OSINT - la granița dintre secret şi public

Abstract

OSINT lies at the basis of the current transformations experienced by the intelligence segment, being both a rich source of information and technological innovation, responding to agencies' various current 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 accomplishes the transition from *secret sources* to *open sources*, enabling us to talk about a specific symbiosis between *classified* and *public* information.

1. Secret *versus* deschis

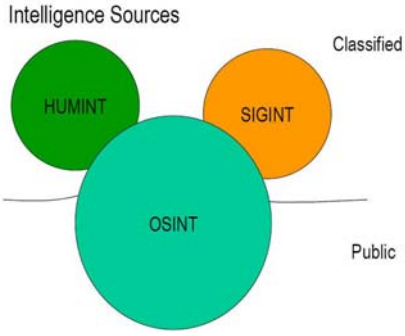

Fig. 1
http://langtech.jrc.it/

Natura ambivalentă - *secret* - *public* - a OSINT este reflectată încă din definiția dată în „NATO Open Source Intelligence Handbook": „OSINT este informația neclasificată, care a fost descoperită deliberat, selectată, filtrată şi 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 specialişti. Subliniind punctele tari şi pe cele slabe ale surselor secrete şi 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 primele[2]. 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 performante[3]. Se apreciază că jurnaliştii, analiştii din cadrul think tank-urilor pot avea cunoştințe mult mai solide într-un domeniu pe care l-au studiat ani de zile ori prin cunoaşterea unei societăți, a unei culturi etc.. Totodată, OSINT oferă informații în zone care, de multe ori, nu sunt foarte bine acoperite de mijloacele de culegere şi analiză tradiționale - infrastructură, economie, evenimente culturale, demografie.

Robert David Steele, unul dintre cei mai înverşunați promotori ai OSINT, afirmă 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”.

---

[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 şi 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 şi nu au capabilități 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 pratică de participare la operațiuni multinaționale şi 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]

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

Şi aceasta pentru că, „în ultimele două decenii de pionierat al OSINT şi până în prezent, în era multinațională, multiinstituțională, multidisciplinară, de analiză şi 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 câtorva, ci să te străduieşti să diseminezi informația pe întreaga planetă în beneficiul întregii comunități”[5].

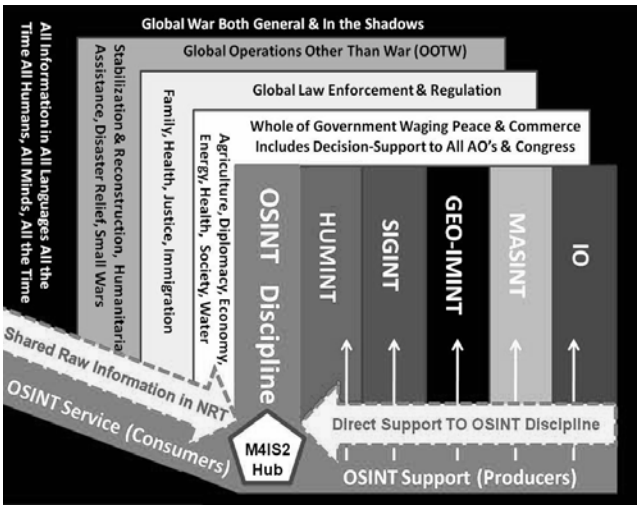

Fig. 2

http://www.phibetaiota.net/?p=

Unii specialişti, precum fostul ofițer CIA Arthur Hulnik, consideră OSINT ca fiind chiar „temelia pe care se construieşte informația secretă”. Acesta estimează că produsele

[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]

obținute din surse deschise contribuie în proporție covârşitoare la baza generală de informații[6].

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

Acesta pare a fi şi punctul de plecare pentru clasificarea datelor şi informațiilor realizată de William J. Lahneman, unul dintre cei mai cunoscuți specialişti în intelligence din spațiul anglo-saxon[8].

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*, cu conținuturi şi beneficiari diferiți.

Fluxurile *secret-secret* (I) şi *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 fluxul II, serviciile de intelligence corelează informațiile, folosind metode şi surse clasificate, produsele rezultate secrete fiind folosite pentru informarea oficialilor guvernamentali.

[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 şi 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

Potrivit autorului, nevoia concretizării fluxului III - *secret - deschis* - a crescut după atentatele de la 11 septembrie 2001, când a fost evident 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 declasificate pentru a fi informate autoritățile locale şi cele cu atribuții în aplicarea legii.

Ultima categorie (IV), *fluxul deschis-deschis*, creşte, 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 şi evaluări asupra diferitelor riscuri de securitate.

Lahneman deschide un nou curent în discuțiile privind exploatarea surselor deschise şi 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 că „deşi produsele OSINT provin din surse publice şi alte tipuri de surse deschise, unele din aceste surse trebuie tratate drept sensibile, iar rezultatul final extras şi analizat clasificat, nu doar pentru a convinge beneficiarul că merită citit”.

Autorul o citează pe Jennifer Sims, expert pe probleme de securitate şi actual director pentru studii în intelligence la Georgetown University, potrivit căreia „intelligence trebuie şi ar trebui să fie clasificat...din cauza înțelegerilor pe care le dobândeşte beneficiarul de la acea sursă”. Unul dintre motivele pentru care OSINT ar trebui să fie clasificat ar fi cel al

[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

copyright-ului. Un altul ar fi acela de a proteja descoperirea unui fapt pe care adversarii doresc să-l ascundă[10].

2. Valorile *secrete* ale OSINT

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

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

Fig. 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* şi *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 şi evaluări strategice, OSINT deține un rol covârşitor în reducerea imprevizibilului, a *incertitudinii* ce caracterizează mediul actual de securitate.

[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
[11] Chris Pallaris, *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]

În cazul avertizărilor timpurii, dacă sunt înțelese situațiile care definesc un fenomen şi factorii care le determină, ar trebui să fie uşor de identificat oportunitățile pentru a sesiza din timp problemele şi a îndrepta lucrurile în direcția bună[12].

Cu toate acestea, avertizarea timpurie înseamnă să se *scaneze* informația conținută pentru sesizarea aşa-numitelor semnale pierdute, care nu sunt foarte evidente, pentru a fi reperate amenințările şi riscurile până atunci necunoscute[13].

La rândul lor, evaluările strategice au ca obiectiv identificarea celor mai importante curente şi a modului în care acestea vor interacționa, astfel încât decidenții politici să formuleze strategii şi 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 şi strategice ale statului şi 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 şi ajustarea priorităților factorilor de decizie[15].

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

Nicholas Taleb[16], profesor, eseist, statician, fost om de afaceri, defineşte această notă de imprevizibil prin sintagma *lebăda neagră*. Taleb consideră că trebuie luate în calcul

[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

[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 şi Ernest J. Wilson III*, The Future of Intelligence Analysis*, vol. I, Center for International and Security Studies at Maryland, 2006

[16] Nicholas Taleb, *Lebăda Neagră: Impactul foarte puțin probabilului,* Bucureşti, Editura Curtea Veche, 2008

surprizele strategice care ar putea răsturna proiecțiile realizate, evenimentele rare care ar putea avea un impact major şi care se află dincolo de aşteptările noastre.

3. Valorile *publice* ale OSINT

Datorită caracterului lor neclasificat, precum şi 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 şi pentru dezvoltarea procesului de *outsourcing*, pe de altă parte[17].

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

Această idee a fost subliniată şi de William J. Lahneman. Proiectul lansat de acesta şi echipa de la Universitatea din Maryland prin care propune valorificarea platformelor colaborative şi a avantajelor OSINT, chiar dacă a fost inițiat în 2006[18], continuă să suscite interes, fiind reluat în 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* şi *să conțină experți atât din sectorul privat, cât şi din structurile de intelligence*. „Această schimbare presupune ca analiştii să partajeze informația

[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 şi 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

cu alți analiști din cadrul organizațiilor de intelligence, dar şi 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 cunoştințe ştiințifice de primă mână, necesare în special în analiza unor amenințări non-militare. Expertiza mediului academic prezintă avantajul unor unghiuri diverse de analiză şi al perspectivelor culturale variate, ce ar putea fi valorificate în cadrul unor proiecte comune de analiză, mese rotunde, seminarii, conferințe etc..

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

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

Externalizarea serviciilor în domeniul OSINT către grupuri de cercetare consacrate oferă posibilitatea structurilor de informații de a-şi confrunta analizele interne şi 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 şi țările nordice), organizează cursuri de masterat şi doctorate în domeniul intelligence, unele dintre acestea fiind destinate cu precădere studiului OSINT.

Studiile post-universitare de acest gen contribuie la crearea unui adevărat spațiu de recrutare pentru structurile de informații[22].

---

[20] Ibid.

[21]***_OSINT Report 1/ 2010_, International Relations and Security Network, disponibil la http://intellibriefs.blogspot.com/2010/04/osint-report-12010.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 şi *Master of Arts in Intelligence Management, Terrrorism 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 şi metodologia de exploatare a surselor deschise - http://www.kcl.ac.uk/schools/sspp/ws/grad/programmes/options/opensource.html.

Promovarea culturii de securitate este o altă misiune ce revine structurilor de intelligence, în contextul actual fiind necesar să se depăşească 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 dezbateriile mediilor de intelligence. Este şi 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 şi consolidarea valorilor democratice, dezvoltarea unei înțelegeri comune a provocărilor şi oportunităților în domeniul securității naționale la nivelul statului şi al societății”[23].

OSINT, prin caracterul său deschis, este cea mai în măsură sursă de intelligence să ajute la promovarea educației de securitate, deoarece dispune de instrumentele şi 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” şi 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

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

palierele de informare şi cunoaştere, la nevoile beneficiarilor crescând pe măsura progreselor ce se înregistrează în acest domeniu.

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

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

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

Bibliografie

I. Lucrări de sinteză

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

II. Studii, articole, comunicări ştiințifice

- Hulnick, S. Arthur (2010), *The Dilemma of Open Source Intelligence: Is OSINT Really Intelligence?*, în "The Oxford Handbook of National Security Intelligence", Loch, K. Johnson, Oxford University Press;

- Steele, Robert David (2007), *Open Source Intelligence*, în Johnson Loch (ed.), *Strategic Intelligence: The Intelligence Cycle*, Westport: Praeger;
- Mercado, Stephen C. (2007), *Sailing the Sea of OSINT in the Information Age*, în *Studies in Intelligence*, vol 48, nr. 3;
- Lahneman,William J. (2010), *The Need for a New Intelligence Paradigm*, în *International Journal of Intelligence and CounterIntelligence*, vol. 23, nr. 2;
- Fingar, Thomas (2009), *Reducing Uncertainty: Intelligence and National Security. Using Intelligence to Anticipate Opportunities and Shape the Future*, lucrare susținută la Stanford University;

III. Surse Internet

- Bean, Hamilton (2006), *Tradecraft versus Science: Intelligence Analysis and Outsourcing Research Institute for European and American Studies*, disponibil la se2.isn.ch/serviceengine/Files/RESSpecNet [iunie 2010];
- Maior, George Cristian (2008), *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];
- ****OSINT Report 1/ 2010*, International Relations and Security Network, disponibil la http://intellibriefs.blogspot.com/2010/04/osint-report-12010.html [iunie 2010];
- Pallaris, Chris (2009), *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];

- Steele, Robert David (2010), *Intelligence for Earth, Clarity, Diversity, Integrity, & Sustainability*, Oakton: Earth Intelligence Network, disponibil la http://www.phibetaiota.net/?p=19357 [iunie 2010];
- http://www.henley-putnam.edu/532-233.html;
- http://www.kcl.ac.uk/schools/sspp/ws/grad/programmes/options/opensource.html;
- http://www.oss.net/dynamaster/file_archive/030201/ca5fb66734f540fbb4f8f6ef759b258c/NATO%20OSINT%20Handbook%20v1.2%20-%20Jan%202002.pdf [iunie 2010];
- http://www.sri.ro/upload/viziunea.pdf [iunie 2010].