MANAGEMENTUL RISCURILOR ÎN SPAȚIUL CIBERNETIC CU APLICAȚII ÎN DOMENIUL MILITAR

RISK MANAGEMENT IN CYBERSPACE WITH APPLICATIONS IN MILITARY FIELD

Col. (r) drd. Cătălin-Iulian BALOG*

Dezvoltarea tehnologică recentă a societății civile și globalizarea infrastructurilor de comunicații au generat schimbări profunde în toate sistemele de securitate. Statele informatizate sunt direct amenințate de atacurile cibernetice care au ca scop perturbarea activităților guvernamentale prin distrugerea sau alterarea resurselor de informații și a infrastructurii critice, sau chiar prin alterarea imaginii publice și inducerea unui sentiment de insecuritate și de neîncredere în capacitatea de apărare a unui stat.

Recent technological development of civil society and the globalization of communications infrastructures have generated profound changes in all security systems. Countries with a very strong computerized infrastructure are directly threatened by cyber-attacks to disrupt the activities of government through destruction or alteration of information resources and critical infrastructure, or by altering public image and creating a sense of insecurity and mistrust in the defense capacity of a state.

Cuvinte-cheie: spațiu cibernetic; riscuri; amenințări; vulnerabilități; management.
***Keywords**: cyberspace; risks; threats; vulnerabilities; confrontation; management.*

Conform *Dicționarului Explicativ al Limbii Române*[1], noțiunea de *risc* este, în general, asociată cu „posibilitatea unei pierderi sau daune, hazard, pericol, primejdie sau pericol, inconvenient mai mult sau mai puțin probabil la care este expus cineva sau ceva”.

Prin definiție, noțiunea de risc implică ideea de pierdere potențială (de orice tip), pierdere provocată de evoluția unor factori (factori de risc) în sens contrar așteptărilor, care reprezintă cauza, iar dacă se manifestă reprezintă o consecință.

Riscul este un eveniment nedorit care poate conduce la neîndeplinirea parțială sau totală a scopului, în timpul solicitat, la nivelul calitativ cerut și la costul stabilit. Riscul este definit ca fiind combinația dintre probabilitatea unui eveniment și consecințele sale[2].

* ***Universitatea Națională de Apărare „Carol I”***
e-mail: *catalin.balog@gmail.com*

Procesul de management al riscurilor cibernetice

Complexitatea tehnologică, aria mare de răspândire a datelor și a informațiilor, precum și numărul mare de amenințări și de incidente informatice la adresa securității și funcționalității sistemelor distribuite reprezintă factori care trebuie luați în considerare la dezvoltarea sistemelor informatice. Scopul principal al procesului de management al riscului pentru o organizație are în vedere protecția organizației și capacitatea sa de a-și îndeplini misiunea, însă nu doar din perspectiva resurselor IT. De aceea, procesul de management al riscului nu trebuie tratat ca o funcție tehnică efectuată de către experții care operează și gestionează sistemul informatic, ci ca o funcție esențială a gestionării organizației.

Dezvoltarea unei strategii de protecție a resurselor organizației este un proces complex și sensibil din punctul de vedere al componentelor pe care le implică un management al riscurilor.

În literatura de specialitate, managementul riscului este definit ca fiind „procesul de identificare a vulnerabilităților și amenințărilor din cadrul unei organizații, precum și de elaborare a unor măsuri de minimizare a impactului acestora asupra resurselor informaționale”[3]. În general, majoritatea organizațiilor se concentrează pe protecția fizică (în special pe vulnerabilitățile infrastructurii de rețea, sisteme de calcul) și nu reușesc să stabilească efectele asupra celor mai importante resurse.

O abordare incompletă produce un decalaj între necesarul operațional și cel al sistemului informatic, lăsând bunuri valoroase sub incidența riscului. Abordările curente pentru managementul riscurilor legate de securitatea informației tind să fie incomplete, deoarece nu reușesc să includă în cadrul analizei toate componentele riscului (bunuri, amenințări și vulnerabilități). Managementul riscului este procesul care permite nivelului managerial să asigure un echilibru între costurile operaționale și resursele financiare necesare pentru implementarea măsurilor de protecție și atingerea obiectivelor privind protejarea resurselor (infrastructurii, sistemelor de calcul, aplicații, date etc.) care susțin activitatea organizației.

Un alt aspect este reprezentat de externalizarea procesului de evaluare a riscurilor: evaluarea rezultată s-ar putea să nu fie adecvată sau există posibilitatea să nu abordeze corect perspectiva organizației. Autoevaluarea oferă contextul înțelegerii riscurilor și posibilitatea luării unor decizii și asumării unor compromisuri în cunoștință de cauză.

Primul pas în managementul riscului securității informației este reprezentat de înțelegerea și de identificarea riscurilor cu care se confruntă organizația. Odată ce riscurile sunt identificate, se pot concepe planuri de rezolvare a acestora.

Conform definiției date de *National Institute of Standards and Technology* (NIST), managementul riscului este „procesul care permite managerilor IT echilibrarea costurilor operaționale și financiare ale măsurilor de protecție pentru a realiza un câștig în raport cu capacitatea de protecție a sistemele informatice și a datelor care sunt suport pentru misiunea organizației”[4]. Această definiție are la bază eventualitatea ca un eveniment (anticipat cu o anumită probabilitate sau neprevăzut de decident) să se materializeze și să afecteze negativ anumite aspecte ale activității operaționale.

Planificarea managementului riscului este procesul prin care se decide modul de abordare și de planificare a activităților de management al riscului. Înainte de inițierea oricăror acțiuni de management al riscurilor trebuie să se evalueze existența unui potențial de risc pentru sistemul analizat cu privire la domeniul de activitate. Această evaluare trebuie să țină cont de toate activitățile care implică sistemul, activități care ar putea să conțină un risc potențial. Se obține astfel o listă de activități și o clasificare a riscurilor potențiale în activități fără risc, cu risc scăzut și cu potențial de risc ridicat.

Astfel, la modul general, se poate spune că *procesul de management al riscului* constă din desfășurarea următoarelor etape[5]:

a) evaluarea riscului – identificarea și clasificarea riscurilor care pot să afecteze organizațiile (planificarea și colectarea colectării datelor legate de risc, ierarhizarea riscurilor);

b) coordonarea procesului decizional – identificarea și evaluarea măsurilor și soluțiilor de control ținând cont de raportul cost-beneficii (definirea cerințelor funcționale, identificarea soluțiilor de control, revizuirea soluțiilor în comparație cu cerințele, estimarea reducerii riscu-rilor, selectarea strategiei de atenuare a riscului);

c) implementarea controalelor – implementarea și rularea unor măsuri de control menite să reducă sau să elimine riscurile (căutarea unor abordări alternative, organizarea soluțiilor de control);

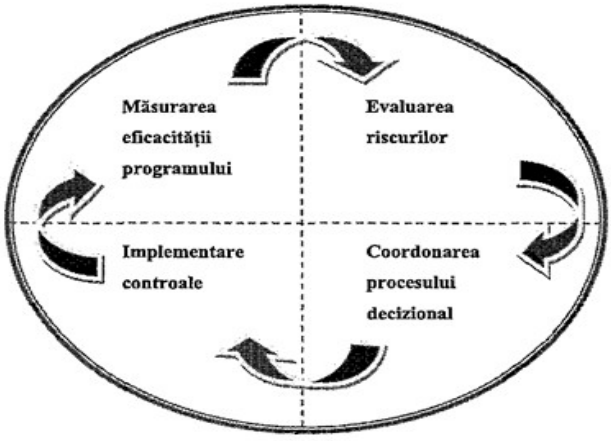

Fig. 1 *Procesul de management al riscurilor*

d) măsurarea eficacității programului – analiza eficacității măsurilor de control adoptate și verificarea controalelor aplicate să asigure gradul de protecție stabilit (fig. 1 *Elaborarea unui formular de risc al securității, măsurarea eficacității controalelor*[6]).

Analiza riscurilor (identificare și evaluare)

Analiza riscurilor reprezintă unul dintre cele mai importante aspecte ale securității, iar în conformitate cu bunele practici din domeniu, organizațiile trebuie să abordeze problema riscului în patru etape[7]:

a) identificarea și evaluarea informațiilor importante;
b) identificarea și evaluarea amenințărilor;
c) evaluarea vulnerabilităților;
d) evaluarea riscului.

Analiza de risc presupune un proces de identificare și de clasificare a riscurilor de securitate, determinarea amplitudinii riscurilor, precum și identificarea zonelor cu potențial mare de risc. Analiza de risc face parte din ansamblul complex de măsuri care poartă denumirea de *management al riscului***.** Evaluarea riscurilor este rezultatul unui proces de analiză a riscurilor.

Reducerea riscurilor presupune adoptarea măsurilor de prevenire în cazul manifestării acestora, iar pentru implementare sunt necesare o serie de costuri la nivel organizațional care trebuie corelate cu dimensiunea daunelor privind exploatarea vulnerabilităților, astfel încât factorii de conducere să decidă care riscuri trebuie prevenite, limitate sau acceptate. Cele mai importante abordări utilizate în procesul de analiză a riscurilor sunt analiza cantitativă, analiza calitativă, analiza pe post de lucru și analiza cost-beneficii.

În esență, analiza riscului reprezintă o metodă (calitativă și/sau cantitativă) utilizată pentru evaluarea impactului riscului asupra deciziilor potențiale într-o situație dată. Scopul unui astfel de demers este acela de a ghida decidentul pentru a soluționa mai bine probleme decizionale marcate de un anumit grad de incertitudine.

Aplicații militare în spațiul cibernetic

Spațiul cibernetic se suprapune peste celelalte câmpuri de luptă (terestru, maritim, aerian și cosmic) și conectează aceste spații fizice prin procese cognitive care utilizează date și informații stocate anterior și actualizate permanent[8] (fig. 2).

Totuși, utilizarea tehnologiilor electronice pentru a crea „puncte de intrare” (breșe de securitate) în spațiul cibernetic, precum și utilizarea energiei și a proprietăților câmpului electromagnetic caracterizează cel mai bine spațiul cibernetic și stabilește caracteristicile esențiale ale acestuia, subliniind ceea ce îl face unic și îl diferențiază de cele patru spații fizice[9] menționate anterior.

Componenta cibernetică a conflictelor militare contemporane

Spațiul cibernetic nu este un loc fizic. El sfidează orice măsură a dimensiunii spațiu-timp fizic sau spațiu-timp continuu. Spațiul cibernetic[10] poate fi considerat un domeniu operațional al cărui caracter distinctiv și unic este relevat de utilizarea dispozitivelor electronice și a spectrului electromagnetic pentru a crea, stoca, modifica, schimba și exploata informații prin intermediul sistemelor interconectate pe baza tehnologiei informației și comunicațiilor și a infrastructurilor

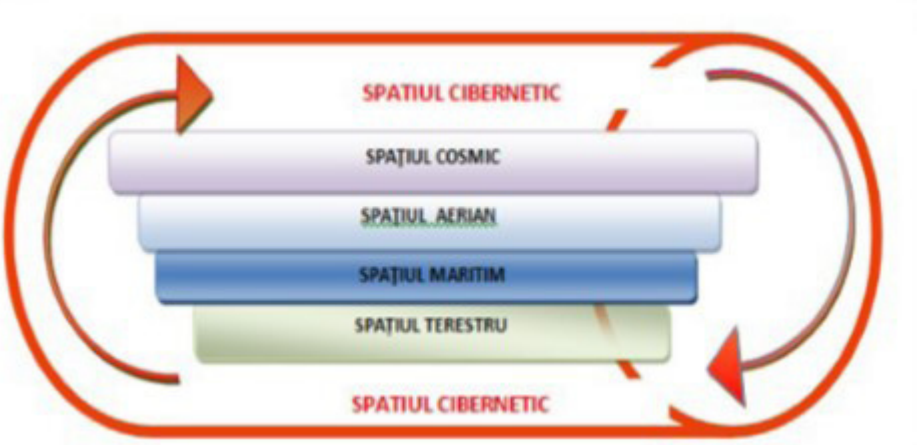

Fig. 2 *Raportul actual dintre spațiile de confruntare militară*

asociate acestora într-un mediu de rețea. Spațiul cibernetic nu se reduce la Internet, văzut ca o rețea deschisă de rețele de calculatoare. Spațiul cibernetic include, pe lângă Internet, multe alte rețele de calculatoare, inclusiv pe acelea despre care se presupune că nu pot fi accesibile prin Internet[11].

În literatura de specialitate, *spațiul cibernetic* este al *cincilea câmp de luptă*, după cel terestru, maritim, aerian și cosmic. Conflictele militare, economice sau politice se desfășoară din ce în ce mai mult în spațiul cibernetic. În acest context, termenul „război cibernetic" a devenit un cuvânt destul de popular și se referă la orice tip de conflict din spațiul virtual, având o dimensiune internațională.

Războiul cibernetic este o subsecțiune a războiului informațional. Ca parte a acestui concept mai larg, care urmărește să influențeze comportamentul și capacitățile leadership-ului advers, la nivel politic și militar și/sau să influențeze atitudinea populației civile în teatrele de operații sau statele țintă, războiul cibernetic include numai activități desfășurate în acest scop în spațiul virtual.

O clasificare conceptuală a variatelor forme de conflict sau război cibernetic nu este riguros stabilită sau acceptată. Ivan Goldberg a definit războiul cibernetic ca fiind „uzul ofensiv și defensiv al informației și al sistemelor informaționale pentru a nega, exploata, corupe sau distruge informația, procesele bazate pe informație, sistemele informaționale și rețelele de calculatoare ale unui adversar, pentru a le proteja pe cele personale"[12].

Războiul cibernetic a fost definit de către expertul guvernamental american Richard A. Clarke, în cartea sa, *CyberWar* (2010), ca fiind „acțiunea desfășurată de un stat-națiune pentru penetrarea computerelor sau rețelelor de computere ale unei alte națiuni, cu scopul de a cauza pagube și disfuncții" [13].

Publicația „The Economist" descrie războiul cibernetic ca pe un al cincilea mediu (domeniu) pentru ducerea războiului, iar William J. Lynn, adjunct al secretarului american al apărării, a precizat că „din punct de vedere doctrinar, Pentagonul a recunoscut în mod formal că spațiul cibernetic a devenit la fel de important pentru operațiunile militare precum celelalte patru spații: terestru, aerian, maritim și spațial"[14].

Astfel, se poate afirma că realitatea conflictelor militare din ultimii 15-20 de ani confirmă existența unei dimensiuni cibernetice a conflictelor militare contemporane, precum și faptul că spațiul cibernetic reprezintă un nou mediu de confruntare militară. Aceste afirmații sunt justificate, pe de o parte, printr-o analiză succintă a acțiunilor cibernetice din această perioadă, desfășurate la nivel mondial – fie pentru pregătirea sau în sprijinul unor acțiuni militare clasice, fie ca acțiuni independente menite să elimine sau să creeze prejudicii infrastructurilor cibernetice naționale, afectând astfel securitatea și afacerile militare la nivel statal – și pe de altă parte, datorită faptului că la baza tuturor acțiunilor militare se află nevoia de comunicare în sensul existenței mediului de rețea și a utilizării tehnologiei ca mijloc de luptă.

Primul exemplu care a făcut obiectul unor intense dezbateri publice și a constituit un element de cotitură în ceea ce privește regândirea strategiilor militare și a concepțiilor de evoluție a luptei armate a fost „cazul Estonia", aprilie-mai 2007. Acest exemplu a constituit un atac cibernetic îndreptat împotriva infrastructurii critice a unui stat, ca urmare a reprimării manifestațiilor stradale proruse din capitala Tallinn. Deși nu a putut fi dovedit clar și nici nu a putut fi determinat tehnic elementul declanșator al atacului ori factorul agresor, prim-ministrul estonian din acea perioadă, Andrus Ansip, a atribuit atacul F. Ruse și organizațiilor rusești care activau în regiune[15].

Atacurile cibernetice din Estonia au constituit primul pas către transformarea conceptului de apărare cibernetică la nivelul NATO, sintetizat prin declarația fostului Secretar General al Alianței, Jaap de Hoop Scheffer, care a subliniat că „apărarea cibernetică reprezintă o responsabilitate națională, dar NATO poate oferi consultanță și poate sprijini cu echipe mobile națiunile, în caz de nevoie"[16].

La un an după evenimentele din Estonia, cu ocazia Summitului NATO de la București (aprilie 2008), șefii de state și de guverne au semnat o declarație în care a fost adoptată, în premieră, o politică primară a alianței care viza domeniul cibernetic (*Policy on Cyber Defence*, paragraful 47)[17]. Astfel, NATO a devenit prima structură militară care a anunțat și apoi a elaborat un pachet de politici în domeniul apărării cibernetice. Politica primară prezentată în cadrul paragrafului 47 al declarației de la București sublinia necesitatea ca statele membre să-și protejeze sistemele informatice cheie, să-și împărtășească cele mai bune practici în

domeniu și să-și asigure capabilități pentru a oferi asistență națiunilor membre, la nevoie, pentru a contracara un atac cibernetic.

Ulterior, în luna mai 2008, șapte state membre NATO și Comandamentul Aliat pentru Transformare au semnat documentele care au stat la baza înființării *Cooperative Cyber Defence (CCD) Centre of Excellence (CoE)* din Tallinn, Estonia.

Un al doilea exemplu a fost „cazul Georgia”, august 2008. Și acest exemplu a constituit un atac cibernetic îndreptat împotriva infrastructurii critice a unui stat, ca urmare a tensiunilor ruso-georgiene referitoare la Osetia de Sud[18], pe fondul unei ofensive militare controversate, concretizată într-o serie de ciocniri între forțele armate guvernamentale georgiene și cele separatiste sud-osetine.

Potrivit lui Scott Borg, director în cadrul *U.S. Cyber Consequences Unit*, în spatele atacurilor cibernetice din Georgia s-au aflat grupuri civile de hackeri ruși ajutați de organizații criminale, sprijiniți de guvernul de la Moscova”[19].

Un al treilea exemplu a fost „cazul Ucraina”, 2013-2014. Și acest exemplu a constituit un atac cibernetic îndreptat împotriva infrastructurii critice a unui stat, ca urmare a mișcărilor de protest generate de refuzul președintelui ucrainean din acea perioadă, Viktor Yanukovych, de a semna Acordul de Asociere cu Uniunea Europeană și a promulgării de către acesta a unui set de legi care instaurau dictatura, limitând drepturile omului și libertatea cuvântului, mișcări care au culminat cu plecarea de la putere a fostului președinte ucrainean, Viktor Yanukovych.

Potrivit unui studiu al companiei de securitate *BAE Systems*, în acest caz, deși nu a fost identificat principalul agresor cibernetic există certitudinea că atacurile au fost produse din zona geografică GMT+4, iar codurile *malware* conțineau caractere rusești. În urma acestor atacuri s-a reușit accesul și preluarea controlului infrastructurii cibernetice critice a statului ucrainean și a organizațiilor nonguvernamentale care militau împotriva operațiunilor paramilitare din Peninsula Crimeea.

Concluzii

Din punct de vedere militar[20] se poate aprecia că în spațiul cibernetic există posibilitatea dezvoltării unor aplicații specifice, după modelul acțiunilor militare clasice, pornind de la instrumente rudimentare și acțiuni de pionierat, până la executarea unor operațiuni cibernetice de tip hibrid. Inspirate de modelul amenințărilor cibernetice clasice, precum existenta unor simpli viruși, acestea s-au transformat în arme complexe și campanii militare, devenind amenințări de securitate majore, cu efecte directe, virtuale, în spațiul cibernetic și efecte indirecte, catastrofale, în spațiul fizic. Deși operațiunile militare cibernetice sunt total diferite de operațiunile militare clasice, prin modul de manifestare și prin regulile de angajare și de executare, ele au același scop, urmărind eliminarea adversarului sau zădărnicirea acțiunilor acestuia în mediul operațional specific, cibernetic sau clasic.

Așadar, războiul secolului XXI nu mai este posibil fără implicarea unor oponenți care dispun de o minimă tehnologie de acces în spațiul cibernetic. Noile concepte operaționale[21], precum războiul bazat pe rețea *(nework centric warfare)* sau informaționalizarea câmpului de luptă *(informationalized battlespace)* nu pot exista în lipsa unor sisteme de apărare prevăzute cu resurse și capabilități cibernetice.

NOTE:

1 Academia Română, *DEX – Dicționarul explicativ al limbii române (ediție revăzută și adăugită)*, Editura Univers Enciclopedic Gold, București, 2012.

2 ISO/IEC, *Guide 73: 2002*.

3 NIST, *Special Publication 800-30: Risk Management Guide for Information Technology Systems,* July 2002.

4 *Ibidem.*

5 *Ibidem.*

6 Preluare și adaptare după NIST, *op.cit*.

7 R.G. Wilsher, H. Kurth, *Security Assurance in Information Systems,* în S.K. Katsikas, D. Gritzalis, ”Information Systems Security: Facing the information society of the 21st century”, Chapman and Hall, 1996.

8 G. Boaru, B. Iorga, *Atacul cibernetic – o amenințare hibridă într-un război hibrid*, București, 2015, The 11th International Scientific Conference „Strategii XXI”, Volumul 3, Universitatea Națională de Apărare „Carol I”, București, 2015, p. 232.

9 D.T. Kuehl, *From Cyberspace to Cyberpower: Defining the Problem*, Information Resources Management College, National Defense University.

10 D.T. Kuehl, *op.cit.*

11 Multe rețele au fost proiectate și dezvoltate cu scopuri precise. De exemplu: GPS – *Global Positioning System* (SUA), GLONASS – *GLObal'naia Navigaționnaia Sputnikovaia Sistema* (FR), GALILEO (UE), ACARS – *Aircraft Communication Addressing and Reporting System, SWIFT – Society for Worldwide Interbank Financial Telecommunication, GSM – Global System for Mobile Communications* etc.

12 *Institute For The Advanced Study Of Information Warfare*, http://www.psycom.net/iwar.1.html, accesat la 07.03.2016.

13 R.A. Clarke, *Cyber War*, Harper Collins, 2010, p. 6.

14 W.J. Lynn, *Defending a new domain: The Pentagon's Cyberstrategy*, în Cyberwar Resources Guide, Item #121, http://www.projectcyw-d.org/resources/items/show/121, accesat la 07.03.2016.

15 C. Maxwell, *Cyberspace: America's New Battleground*, SANS Institute InfoSec Reading Room, https://www.sans.org/reading-room/whitepapers/warfare/cyberspace-americas-battleground-35612, accesat la 07.01.2016.

16 http://www.nato.int/docu/speech/2008/s080208c.html, Press Conference, VILNIUS Estonia, 2008, accesat la 07.01.2016.

17http://www.ingepo.ro/download-materiale/110/SuplimentBuletin27Ro.pdf, accesat la 07.01.2016.

18 Regiune separatistă a Georgiei, autoproclamată republică şi nerecunoscută de comunitatea internaţională, cu excepţia Federaţiei Ruse.

19 http://www.registan.net/wp-content/uploads/2009/08/USCCU-Georgia-Cyber-Campaign-Overview.pdf, accesat la 07.01.2016.

20 Preluare şi adaptare după G. Boaru, B. Iorga, *op.cit*.

21 G. Văduva, *Războiul bazat pe reţea în fizionomia noilor conflicte militare*, Editura Universităţii Naţionale de Apărare „Carol I”, Bucureşti, 2005.

BIBLIOGRAFIE

Academia Română, *DEX – Dicţionarul explicativ al limbii române* (ediţie revăzută şi adăugită), Editura Univers Enciclopedic Gold, Bucureşti, 2012.

Institute For The Advanced Study Of Information Warfare, http://www.psycom.net/iwar.1.html, accesat la 07.03.2016.

ISO/IEC, Guide 73:2002.

NIST, Special Publication 800-30: Risk Management Guide for Information Technology Systems, July 2002.

Boaru G., Iorga B., *Atacul cibernetic − o ameninţare hibridă într-un război hibrid*, Bucureşti, 2015, The 11th International Scientific Conference „Strategii XXI”, Volumul 3, Universitatea Naţională de Apărare „Carol I”, Bucureşti, 2015.

Clarke R.A., *Cyber War*, Harper Collins, 2010.

Kuehl D.T., *From Cyberspace to Cyberpower: Defining the Problem*, Information Resources Management College, National Defense University.

Lynn W.J., *Defending a new domain: The Pentagon's Cyberstrategy*, în Cyberwar Resources Guide, Item #121, http://www.projectcyw-d.org/resources/items/show/121, accesat la 07.03.2016.

Maxwell C., *Cyberspace: America's New Battleground*, SANS Institute InfoSec Reading Room, https://www.sans.org/reading-room/whitepapers/warfare/cyberspace-americas-battleground-35612, accesat la data de 07.01.2016.

Văduva G., *Războiul bazat pe reţea în fizionomia noilor conflicte militare*, Editura Universităţii Naţionale de Apărare „Carol I”, Bucureşti, 2005.

Wilsher R.G., Kurth H., *Security Assurance in Information Systems,* în S.K. Katsikas, D. Gritzalis, *Information Systems Security: Facing the information society of the 21st century*, Chapman and Hall, 1996.

http://www.ingepo.ro/download-materiale/110/SuplimentBuletin27Ro.pdf, accesat la 07.01.2016.

http://www.nato.int/docu/speech/2008/s080208c.html, Press Conference, VILNIUS Estonia, 2008, accesat la 07.01.2016.

http://www.registan.net/wp-content/uploads/2009/08/USCCU-Georgia-Cyber-Campaign-Overview.pdf, accesat la 07.01.2016.