Impactul evoluțiilor tehnologice asupra OSINT

Dragoş DINU
Maria Daniela BUNOIU
Serviciul Român de Informații
e-mail: **ani@sri.ro**

Abstract

One of the most effective ways to meet the new security challenges seems to be „taming" the information, by finding new methods to collect, process, and disseminate it. Also, as both the national and international security environment change, intelligence agencies must find ways to dynamically reinvent themselves by learning and adapting.

Keywords: new-technology, competitive, intelligence multidimensional resources, cyber operation.

„Este prima specie de pe această planetă care se autoreproduce şi al cărei părinte este un computer". Acum câteva decenii – ar fi inutil să mai vorbim de secole – o astfel de frază ar fi zguduit lumea ştiinţifică, comunităţile religioase şi culturale şi ar fi condus, probabil, la proteste în masă. În prezentul în perpetuă schimbare, era doar o chestiune de timp până când cineva o va pronunța[1].

Evoluțiile înregistrate în domeniul biologiei, biogeneticii, roboticii, nanotehnologiei au făcut ca noțiuni precum inteligență artificială, date biometrice, energii alternative, armament electromagnetic, capacități nucleare şi încălzire globală să devină subiecte la ordinea zilei.

Dacă sistemele militare ale secolului precedent s-au bazat pe progrese în domeniul fizicii, ingineriei, informaticii şi matematicii, viitorul prezintă o noua gamă de amenințări şi „arme" din ce în ce mai inventive. Tendințele în domeniul informaticii, conectivitatea şi schimbul de informații generează noi oportunități, dar şi riscuri la adresa securității naționale[2].

[1] Autorul este biologul american Craig Venter, care a anunțat, în luna mai a.c., că a creat prima celulă sintetică din lume, bacteria Mycoplasma mycoides.

[2] Unii experți susțin că această tendință contribuie la descentralizare sau la trecerea puterii de la națiuni la indivizi sau grupări, care nu pot fi definite prin granițele politice.

„Societate bazată pe informație”[3], „interdependență”, „globalizare” reprezintă concepte care au marcat profund actualul mediu de securitate, astfel încât este nevoie mereu de perfecționare şi adaptare a strategiilor, tacticilor, managementului. O comunitate de informații trebuie să se reinventeze permanent, într-un mod dinamic, prin învățare continuă şi prin adaptare[4].

Resursele multilaterale pot fi avantajate de creşterea capacității națiunilor şi entităților de a răspunde la amenințările care survin, prin îmbunătățirea schimbului de informații şi prin colaborare strânsă ca răspuns la amenințările manifestate. Totodată, securitatea colectivă poate fi îmbunătățită prin extinderea modalităților şi oportunităților structurilor marginale de a participa în acțiuni sincronizate împotriva amenințărilor comune la adresa ordinii internaționale[5].

Propagarea tehnologiilor de ultimă oră, care ar putea fi folosite în detrimentul intereselor naționale de securitate, nu mai este rezervată națiunilor „de elită”. Rezultatul este sporirea potențialelor amenințări şi creşterea incertitudinii. Deşi oferă beneficii, îmbunătățind răspunsurile globale colective fără costuri semnificative, prin schimbarea modului în care resursele şi capacitățile globale sunt gestionate, progresele tehnologice creează paradigme de securitate problematice.

Dacă în trecut identificarea adversarului era relativ uşoară, în contextul a ceea ce a primit numele de „noua normalitate cibernetică” identificarea reprezintă excepția.

Grupările paramilitare sau insurgente, precum şi alți participanți non-statali şi forțe militare din state în curs de dezvoltare achiziționează din ce în ce mai multă tehnologie şi îşi transformă metodele de acțiune.

---

[3] În revoluția informațională, pentru preocupările strategice au fost considerate relevante, inițial, trei „curente”: utilizarea la scară largă a telefoniei mobile, transparența şi războiul cibernetic.

[4] Andrus D. Calvin, „The Wiki and the Blog: Toward A Complex Adaptive Intelligence Community”, iulie 2005.

[5] Un prim pas în dezvoltarea comunităților este armonizarea legilor interne şi internaționale, precum şi ajungerea la un acord cu privire la activitățile care ar trebui contracarate, cum ar fi terorismul, atacurile cibernetice şi traficul de armament. De asemenea, este necesară o infrastructură de bază (supraveghere şi schimb de informații), care să gestioneze amenințările globale şi să înlocuiască modelele de securitate fragile şi antagonice, limitate la protejarea frontierelor.

Rețeaua „al-Qaida", de exemplu, împreună cu afiliații şi susținătorii săi, foloseşte Internetul pentru a-şi propaga doctrina. Grupul consideră atenția media şi prozelitismul („dawa") ca fiind de o importanță egală sau mai mare decât violența. Materialele sunt diseminate în scopul planificării, instructajului, propagandei şi radicalizării.

Dacă în trecut războiul asimetric era considerat „arma celui mai slab" sub aspectul aplicării metodelor neconvenționale pentru a profita de vulnerabilitățile celui puternic, în actualul mediu, reprezintă „arma celui mai inteligent". Cibernetica este omniprezentă: toată lumea atacă pe toată lumea, astfel încât, „sentințe" precum cea dată de Jim Langevin, membru al Comisiei pentru securitate internă a Camerei Reprezentanților, din Congresul SUA, conform căreia „niciodată nu vom mai asista la un război major fără o importantă componentă cibernetică", s-ar putea dovedi valabile[6].

Cum informațiile sunt elementul esențial în eforturile de asigurare a securității, iar procesul de colectare şi analizare a lor necesită, în prezent, o mobilizare de resurse tehnologice impresionantă şi un efort uman semnificativ, numeroase agenții guvernamentale analizează, în prezent, implicațiile stocării datelor pe termen nedefinit, în scop operativ, legal, administrativ sau istoric. Este necesară, însă, şi elaborarea unei serii de reglementări privind gestionarea şi schimbul de informații clasificate, care să corespundă capacităților tehnologice avansate de colectare, stocare şi analiză a datelor, consolidarea măsurilor de securitate şi protecție fiind, de asemenea, esențială.

Evoluțiile în domeniul tehnologic au condus şi la o reorientare în ceea ce priveşte politica de personal, atât la nivelul organizațiilor private, cât şi la cel al serviciilor de informații. Abilitățile comunicaționale şi utilizarea mediului online ar putea deveni esențiale în procesul de recrutare. O rețea de angajați ce comunică virtual, mult mai rapid, ar conduce la o eficientizare a lucrului în echipă, dar şi a procesului de analiză.

Suplimentarea numărului de specialişti în structurile de securitate, în vederea combaterii criminalității cibernetice, este de asemenea utilă pentru combaterea atacurilor altor state, organizațiilor sau hackerilor, astfel încât instruirea în domeniul IT, dar şi recrutarea de personal pregătit din sectorul privat s-au transformat în necesitate[7].

---

[6] Stephen W. Korns, „Cyber Operations. The New Balance".

[7] „Cyber In-Security. Strenghtening the Federal Cybersecurity Workforce", Booz Allen Hamilton, iulie 2009.

În vederea soluționării problemelor existente, agențiile de informații americane caută în afara structurilor guvernamentale / de specialitate experți IT. Un oficial din cadrul Departamentului de Securitate Internă a estimat că 83% din personalul din cadrul biroului ofițerilor superiori de informații este reprezentat de contractori din mediul privat. Administrația nu trebuie doar să recruteze şi să instruiască mai multe persoane cu calificare în domeniul IT, ci are nevoie efectiv de specialişti capabili să activeze în cadrul structurilor ce asigură securitatea cibernetică.

Comunicare neîngrădită

Blogul, email-ul, rețelele sociale, mesajele text au deschis noi perspective, noi medii în care schimbul de informații poate avea loc, teoretic, neîngrădit. Eliminarea treptată a barierelor „tehnice" nu putea rămâne fără urmări, astfel încât libertatea de exprimare a condus la transformarea acestor medii în ținte sigure pentru ceea ce unii ar numi „cenzură", iar alții – „echilibru", „coordonare" sau „mediere a conținutului"[8].

Creşterea numărului şi tipurilor de surse a condus şi la dezvoltarea conținutului ce trebuie analizat şi validat, astfel încât a apărut o preocupare deosebită pentru găsirea unor metode de a „controla" volumul de informații, fie prin extinderea prerogativelor instituțiilor de stat, fie prin crearea unor baze de date în vederea monitorizării şi stocării informațiilor comunicate prin telefon sau rețele sociale (Marea Britanie, SUA, Suedia).

Dezvoltarea şi menținerea unei rețele de angajați şi contactelor externe, în vederea asigurării de informații despre evoluțiile de piață din cadrul industriei respective au constituit o provocare şi pentru departamentele corporatiste de *competitive intelligence*. Crearea şi menținerea „rețelelor de surse umane" reprezintă o bună practică de intelligence competitiv ce asigură atât achiziționarea de informații unice, nepublicate, cât şi opinii şi comentarii profesioniste în vederea sprijinirii procesului de analiză de intelligence[9]. Introducerea de sisteme colaborative în munca de analiză a facilitat realizarea

[8] Într-un discurs ținut la 21 ianuarie 2010, secretarul american de stat, Hillary Clinton, sublinia: „Considerăm că este critic ca utilizatorilor de Internet să le fie asigurate anumite libertăți de bază. Iar libertatea de exprimare este prima dintre ele. Aceasta nu mai este definită doar de posibilitatea ca cetățenii să meargă în piața publică şi să critice autoritățile fără a se teme de consecințe".

[9] Rețelele de socializare şi aplicațiile web 2.0 oferă practicienilor o multitudine de noi „instrumente" ce pot facilita dezvoltarea de rețele de surse umane atât în interiorul, cât şi în afara „proiectului".

unor rapoarte mai complexe, chiar dacă nu pot fi eliminate toate obstacolele întâmpinate în cadrul muncii în echipă. Cei care iau decizii în funcție de informațiile de care dispun, precum şi cei care îşi duc la îndeplinire misiunile bazându-se pe resursele informaționale trebuie să beneficieze de dreptul de a face schimb de informații, pentru a se asigura că primesc cele mai relevante date.

Ideea[10] a fost extinsă, astfel încât, în mediul actual, extinderea cooperării şi a schimbului de informații între organizații sau națiuni tinde să se transforme în regulă. Un factor de influență l-a constituit, probabil, şi dezvoltarea incredibilă a riscurilor şi amenințărilor. Societatea prezentă este atât de dominată de tot ceea ce înseamnă IT, încât orice descoperire sau evoluție în domeniu conduce rapid la apariția de modalități de decriptare sau de speculare a punctelor slabe.

În consecință, cadrul pentru realizarea schimbului de informații trebuie să includă şi instrumente tehnologice pentru reducerea riscului dezvăluirii neintenționate a informațiilor personale, inclusiv instrumentele de criptare, de asigurare a anonimatului şi managementul drepturilor digitale.

Instrumente noi la riscuri noi

În prezent, se poate spune că tehnologia dictează tendința de dezvoltare pe care domeniul intelligence trebuie să o urmeze.

Îndepărtarea Internetului de computere conectate fizic într-o rețea şi apropierea acestuia de terminalele mobile a determinat o abordare nouă a metodelor de diseminare a informațiilor (achiziționarea de terminale iPhone, iPad, BlackBerry).

Noul Internet se reorientează în viitorul apropiat, adoptând o nouă sintagmă: „Everything, everywhere, always". Implementarea tehnologiilor „web-ului semantic" va elimina confuziile generate de informațiile nestructurate, trasând astfel delimitări clare între Internetul serviciilor, Internetul mobil şi Internetul lucrurilor.

Progresele tehnologiei au condus la apariția unor soluții din ce în ce mai eficiente pentru realizarea unui ciclu complet OSINT, iar această

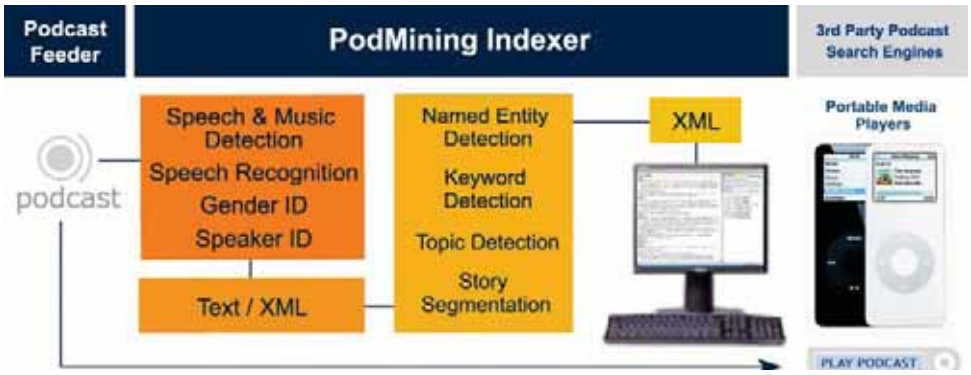
[10] „Revoluția" a început în 2005 cu introducerea mai multor servicii de colaborare: Intellipedia, serviciul mesagerie rapidă în întreaga agenție, o funcție socială similară del.icio.us., o capacitate de căutare şi blog-urile la nivelul organizației. Intellipedia se bazează pe acelaşi tip de programe ca şi Wikipedia, enciclopedia on-line, dar când Intellipedia a fost lansată, comunitatea de intelligence a hotărât că nu va putea fi folosită ca o enciclopedie, ci pentru a deveni un loc pentru colaborarea directă.

dezvoltare forțează organizațiile din domeniul intelligence să se alinieze la ultimele apariții în domeniu.

Pornind de la automatizarea culegerii datelor din diverse surse (audiovideo şi Internet) şi continuând cu procesarea acestora până la diseminarea informațiilor, ciclul OSINT se închide cu feedbackul, uneori dedus din desfăşurarea directă a evenimentelor. Diseminarea cu rapiditate a informațiilor provenite din surse deschise este şi trebuie să fie unul din punctele focale ale procesului OSINT. Varietatea formelor şi viteza de diseminare, precum şi calitatea informațiilor din surse deschise vor face diferența între organizațiile din domeniul intelligence.

Problema cea mai importantă de soluționat în momentul în care există enorme baze de date din surse deschise este descoperirea unui mod de a le „converti" în intelligence.

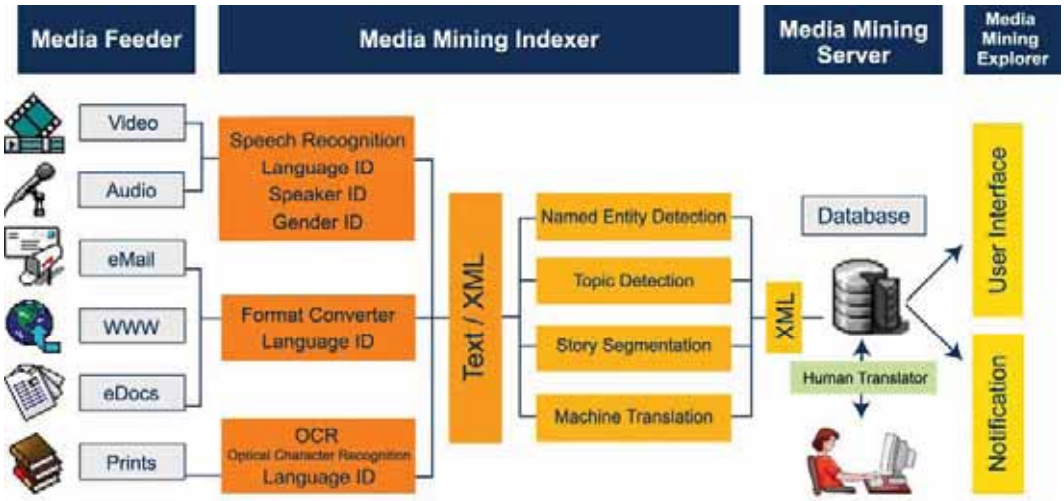
Au apărut, astfel, companii care pun la dispoziție instrumentele necesare monitorizării surselor şi facilitării, colectării şi procesării informațiilor. „Sail Labs" (cu sediul în Viena), de exemplu, este una dintre cele mai importante companii ce activează în domeniul „speech technology" şi oferă servicii destinate eficientizării procesului de colectare a informației (sisteme de *media*, *text / podcast mining*), cu ajutorul cărora date nestructurate din surse multiple (televiziune, radio, podcast-uri, streaming media) sunt procesate în informație structurată, uşor de căutat şi accesibilă. În cadrul acestui proces, conținutul unui fişier video sau audio este transcris, tradus şi indexat în mod automat, în timp real, în funcție de limbă, vorbitor, subiect, nume sau cuvinte-cheie.



Sistem media mining[11]

[11] http://www.sail-technology.com.

Sistem podcast mining[12]



Conținutul informațional poate fi „descoperit" prin eliminarea / depăşirea segmentelor irelevante, urmărirea datelor de interes printr-un sistem de alertă automată şi afişarea sintetizată a surselor în timp real[13].

În ceea ce priveşte traducerea automată aproximativ în timp real, aplicațiile pentru dispozitivele „smart" sunt pe punctul de a deveni general valabile în cel mult trei ani, dat fiind că cercetătorii sunt aproape de a definitiva tehnologia necesară şi de a o aplica sub forma *smart phones*, fiind utilizate, în cadrul procesului, un soft optic pentru recunoaşterea caracterelor şi tehnologia *Google Translate*[14].

Un dispozitiv de comunicare unidirecțional este folosit de câțiva ani în domeniul militar. Phraselator P2, produs de compania „Voxtec", asigură comunicarea a mii de fraze, cu ajutorul unor traduceri înregistrate în prealabil. În cel mult 18 luni, „Voxtec" speră să obțină un dispozitiv de comunicare bidirecțional limitat[15].

---

[12] http://www.sail-technology.com.
[13] Site-ul companiei „Sail Labs", http://www.sail-technology.com.
[14] De asemenea, tehnologii precum „Languageweaver" asigură traduceri aproximativ în timp real din mai multe limbi arabe.
[15] Felix Juhl, Chris Pallaris, Florian Schaurer, *OSINT Report 1/2010 – Technology Trends*, publicat de „International Relations and Security Network".

Progresul impune şi necesitatea găsirii unor noi modalităţi de validare, de exemplu, şi conţinutul generat de utilizator se numără, în prezent, printre „sursele" de interes. Ceea ce era până acum suficient pentru evaluarea acurateţii şi credibilităţii informaţiei-text nu se mai aplică şi altor tipuri de conţinut, mai ales că sursele „scrise" constituie, în prezent, un procentaj minor din masa enormă de informaţii utilizate de analiştii OSINT. Din această perspectivă, a devenit evident faptul că, pentru a depăşi obstacolele, trebuie conştientizat că OSINT nu se limitează la „Internet mining" sau monitorizarea presei, ci solicită de la cei implicaţi abilităţi sociale şi culturale considerabile.

Concluzii

În noul mediu de securitate, schimbul de informaţii interagenţii sau interstatal, precum şi desfăşurarea activităţii într-un sistem colaborativ au devenit extrem de importante în vederea contracarării riscurilor emergente.

Progresele în materie de sisteme media sau comunicare au transformat domeniul intelligence, desfăşurarea activităţii de analiză fiind, practic, imposibilă, în prezent, fără conştientizarea necesităţii alinierii la cele mai noi descoperiri tehnologice.

Bibliografie

1. Ackerman, Robert K., *Intelligence Community Embraces Virtual Collaboration*, publicat pe site-ul Armed Forces Communications and Electronics Association / AFCEA, mai 2009.

2. Andrus, Calvin, *The Wiki and the Blog: Towards a Complex Adaptive Intelligence Community*, iulie 2005.

3. Juhl, Felix, Pallaris, Chris, Schaurer, Florian, *OSINT Report 1/2010 – Technology Trends*, publicat de International Relations and Security Network.

4. Korns, Stephen W., *Cyber Operations. The New Balance*, publicat în revista „Joint Force Quarterly", nr. 54, 2009, elaborată de National Defense University Press.

5. *Cyber In-Security*, publicat de asociaţia „Booz Allen Hamilton", iulie 2009.

6. http://www.sail-technology.com.