TENDINŢE ÎN INTELLIGENCE

1. Provocări în activitatea de intelligence

2. *Joint intelligence*

3. Securitatea – rezultat al unui efort comun al întregii societăţi

4. Relaţia bi-direcţională cu beneficiarii

5. Un nou rol pentru OSINT

6. Concluzii

Rezumat

Avansul tehnologic, globalizarea şi efervescenţa *versiunii deschise* a modului de obţinere a informaţiilor au transformat profund procesul de *intelligence*.

Într-un univers dual, *online - offline*, caracterizat de conectivitate şi, totodată, atomizare, de circulaţie largă, rapidă, în reţele extrem de eterogene, s-au amplificat incertitudinile atât în ceea ce priveşte procesele actuale, dar mai ales predictibilitatea celor viitoare.

În societatea cunoaşterii, securitatea a devenit, mai mult decât oricând, un bun comun, iar principala caracteristică a noilor realităţi este „transparenţa determinată de multiple interdependenţe".

Pentru a face faţă acestor provocări, administraţiile moderne implementează strategii de securitate în care rolul serviciilor specializate se transformă radical, devin parte a unui efort naţional care implică deopotrivă instituţiile guvernamentale şi civile, mergând până la responsabilizarea individuală a cetăţeanului.

În perspectivă, serviciile de *intelligence* tind să devină furnizoare de cunoaştere, în cadrul unei reţele interdisciplinare, în care rolurile de beneficiar şi furnizor sunt complementare, interşanjabile perpetuu.

Pentru ca această concepţie să-şi găsească un corespondent în realitate, este necesară transformarea culturii secretului, cea mai bună cale de exersare a deschiderii şi a beneficiilor pe care le aduce cooperarea fiind oferită de sursele deschise, alături de „informaţiile de încredere".

Cuvinte-cheie: intelligence, securitate, surse deschise, informaţii, tehnologie

1. Provocări în activitatea de intelligence

Ultimii 20 de ani au însemnat, pentru serviciile de informaţii, o continuă reinventare, pentru a gestiona probleme de securitate tot mai complexe.

Proliferarea formelor asimetrice, neconvenţionale de conflict, şi caracterul transnaţional al ameninţărilor s-au suprapus apariţiei de noi medii de comunicare, în care transmiterea şi schimbul de informaţii pot avea loc neîngrădit, la adăpost de intervenţia forţelor de securitate, prin eliminarea treptată a barierelor „tehnice", dar în care intenţiile şi identitatea emitentului sunt dificil de stabilit.

Ameninţări precum spionajul şi criminalitatea organizată, considerate „tradiţionale" în structurile de intelligence, au dobândit dimensiuni suplimentare, legate de dezvoltarea tehnologică.

În plus, au apărut pericole noi, precum cele cibernetice, a căror natură difuză, anarhică şi interconexată, le face extrem de greu de identificat şi gestionat.

De altfel, Robert Cooper avertiza, în lucrarea sa “Destrămarea naţiunilor - geopolitica secolului al XXI-lea” (2007), că “secolul în care tocmai am intrat riscă să fie deturnat de anarhie şi tehnologie, iar aceşti doi mari distrugători s-ar putea susţine reciproc”.

Vechile paradigme de explicare a cadrului internaţional sunt tot mai contestate sau insuficiente, iar o nouă teorie unanim acceptată se lasă aşteptată. Statele sunt mai vulnerabile (în cel mai bun caz, mai nepregătite) ca oricând la aceste provocări.

Accesul la tehnologie, la mijloace de comunicare şi propagandă, la diferite alte resurse de putere, care s-au aflat în mod tradiţional în monopolul statului, este acum la îndemâna a ceea ce generic s-a numit „nonstat”, care a profitat de propagarea inovaţiilor, şi-a modificat metodele de acţiune şi le-a folosit în detrimentul intereselor globale de securitate.

În acest univers dual, *online - offline*, caracterizat de circulaţie largă, rapidă, în reţele extrem de eterogene, s-au amplificat incertitudinile atât în ceea ce priveşte procesele actuale, dar mai ales predictibilitatea celor viitoare. A devenit evident că lumea se află într-o criză de adaptare care, comparativ cu alte etape în evoluţia societăţii umane, prin rapiditatea şi spaţiile pe care le acoperă, demonstrează că, pentru o înţelegere reală, nu mai este suficientă calea reducţionistă.

Toate aceste evoluţii au transformat profund procesul de *intelligence*, obligând structurile informative să adapteze permanent şi în timp foarte scurt strategii, planuri, tactici şi forme de management.

2. *Joint intelligence*

Administraţiile moderne implementează strategii de securitate în care rolul serviciilor specializate se transformă radical, acestea devenind parte a unui efort naţional care implică, deopotrivă, instituţiile guvernamentale şi civile, mergând până la responsabilizarea individuală a cetăţeanului.

Din această perspectivă, un principiu fundamental este „cultura de securitate”, ce presupune promovarea şi consolidarea valorilor democratice prin dezvoltarea unei înţelegeri comune a provocărilor şi oportunităţilor în domeniul securităţii naţionale, la nivelul statului şi al societăţii.

Abordarea mai profundă a conceptului a condus la o redimensionare a *joint intelligence-ului,* care presupune cooperare, comandă şi direcţie integrată, precum şi folosirea resurselor şi a informaţiilor din toate sursele disponibile pentru realizarea analizei şi informarea decidenţilor.

Colaborarea, pe verticală şi orizontală, specifică *joint intelligence*-ului, deţine un rol covârşitor în formarea acelei gândiri strategice necesare pentru a rezista prezentului imprevizibil şi surprizelor viitorului.

3. Securitatea – rezultat al unui efort al întregii societăţi

În societatea cunoaşterii, securitatea a devenit, mai mult decât oricând, un bun comun, iar principala caracteristică a noilor realităţi este „transparenţa determinată de multiple interdependenţe”.

Astfel, serviciile de *intelligence* tind să devină furnizoare de cunoaştere, în cadrul unei reţele interdisciplinare, în care rolurile de beneficiar şi furnizor sunt complementare, interşanjabile perpetuu.

Din acest punct de vedere, este vitală relaţia pe care structurile de securitate o stabilesc cu opinia publică. Mass-media, prin funcţia sa de filtrare şi traducere a mesajului organizaţiilor, se dovedeşte a fi extrem de importantă. Similar, colaborarea public-privat, consilierea şi influenţa exercitate de organizaţii neguvernamentale au un efect important asupra eficienţei deciziilor politice adoptate de stat pentru asigurarea securităţii.

Totodată, *think tank*-urile, universităţile şi institutele de cercetare contribuie la procesul de intelligence, expertiza mediului academic prezentând avantajul cercetării ştiinţifice aprofundate, al dezbaterilor critice şi al perspectivelor culturale variate.

Educarea cetăţenilor într-un spirit participativ, în propriul beneficiu, reprezintă însă cea mai mare provocare, mai ales în societăţile care s-au confruntat cu regimuri autoritare.

Beneficiile unei abordări bazate pe comunicare activă sunt majore:

- ⇨ consolidarea încrederii între părţi;
- ⇨ responsabilizarea societăţii, precum şi întărirea convingerii cetăţenilor că aceştia nu sunt doar beneficiari, ci şi contributori la satisfacerea propriilor nevoi de securitate.

4. Relaţia bi-direcţională cu beneficiarii

În ultimul deceniu, s-a accentuat progresiv preocuparea serviciilor de informaţii de a se apropia de destinatarul final al produselor lor şi de a revizui, permanent, raporturile bilaterale. Comunitatea de informaţii a înţeles că trebuie să asigure nu numai informaţii, ci şi „judecăţi" şi „ipoteze asupra sensului" acelor date şi posibilele lor efecte asupra direcţiei politice.
În aceste condiţii, accentul se deplasează de la „încredere în date" la „încredere în furnizorul de servicii".

Astfel, se produce o reinventare a intelligence-ului ca interlocutor axat pe implicarea în dialoguri cu beneficiarul, centrate pe scop, altfel spus, acesta tinde să devină mai degrabă furnizor de servicii (prin şedinţe de informare) decât producător de informaţii.

O relaţie strânsă conduce la următoarele situaţii:

- ⇨ când factorul de decizie cunoaşte capacitatea/ posibilităţile/ aptitudinile furnizorului de informaţii, poate schimba dimensiunea cerinţelor/ solicitărilor sale;
- ⇨ când furnizorul cunoaşte cerinţele, îşi poate desfăşura resursele astfel încât să îşi optimizeze capacitatea de reacţie.

Într-o relaţie furnizor - client, acesta din urmă nu îşi concentrează încrederea în produsele analitice sau platforme de colectare, ci în abilitatea primului de a plasa datele în context, de a înţelege modul în care acţiunile, evenimentele şi actorii ar putea interacţiona şi influenţa rezultate.

5. Un nou rol pentru OSINT

Intelligence nu înseamnă numai culegerea de informaţii şi transmiterea acestora către beneficiari, ci cunoaştere în sensul cel mai înalt al termenului, un mod de a înţelege lumea utilizând toate sursele.

Din această perspectivă, *Open Source Intelligence*/ OSINT reprezintă un concept vital în strategia de intelligence a NATO şi nu numai, majoritatea serviciilor de informaţii dezvoltând departamente special destinate exploatării surselor deschise.

Creşterea importanţei OSINT este direct legată de deschiderea analiştilor comunităţii de informaţii către schimbul de experienţă şi cunoştinţe cu experţi din mediul academic, de afaceri şi din centrele de cercetare.

Pentru ca această concepţie să-şi găsească un corespondent în realitate, s-a impus transformarea culturii tradiţionale a secretului, iar după momentul 11 Septembrie 2001 a devenit imperativă realizarea binomului secret - deschis, altfel spus reunirea eforturilor tuturor zonelor de analiză în scopul protejării de agresiuni.

Pentru soluţionarea acestei probleme, cercetătorul american William Lahneman a propus promovarea unui nou concept al procesului de *intelligence,* în care între “informaţia secretă” şi “informaţia deschisă” este plasată “informaţia de încredere” (*trusted information*), care circulă într-o “reţea a încrederii” (*trusted networks*).

Sistemul creat pe această bază ar fi utilizat în mod responsabil, contributorii urmând să alimenteze, după nişte reguli prestabilite, numai informaţii validate. Printre membri pot fi agenţii guvernamentale, companii private, ONG-uri, comunităţi de interese şi chiar indivizi în mod particular.

Alături de „informaţiile de încredere”, o cale eficientă de exersare a deschiderii şi a beneficiilor pe care le aduce cooperarea este oferită de sursele deschise.
OSINT nu se limitează la *Internet mining* sau monitorizarea presei, aşa cum consideră unii teoreticieni în domeniu, ci solicită de la cei implicaţi cunoştinţe sociale şi culturale ridicate, având potenţial ca resursă tactică, operaţională şi strategică şi deţinând un rol substanţial în reducerea imprevizibilului, a incertitudinii ce caracterizează mediul de securitate.

Exploatarea surselor deschise de informare este cu atât mai mult necesară în societatea actuală cu cât dezvoltarea exponenţială a acestora, cantitativă şi calitativă, constituie una dintre caracteristicile modernităţii.

6. Concluzii

Deşi a fost un proces dificil, serviciile de informaţii au înţeles că, pentru a fi eficiente, trebuie să fie capabile să se reinventeze, să genereze reţele colaborative care să ofere produse informaţionale anticipative, oportune, complete, obiective, care să sprijine procesul decizional în sfera securităţii şi să sporească încrederea în capacitatea statului de a-şi proteja cetăţenii.

Efectele benefice ale acestei schimbări de paradigmă nu sunt, neapărat, vizibile publicului larg, dar constituie un fundament esenţial pentru crearea unui parteneriat real între *intelligence* şi cetăţeni, al cărui scop final este asigurarea condiţiilor pentru obţinerea de bunăstare socială, în condiţii de siguranţă.

În acest proces, de conectare a nodurilor – instituţii publice, organizaţii neguvernamentale, companii private şi indivizi - OSINT reprezintă un liant, reuşind să aducă la un loc cea mai bună expertiză – cea a întregii societăţi şi a celor mai capabili membri ai săi.

Viitorul în *intelligence* duce OSINT în avangarda comunităţii de informaţii, într-o reţea din care nu lipseşte aportul sectorului privat, respectiv al polilor de cunoaştere din societate - mediul academic, think tank-uri şi chiar analişti *freelancer*.

Bibliografie

1. Andrus, D. Calvin, *The Wiki and the Blog: Toward A Complex Adaptive Intelligence Community*, iulie 2005, disponibil online la adresa https://www.cia.gov.
2. Bean, Hamilton, *Tradecraft versus Science: Intelligence Analysis and Outsourcing Research*, Institute for European and American Studies, 2006, disponibil online la se2.isn.ch/serviceengine/Files/RESSpecNet.
3. Bodnar, John W., *Warning Analysis for the Information Age: Rethinking the Intelligence Process*, Joint Military Intelligence College, decembrie 2003.
4. Chirot, Daniel, *Societăţi în schimbare*, Editura Athena, Bucureşti, 1996.
5. Cooper, Robert, *Destrămarea naţiunilor*, Ed. Univers Enciclopedic, 2007.
6. Fingar, Thomas, *Reducing Uncertainty: Intelligence and National Security. Using Intelligence to Anticipate Opportunities and Shape the Future*, Stanford University, octombrie 2009.
7. Haass, Richard, *Think Tanks and U.S. Foreign Policy: A Policy-Maker's Perspective*, în „U.S. Foreign Policy Agenda - The Role of Think Tanks in U.S. Foreign Policy", volumul 7, nr. 3, noiembrie 2002.
8. Kerbel, Josh, Olcott, Anthony, *Synthesis with the Client, Not Analysing for Customers*, în „Studies in Intelligence", vol. 54, nr. 4, decembrie 2010.
9. Korns, Stephen W., *Cyber Operations. The New Balance*, disponibil online la adresa http://www.carlisle.army.mil.
10. Lahneman, William J., Gansler, Jacques S., Steinbruner, John D., Wilson III, Ernest J., *The Future of Intelligence Analysis*, vol. I, Center for International and Security Studies at Maryland, 2006.
11. Lahneman, William J., Gansler, Jacques S., Steinbruner, John D., Wilson III, Ernest J., *The Future of Intelligence Analysis. Final Report*, Center for International and Security Studies at Maryland, martie 2006.
12. Lahneman, William J., *The Need for a New Intelligence Paradigm*, în „International Journal of Intelligence and CounterIntelligence", vol. 23, nr. 2, 25 februarie 2010.
13. Maior, George Cristian, *Intelligence eficient: de la control la cooperare*, în „22", 23-29.12.2008, disponibil online la http://www.sri.ro/upload/Rev22dec2008.pdf.
14. Maior, George Cristian, *Incertitudine. Gândire strategică şi relaţii internaţionale în secolul XXI*, Editura RAO, Bucureşti, 2009.
15. McGann, James G., *Think Tanks and Policy Advice in the U.S.*, Foreign Policy Research Institute, august 2005.
16. ****Cyber In-Security. Strenghtening the Federal Cybersecurity Workforce*, Booz Allen Hamilton, iulie 2009, disponibil online la adresa http://www.boozallen.com.
17. *****OSINT Report 1/ 2010*, International Relations and Security Network, disponibil online la http://intellibriefs.blogspot.com/2010/04/osint-report-12010.html.
18. Pallaris, Chris, *Open Source Intelligence (OSINT) and the Future of IR Librarianship*, pentru a 19-a conferinţă EINIRAS - International Relations and Security Network, Madrid, Spania, 18 septembrie 2009, disponibil online la http://www.einiras.org/conf/conferences/documents/CPallaris_EINIRAS09.pdf.
19. Taleb, Nicholas, *Lebăda Neagră: Impactul foarte puţin probabilului,* Bucureşti, Editura Curtea Veche, 2008.