Rolul noilor tehnologii în transformarea open-source intelligence

Gabriela TATU

Institutul Național de Cercetare-Dezvoltare în Informatică, ICI București

gabriela.tatu@ici.ro

Rezumat: Noile tehnologii schimbă paradigma informației în societate. Calitatea și utilizarea intelligence depind de calitatea informațiilor, de informații și de factorii de decizie. Noile tehnologii oferă oamenilor puterea de a dobândi și de a crea informații de mai bună calitate și cu un impact major în influențarea evenimentelor. Factorul uman va rămâne cel mai important punct în procesul de intelligence. Criteriile pentru evaluarea OSINT, sunt acuratețea, fiabilitatea, oportunitatea și, în principal, obținerea de avantaje, OSINT fiind printre cele mai mari oportunități de consolidare a leadership-ului.

Cuvinte cheie: intelligence, informații, internet, tehnologii, informații din surse deschise.

The role of new technologies in transforming open-source intelligence

Abstract: The new technologies change the paradigm of information in society. The quality and use of intelligence depend on the quality of information, information and decision-makers. New technologies offer people the power to acquire and create better quality information and with a major impact in influencing events. The human factor will remain the most important point in the intelligence process. The criteria for OSINT assessment are accuracy, reliability, opportunity, and mainly obtaining the benefits, OSINT being among the greatest opportunities for leadership consolidation.

Keywords: intelligence, information, Internet, technologies, open source intelligence.

Introducere

Pe măsură ce tehnologia avansează, nu mai poate fi pus la îndoială faptul că informația înseamnă putere și că folosirea ei, în diferite scopuri, poate face la fel de mult rău ca și utilizarea armelor. Societatea este surprinsă de emergența tehnologiilor informaționale și de comunicare datorită creșterii puternice a spațiului virtual. Tranziția către o societate a cunoașterii susținută de transformările suferite de tehnologiile de comunicare atrage o dezvoltare a social media la nivel mondial. Spațiul virtual se bucură de lipsa frontierelor, dinamism, anonimat și generează atât oportunități de dezvoltare a societății informaționale, cât și riscuri la adresa securității informatice a acesteia.

Odată cu creșterea gradului de automatizare a prelucrării datelor, creșterea nivelului informațiilor și cunoștințelor, transformările nu rămân fără urmări la adresa securității, ci dezvoltă noi amenințări, astfel încât s-a impus dezvoltarea de metode noi de culegere a informațiilor despre persoane și activitățile acestora în cadrul rețelelor de socializare.

Informațiile din spațiul social media sunt disponibile oricui, provin din ziare, internet, reviste de carte, publicații periodice, radio, televiziune, baze de date comerciale și literatură gri, cum ar fi studii de tip think-tank, rapoarte de activitate, cercetări științifice, broșuri corporative etc.

Corecta utilizare a datelor din social media, asamblate și analizate corespunzător, poate oferi agențiilor de informații o mai bună viziune strategică, tactică sau date operaționale pentru a obține o imagine, în timp real și în continuă evoluție, a fenomenului infracțional.

Odată cu apariția Internetului, informațiile partajate au avut un impact extraordinar asupra tuturor aspectelor vieții politice, sociale și economice moderne. De reținut, este că Internetul în sine nu este o sursă propriu-zisă, ci un mijloc de a transporta datele și o locație virtuală.

Datele colectate prin intermediul Internetului au fost privite, inițial, cu scepticism, întrucât metoda preferată de agențiile secrete pentru a dobândi avantaje informaționale era prin utilizarea de metode clandestine. Întrucât, în majoritatea cazurilor, era mai dificil, mai riscant și mai costisitor să se aplice astfel de metode pentru a obține informații secrete, se credea că aceste surse au o valoare mai mare decât sursele deschise, confundându-se ideea de a ști secrete cu ideea de cunoaștere.

Rolul noilor tehnologii în obținerea informațiilor

În prezent, se estimează că informațiile obținute din surse deschise (OSINT) furnizează între 80% și 95% din totalul datelor folosite de comunitatea de informații, la nivel mondial. În acest mod se asigură cunoașterea datelor istorice și culturale strategice, se obțin informații utile din punct de vedere operațional despre infrastructură și evoluții actuale și informații geospațiale comerciale vitale din punct de vedere tactic, care nu pot fi obținute prin alte mijloace.

Pe măsură ce societatea și tehnologia au evoluat, se conștientizează tot mai mult că tehnicile de colectare a informațiilor, deja consacrate, încep să fie depășite și, adesea, destul de scumpe pentru ceea ce oferă. Nevoia actuală determină investiții în tehnologii mai noi, mai eficiente și mai rentabile.

Pentru a fi eficiente, organizațiile de intelligence trebuie să aibă acces la toate tipurile de informații. Odată cu apariția unor tehnologii mai sofisticate, cum ar fi inteligența artificială (AI) și multitudinea de posibilități de a extrage date din surse deschise (pe piață regăsindu-se multe produse la prețuri accesibile sau freeware), devine din ce în ce mai necesar ca organizațiile de intelligence să integreze cele mai noi tehnologii AI și OSINT. Cu ajutorul acestora, se pot desfășura investigații mai eficiente și se poate obține un mai bun control al nivelului criminalității.

Inteligența artificială este definită ca abilitatea unui computer de a învăța și de a aplica ceea ce a învățat anumitor sarcini. Astfel, companii și diferite organizații din întreaga lume experimentează metode asistate de inteligența artificială pentru prevenirea și reducerea atacurilor cibernetice și pentru a încerca să le soluționeze într-un timp cât mai scurt. Deși acest tip de tehnologie are costuri ridicate, reducerea timpului petrecut de o persoană să ajungă la același rezultat este semnificativă. În plus, dacă amenințările pot fi identificate înainte să producă efecte, dacă numărul victimelor poate fi redus și dacă sunt identificate și destructurate rețele criminale, costurile ulterioare asociate activităților investigative vor fi diminuate.

OSINT poate ajuta la verificarea și clasificarea fenomenelor sociale, identificarea infractorilor și a tendințelor criminalității emergente și înțelegerea diferitelor ideologii. În ultimii ani, utilitatea OSINT a început să fie din ce în ce mai recunoscută, prin această metodă reușind să se obțină o imensă cantitate de date ce sunt utilizate de organizațiile de intelligence pentru a identifica riscuri și pentru a lua decizii strategice eficiente și la timp.

Poate că cel mai mare avantaj este costul mai redus decât al instrumentelor tradiționale de colectare a informațiilor. Resursele disponibile trebuie gestionate cât mai eficient și este necesar să se implementeze tehnologii care sunt nu numai eficiente, ci și mai puțin costisitoare. Un alt beneficiu al utilizării OSINT este că informațiile pot fi ușor diseminate către alte agenții sau parteneri. De asemenea, persoanele și grupurile extremiste doresc, de multe ori, să împărtășească scopurile și convingerile lor, astfel încât tind să posteze frecvent în mediul on-line pentru a răspândi mesajul. Mai mult, Internetul oferă infractorilor un mediu în care se bucură de anonimat

iar platformele sociale au devenit un nod central de îndoctrinare și de radicalizare teroristă, astfel, pentru a putea crește gradul de securitate națională agențiile de intelligence trebuie să profite de această sursă incredibilă de informații.

Cele mai bune surse includ publicații periodice, ziare, emisiuni de televiziune și radio, baze de date publice, registre, forumuri, rapoarte guvernamentale, buletine de știri, bloguri, platforme social media, anunțuri comerciale, motoare de căutare, feeduri RSS și site-uri web.

Avantaje și dezavantaje ale utilizării informațiilor din surse deschise

Creșterea rapidă a Internetului a făcut din OSINT o sursă majoră de cunoștințe iar o preocupare deosebită este conștientizarea faptului că această cantitate nu înseamnă neapărat calitate, astfel încât orice informație provenită din surse deschise ar trebui analizată, verificată și coroborată astfel încât să ofere credibilitate și veridicitate.

În acest sens, un dezavantaj este reprezentat de riscul de supraîncărcare a informațiilor din cauza cantității mari de „zgomot" de pe Internet. Astfel, identificarea informației corecte poate deveni destul de consumatoare de timp. În plus, OSINT nu este, în general, gata de utilizat însă, analiza datelor brute este necesară pentru a identifica informații credibile, valide și verificabile. Chiar dacă informațiile inițiale ar putea să nu fie cele mai bune, acestea pot oferi un punct de plecare pentru investigații suplimentare. Un factor important ce creează o vulnerabilitate a OSINT-ului este resursa umană (analistul) folosită pentru a da curs solicitărilor.

Există posibilitate ca aceasta să nu dispună de expertiza necesară pentru a identifica datele adecvate întrucât domeniul pe care îl documentează îi este necunoscut și, de asemenea, părerile și prejudecățile fiecăruia contribuie la reducerea potențialului acestor informații. Alte dezavantaje sunt reprezentate de lipsa unor instrumente analitice eficiente și de faptul că mai multe publicații media raportează aceeași știre, atribuindu-i astfel o credibilitate mai mare decât cea reală.

Amenințările cibernetice sunt din ce în ce mai sofisticate și activitățile cibernetice complexe fapt ce a impus utilizarea OSINT. Mai mult, informațiile extrase permit companiilor să creeze analize complexe pe baza cărora poate fi prezis comportamentul consumatorilor, ajutând la dezvoltarea de bunuri și servicii, informațiile din surse deschise fiind considerate vitale în crearea de strategii de afaceri de succes.

Noile tehnologii de intelligence creează atât oportunități cât și amenințări. Schimbă paradigma informației în societate deoarece oferă oamenilor puterea de a dobândi, de a crea mai multe și mai bune informații având, în acest mod, posibilitatea de a influența evenimente.

Noile tehnologii reprezintă o combinație extinsă de instrumente care schimbă natura societății și mediul de informare cum ar fi gadget-uri, laptop-uri, telefoane mobile, motoare de căutare, software, platforme de comunicații și comunicații, rețele de transmisie de date de mare viteză, sateliți, mass-media socială, mass-media tradițională (TV / radio), plus inovațiile lor dar, cu toate acestea sursele deschise înseamnă mai mult decât Internetul.

Spațiul virtual se extinde continuu și preia părți, din ce în ce mai mari, ale activităților oamenilor și necesită tehnologie, competențe și atitudine potrivită. O teorie pentru securitatea națională poate fi susținută de paradigma faptului că societatea va fi mai sigură atunci când, teoretic și practic, atacurile constante din spațiul cibernetic vor fi abordate și privite ca un război, dincolo de criminalitatea informatică.

Creșterea dependenței de spațiul cibernetic, disponibilitatea noilor tehnologii și informații, trăsăturile cibernetice și atacurile asupra tuturor aspectelor societății creează vulnerabilitate și necesită apărare.

Noile tehnologii sunt democratice, oferă un acces egal la utilizarea sau crearea de surse deschise (cenzurate sau restricționate de regimuri antidemocratice), indiferent de statutul personal sau de ierarhia lor. Ele exprimă și sprijină piața liberă, ajută aplicarea legii în lupta împotriva criminalității și a spionajului. Impactul pasiv și activ afectează puterea de stat.

Sortarea informațiilor valoroase din masa neorganizată și inutilă, identificarea informațiilor corecte, procesarea și utilizarea acestora îmbunătățesc calitatea, precizia, fiabilitatea, eficiența și valoarea adăugată a procesului de informații, atât pe partea de colectare, cât și pe partea de producție.

Impactul noilor tehnologii în colectarea de informații din surse publice este semnificativ și înglobează redefinirea și creșterea mobilității, disponibilitatea și modalitățile de accesare, colectare, procesare, stocare și utilizare a surselor și dezvoltarea de noi interpretări. Reducerea, eliminarea, pătrunderea sau modificarea barierelor, limitărilor și constrângerilor în accesul la cunoștințe, informație, educație, spectru de surse, procese de informații, cooperare, muncă, împărtășire și influențare a evoluțiilor sunt beneficii de informație, sunt disponibile oriunde, în timp real, tot timpul și în moduri noi, indiferent de geografie, tehnologie, statut formal, ierarhie sau reguli.

Creșterea verificabilității informațiilor oferă o imagine mai completă, ajutând la monitorizarea și dobândirea unui spectru de date (date, analize, opinii) pentru o gândire mai largă și pentru alternative și interpretări crosschecking (locale, regionale etc.). Identifică și ajută la analizarea (în contextul tuturor surselor) percepțiilor publice ale evenimentelor și tendințelor, a relațiilor dintre actori (organizații, grupuri, țări) și a modelor în comportament, inclusiv a discrepanțelor (imaginea publică prezentată vs. intențiile ascunse, deoarece oricare dintre ele poate suferi modificări).

Puterea noilor tehnologii creează oportunități și amenințări, interconectate, cu potențial de schimbare rapidă. Tehnologiile noi ajută la localizarea, procesarea și difuzarea unor cantități mari de date și pregătirea acestora pentru analiști, dar rolul central în analiză va continua să îl aibă mintea analistului, un obiect și un subiect pentru noile tehnologii.

Noile tehnologii schimbă modurile în care oamenii gândesc, lucrează, trăiesc, comunică, se comportă, obțin, procesează și utilizează informații. Creșterea numărului de vieți ale generațiilor noi petrecute pe noile tehnologii va avea un impact asupra procesului de intelligence și asupra muncii și gândirii analistului, deși structura competențelor de bază nu se va schimba. Cu toate slăbiciunile, creierul uman, este fără egal și de neînlocuit ca elementul central de a dezvolta aspectele tehnice și creative decisive (sortarea, analiza și compararea dovezilor, generarea unor ipoteze, judecăți alternative, detectarea și minimizarea surselor de vulnerabilitate față de rețele, instituții, întreprinderi, societate) sau pentru a face față provocărilor noilor tehnologii.

Tehnologiile noi pot îmbunătăți calitatea, eficiența și rezultatele pregătirii profesionale a analistului prin educație și gadgeturi și aplicații, cu programe complete sau parțiale, inclusiv despre spațiul cibernetic, tehnologii și analize. Lumea viitoare competitivă necesită o cantitate și o calitate mai bună a know-how-ului (toată lumea știe mai mult, spre deosebire de trecut când doar câțiva oameni aveau acces la cele mai bune cărți și alte surse) și o mentalitate, curioasă și inventivă.

Amenințările generate de noile tehnologii pot afecta societatea sau securitatea prin implicațiile și abuzurile lor ca arme sau medii pentru alte amenințări. Utilizatorii pot fi "supuși puterii coercitive a tehnologiei", în timp ce dezvoltatorii de tehnologie încearcă "să înțeleagă nevoile utilizatorilor și să evalueze puterea transformatoare a tehnologiei".

Implicațiile în securitate ale noilor tehnologii sunt importante deoarece noile tehnologii creează o nouă dimensiune a amenințărilor tradiționale prin eficiența sporită a armelor inamice, noi tipuri de amenințări prin construirea spațiului cibernetic, care să împuternicească actorii ostili colectivi și individuali și să mărească individualizarea amenințărilor prin actorii necinstiți din tehnologie. Actorii instigatori pot abuza noile tehnologii - direct sau ca mediu - pentru a atrage libertatea, puterea și prosperitatea, pentru a încuraja, săvârși sau provoca diferite controverse

politice, pentru a dezvolta noi tipuri de amenințări prin lansarea atacurilor cibernetice, pentru a fura secrete de stat, pentru a spori activitățile criminale și spionajul și pentru răspândirea greșită a informațiilor, dezinformare și propagandă (este diferită de masa informațiilor înșelătoare aleatoare de calitate inferioară, nonwarfare).

Concluzii

Noile tehnologii au creat o nouă lume, au schimbat societatea, comunicarea și munca. Nivelul lor, rapid și greu de anticipat, impactul avut odată cu extinderea cantității și a calității informațiilor și tehnologiilor disponibile la nivel global, capacitatea de a influența evenimentele și dependența de spațiul cibernetic creează oportunități și amenințări pentru societate și pentru comunitatea de intelligence.

Impactul noilor tehnologii asupra OSINT nu rezolvă toate nevoile de informații și nu trebuie să aducă atingere serviciilor secrete sau organizațiilor de intelligence, dar crește rolul OSINT și necesită o analiză continuă. Noile tehnologii au un impact complex, fiind cea mai mare schimbare de paradigmă a informațiilor de la tipărire. Oportunitățile și amenințările în domeniul cibernetic nu sunt doar pentru profesioniștii din domeniul informațiilor, ci și pentru publicul larg.

Punctul central al intelligence va rămâne mintea umană. Complexitatea impactului noilor tehnologii necesită implicarea celor mai bune talente și construirea unui know-how instituțional și individual la care centralizarea este complexă, interdisciplinară, înaltă, în creștere și continuă. „Analiza este cel mai important aspect al intelligence". Abordarea corectă, educația și resursele umane și materiale vor fi din ce în ce mai necesare pentru a studia și conduce acești factori pentru a proteja libertatea, prosperitatea și securitatea națională.

BIBLIOGRAFIE

1. Bazzell, Michael - *Open Source Intelligence Techniques: Resources for Searching and Analyzing Online Information*, Create Space Independent Publishing Platform, 2016;
2. https://en.wikipedia.org/wiki/Artificial_intelligence - *Artificial intelligence*, 2018;
3. https://archive.org/details/NATOOSINTHandbookV1.2 - *NATO OSINT Handbook*, 2001;
4. Kramer, Franklin D., Starr, Stuart H., and Wentz, Larry K. - *Cyberpower and National Security* - Center for Technology and National Security Policy, 2016;
5. Montagnese, A. - *Impact of Social Media on National Security* - Diss. Military Center of Strategic Studies, 2011;
6. Schaurer, Florian și Störger, Jan - *Evolution of Open Source Intelligence*, The Intelligencer Association of Former Intelligence Officers, vol. 19, nr. 3, 2013, https://www.afio.com/publications/Schauer_Storger_Evo_of_OSINT_WINTERSPRING2013.pdf;
7. Vevera, Adrian Victor - *Privatizarea serviciilor de informații*, Studia Securitatis, 2014;
8. www. Expertsystem. com/osint-applications-3-examples - *3 examples of OSINT applications against criminality*, 2016;
9. www.sri.ro/fisiere/studii/ATUURI_SI_LIMITE_OSINT.pdf - *Atuuri şi limite ale utilizării OSINT în activitatea de intelligence*;
10. www.sri.ro/ upload/Ghid_OSINT.pdf - *Ghid OSINT*, Serviciul Român de Informații – Centrul Surse Deschise, 2018.

Gabriela TATU lucrează în prezent la Institutul Național de Cercetare-Dezvoltare în Informatică - ICI București în calitate de Expert în Fondurile Structurale și de Coeziune Europene din cadrul Departamentului Cybersecurity și Infrastructuri Critice. Absolventă a Universității "Spiru Haret", cu diploma de licență în psihologie, principalele interese de cercetare ale doamnei Tatu sunt: securitatea informatică, detectarea comportamentului simulat, protecția infrastructurii critice, proiectele de cercetare finanțate de UE și studiile de intelligence.

Gabriela TATU is currently working at the National Institute for Research and Development in Informatics - ICI Bucharest as an Expert in European Structural and Cohesion Funds within the Department of Cybersecurity and Critical Infrastructures. A graduate of "Spiru Haret" University with a BSc in Psychology, Mrs. Tatu's main research interests are: cybersecurity, simulated behaviour detection, critical infrastructure protection, European funded research projects and intelligence studies.