfel încât influenţa acestora poate fi diminuată sau chiar înlăturată complet.

Spre deosebire de aceştia, factorii externi pot fi cunoscuţi din timp, pe baza studiului doctrinelor, legilor şi acţiunilor statelor şi organizaţiilor (forţelor) potenţial ostile, dar conţinutul lor concret va depinde de condiţiile din mediul politic, economic şi de securitate din sfera internaţională şi de atingerea pe care o aduce intereselor organizaţiei. Desigur, ameninţările externe vor exploata la maxim vulnerabilităţile sistemelor informaţionale şi, în mod logic, rezultă că pentru diminuarea acestora se impune reducerea vulnerabilităţilor, continua perfecţionare şi protecţie a sistemelor, eventual activarea în caz de pericol a unor metode şi tehnici de lucru păstrate în secret.

---

[8] *Noul dicţionar universal al limbii române*, Editura Litera Internaţional, Bucureşti-Chişinău, 2006, p. 66.

[9] C. Alexandrescu, *Ameninţări informaţionale asupra sistemelor de comandă şi control în acţiunile militare moderne*, în volumul Sesiunea de comunicări ştiinţifice a UNAp „Carol I" „Sisteme informaţionale SI-2007" (ISBN 978-973—663-496-3), pp. 116-122.

Ameninţări informaţionale interne

Experienţa dobândită de specialiştii în domeniu evidenţiază următorii factori interni, care pot constitui ameninţări asupra sistemelor informaţionale:

- lipsa de preocupare pentru dobândirea superiorităţii informaţionale asupra organizaţiilor adversare (concurente), potenţial ostile;
- neconcordanţă între cerinţele de informaţii pentru luarea deciziilor şi conducerea acţiunilor şi posibilităţile reale de dobândire a acestora;
- proiectarea, organizarea sau funcţionarea necorespunzătoare a sistemelor informaţionale;
- dotarea sistemelor informaţionale cu mijloace de culegere a datelor, comunicaţii şi calculatoare neperformante, greu de exploatat şi de asigurat protecţia, utilizarea incorectă a acestora;
- organizarea necorespunzătoare a bazelor de date, existenţa unor produse software neperformante sau cu erori intenţionate, pentru gestiunea, prelucrarea şi afişarea informaţiilor, lipsa de preocupare privind utilizarea inteligenţei artificiale pentru realizarea activităţilor informaţionale şi a celor de management;
- slaba pregătire profesională şi experienţa redusă a personalului implicat în organizarea, exploatarea şi asigurarea funcţionării neîntrerupte a sistemelor informaţionale;
- clasificarea necorespunzătoare a categoriilor de informaţii şi date, certificarea eronată a dreptului de acces la acestea a personalului;
- neloialitatea unor persoane care exploatează echipamentele tehnice ale sistemelor informaţionale;
- securitatea redusă a datelor şi a informaţiilor pe timpul transmiterii, memorării, prelucrării şi afişării acestora, accesul neautorizat al unor persoane străine.

Fragilitatea superiorităţii informaţionale este dată de calitatea informaţiei de a fi obţinută în timp real, cu forţele şi mijloacele structurilor de informaţii specializate, precum şi din surse deschise sau primite de la organele cu care cooperează. Caracterul nonliniar al informaţiei[10] determină ca mici intrări de date la adversar să poată produce efecte disproporţionate asupra organizaţiei.

Organizarea necorespunzătoare a sistemelor informaţionale, lipsa de preocupare pentru funcţionarea acestora şi înlăturarea defecţiunilor ce pot să apară, constituie cauza principală a lipsei de informaţii relevante şi a imposibilităţii dobândirii superiorităţii informaţionale asupra organizaţiilor aflate în competiţie. Trebuie să se aibă în vedere că informatica şi comunicaţiile moderne, deşi au un rol hotărâtor, prezintă şi numeroase vulnerabilităţi tehnologice care trebuie diminuate sau înlăturate prin măsuri organizatorice şi tehnice adecvate.

[10] M. Staş, V. Păun, *Spaţiul de conflict informaţional*, Editura Pro Humanitate, Bucureşti, 1998, p.63.

Chiar dacă nu sunt supuse atacului informaţional al adversarilor potenţiali, bazele de date şi produsele software pot crea neajunsuri serioase în cazul când nu sunt organizate, realizate şi exploatate corespunzător. Principala răspundere pentru funcţionarea lor eficientă revine personalului de specialitate din sistemul informaţional, mai ales inginerilor, analiştilor şi programatorilor, precum şi operatorilor de la mijloacele de comunicaţii.

Corelat cu aceasta, un impact major asupra informaţiilor îl are realizarea unei securităţi reduse a acestora în toate verigile sistemelor informaţionale, care creează posibilităţi de acces neautorizat şi de transmitere la adversar a unor date, datorită lipsei de loialitate a unor persoane care sunt implicate în vehicularea fluxurilor informaţionale.

De asemenea, există şi cauze tehnice care pot constitui ameninţări informaţionale interne, rezultate mai ales din dotarea necorespunzătoare cu echipamente moderne de culegere, transmitere şi prelucrare a informaţiei, precum şi cu loturi de rezervă pentru acestea.

Se impune, aşadar, efectuarea unor cheltuieli importante pentru dotarea sistemelor informaţionale cu tehnică modernă pentru obţinerea succesului în realizarea obiectivelor organizaţiei.

Ameninţări informaţionale externe

Ameninţările informaţionale externe cuprind ansamblul acţiunilor specifice, executate de adversarii potenţiali, pentru interzicerea sau îngreuierea executării funcţiilor decizionale şi operaţionale ale organizaţiei. Acestea urmăresc limitarea sau excluderea activităţilor proprii privind culegerea de informaţii, deteriorarea sau distrugerea senzorilor şi a altor surse de date şi interzicerea funcţiilor informaţionale.

Conform concluziilor formulate în literatura de specialitate[11], principalele ameninţări informaţionale externe asupra structurilor decizionale şi acţionale ale organizaţiei sunt următoarele:

- atacul fizic împotriva surselor de date şi a mijloacelor de transmitere, prelucrare şi afişare a informaţiilor;
- atacul electronic asupra mijloacelor de culegere, transmitere şi prelucrare a informaţiilor;
- atacul cibernetic împotriva sistemelor informaţionale ale organizaţiilor economice, financiare, militare etc.;
- pirateria software;
- atacul fizic şi electronic asupra organelor decizionale ale organizaţiei;
- atacul psihologic asupra tuturor structurilor decizionale şi acţionale ale organizaţiei.

Aceste ameninţări nu sunt noi, ele fiind generate de însăşi dezvoltarea societăţii informaţionale, dar trebuie cunoscute, studiate cu atenţie şi stabilite cu precizie măsurile corespunzătoare pentru combaterea lor.

---

[11] J. S. Gansler, H.Binnendijc, *Information Assurance, Trends in Vulnerabilities, Threats and Technologyes*, pp. 18-22.

Atacul cibernetic reprezintă o ameninţare informaţională deosebit de importantă, ce are în vedere „*spaţiul virtual*" care vizează mai ales produsele software şi firmware, protocoalele şi bazele de date ale sistemelor informatice utilizate în reţelele de calculatoare şi de comunicaţii. El reprezintă confruntarea dintre două tendinţe privind securitatea şi insecuritatea în cadrul aceluiaşi sistem informatic, dusă cu mijloace software şi alte produse specifice, fără respectarea regulilor şi standardelor de lucru în cadrul acestuia, în scopul distrugerii sau modificării produselor program şi sustragerii de date şi informaţii.

Acţiunile externe specifice atacului cibernetic au în vedere reducerea însemnată a posibilităţilor de efectuare corectă a serviciilor în cadrul sistemului informaţional, deteriorarea software-ului de aplicaţie ce are, de regulă, caracter confidenţial sau secret, pentru a genera informaţii greşite din datele prelucrate, care afectează procesele decizionale.

Aceste ameninţări externe sunt favorizate de neaplicarea anumitor reguli de protecţie şi securizare a informaţiilor pe timpul transmiterii şi prelucrării datelor culese de către surse. Ele fructifică lacune şi/sau slăbiciuni existente în structura sistemului de securitate a reţelelor proprii de comunicaţii şi calculatoare.

Atacul cibernetic are legături cu pirateria software[12], care poate fi desfăşurată de agresori locali sau plasaţi în orice punct din spaţiul informatic interconectat şi urmăresc, după caz, paralizarea completă a sistemelor informatice sau defectarea (căderea) lor intermitentă la momente de timp dinainte stabilite.

Pentru penetrarea reţelelor de calculatoare se pot utiliza diferite procedee bazate pe software cu acţiune distructivă. Acesta este denumit malsoftware (software rău intenţionat) şi cuprinde produse software cu combinaţii sofisticate de rutine, pentru atac la ţintă precisă, în vederea obţinerii de către inamic a unor avantaje imediate sau ulterioare.

Dintre tipurile de produse software distructive se pot menţiona, în principal, viruşii informatici, bombele logice şi caii troieni. Aceştia pot fi implementaţi din timp în sistemele informatice şi pot acţiona prin diferite procedee, cum ar fi produse software instalate fraudulos în diferite reţele de comunicaţii şi de calculatoare, comandate de la distanţă prin impulsuri electromagnetice sau secvenţe de programe cu viruşi introduse în calculatoare sub formă de mesaje, prin poşta electronică sau pe altă cale.

Surse ale produselor software rău intenţionate sunt în principal din exteriorul sistemelor informaţionale proprii (hackeri, spioni etc.), dar pot fi şi din interiorul acestora (personal neloial, sabotori).

Atacul cibernetic urmăreşte şi deteriorarea programelor (sistemelor expert) folosite în procesele decizionale şi acţionale, ceea ce depăşeşte cu mult sfera informaţională propriu-zisă şi poate genera decizii greşite care, într-o formă sau alta, să avantajeze adversarii potenţiali.

[12] M. Staş, V. Păun, *op. cit.,* p.52.

Prin urmare, organizarea optimă a sistemelor informaționale constituie condiția fundamentală pentru funcționarea eficientă a acestora, reconfigurarea, mobilitatea şi adaptabilitatea lor la mediul de informații în continuă dezvoltare.

Condițiile, restricțiile şi standardele ce trebuie avute în vedere ca țară membră a UE şi NATO se impun a fi respectate în totalitate şi aplicate cu fermitate, pentru a se îndeplini criteriile de compatibilitate şi interoperabilitate cu alte organizații din țară şi din exterior.

Informațiile clasificate vor fi diseminate numai persoanelor care dețin un certificat de securitate corespunzător.

Conform reglementărilor NATO[13], aplicarea standardelor minime de asigurare a securității informațiilor este obligatorie pentru tot personalul sistemului informațional, iar protecția informațiilor[14] clasificate este responsabilitatea fiecărei persoane care deține, procesează sau are cunoştință de asemenea informații. Vulnerabilitățile şi amenințările detaliate anterior impun, în mod necesar, adoptarea unor măsuri corespunzătoare de securitate a sistemelor informaționale.

Securitatea informației şi a sistemelor informaționale militare

Măsurile de protecție trebuie să asigure continuitatea *serviciilor informaționale*[15], care cuprind: infrastructura tehnologiei informației şi comunicațiilor, managementul informației şi al spectrului electromagnetic, căile de comunicații, puterea de calcul (rețele de calculatoare, software şi baze de date), operațiile în rețea incluse în rețeaua informațională globală.

Aceste măsuri includ, cel puțin:

- securitatea operațiilor (OPSEC);
- securitatea informațiilor (INFOSEC);
- protecția împotriva acțiunilor inamicului privind supravegherea şi recunoaşterea spațiului de luptă şi achiziția țintelor.

Dintre componentele menționate, avem în vedere numai partea privind securitatea informațiilor (INFOSEC) care implică nemijlocit şi securitatea sistemelor informaționale (INFOSYS).

Războiul cybernetic (CYBERWAR)

Spațiul digital, cunoscut sub numele de cyberspace, a devenit al cincilea spațiu de luptă, după pământ, apă, aer şi spațiul cosmic. Pentagonul a recunoscut oficial cyberspace-

---

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

[14] *Protecția informațiilor* este determinată de diversitatea şi specificitatea domeniilor, problemelor şi profilurilor de activitate, de particularitățile mediului informațional, de perfecționarea şi diversificarea accentuată a mijloacelor, tehnicilor şi tehnologiilor de obținere, prelucrare, analiză, procesare şi transmitere operativă a datelor, informațiilor şi produselor informaționale, precum şi de pericolul sustragerii, accesării şi utilizării ilegale a informațiilor de către persoane neautorizate [1, p.29].

[15] Information Operations, Air Force Doctrine, doc.2-5/2002, p.70.

ul ca nou spaţiu al războiului, considerat la fel de critic pentru operaţiile militare, precum şi celelalte patru domenii: pământul, aerul, apa şi spaţiul cosmic[16].

În SUA există îngrijorări, la cel mai înalt nivel al instituţiilor statului, referitoare la riscurile şi implicaţiile unui eventual atac asupra infrastructurii IT a SUA. Rapoartele oficialilor recunosc că securitatea naţională, prosperitatea economică, precum şi buna funcţionare a guvernului depind de infrastructura informaţională, care include: telecomunicaţiile, reţelele de calculatoare şi informaţiile stocate pe acestea[17].

Deşi statele moderne sunt extrem de sensibile în legătură cu informaţiile despre noul domeniu, au apărut deja scenarii privind folosirea cyberspace-ului, ca spaţiu al acţiunilor de luptă şi/sau operaţiilor. Se ştie, deja, că reţelele de socializare oferă un spaţiu generos pentru serviciile de informaţii pentru a colecta informaţii despre adversari, direct, prin folosirea informaţiilor postate de către utilizatorii naivi ai acestor reţele, sau prin penetrarea sistemelor conectate la Internet dar insuficient protejate. În plus, grupări teroriste sau guverne alte unor ţări adverse pot penetra reţelele conectate la Internet care permit folosirea serviciilor reţelelor de socializare şi a sit-urilor cu tehnologii Web 2.0, pentru compromiterea informaţiilor stocate pe acestea, compromiterea acestora, sau folosirea acestora drept bot.

Cyberwar, armele acestuia şi măsurile de apărare

Părerile specialiştilor cyberwar sunt de multe ori antagoniste; „*mouse-ul şi tastatura sunt noile arme ale viitorului*[18] contra posibilitatea „*unui atac apocaliptic asupra infrastructurii SUA*" este mai degrabă scenariu de film.

Războiul cibernetic, Cyberwar, este definit ca „*acţiunile unui stat de a penetra calculatoarele sau reţelele de calculatoare ale altui stat, cu scopul de a le distruge, scoate din funcţiune, sau neasigurarea serviciului*"[19].

Pentru cei care încă se mai îndoiesc de existenţa şi eficacitatea armelor cibernetice, menţionăm că grupul de experţi NATO, conduşi de către fostul secretar al apărării al SUA, doamna Madeleine K. Albright, a recomandat includerea în cadrul Noului Concept Strategic NATO, atacul cibernetic, ca a treia ameninţare la adresa NATO, după armele de distrugere în masă şi terorism. Mai mult decât atât, escaladarea unui atac cibernetic poate duce, după caz, chiar la invocarea art. V din tratatul NATO.

Directorul National Intelligence al SUA, Dennis Blair, a făcut public faptul că SUA sunt „ameninţate sever" de atacurile cibernetice „extrem de sofisticate" şi, pe poziţia a doua,

[16] William J. Lynn, Adjunctul secretarului de stat al apărării SUA.
[17] Dennis C. BLAIR, Director of National Inteligence, Annual Threat Assesment of the US Intelligence Community for the Senate Select Committee on Intelligence, 2010.
[18] The Economist, *War in the Fifth domain*, July 2010.
[19] Richard A. CLARCK, Cyber War, 2010.

de organizația teroristă Al-Quaeda. Blair a afirmat că SUA sunt amenințate în cyberspace de către statele ostile, rețelele teroriste şi grupurile de crimă organizată[20].

Dmitri Alperovich, vicepreşedintele centrului de cercetare a amenințărilor de la McAfee, consideră că „*nu există cazuri de război cibernetic. Țările sunt reticente să lanseze un astfel de război, întrucât un astfel de atac ar afecta semnificativ propria țară*". Dar grupările teroriste, sau țările eşuate pot trece uşor peste aspectele etice şi vor folosi aceste arme ieftine şi eficiente împotriva țărilor inamice, pentru atingerea scopurilor.

Echilibrul de putere în noul spațiu de război este foarte subțire. Luptele se dau tăcut, într-un spațiu construit special să nu fie stăpânit de nimeni. Puterea este, în special, a minții, software, dar şi infrastructura, hardware-ul, are un rol important.

Armele cibernetice sunt dezvoltate în secret, fără a se cunoaşte foarte multe informații referitoare la cum şi când vor fi folosite. Forța de distrugere a acestora nu este cunoscută cu precizie de nimeni, ca urmare, țările trebuie să se pregătească pentru ce este mai rău.

Anonimitatea dezvoltării şi folosirii acestora le aproprie, ca nivel distructiv, de paranoia armelor de nimicire în masă şi poate conduce la o escaladare a conflictului, fără a exclude folosirea armamentului de distrugere în masă. Iranul susține că este a doua putere militară în spațiul cibernetic. Rusia, Israelul, Franța şi Coreea de Nord îşi dezvoltă capacitățile militare din domeniul atacului cibernetic, iar SUA a înființat noul Comandament Cyber[21].

Arsenalul cibernetic include un număr mare de produse software proiectate pentru afectarea sistemelor informatice (malware), de la clasicele bombele logice, viruşi, viermii de calculator, până la spamul şi blocarea serviciului folosind mii, până la milioane de calculatoare compromise (zombi), pentru crearea de rețele de bots (botnet[22]), ca platforme de lansare a atacurilor distribuite, de tip Distributed-Denial-of- Services (DDoS).

Scopul este de a afecta, bloca sau anihila capacitatea infrastructurii IT a unei țări de a oferii servicii utilizatorilor, unele dintre ele critice[23]. În general, amenințările cibernetice pot fi încadrate în cinci mari categorii de atacuri care pot afecta componentele cheie ale Internetului:

- DDoS;
- viermi/viruşi;

---

[20] Dennis C. BLAIR, Director of National Intelligence, *Annual Threat Assesment of the US Intelligence Community for the Senate Select Committee on Intelligence,* 2010.

[21] The Economist, *Cyberware*, July 2010.

[22] O rețea botnet este compusă din computere (bots) care, fără ştirea utilizatorului au fost compromise prin exploatarea vulnerabilităților de către o aplicație malware pentru a derula activități nocive cum ar fi trimiterea de mesaje spam sau spyware către alte computere de pe Internet. Aceste computere „bot" acționează sub comanda unui singur hacker (sau a grup de hackeri de dimensiuni reduse) denumit „botmaster". Pentru detalii- vezi sursa Gecadnet.ro.

[23] The Economist, *War in the Fifth domain*, July 2010.

- atacuri asupra Internet Domain Name System (DNS);
- atacuri asupra/sau folosind rutere;
- criminalitatea cibernetică (phishing, furtul de la distanță al datelor, spionajul, vânzarea / cumpărarea/închirierea de timp/botnets).

În toată istoria umanității atunci când dezvoltarea tehnologică a vremii a scos la iveală tehnologii ce au avut potențial de a aduce supremație statelor dezvoltate la vremea respectivă sau tehnologii care le puteau amenința, acestea au asimilat imediat tehnologiile, au continuat cercetările şi au dezvoltat strategii pe baza lor. În prezent, referitor la cyberwar, SUA, prin Preşedintele Barack Obama, a declarat infrastructura digitală a Americii drept infrastructură critică, de importanță națională şi fostul şef al securității de la Microsoft a fost numit ca responsabilul acesteia. În plus, Pentagonul a înființat noul Comandament Cyber (Cybercom), condus de un general cu patru stele, Keith Alexander, directorul Agenției Naționale de Securitate (NSA). Misiunea acestuia este aceea de a apăra, cu prioritate, rețelele militare ale SUA de un eventual atac[24].

Britanicii au înființat un centru operațional în domeniul securității cibernetice, în cadrul Comandamentului Comunicațiilor Guvernamentale, Government Communications Headqurters (GCHQ).

China a devenit una dintre cele mai puternice şi ofensive țări în domeniul războiului cibernetic. Astfel, spionajul cibernetic al Chinei este considerat unul dintre cele mai mari dezastre în domeniul intelligence al SUA, de la furturile secretelor privind programul nuclear (sfârşitul anilor 1940).

Rusia şi Israelul se numără printre țările care sunt foarte bine echipate pentru a duce un eventual război în spațiul cibernetic. Este demn de arătat că, dacă Rusia este menționată ca fiind implicată în atacurile cibernetice asupra Estoniei şi Georgiei, există voci în media şi rapoarte ale experților în securitate IT care sugerează că Israelul, prin unitatea sa specializată, Unit 8200 ar fi în spatele celui mai sofisticat vierme de calculator, Stuxnet, produs pentru a ataca şi distruge facilitățile nucleare ale Iranului. Dacă China este percepută ca fiind cea mai virulentă în folosirea arsenalului din spațiul cibernetic pentru spionaj economic şi militar, Rusia este considerată ca având cele mai complexe şi subtile metode de atac şi apărare, iar aparenta lipsa de răspuns şi ambiguitatea pozițiilor oficialilor țărilor vestice față de atacurile informatice lasă impresia că şi acestea au platforme cibernetice cel puțin la fel de puternice.

În România, începând cu anul 2009, funcționează Centrul Național de Răspuns la Incidente informatice (CERT-RO). Acesta se află în coordonarea Ministerului Comunicațiilor şi Tehnologiei Informațiilor ca parte a Institutului Național de Cercetare Dezvoltare în Informatică, ICI Bucureşti. CERT-RO a fost creat atât ca un centru de excelență în domeniul securității informatice, echipamentelor, rețelelor şi echipamentelor informatice, dar şi pentru

[24] Ibidem.

transferul de expertiză între specialiştii IT&C, precum şi realizarea unor parteneriate între autorităţi în scopul realizării securităţii spaţiului virtual al României. Cu ocazia unor manifestări publice[25] autorităţile române au atras atenţia asupra necesităţii implementării unui set de standarde de apărare în domeniul securităţii cibernetice, în contextul interconectărilor tot mai dezvoltate din infrastructura statală. O provocare pentru instituţiile din domeniul securităţii cibernetice va fi Sistemul Informatic Unic Integrat apărut odată cu introducerea cardului naţional de asigurări sociale de sănătate.

De asemenea, importanţa pe care statul român o dă securităţii cibernetice este evidenţiată prin cuprinderea în Strategia Naţională de Apărare a asigurării securităţii cibernetice ca obiectiv naţional de securitate, apărând de aici chiar şi necesitatea elaborării şi operaţionalizării strategiei naţionale de securitate cibernetică.

Fenomenul criminalităţii informatice în România

La nivel naţional, au fost identificate următoarele forme de manifestare a riscurilor şi vulnerabilităţilor asociate atacurilor informatice, structurate pe tipurile de ameninţări specifice domeniului criminalităţii informatice:

1. Lezarea drepturilor şi libertăţilor fundamentale ale cetăţenilor privind asigurarea secretului corespondenţei electronice şi a protecţiei datelor personale în format electronic, atingeri aduse confidenţialităţii, integrităţii şi disponibilităţii datelor cu acces regulamentar, precum şi derularea de acţiuni frauduloase prin utilizarea unor metode şi mijloace nelegitime:

- accesarea şi extragerea ilegală a datelor personale şi de identificare aferente cardurilor bancare ce aparţin unor terţe persoane, în scopul reproducerii neautorizate a instrumentelor de plată electronice şi al efectuării de operaţiuni financiare ilicite prin care se aduce un prejudiciu patrimonial persoanelor ţintă sau în scopul obţinerii unor elemente de identificare a utilizatorilor legali ai unor sisteme/reţele informatice (prin folosirea unor procedee specifice, denumite uzual „phishing", „pharming", „skimming", „nigerian letter");

- fraudarea persoanelor fizice sau juridice prin tranzacţii sau licitaţii on-line trucate, procese administrative prin intermediul unor servicii web specializate în activităţi de comerţ electronic;

- acţiuni de obţinere frauduloasă de informaţii din diverse domenii de activitate (spionaj informatic), prin accesarea neautorizată a unor date/baze de date în format electronic/resurse web care aparţin unor instituţii publice/private din România sau străinătate, în scopul copierii acestora şi utilizării lor în alte scopuri decât cele pentru care au fost constituite (aplicaţii software dedicate în acest sens, cum ar fi aplicaţiile de tip „troian – trojan", „viermi informatici Internet worm", aplicaţii de tip „spyware";

[25] Conferinţa internaţională Cyber Security in the context of New NATO Strategie Concept, Bucureşti, 2 iunie 2010.

- utilizarea metodelor şi mijloacelor specifice criminalităţii informatice pentru operaţiuni ilegale asociate cu spălarea de bani (exemplu: servicii destinate transferului de monedă virtuală: E-gold, Web Money).

2. Distrugerea, degradarea ori aducerea în stare de neîntrebuinţare a unor reţele şi sisteme informatice, sau echipamentelor electronice aferente acestora, prin intermediul cărora sunt procesate, stocate sau transferate baze de date la nivelul unor instituţii publice, guvernamentale, instituţii financiar bancare, medicale, educaţionale, operatori de comunicaţii electronice, sau prin intermediul cărora sunt gestionate procese critice a căror întrerupere/afectare ar putea constitui ameninţări la adresa securităţii naţionale:

- atacuri DDoS (Distributed Denial of Service) prin care se obţine o degradare a parametrilor tehnici necesari menţinerii stabilităţii şi funcţionării optime a unui serviciu de comunicaţii electronice, fiind afectate accesibilitatea şi disponibilitatea serviciilor în cauză şi, implicit, a celorlalte procese asociate cu funcţionarea acestora;

- răspândirea de programe şi aplicaţii software ce intră sub incidenţa criminalităţii informatice, precum şi utilizarea acestora în vederea producerii de blocaje, perturbaţii sau daune în funcţionarea echipamentelor tehnice şi resurselor informatice aferente acestora.

3. Acţiuni ilegale orientate către conţinut: iniţierea, organizarea, săvârşirea sau sprijinirea, prin intermediul sistemelor informatice, a acţiunilor de factură teroristă, totalitariste sau extremiste de origine comunistă, fascistă, legionară sau de orice altă natură, rasiste, xenofobe care pot pune în pericol sub orice formă unitatea şi integritatea teritorială a României, precum şi difuzarea reprezentărilor grafice pornografice cu minori, interzise prin lege:

- realizarea de pagini web şi transmiterea de mesaje nesolicitate, prin intermediul căsuţelor poştale electronice, în scopul promovării şi diseminării rapide a materialelor sau documentelor cu conţinut ilegal sau vătămător în problematica de referinţă;

- utilizarea facilităţilor oferite de serviciile publice şi private de partajare a fişierelor, constituite la nivelul firmelor autohtone furnizoare de servicii Internet, în scopul desfăşurării uor activităţi ilegale de răspândire şi punere la dispoziţie, în mod disimulat, a materialelor în format electronic care promovează idei/concepte şi imagini cu potenţial pericol social sau infracţional incriminat prin lege.

4. Reproducerea ilegală şi punerea la dispoziţia publicului, prin intermediul reţelei Internet, a unor opere/lucrări protejate de legislaţia în domeniul drepturilor de autor şi al drepturilor conexe (proprietate intelectuală).

*

* *

Tematica abordată evidenţiază complexitatea sistemelor informaţionale moderne, determinată de încorporarea în acestea a celor mai avansate cunoştinţe din cibernetică, teoria sistemelor şi a informaţiei, cercetarea operaţională, electronică şi ştiinţa calculatoarelor, precum şi din inteligenţa artificială, acestea constituind cea mai elocventă

expresie a avantajelor obținute prin utilizarea tehnologiei moderne a informației şi comunicațiilor dar şi vulnerabilitatea acestora.

Pe teritoriul României au fost identificate nuclee de criminalitate informatică care dispun de capacitățile (resurse logistice, tehnologie, acces la rețeaua Internet) necesare inițierii unor atacuri informatice semnificative din punctul de vedere al potențialului distructiv şi al complexității tehnice, deşi până în prezent, nu au fost identificate persoane/grupări/organizații autohtone ale căror acțiuni derulate în mediul virtual să fie îndreptate spre obiective țintă de interes strategic sau de natură a pune în pericol securitatea națională.

Un factor determinant pentru evaluarea nivelului de risc privind *afectarea securității infrastructurilor informatice critice* în constituie disponibilitatea relativ facilă a resurselor hardware şi software necesare inițierii unor atacuri informatice, acestea putând fi descărcate/achizionate direct prin intermediul rețelei Internet, în multe situații această activitate putând fi realizată în condiții de anonimitate.

BIBLIOGRAFIE

*** *Legea nr.182 din 12.04.2002 privind protecția informațiilor clasificate*, publicată în Monitorul Oficial nr. 248/2002.

*** *Legea nr.423/2004 privind Aderarea României la Acordul dintre părțile la Tratatul Atlanticului de Nord pentru securitatea informațiilor,* adoptat la Bruxelles la 06.03.1997.

*** *Hotărârea Guvernului nr. 585/2002 pentru aprobarea standardelor naționale de protecție a informațiilor clasificate în România.*

*** *Hotărârea Guvernului nr. 353/2002 pentru aprobarea Normei privind protecția informațiilor clasificate ale Organizației Tratatului Atlanticului de Nord în România*.

*** *Doctrina națională a informațiilor pentru securitate*, Editura Serviciului Român de Informații, Bucureşti, 2004.

*** AJP 2.0 / STANAG 2190, *Allied Joint Intelligence and Security Doctrine NATO* / Pfp, 2003.

*** AAP-6 2008, *NATO Glossary of Terms and Definitions*, 01 April 2008.

*** ORNISS, *Doctrine, norme şi ghiduri privind securitatea informațiilor.*

LUCRĂRI DE AUTOR

Alexandrescu C., Alexandrescu G., Boaru Gh., *Sisteme informaționale – fundamente teoretice*, Editura Universității Naționale de Apărare „Carol I", Bucureşti, 2009.

Alexandrescu C., Alexandrescu G., Boaru Gh., *Sisteme informaţionale militare – servicii şi tehnologie*, Editura Universităţii Naţionale de Apărare „Carol I", Bucureşti, 2010.
Blair Dennis C., Director of National Inteligence, *Annual Threat Assesment of the US Intelligence Community for the Senate Select Committee on Intelligence,* 2010.
Clarke Richard, Knacke Robert, Cyber War: Te Next Threat to National Security and What to Do About It, 2010.
Dunningan James, *Noua ameninţare mondială, Cyber-Terorismul,* Editura Curtea Veche, 2010.
Gansler J., Binnendijc H., *Information Assurance:Trend in Vulnerabilities, Threat and Technologies,* Internet, 2008.
Rădoi Mireille, *Serviciile de informaţii şi decizia politică*, Editura Tritronic, Bucureşti, 2003.
Vlădoiu Nasty, *Protecţia informaţiilor*, Editura Tritronic, Bucureşti, 2005.

PUBLICAŢII PERIODICE, SURSE INTERNET

Emission Security, Internet (http://en. wikipedia.org/wiki/emision security), 2009.
Conferinţa Internaţională Cyber Security in the context of the new NATO Strategie Concept, Bucureşti, 2010.
Intelligence, revista Serviciului Roman de Informatii, nr 18, 2010.
Intelligence, revista Serviciului Roman de Informatii, nr 15, 2009.
The Economist, *Cyberware*, July 2010.
The Economist, *War in the Fifth domain*, July 2010.
Wikipedia, *Information Security* (http:/en. Wikipedia. org/wiki/information security), 2009.
Wikipedia, *Computer Security*, (http://en.wikipedia. org/wiki/computer security), 2010.
Wikipedia, *Communications Security* (http://en. wikipedia. org/wiki/Communications security, 2010.
Wikipedia, *Database Security* (http://en.wikipedia. org/wiki/database security), 2010.
http://www.sri.ro
http://www.rap.freehosting.net/Infract/P5.html
http://www.adevarul.ro/international/Iran_a_inceput_razboiul_cibernetic_0_343166231.html