
SOCIAL MEDIA INTELLIGENCE-A RADIOGRAPHY OF THE NEWEST INT**Raluca Luțai, PhD Student, “Babeș-Bolyai” University of Cluj-Napoca**

Abstract: In a world of complex interdependence, dominated by technological advances and information the one who holds the information still has the power. The internet, an important globalization vector,

has conquered the world and has secured his role as the main information generator in nearly all areas, producing true metamorphosis in everyday life.

In this context, the intelligence community is widening the spectrum of methods and spaces that can be used to collect and analyze intelligence. One of these methods that produce large mutations in the system is linked to the world of social media, a large source of information with many implications. Social media gives us the ability to develop an avatar through which we can express our arguments, visions but also the main important events in our lives. This leads to the development of new forms of communication with major implications in many areas, and one of these areas is concerning the intelligence community.

Based on these issues, this paper proposes a general characterization of the most important aspects of Social Media Intelligence a brand new way for the intelligence community to collect and analyze information for national security purposes (but not only). This paper will try to define the concept, to look inside its history, to see a classification and also the role of SOCMINT in the intelligence community.

Keywords: *internet, social media, intelligence communities, SOCMINT*

Serviciile de informații în noul mileniu-o introducere

Sfârșitul Războiului Rece a provocat mutații profunde atât la nivelul sistemului internațional cât și la nivelul comunităților de informații. Sistemul multiploar, aharnic și interdependent care s-a format după dispariția Cortinei de Fier a fost și este mânat de un proces de globalizare intens care afectează fiecare sector al vieții individului și a statului. Comunitățile de intelligence s-au aflat în fața unor provocări ce priveau actualizarea la noile cerințe atât în ceea ce privește identificarea și colectarea datelor și informațiilor cât și în ceea ce privește analiza, gestionarea și transformarea lor în intelligence strategic, operațional sau tactic.

Progresele tehnologice și informaționale au devenit o constantă și au modificat structura și activitatea serviciilor de informații din întreaga lume. Dezvoltarea internetului a făcut ca acesta să fie integrat în fiecare etapă a ciclului de intelligence. Internetul oferă comunităților de informații noi instrumente și noi metode de lucru dar în același timp impune și o serie de noi riscuri. Tot datorită progreselor tehnologice și informaționale, spectrul INT-urilor se lărgeste și noi metode de colectare a intelligence-ului apar. Rolul surselor deschise se intensifică în aceste condiții, în timp ce Social Media Intelligence se dovedește a fi din ce în ce mai util pentru comunitățile de intelligence.

Noul mileniu se deschide cu noi provocări pentru comunitățile de informații din întreaga lume. Lumea postmodernă este o lume a exploziei informațiilor în care colapsul granițelor este din ce în ce mai evident, o lume în care accentul se pune pe individ și nu pe stat. Postmodernismul crează o lume a riscului, incertă, ambiguă și interdependentă.

Pornind de la aceste schimbări, în paginile următoare ne vom îndrepta atenția asupra înțelegerii rolului pe care Social Media Intelligence îl are în cadrul comunităților de informații din întreaga lume, analizând provocările și avantajele pe care le impune.

Social Media Intelligence: conceptualizare. istoric. clasificare

SOCMINT este un concept inedit, complex, interdisciplinar și destul de recent pentru a se bucura la ora actuală de o definiție clară și general acceptată de toți specialiștii din domeniu.

Cel care a folosit pentru prima dată termenul de Social Media Intelligence abreviat SOCMINT și cel care este considerat părintele fondator al acestui concept este Sir David Omand, funcționar de rang înalt al comunității de intelligence din Marea Britanie. În lucrarea *"Introducing Social Media Intelligence"* apărută în jurnalul *Intelligence and National Security* în anul 2012, Omand alături de alți autori tratează în detaliu problematica acestui concept pe care îl definește ca fiind un ansamblu de aplicații, tehnici și capacități disponibile prin intermediul colectării și utilizării datelor obținute din social media¹.

Social Media Intelligence (SOCMINT) reprezintă astfel procesul prin care se identifică, validează, colectează și analizează datele și informațiile din social media, folosind atât metode intruzive cât și metode ne-intruzive, cu scopul elaborării de produse ce corespund cerințelor de intelligence și care au o oarecare relevanță pentru securitatea națională². La fel ca orice altă formă de intelligence, scopul SOCMINT este acela de a reduce "necunoscutul" din ecuația procesului decizional, oricare ar fi natura acestui proces.

Discuțiile legate de folosirea datelor și informațiilor din social media în direcția prezervării securității naționale au apărut în cadrul comunității de informații din Marea Britanie în contextul revoltelor ce au avut loc pe străzile Londrei în anul 2011³. Violențele înregistrate de forțele de ordine londoneze au dus la înțelegerea incapacității serviciilor de informații și a forțelor de ordine de a culege, corobora și disemina informațiile pe care rețelele sociale le pun la dispoziție. Imediat după acestea, observând și efectul pe care social media îl are în cadrul revoluțiilor și revoltelor din zona Africii de Nord și a Orientului Mijlociu, serviciile de informații și-au îndreptat mai mult atenția asupra oportunităților pe care mediul social media le aduce comunităților de informații.

Teoreticianul conceptului de Social Media Intelligence (SOCMINT) este David Omand un oficial de rang înalt în comunitatea de informații britanică, care împreună cu colegii săi din think-tank-ul DEMOS (Carl Miller, Jamie Bartlet) au adus în discuție în fața lumii academice dar și a oficialilor direct interesați de acest aspect, câteva din cele mai importante elemente ale SOCMINT. Pe lângă eforturile de teoretizare ale oficialilor englezi se mai pot identifica și eforturile altor teoreticieni care au încercat să sublinieze oportunitățile pe care social media le poate aduce comunităților de informații.

¹ David Omand, Jamie Bartlet, Carl Miller, "Introducing Social Media Intelligence (SOCMINT)" în *Intelligence and National Security*, vol.27. no.6, decembrie 2012.p.3.

²Richard Norton-Taylor, "Former spy chief calls for laws on online snooping", disponibil la <http://www.theguardian.com/technology/2012/apr/24/former-spy-chief-laws-snooping>, accesat în 30.05.2014.

³ Florian Schaurer, *Social Media Intelligence (SOCMINT). Same song, different melody?* Disponibil la <http://osintblog.org/?p=1462> accesat în 27 mai 2014.

Din punct de vedere al clasificării, literatura de specialitate consemnează două mari forme de Social Media Intelligence: a. *Open SOCMINT* sau SOCMINT-ul obținut prin mijloace și metode non intruzive și b. *Surveillance SOCMINT*⁴ SOCMINT-ul obținut prin mijloace și metode intruzive care sunt reglementate de un cadru legal.

Prima categorie de SOCMINT, cea care este rezultatul unui proces non intruziv, deschis, poate fi utilizată nu numai de comunitățile de informații ci și de companii comerciale, universități sau alți actori non-statali.

Cea de-a doua categorie este apanajul exclusiv al instituției statului care prin intermediul agențiilor și serviciilor de informații pe care acesta le deține acționează în funcție de un cadru legal reglementat. Comunitățile de informații au capacitatea de a identifica indivizi și de a avea acces la informații. Surveillance SOCMINT poate merge de la analiza datelor publice ale individului până la interceptarea sau citirea corespondenței acestuia⁵.

Rolul SOCMINT în cadrul comunităților de informații

Când societatea devoltă noi forme de comunicare, cum este social media, instituțiile publice inclusiv serviciile de informații trebuie să fie suficient de responsabile pentru a reacționa și pentru a se adapta noilor trenduri. Acest lucru se aplică și în cazul Social Media Intelligence, cel mai nou membru al familiei INT-urilor.

Ultimii ani ai acestui deceniu au demonstrat faptul că tot mai mulți indivizi își transferă interacțiunile, identitățile, argumentele și viziunile în mediul online, transformându-l într-o sursă valoroasă de intelligence pentru serviciile de informații. Rețelele de socializare ca Facebook și Twitter transformă mediul online într-un imens spațiu public în care fiecare dintre noi contribuie cu informații, în care fiecare dintre noi ne expunem într-un fel sau altul. Social Media transformă societățile prin extinderea spațiului virtual iar acest lucru afectează modul în care se gestionează cantitatea de informații. În aceste condiții spațiul online devine un spațiu de interes pentru comunitățile de informații iar acest lucru atrage după sine o serie de metamorfoze care trebuiesc să se realizeze la nivelul modului în care colectează și analizează informațiile dar și modul în care utilizează aceste informații.

Din moment ce fiecare fațetă a vieții cotidiene este prezentă în mediul online, prin caracteristicile pe care le are dar mai ales prin oportunitățile pe care le are în față, Social Media Intelligence contribuie în mod pozitiv la activitatea pe care serviciile de intelligence o desfășoară.

Contribuția SOCMINT poate fi identificată atât la nivel operațional și tactic cât și la nivel strategic. Analiza și monitorizarea datelor și informațiilor din social media poate duce la înțelegerea mai multor fenomene. Prin cantitatea mare de informații la care are acces, analistul care utilizează social media intelligence reușește să ”ia temperatura” comunităților, să analizeze nemulțumirile și starea generală a acestora. În acest sens, prin înțelegerea conținutului disponibil în social media, analiștii care ascultă ”vocea mulțimii”⁶ sunt capabili să furnizeze decidenților informații ce contribuie la înțelegerea nevoilor publicului pe care îl

⁴*Ibidem*.p.14.

⁵ *Ibidem*.

⁶Omand David, Bartlet Jamie ,” A balance between security and privacy online must be struck..” în DEMOS,2012.p.17

serve⁷. Cel mai concludent exemplu în acest sens este dat revoltele din Primăvara Arabă. Doar în cazul revoluției din Egipt din anul 2011, specialiștii au aproximat că s-au format 32.000 de grupuri și mai mult de 14.000 de pagini pe Facebook⁸. La acest lucru se mai cuvine să precizăm și caracterul mobilizator al acestor rețele care pentru prima dată au arătat scenei internaționale puterea care acestea o au în anul 2011.

Prin intermediul formelor de comunicare social media, serviciile de informații pot asigura o mai bună comunicare între cetățeni și guvern atât în timpul unor crize cât și în perioade de normalitate. Prin intermediul acestei comunicări serviciile de informații vor fi capabile să transmită informații relevante în legătură cu anumite chestiuni ce sunt importante. În momentele de criză, social media poate contribui la dezvoltarea unor reziliențe care să fie resimțită la nivelul modului în care se gestionează evenimentele. Prin activitatea lor în mediul online și mai exact în social media, serviciile de informații pot contribui la destructurarea unor zvonuri greșite sau teorii conspiraționiste, pot împiedica manipulările evidente și pot stabili o relație mult mai transparentă cu societatea civilă, relație care va duce la creșterea gradului de încredere pe care aceasta le-o conferă.

În contextul în care social media este o sursă de real time intelligence, prin intermediul SOCMINT, serviciile de informații au capacitatea de a obține informații referitoare la evenimentele în curs de desfășurare. În condițiile în care oricine poate deveni azi jurnalist cu ajutorul unui smartphone, pentru serviciile de informații va fi mult mai ușor să radiografieze situația și să ia măsurile cele mai optime⁹. Răspunsul serviciilor va fi mult mai rapid și mai eficient.

SOCMINT poate genera intelligence care să identifice activitățile ce se înscriu în registre criminale și poate oferi informații prețioase despre indivizi și grupuri care pot fi folosite atât de serviciile de informații cât și de forțele de ordine și siguranță publică sau de cele judiciare. Prin triangularea unor informații obținute din social media, SOCMINT poate acționa în direcția prevenirii și combaterii actelor criminale ce se pot desfășura sau care pot fi facilitate de mediul online (pornografie infantilă, extorcherii, cyberbully), poate duce la deșeurarea și deșeurarea grupărilor criminale, identifică complici și moduri de operare, sau contribuie la construcția unor capete de acuzare sau apărare mult mai solide în anumite anchete judiciare.

Exploatarea social media poate oferi serviciilor de informații un bun ”insight” în cazul unor grupări. SOCMINT contribuie, fără doar și poate, la înțelegerea mai atentă a activităților și comportamentelor unor grupări care reprezintă un interes pentru comunitatea de informații. Grupările teroriste care sunt din ce în ce mai prezente în mediul online sunt un exemplu în această direcție. Prin analiza grupurilor de acest fel se pot identifica tendințele viitoare sau se poate determina nivelul de nervozitate a grupului în legătură cu anumite chestiuni¹⁰.

Urmând aceeași ordine de idei, SOCMINT are o funcție de cercetare și înțelegere a fenomenelor, comportamentelor și tendințelor care pot atenta într-un fel sau altul la siguranța națională. Prin intermediul monitorizării și analizei datelor coroborate din mai multe surse,

⁷ *Ibidem*, p.18.

⁸ Carl Miller, Jamie Bartlett, ”The state of the art: a literature review of social media intelligence capabilities for counter-terrorism” în *DEMOS*, noiembrie 2013, p.27.

⁹ David Omand, Jamie Bartlett, *op.cit*, p.26.

¹⁰ *Ibidem*, p.27.

serviciile de informații pot identifica procesele de radicalizare sau pot analiza modul în care ideile circulă și se schimbă. Ținând cont de acest aspect și de cel prezentat mai sus legat de înțelegerea unor grupări, putem concluziona că SOCMINT are o valoare importantă în sistemul de avertizare timpurie (early warning). SOCMINT poate fi dovedit foarte valoros în acțiunile de prevenire dar și în cele de combatere.

Concluzionând cele discutate mai sus putem afirma că SOCMINT își dovedește utilitatea în activitatea comunităților de intelligence deoarece:

- ✓ ”Ia pulsul” comunităților și ascultă ”înțelepciunea mulțimii”
- ✓ Este un indicator al modului în care indivizii și grupurile interacționează
- ✓ Identifică și poate contribui la combaterea activităților criminale
- ✓ Poate asigura o mai bună gestionare a situațiilor de criză
- ✓ Poate crea reziliență în cazul mai mult fenomene sau aspecte ce pot contribui la perturbarea siguranței și securității
- ✓ Poate oferi informații despre anumite grupări
- ✓ Poate anticipa și monitoriza procesele de radicalizare sau comportamentele violente
- ✓ Poate contribui la înțelegerea unor fenomene și la predicția trendurilor viitoare

Explozia social media a dus la transferarea mai multor elemente din viața cotidiană în mediul online, în social media. Aproape fiecare aspect al vieții noastre devine măsurabil și înregistrabil¹¹. În aceste condiții, considerăm că social media poate reprezenta o adevărată oportunitate pentru serviciile de informații contribuind la reducerea incertitudinii. SOCMINT poate reprezenta o contribuție eficientă la siguranța și securitatea națională. Din acest considerent toate serviciile de intelligence trebuie să își orienteze activitatea în direcția utilizării celui mai nou membru al familiei de INT-uri.

Concluzii

SOCMINT reprezintă deci unul dintre cele mai noi oportunități și totodată provocări pe care comunitățile de informații trebuie să le gestioneze în contextul expresiei tot mai intense a individului în mediul online.

Teoretizat de Sir David Omand imediat după revolte din Londra anului 2011, SOCMINT sau Social Media Intelligence reprezintă un proces prin care prin intermediul identificării, colectării analizei și coroborării datelor și informațiilor din social media se ajunge la crearea unor produse cu relevanță pentru securitatea națională. În funcție de modul în care se colectează datele și informațiile, există două mari categorii de SOCMINT cel deschis și cel intruziv. Cel deschis operează prin mijloace și metode non intruzive iar surveillance SOCMINT este bazat pe o serie de mijloace și metode intruzive care sunt reglementate, sau ar trebui să fie reglementate de un cadru legal.

SOCMINT reprezintă un plus pentru comunitățile de informații atât la nivel tactic cât și la nivel operativ sau chiar strategic¹². Funcționând pe baza principiului legalității și

¹¹ David Omand, Jamie Bartlet, Carl Miller, *op.cit.*,p.31.

¹² Jeremiah Burgess, *The who, what and how of social media exploitation for a combatant commander*, Naval War College, 2013.,p.7.

proporționalității, comunitățile de informații care utilizează SOCMINT vor fi capabile să monitorizeze comunitățile din proximitate și vor putea să influențeze decidenții politici și beneficiarii procesului de intelligence cu privire la alegerea celor mai optime decizii. Prin intermediul SOCMINT se pot determina modele comportamentale pentru anumite grupuri sau pentru anumiți indivizi sau se pot cunoaște mai în detaliu anumite grupări. În momentele de criză, SOCMINT reprezintă o sursă de informații actuale și un element important în gestionarea acestora. Tot în această direcție, SOCMINT poate fi folosit de serviciile de informații pentru a crea reziliență în cazul mai mult fenomene sau aspecte ce pot contribui la perturbarea siguranței și securității, poate anticipa și monitoriza procesele de radicalizare sau comportamentele violente, contribuind la înțelegerea unor fenomene și la predicția trendurilor viitoare.

Comunitățile de informații trebuie să se adapteze modului în care indivizii crează și distribuie informații, iar în acest context, social media oferă oportunitatea și provocarea de a fi cu un pas în fața problemei. Comunitățile de informații trebuie să înțeleagă beneficiile pe care acest INT le oferă și să învețe să îl utilizeze la adevărata lui valoare. Viitorul SOCMINT este asigurat de individul care își cantonează tot mai multe elemente din viața în mediul online. Jamie Bartlett susține această ultimă idee, apreciând că în 10-15 ani fiecare departament al guvernului va avea propriul centru de analiză social media¹³.

BIBLIOGRAFIE:

Burgess Jeremiah, *The who, what and how of social media exploitation for a combatant commander*, Naval War College, 2013.

Miller Carl, Bartlett Jamie, "The state of the art: a literature review of social media intelligence capabilities for counter-terrorism" în *DEMOS*, noiembrie 2013.

Omand David, Bartlett Jamie, "A balance between security and privacy online must be struck.." în *DEMOS*, 2012.

Omand David, Bartlett Jamie, Miller Carl, "Introducing Social Media Intelligence (SOCMINT)" în *Intelligence and National Security*, vol.27. no.6, decembrie 2012.

Omand David, *The future of intelligence*, disponibil la <http://www.afcea.org/mission/intel/SirDavidOmand.pdf>.

Richard Norton-Taylor, "Former spy chief calls for laws on online snooping", disponibil la <http://www.theguardian.com/technology/2012/apr/24/former-spy-chief-laws-snooping>, accesat în 30.05.2014.

Schauer Florian, *Social Media Intelligence (SOCMINT). Same song, different melody?* Disponibil la <http://osintblog.org/?p=1462> accesat în 27 mai 2014.

¹³ Janson Leavey, *Social media and public policy. What is the evidence?*, Septembrie 2013, p.5.