

OSINT – la granița dintre secret și public

Theodor MITU

Daniela MITU

Serviciul Român de Informații

e-mail: ani@sri.ro

Abstract

OSINT lies at the basis of the current transformations experienced by the intelligence sector, being both a rich source of information and technological innovation, responding to agencies' various challenges.

Besides the operational advantages provided, open sources play an important role in public communication, functioning both as a PR platform, encouraging the relations with beneficiaries and academic circles, and a promoter of security culture.

OSINT manages to accomplish the transition from secret sources to open sources, enabling us to talk about a specific symbiosis between classified and public information.

Keywords: open source intelligence, secret vs. open, multiple source analysis

1. Secret versus deschis

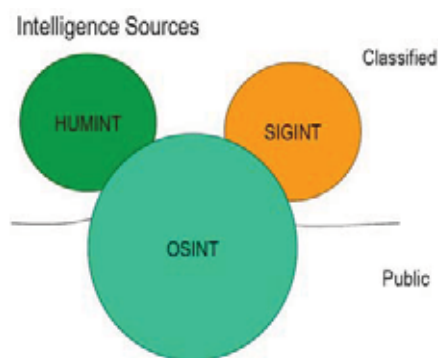


Figura nr. 1

<http://langtech.jrc.it/>

Natura ambivalentă – *secret* – *public* – a OSINT este reflectată încă din definiția dată în lucrarea „NATO Open Source Intelligence Handbook”: „OSINT este informația neclasificată, care a fost descoperită deliberat, selectată, filtrată și diseminată pentru o audiență specifică în vederea răspunderii la o anumită solicitare. [...] Aplicate într-un mod sistematic, produsele OSINT pot reduce cererile de colectare a informațiilor secrete,

limitând aceste solicitări doar la acele subiecte la care nu se poate oferi un răspuns din surse deschise”¹.

Modul în care se completează reciproc informațiile din surse deschise (OSINT) cu cele din surse secrete (HUMINT) s-a aflat în atenția mai multor specialiști. Subliniind punctele tari și pe cele slabe ale surselor secrete și ale celor deschise, autorii fie pledează pentru importanța acordată uneia sau alteia dintre categorii, fie pentru fuziunea informațiilor obținute din acestea.

S-a susținut că HUMINT sunt mai importante decât OSINT, care au doar rolul de a umple *casetele libere* lăsate de primele². Sursele secrete prezintă avantajul de a *pătrunde*, prin metode specifice, acolo unde corespondenții ziarelor nu pot ajunge, exemplul extrem fiind în preajma organizațiilor teroriste.

Alte comentarii favorizează OSINT, care pot face ca serviciile de intelligence să devină mai performante³. Se apreciază că jurnaliștii, analiștii din cadrul think tank-urilor pot avea cunoștințe mult mai solide într-un domeniu pe care l-au studiat ani de zile ori prin cunoașterea unei societăți, a unei culturi etc. Totodată, OSINT oferă informații în zone care, de cele mai multe ori, nu sunt foarte bine acoperite de mijloacele de culegere și analiză tradiționale – infrastructură, economie, evenimente culturale, demografie.

Robert David Steele, unul dintre cei mai înverșunați promotori ai OSINT, afirmă faptul că intelligence-ul din surse deschise „contextualizează nevoia de informații, oferind matricea în care pot acționa celelalte tipuri de intelligence, orientează acțiunea pentru ca acestea să devină mai eficiente”.

Expertul consideră că OSINT „ar trebui să fie fundamentul pentru toate disciplinele de colectare a informațiilor secrete și (...) ar putea fi

¹ http://www.oss.net/dynamaster/file_archive/030201/ca5fb66734f540fbb4f8f6ef759b258c/NATO%20OSINT%20Handbook%20v1.2%20-%20Jan%202002.pdf.

² Rob Johnston, *Analytic Culture in the US Intelligence Community. An Ethnographic Study*, The Center for the Study of Intelligence, Washington, 2005.

³ „Comunitatea nordică (Danemarca, Finlanda, Norvegia și Suedia) a luat locul Canadei [...] în suportul direct al intelligence-ului care susține misiunile de pace ale ONU. Acest lucru se poate datora faptului că autoritățile de la Ottawa sunt mult prea dependente de informațiile din surse secrete furnizate de SUA și nu au capacități proprii la nivel global. Un alt motiv ar putea fi acela al combinării, de către nordici, a două percepții: înalta apreciere față de OSINT, respectiv îndelungata practică de participare la operațiuni multinaționale și centre de intelligence” în Robert David Steele (2010), *Intelligence for Earth, Clarity, Diversity, Integrity, & Sustainability*, Oakton, Earth Intelligence Network, p. 52 disponibil la <http://www.phibetaiota.net/?p=19357> [iunie 2010].

punctul de plecare pentru punerea în aplicare a conceptului mai larg de intelligence național sau global, ceea ce unii numesc intelligence colectiv sau creierul lumii”⁴.

Și aceasta pentru că, „în ultimele două decenii de pionierat al OSINT și până în prezent, în era multinațională, multiinstituțională, multidisciplinară, de analiză și partajare a informației în mai multe domenii (*Multinational, Multiagency, Multidisciplinary, Multidomain Information-Sharing and Sense-Making – M4IS2*), factorul uman a devenit tot mai important, deoarece esența secolului al XXI-lea este nu să furi un secret de la o persoană pentru beneficiul unora, ci să te străduiești să diseminezi informația pe întreaga planetă în beneficiul întregii comunități”⁵.

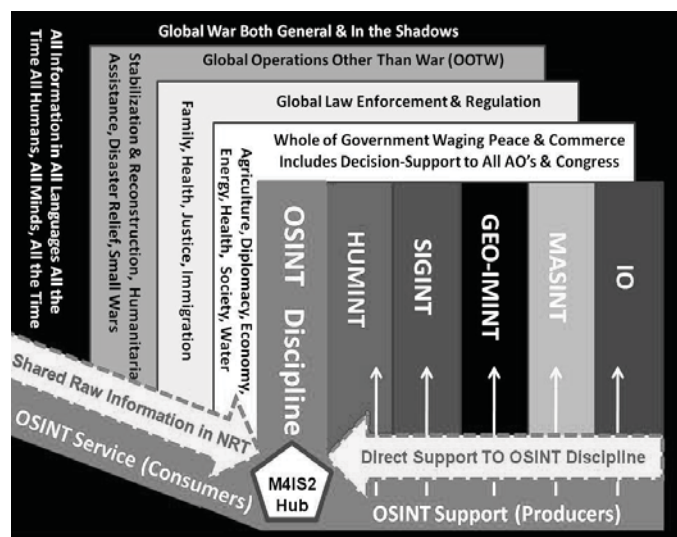


Figura nr. 2

<http://www.phibetaiota.net/?p=19>

Unii specialiști, precum fostul ofițer CIA Arthur Hulnick, consideră OSINT ca fiind chiar „temelia pe care se construiește informația secretă”.

⁴ Robert David Steele, „Open Source Intelligence”, în Johnson Loch (ed.), *Strategic Intelligence: The Intelligence Cycle*, Westport, Praeger, 2007, p. 97.

⁵ Robert David Steele, *Intelligence for Earth, Clarity, Diversity, Integrity, & Sustainability*, Oakton, Earth Intelligence Network, 2010, p. 163, disponibil la <http://www.phibetaiota.net/?p=19357> [iunie 2010].

Acesta estimează că produsele obținute din surse deschise contribuie în proporție covârșitoare la baza generală de informații⁶.

Cele mai multe opinii merg însă pe ideea potrivit căreia „un amestec de OSINT, HUMINT și celelalte tipuri de intelligence (*all-source fusion of intelligence*) este vital și poate produce sinergii importante”⁷.

Acesta pare a fi și punctul de plecare pentru clasificarea datelor și informațiilor realizată de William J. Lahneman, unul dintre cei mai cunoscuți specialiști în intelligence din spațiul anglo-saxon⁸.

Conform acestuia, datele sunt fie secrete (clasificate), fie nesecrete (neclasificate) – *secret versus open*. Orice informație de securitate națională care rezultă din acestea este folosită pentru a fi combinată cu produse informaționale secrete sau nesecrete (care provin din surse deschise). Reies patru tipuri de *fluxuri informaționale*, ce au conținut și beneficiari diferiți.

Fluxurile *secret-secret* (I) și *deschis-secret* (II) sunt asociate cu activitatea tradițională de intelligence.

Astfel, în fluxul I informațiile de securitate națională provin din surse secrete sensibile, care ulterior sunt analizate prin intermediul canalelor secrete pentru a fi realizate produse informaționale clasificate.

În cazul celui de al II-lea flux, serviciile de intelligence corelează informațiile, folosind metode și surse clasificate, astfel produsele rezultate secrete fiind folosite pentru informarea oficialilor guvernamentali.

Potrivit autorului, nevoia concretizării fluxului III – *secret-deschis* – a crescut după atentatele din data de 11 septembrie 2001, când a fost evident faptul că nivelul de clasificare a informațiilor a constituit un obstacol în partajarea acestora între diferitele entități ale statului.

Fluxul III presupune ca informațiile obținute prin metode specifice din surse secrete sensibile să fie declassificate pentru a fi informate autoritățile locale și cele cu atribuții în aplicarea legii.

⁶ Stephen C. Mercado, „Sailing the Sea of OSINT in the Information Age”, în *Studies in Intelligence*, vol. 48, nr. 3, 2007.

⁷ Peter Gill, Stephen Marrin și Mark Phytian, *Intelligence Theory. Key Questions and Debates*, London & New York, Routledge, 2009.

⁸ William J. Lahneman, „The Need for a New Intelligence Paradigm”, în *International Journal of Intelligence and CounterIntelligence*, vol. 23, nr. 2, 25 februarie 2010, pp. 212-214.

Ultima categorie, cea de-a IV-a, *fluxul deschis-deschis*, crește, în opinia lui Lahneman, ca importanță, „de vreme ce oficialii guvernamentali monitorizează constant raportările mass-media”⁹. Practic, relatările presei sunt folosite pentru realizarea de avertismente și evaluări asupra diferitelor riscuri de securitate.

Lahneman deschide un nou curent în discuțiile care privesc exploatarea surselor deschise și realizarea produselor de intelligence în baza acestora, prin transferul dezbaterilor de la paradigma *secret-deschis* la cea *clasificat-neclasificat*, arătând prin aceasta importanța OSINT.

În recentul *The Oxford Handbook of National Security Intelligence*, Arthur Hulnick apreciază faptul că „deși produsele OSINT provin din surse publice și alte tipuri de surse deschise, unele din aceste surse trebuie tratate drept sensibile, iar rezultatul final extras și analizat clasificat, nu doar pentru a convinge beneficiarul că merită citit”.

Autorul o citează pe Jennifer Sims, expert pe probleme de securitate și actual director pentru studii de intelligence la Georgetown University, potrivit căreia „intelligence trebuie și ar trebui să fie clasificat... din cauza înțelegerilor pe care le dobândește beneficiarul de la acea sursă”. Unul dintre motivele pentru care OSINT ar trebui să fie clasificat ar fi cel al copyright-ului. Un altul ar fi acela de a proteja descoperirea unui fapt pe care adversarii doresc să-l ascundă¹⁰.

2. Valorile secrete ale OSINT

Ca produs informațional independent, analiza OSINT constituie o importantă capacitate pentru factorii de decizie, prin furnizarea de imagini asupra aspectelor critice ale agendei de securitate, pentru ca aceștia să poată stabili și, mai ales, aplica politici pe termen lung, întărind capacitatea de prevenire și de răspuns la eventualele crize.

⁹ William J. Lahneman, „The Need for a New Intelligence Paradigm”, în *International Journal of Intelligence and CounterIntelligence*, vol. 23, nr. 2, 25 februarie 2010, pp. 212-214.

¹⁰ Arthur S. Hulnick, *The Dilemma of Open Source Intelligence: Is OSINT Really Intelligence?*, în „The Oxford Handbook of National Security Intelligence”, Loch, K. Johnson, Oxford University Press, 2010.

Pe de altă parte, informațiile deținute din surse deschise contribuie la realizarea analizei multisursă, atât prin identificarea unor elemente necesare înțelegerii contextului general cât și prin facilitarea accesului la anumite tipuri de expertiză din mediile academice.



Figura nr. 3
<http://www.einiras.org/>

Indiferent că este vorba de OSINT produs independent sau componentă a analizei multisursă, experții subliniază potențialul său de *resursă tactică, operațională și strategică*¹¹.

Fie că este vorba despre oferirea de informații cu privire la activitatea unei organizații teroriste ori că ajută la realizarea de avertizări timpurii și evaluări strategice, OSINT deține un rol covârșitor în reducerea imprevizibilului, a *incertitudinii* ce caracterizează mediul actual de securitate.

În cazul avertizărilor timpurii, dacă sunt înțelese situațiile care definesc un fenomen și factorii care le determină, ar trebui să fie ușor de identificat oportunitățile pentru a sesiza din timp problemele și a îndrepta lucrurile în direcția dorită¹².

¹¹ Chris Pallaris, *Open Source Intelligence (OSINT) and the Future of IR Librarianship*, pentru cea de-a 19-a conferință EINIRAS – International Relations and Security Network, Madrid, Spania, 18 septembrie 2009, disponibil la http://www.einiras.org/conf/conferences/documents/CPallaris_EINIRAS09.pdf [iunie 2010].

¹² Thomas Fingar, *Reducing Uncertainty: Intelligence and National Security. Using Intelligence to Anticipate Opportunities and Shape the Future*, lucrare susținută la Stanford University, octombrie 2009.

Cu toate acestea, avertizarea timpurie înseamnă să se *scaneze* informația conținută pentru sesizarea așa-numitelor semnale pierdute, care nu sunt foarte evidente, pentru a putea fi reperate amenințările și riscurile până atunci necunoscute¹³.

La rândul lor, evaluările strategice au ca obiectiv identificarea celor mai importante curente și a modului în care acestea vor interacționa, astfel încât decidenții politici să formuleze strategii și politici pentru a menține traiectoria pozitivă a evenimentelor.

Evaluările strategice reflectă „eficiența unui serviciu în slujba națiunii, aceasta fiind dată de modul său de raportare la actul de guvernare, la obiectivele politice și strategice ale statului și societății”¹⁴. Acestea îndeplinesc cel puțin două obiective: adaugă plus valoare informației existente, prezentând factorilor de decizie acele elemente care ajută la realizarea, pe termen lung, a obiectivelor prevăzute în strategia națională de securitate; contribuie la planificarea strategiei de informații și ajustarea priorităților factorilor de decizie¹⁵.

Date fiind numărul mare de variabile și de jucători, caracterul dinamic al evenimentelor, elaborarea de scenarii în care se pot încadra evenimentele anticipate s-a dovedit în multe dintre situații eronată. Întotdeauna există o doză de imprevizibil care poate răsturna și cele mai bine fundamentate concluzii despre cum va arăta viitorul.

Nicholas Taleb¹⁶, profesor, eseist, statistician, fost om de afaceri, definește această notă de imprevizibil prin sintagma *lebedă neagră*. Taleb consideră că trebuie luate în calcul *surprizele strategice* care ar putea răsturna proiecțiile realizate, evenimentele rare ce ar putea avea un impact major și care se află dincolo de așteptările noastre.

¹³ ***OSINT Report 1/2010, International Relations and Security Network, disponibil la <http://intellibriefs.blogspot.com/2010/04/osint-report-12010.html> [iunie 2010].

¹⁴ George Cristian Maior, „Intelligence eficient: de la control la cooperare”, în *Revista 22*, 23-29.12.2008, disponibil la <http://www.sri.ro/upload/Rev22dec2008.pdf> [iunie 2010].

¹⁵ William J. Lahneman, Jacques S. Gansler, John D. Steinbruner și Ernest J. Wilson III, *The Future of Intelligence Analysis*, vol. I, Center for International and Security Studies at Maryland, 2006.

¹⁶ Nicholas Taleb, *Lebedă Neagră: Impactul foarte puțin probabilului*, București, Editura Curtea Veche, 2008.

3. Valorile publice ale OSINT

Datorită caracterului lor neclasificat, precum și al produselor rezultate, sursele deschise sunt cele mai indicate pentru *implicarea experților din cadrul mediilor academice* în activitatea de analiză pe anumite probleme de securitate, pe de o parte, precum și pentru dezvoltarea procesului de *outsourcing*, pe de altă parte¹⁷.

Numeroase opinii, lansate inclusiv în spațiul românesc, pledează pentru ca, printre analiștii de intelligence, să se regăsească experți din domenii cum ar fi cel economic, religie, sociologie, psihologie etc.

Această idee a fost subliniată și de William J. Lahneman. Proiectul lansat de acesta și de echipa de la Universitatea din Maryland prin care se propune valorificarea platformelor colaborative și a avantajelor OSINT, chiar dacă a fost inițiat în anul 2006¹⁸, continuă să suscite interes, fiind reluat în anul 2010, într-o prezentare în prestigioasa publicație „*International Journal of Intelligence and CounterIntelligence*”¹⁹.

Pentru a fi eficiente, serviciile de informații trebuie să fie capabile să genereze *rețele colaborative* care să ofere produse informaționale ce necesită analiza interdisciplinară. *Aceste rețele trebuie să integreze OSINT și să conțină experți atât din sectorul privat, cât și din structurile de intelligence.* „Această schimbare presupune ca analiștii să partajeze informația cu alți analiști din cadrul organizațiilor de intelligence, dar și cu instituții din afară pentru a produce produse informaționale de calitate referitoare la probleme complexe”²⁰.

Contactele cu mediile de experți din afara structurilor de informații le permite ofițerilor să aibă acces la cunoștințe științifice de primă mână, necesare în special în analiza unor amenințări nonmilitare. Expertiza mediului academic prezintă avantajul unor unghiuri diverse de analiză și al perspectivelor culturale variate, care ar putea fi valorificate în cadrul unor proiecte comune de analiză, mese rotunde, seminare, conferințe etc.

¹⁷ Hamilton Bean, *Tradecraft versus Science: Intelligence Analysis and Outsourcing Research Institute for European and American Studies*, 2006, disponibil la se2.isn.ch/serviceengine/Files/RESSpecNet [iunie 2010].

¹⁸ William J. Lahneman, Jacques S. Gansler, John D. Steinbruner și Ernest J. Wilson III, *The Future of Intelligence Analysis. Final Report*, Center for International and Security Studies at Maryland, martie 2006.

¹⁹ William J. Lahneman, „The Need for a New Intelligence Paradigm”, în *International Journal of Intelligence and CounterIntelligence*, vol. 23, nr. 2, 25 februarie 2010.

²⁰ Ibidem.

Un alt element al dimensiunii publice a OSINT este cel de *outsourcing*, care s-a extins atât pe componenta de colectare, cât și pe cea de analiză.

Acesta presupune angrenarea în activitatea de intelligence a anumitor think tank-uri și institute academice de cercetare, care să contribuie cu perspective diverse de abordare, metodologii și, în general, cu întreaga lor expertiză.

Externalizarea serviciilor în domeniul OSINT către grupuri de cercetare consacrate oferă posibilitatea structurilor de informații de a-și confrunta analizele interne și hărțile de riscuri proprii cu cele venite din afară.²¹

Pregătirea în exploatarea surselor deschise în mediul universitar este o altă latură a caracterului public al OSINT. Mai multe centre universitare prestigioase (din SUA, Marea Britanie, Canada și țările nordice), organizează cursuri de master și doctorate în domeniul intelligence, unele dintre acestea fiind destinate cu precădere studiului OSINT.

Studiile postuniversitare de acest gen contribuie la crearea unui adevărat spațiu de recrutare pentru structurile de informații²².

Promovarea culturii de securitate este o altă misiune ce revine structurilor de intelligence, în contextul actual fiind necesar să se depășească simpla raportare privind activitatea pe care aceste organizații o fac publică anual.

Concept care se înscrie pe linia de comunicare publică a serviciilor de informații, cultura de securitate se impune tot mai mult în dezbaterile mediilor de intelligence. Este și unul dintre cele cinci principii pe care se fundamentează transformarea Serviciului Român de Informații.

Cultura de securitate presupune participarea întregii societăți la asigurarea securității, prin „promovarea și consolidarea valorilor democratice, dezvoltarea unei înțelegeri comune a provocărilor și oportunităților în domeniul securității naționale la nivelul statului și al societății”²³.

²¹ ****OSINT Report 1/2010*, International Relations and Security Network, disponibil la <http://intellibriefs.blogspot.com/2010/04/osint-report-1/2010.html> [iunie 2010].

²² Universitatea Henley-Putnam / San Jose, California, SUA, oferă *Bachelor or Master of Science Degree in Intelligence Management* cu tema „Abilități avansate de învățare în Analiza OSINT”, precum și *Master of Arts in Intelligence Management, Terrorism and Counterterrorism Studies, Management of Personal Protection*, care include un modul de OSINT avansat – <http://www.henley-putnam.edu/532-233.html>.

La rândul său, King's College, Londra, Marea Britanie, deține un centru – International Centre for Security Analysis – implicat în studierea mai multor problematici, printre care și metodologia de exploatare a surselor deschise – <http://www.kcl.ac.uk/schools/sspp/ws/grad/programmes/options/opensource.html>.

²³ <http://www.sri.ro/upload/viziunea.pdf> [iunie 2010].

OSINT, prin caracterul său deschis, este cea mai în măsură sursă de intelligence să ajute la promovarea educației de securitate, deoarece dispune de instrumentele și de statutul necesar pentru a rezolva această cerință, prin organizarea de evenimente publice care să reliefeze provocările majore ale securității.

O abordare matură în problematica de securitate națională bazată pe comunicare activă are capacitatea de a elimina o parte dintre „frustrările” și percepțiile eronate din societatea românească asupra instituțiilor de securitate, fiind un bun exercițiu de imagine.

Concluzii

În actualul context geopolitic, să ignori potențialul de valorificare a OSINT reprezintă o imensă vulnerabilitate de securitate, capacitatea surselor deschise de a răspunde, pe toate palierele de informare și cunoaștere, la nevoile beneficiarilor crescând pe măsura progreselor care se înregistrează în acest domeniu.

Includerea, în activitățile specifice OSINT, a unor reprezentanți din mediile academice este deosebit de importantă, în special datorită expertizei și informațiilor din noi surse pe care aceștia le dețin.

Strategiile serviciilor de informații ar trebui să prevadă încurajarea mediilor universitare de a-și extinde curricula în domeniul studiilor de securitate, intelligence și OSINT.

Nu în ultimul rând, prin intermediul surselor deschise, serviciile de informații pot contribui la promovarea și dezvoltarea, în rândul societății civile, a valorilor de securitate.

Bibliografie

I. Lucrări de sinteză

1. Gill, Peter; Marrin, Stephen și Phytian, Mark, *Intelligence Theory. Key Questions and Debates*, London & New York: Routledge, 2009.
2. Lahneman, William J.; Gansler, Jacques S.; Steinbruner, John D. și Wilson, Ernest J. III, *The Future of Intelligence Analysis. Final Report*, Center for International and Security Studies at Maryland, 2006.
3. Taleb, Nicholas, *Lebăda Neagră: Impactul foarte puțin probabilului*, București: Editura Curtea Veche, 2008.

II. Studii, articole, comunicări științifice

1. Hulnick, S. Arthur, *The Dilemma of Open Source Intelligence: Is OSINT Really Intelligence?*, în „The Oxford Handbook of National Security Intelligence”, Loch, K. Johnson, Oxford University Press, 2010.
2. Steele, Robert David, *Open Source Intelligence*, în Johnson Loch (ed.), *Strategic Intelligence: The Intelligence Cycle*, Westport: Praeger, 2007.
3. Mercado, Stephen C., *Sailing the Sea of OSINT in the Information Age*, în *Studies in Intelligence*, vol. 48, nr. 3, 2007.
4. Lahneman, William J., *The Need for a New Intelligence Paradigm*, în *International Journal of Intelligence and CounterIntelligence*, vol. 23, nr. 2, 2010.
5. Fingar, Thomas, *Reducing Uncertainty: Intelligence and National Security. Using Intelligence to Anticipate Opportunities and Shape the Future*, lucrare susținută la Stanford University, 2009.

III. Surse Internet

1. Bean, Hamilton, *Tradecraft versus Science: Intelligence Analysis and Outsourcing Research Institute for European and American Studies*, disponibil la se2.isn.ch/serviceengine/Files/RESSpecNet [iunie 2010], 2006.
2. Maior, George Cristian, *Intelligence eficient: de la control la cooperare*, în *Revista 22*, 23-29.12.2008, disponibil la <http://www.sri.ro/upload/Rev22dec2008.pdf> [iunie 2010], 2008.
3. ****OSINT Report 1/2010*, International Relations and Security Network, disponibil la <http://intellibriefs.blogspot.com/2010/04/osint-report-12010.html> [iunie 2010].
4. Pallaris, Chris, *Open Source Intelligence (OSINT) and the Future of IR Librarianship*, pentru a 19-a conferință EINIRAS – International Relations and Security Network, Madrid, Spania, 18 septembrie 2009, disponibil la http://www.einiras.org/conf/conferences/documents/CPallaris_EINIRAS09.pdf [iunie 2010], 2009.
5. Steele, Robert David, *Intelligence for Earth, Clarity, Diversity, Integrity, & Sustainability*, Oakton: Earth Intelligence Network, disponibil la <http://www.phibetaiota.net/?p=19357> [iunie 2010], 2010.
6. <http://www.henley-putnam.edu/532-233.html>.
7. <http://www.kcl.ac.uk/schools/sspp/ws/grad/programmes/options/opensource.html>.
8. http://www.oss.net/dynamaster/file_archive/030201/ca5fb66734f540fb_b4f8f6ef759b258c/NATO%20OSINT%20Handbook%20v1.2%20-%20Jan%202002.pdf [iunie 2010].
9. <http://www.sri.ro/upload/viziunea.pdf> [iunie 2010].