EMERGENŢA FENOMENULUI SOCIAL MEDIA INTELLIGENCE

Rareş-Adrian RAICU*

Motto:
„There are three kinds of intelligence: one kind understands things for itself, the other appreciates what others can understand, the third understands neither for itself nor through others. This first kind is excellent, the second good, and the third kind useless."
(Niccolo Machiavelli)

Abstract

In a world of constant change and with an environment of transnational security which varies depending on the fluctuations of international reality, intelligence undergoes a series of mutations focused on new typology of vulnerabilities, risks and threats to national, regional and international security. At the beginning of the millennium, the stages of globalization leave a prominent mark on society, as well asaccelerated developments of information technology and science, all these meant to facilitate the transition from the industrial age to the informational era and then to the knowledge society. In this context, asymmetric threats have diversified, both in number and intensity. Developments in technology and the shift from industrial society to information society facilitated dissemination means of these threats, intelligence being forced to adjust to the new requirements of the security environment and to develop new ways and methods to counter modern threats and risks.

Keywords: social media intelligence, modern threats and risks, informational era, knowledge society.

Introducere

Într-o lume aflată într-o continuă schimbare şi cu un mediu transnaţional de securitate ce variază în funcţie de fluctuaţiile realităţii internaţionale, activitatea de intelligence suferă o serie de mutaţii concentrate pe noua tipologie a vulnerabilităţilor, riscurilor şi ameninţărilor la adresa securităţii naţionale, regionale şi internaţionale. La început de mileniu, asupra societăţii, îşi lasă o amprentă proeminentă etapele globalizării, precum şi evoluţiile accelerate ale tehnologiei informaţionale şi ştiinţei, toate acestea

* Academia Naţională de Informaţii „Mihai Viteazul".

facilitând tranziţia de la era industrială la era informaţională şi mai apoi la societatea cunoaşterii.

«Expansiunea lumii virtuale a condus la emergenţa unei noi dimensiuni a puterii statale, „puterea digitală", cu efecte pe termen lung asupra cunoaşterii strategice şi acţiunilor statului în plan naţional şi internaţional. De asemenea, individul a dobândit noi instrumente de acţiune, prin intermediul accesului la baze de date şi reţelele informatice, instrumente prin care poate influenţa în mod direct exercitarea puterii în plan intern sau internaţional. Recurenţa revoluţiilor „Facebook" sau „Twitter" din Europa până în Orientul Mijlociu demonstrează impactul acestor instrumente virtuale asupra regimurilor politice, impact de neimaginat acum mai puţin de un deceniu. Formele de evoluţie a „puterii digitale" vor reprezenta, în egală măsură, oportunităţi de dezvoltare, dar şi vulnerabilităţi şi provocări la adresa securităţii, iar gestionarea acestora va fi determinată de capacitatea de accesare, decelare şi utilizare a informaţiei» (Maior, 2011, p.2).

În acest context, ameninţările asimetrice s-au diversificat, atât ca număr, cât şi ca intensitate. Evoluţia tehnologiei şi trecerea de la societatea industrială la societatea informaţională au facilitat mijloacele de propagare a acestor ameninţări, serviciile de informaţii fiind nevoite să se racordeze la noile cerinţe ale mediului de securitate şi să dezvolte noi mijloace şi metode de contracarare a ameninţărilor şi riscurilor moderne.

Aparte, întrepătrunderea şi coexistenţa unor elemente aparţinând erei informaţionale alături de componentele şi stratul şi substratul noii societăţi a cunoaşterii, creează contextul actual în care se regăseşte lumea în secolul XXI.

Astfel, se poate vorbi despre o necesitate permanentă de adaptare a activităţii specifice de intelligence la noile tipologii ale provocărilor, riscurilor şi ameninţărilor emergente ale societăţii cunoaşterii şi a celor conexe erei informaţionale, acestea fiind caracterizate de dinamism şi impredictibilitate. Astăzi, tehnologiile informaţionale se dezvoltă într-un ritm alert, fiind diseminate şi mai rapid, adesea nefiind utilizate în scopuri favorabile creării unui climat de securitate, indiferent de natura lui: naţional, regional sau internaţional. Expansiunea ameninţărilor asimetrice, amintită mai sus, materializată sub forma grupărilor teroriste sau extremiste sau, mai nou, sub forma modernului *cyberthreat*, foloseşte toate avantajele pe care societatea informaţională le poate oferi. Astfel, dacă până acum se vorbea, spre exemplu de un terorism convenţional propagat rapid de fenomenul globalizării, care a oscilat între defensivitate şi ofensivitate, între formă de apărare şi mijloc de atac, materializându-se prin exploatarea breşelor de securitate existente la nivel statal şi internaţional, dar mai ales în spaţiul fizic, astăzi se poate vorbi despre un terorism adaptat la noile provocări ale erei informaţionale şi mai

ales la cele ale societăţii cunoaşterii şi care exploatează oportunităţile virtuale întru totul.

Aşadar, activitatea de intelligence trebuie reconceptualizată şi orientată către o culegere de date şi informaţii din toate sursele avute la dispoziţie, fie ele clandestine sau publice. Deschiderea serviciilor de intelligence şi a celor de securitate către sectorul civil, precum şi creşterea exponenţială a utilităţii spectrului OSINT, fără a neglija sau a plasa în umbră elementul HUMINT (Lesidrenskaşi Bancheva, 2014, p. 151), precum şi celelalte *INT*-uri, fie că este vorba de MASINT, SIGINT, IMINT sau chiar mijloacele şi metodele specifice activităţii de intelligence pot garanta succesul serviciilor de intelligence în prevenirea şi contracararea riscurilor şi ameninţărilor societăţii cunoaşterii.

Aşa cum a fost amintit anterior, emergenţa tehnologiilor informaţionale şi de comunicare a atras cu sine, aparte de oportunităţi, şi o serie de vulnerabilităţi a căror exploatare ar putea aduce atingeri grave climatului de securitate internaţională. Evoluţia rapidă a ceea ce înseamnă fenomenul *social media* şi tendinţa actuală a societăţii de interacţiona şi comunica, datorită facilităţilor *on-line*, mult mai mult în cadrul acestui spaţiu fără frontiere, a făcut ca anumite grupuri şi grupări să acţioneze, dincolo de realitatea tangibilă, şi în sfera virtuală. Astfel, prin prisma misiunilor asumate, de a preveni şi combate riscurile şi ameninţările, pe de-o parte, iar pe de altă parte de a promova şi conserva valorilor naţionale, a fost de datoria serviciilor de intelligence să-şi orienteze activitatea şi către acest spaţiu, căruia nu îi fusese acordată o atenţie deosebită până în anul 2011, moment pe care îl considerăm o bornă de început în înţelegerea efectelor lumii virtuale asupra realităţii.

Punctul de plecare al necesităţii abordării fenomenului *social media* – dintr-o altă perspectivă îl constituie de fapt vara anului 2011, mai exact pe 6 august, atunci când în Londra se declanşează o serie de violenţe de stradă, cu un puternic impact social. Nemulţumirile în rândul populaţiei încep odată cu împuşcarea lui Mark Duggan, rezident de culoare din Tottenham, în nordul Londrei, de către un ofiţer de poliţie care încerca să îl aresteze. Deşi motivul arestării acestuia nu a fost făcut public, există o serie de ipoteze, conform cărora, arestarea bărbatului ar fi trebuit să facă parte dintr-o operaţiune a Poliţiei Metropolitane, *Trident*, ce investiga deţinerea ilegală de armament şi utilizarea acestuia în traficul de droguri de către minoritatea de culoare din Anglia. În următoarele zile, nemulţumirea socială se răspândeşte în toată Londra şi chiar în alte oraşe ale Marii Britanii, căpătând diverse forme, preponderent demonstraţii împotriva structurilor de poliţie. Ulterior,

nemulţumirea socială[1] se transformă în vandalism şi furturi (Philips, Frost, Singleton, 2012, p. 1).

După uciderea lui Mark Duggan de către poliţia din Anglia, o serie de ipoteze privind moartea acestuia au început să se răspândească în cadrul comunităţii de culoare, acestea generând tensiuni şi mai mari, ce au degenerat rapid. Dacă la început se vorbea despre un protest a unui grup de 200 de persoane care cerea explicaţii privind moartea bărbatului, în scurt timp, lucrurile se complică odată cu diversificarea ipotezelor ce făceau referire la moartea acestuia. În acest sens, apar o serie de speculaţii conform cărora acesta ar fi fost ucis intenţionat de către poliţistul care l-a arestat şi că ar fi fost împuşcat în piept după ce a fost încătuşat. O altă speculaţie viza faptul că acesta ar fi transmis cu 15 minute înainte, de moartea acestuia prietenilor săi, că a fost încercuit de către poliţie, dar că este în siguranţă (Lewis, 7 august 2011). Ceea ce ar fi creat de fapt nemulţumire în rândul protestatarilor a fost, în esenţă, incertitudinea asupra morţii lui Mark Duggan, aceştia acuzând Poliția Metropolitană că nu a existat un schimb de focuri, bărbatul neavând o armă în posesia sa şi că omorârea acestuia contravine legii. Rapoartele poliţiei ar fi arătat faptul că acesta avea asupra sa o armă de foc, pe care o procurase chiar înainte de a fi arestat, de la Kevin Hutchinson-Foster. Interogatoriile şi procesele pe care acesta din urmă le-a avut nu au putut demonstra şi proba această acuzaţie, abia pe data de 8 ianuarie 2014 ajungându-se la verdictul că omorârea lui Mark Duggan nu a survenit în niciun fel prin încălcarea legii (*Mark Duggan inquest and reaction*, BBC News).

Astfel, după cum a fost amintit, pe fondul acestor incertitudini şi în baza nemulţumirii comunităţii de culoare din Anglia, încep protestele. Dacă la început s-a vorbit despre un protest paşnic, în noaptea de 7 august 2011, protestele degenerează şi creează violenţă şi tensiune. Astfel, au apărut o serie de întrebări în legătură cu viteza transformării unor proteste paşnice reduse ca localizare şi număr de participanţi în manifestări violente pe scară largă. Iniţial cauzele degenerării protestelor au fost identificate în modalitatea de prezentare e evenimentelor în presa locală şi posturile de televiziune cu acoperire naţională. *Totul a fost pus pe seama presei locale pe de-o parte, iar pe de altă parte pe fondul televiziunii din Marea Britanie.* Totuşi ceea ce a particularizat violenţele din Londra a fost promovarea masivă a fenomenului în *social media*.

În acest sens, în cadrul reţelei de socializare Facebook, protestatarii încep să creeze diverse grupuri, sub diferite denumiri (*Justice For Mark Duggan and Those Killed by Police* – Dreptate pentru Mark Duggan şi cei uciși

[1] Vezi detalii privind mecanismele specifice mişcărilor sociale în Gustave le Bon, (2012), *Psihologia Mulțimilor*, Editura Antet.

de poliţie, *Justice for Mark Duggan aka Starrish Mark. Sho! Sho* – Dreptate pentru Mark Duggan aka Starrish Mark. Sho! Sho, *R. I. P Mark Duggan* – Odihnească-se în pace Mark Duggansau *Justice for Mark Duggan* – Dreptate pentru Mark Duggan), comunităţi *on-line* care după începerea protestelor se extind rapid, unele dintre ele ajungând chiar la 34.841 de membrii (*Pagina oficială de facebook R. I. P. Mark Duggan*). Deşi apar mai multe astfel de grupuri, toate îşi îndreaptă atenţia către acelaşi gen de conţinut promovat, administratorii grupurilor cerând sprijinul susţinătorilor de a ieşi în stradă şi de a cere dreptate în cazul lui Mark Duggan. Exemplele de postări în acest sens (utilizatorul Shannon Loch: *Screw Police Brutality* – Împotriva brutalităţii poliţiei sau utilizatorul Milad Gh.: *Hey guys come on… I waiting for YOU! Are YOU with me?* – Haideţi cu toţii… Vă aştept! Sunteţi cu mine?) au folosit în general un limbaj mult mai tendenţios, însoţit adesea de cuvinte obscene la adresa poliţiei sau la adresa celor întâmplate. Majoritatea postărilor din cadrul reţelei de socializare Facebook au avut ca scop principal, pe lângă blamarea celor întâmplate şi mai ales a poliţiei londoneze, strângerea unui număr cât mai mare de susţinători *care* sunt dornici să iasă în stradă şi să participe la proteste, după cum se vede şi în postarea utilizatorului Milad Gh.

La mai bine de 3 ani jumătate de la moartea lui Mark Duggan şi de la revoltele sângeroase din Anglia, aceste pagini nu şi-au încheiat activitatea, administratorii acestor continuând să posteze mesaje împotriva poliţiei şi să solicite solidaritatea pentru cei ucişi de către ofiţerii de poliţie *(The Police are the biggest Mafia, but only in this case in a uniform. Fact! BirminghamStrong Justice 4 ALL Justice For Mark Duggan aka Starrish Mark.Sho!Sho Stephen Lawrence Charitable Trust Campaign for Justice for Smiley Culture* – Poliţia este cea mai mare mafie, doar că în acest caz poartă uniformă. Fapt dovedit!, urmând o înşiruire a unor pagini care îi susţin pe cei ucişi de poliţie). Totodată, aceştia îşi exprimă frecvent nemulţumirea faţă de evenimentele întâmplate, iar pe parcursul procesului lui Kevin Hutchinson-Foster a fost cerută din nou ieşirea în stradă şi susţinerea cauzei lui Mark Duggan (*Judgement Day 2013! Let's make it big! Look on the post below for more info. Let's do this 1 time! March 15 at 1:00pm* – Ziua judecăţii 2013! Haideţi să o facem încă o dată! 15 martie la ora 1 sau *Who coming Birmingham today for demo? Admin Tommy D, Plan B* – Cine vine în Birmingham astăzi pentru o demonstraţie? Admin Tommy D, Planul B).

Aşadar, în ceea ce priveşte Facebook, a putut fi observată ofensivitatea de care a dat dovadă comunitatea *on-line* în susţinerea şi apărarea lui Mark Duggan, având lideri virtuali informali, un limbaj codat specific, promovând chiar şi conţinut multimedia care să instige şi să atragă cât mai mulţi

protestatari care să ia parte la violenţe, aceştia aflând foarte uşor din *social media* despre locul şi ora violenţelor.

Pe lângă utilizarea aplicaţiei Facebook, protestatarii recurg şi la exploatarea platformei de socializare Twitter, pentru a se face auziţi în susţinerea cauzei lui Mark Duggan. Prin intermediul *tweet*-urilor, utilizatorii reţelei au reuşit să răspândească informaţiile rapid, profitând de ideea de *SMS*-ul *Internetului* şi de toate avantajele acesteia. Astfel, prin intermediul unor mesaje scurte, aceştia au comunicat rapid date, în special cu privire la ora şi locul protestelor şi mesaje care solicitau venirea unui număr cât mai mare de protestatari. Un exemplu în acest sens poate fi reprezentat de *tweet*-ul utilizatorului @carboia, care afirma *Spoke to them. They're on their way. Be with you soon* – Vorbiţi cu ei. Sunt pe drum. O să fiu cu voi curând, făcând referire la reunirea tuturor protestatarilor.

Aparte de aceste mesaje de chemare a susţinătorilor şi a protestatarilor, în cazul Twitter şi al revoltelor din Londra se poate vorbi şi despre propaganda *social media*. În zilele cuprinse între 6 şi 11 august, în cadrul postărilor din reţeaua Twitter, apar o serie de zvonuri cu privire la nemulţumirea socială a comunităţii şi asupra formelor pe care le-au îmbrăcat protestele acestora. În acest sens, au apărut *tweet*-uri ale utilizatorilor care susţineau faptul că protestatarii au atacat grădina zoologică din Londra şi au reuşit să elibereze animalele. Astfel @Twiggy_Garcia, un utilizator al reţelei Twitter care avea 5.178 de susţinători, este primul care răspândeşte în cadrul platformei zvonuri conform cărora protestatarii au intrat în grădina zoologică şi eliberează toate animalele. Această informaţie apare şi cu *hashtag*-ul Twitter #LondonRiots. La ora 2 dimineaţa, în data de 7 august, utilizatorul @Deadfreaks răspândeşte o serie de informaţii conform cărora revoltele au degenerat, iar protestatarii au reuşit chiar să intre în lanţul de fast-food-uri McDonald's şi îşi gătesc singuri mâncarea, zvon ce apare cu *hashtag*-ul #Tottenham. Tot în cadrul aceluiaşi *hashtag*, @DeclanJMN oferă câteva informaţii ce fac referire la faptul că o fetiţă de 16 ani ar fi fost bătută de către poliţia londoneză, lucru ce ar fi alimentat şi mai tare tensiunile şi nemulţumirea socială. Lucrurile merg însă mult mai departe, iar @zadio postează în cadrul *hashtag*-urilor #LondonRiots, #Londonriot şi #Prayforlondon imagini cu Ochiul Londrei în flăcări, *tweet*-ul fiind preluat rapid şi răspândit cu uşurinţă, înăsprindu-se starea de incertitudine şi tensiune în rândul populaţiei. Un alt exemplu în acest sens, îl constituie faptul că @jazz_kaur răspândeşte, folosindu-se de #Londonriots şi #birminghamriots, un zvon conform căruia protestatarii se îndreaptă către Spitalul de Copii din Birmingham (*The Guardian*, 7 decembrie 2011).

Cu toate acestea, toate zvonurile promovate de către utilizatorii amintiți mai sus prin intermediul rețelei Twitter s-au dovedit a fi false, iar în cele din urmă au fost infirmate chiar de către organele de poliție londoneze. Toate aceste informații au avut menirea clară de a crea panică și tensiune în rândul populației, care nu știa exact ce se întâmplă. Protestatarii s-au folosit de toate aceste zvonuri pentru a-și putea promova acțiunile violente și să câștige imagine în fața restului comunității, răspândind în acest fel haos și, cel mai grav, o stare de tensiune.

Așadar, informațiile disponibile din Facebook și zvonurile răspândite în cadrul Twitter au dovedit o posibilă stare de tensiune ce urma să se întindă la nivelul întregii Marii Britanii. În doar câteva zile, lucrurile au degenerat și în *social media* și de la simple postări legate de moartea lui Mark Duggan și dorința de a se face dreptate privind uciderea acestuia, s-a ajuns cu rapiditate la postări care arătau intenții violente sau organizări masive ale comunității pentru a-și exprima în mod vădit intențiile și nemulțumirile față de poliție, totul transformând-se practic într-o revoltă stradală, construită din violențe, furturi și conflicte ce s-au soldat cu victime.

După ce tensiunile au dispărut, calmându-se atât starea de spirit a protestatarilor, cât și adversitatea acestora față de poliție, iar într-un final au dispărut și revoltele stradale, rapoartele Poliției Metropolitane au demonstrat că aceasta a fost luată prin surprindere de emergența fenomenului *social media* și că nu ar fi presupus că desfășurând activitatea de intelligence în acest spațiu virtual, cu tot ce presupune ea, de la culegere și verificare, la analiză și integrare, aceasta ar fi putut ajuta ofițerii să prevină și să contracareze acțiunile violente ale protestărilor. Astfel, ia naștere necesitatea și oportunitatea creării în cadrul departamentelor de informații, a unui birou care să culeagă și să coroboreze informațiile disponibile, public, în cadrul rețelelor de socializare.

Intelligence post Londra 2011. Emergența unei noi discipline de culegere a informațiilor – SOCMINT

Evenimentele din Londra anului 2011 au reprezentat momentul zero în ceea ce privește emergența *social media intelligence*. Cu toate acestea, acest concept apare destul de târziu în terminologia serviciilor de informații, dacă ar fi să se țină cont de promovarea masivă a unor fenomene în cadrul rețelelor de socializare, spre exemplu Revoluția Twitter din Republica Moldova din anul 2009 sau Primăvara Arabă din anul 2010. Însă literatura de specialitate acceptă revoltele din Londra ca fiind punctul de plecare în analiza și utilizarea a ceea ce înseamnă *social media intelligence* sau SOCMINT, deoarece evenimentele au fost ca o lecție învățată pentru Poliția Metropolitană, fiind

prima care conştientizează nevoia culegerii de informaţii şi din acest spaţiu. Revoluţia Twitter din Republica Moldova şi Primăvara Arabă au fost puse sub semnul politicului, fiind ample mişcări de organizare a populaţiei pentru a deturna regimurile aflate la putere, în special cele comuniste, ale căror instituţii de informaţii nu au luat în calcul sau doar au condamnat şi blamat implicarea reţelelor de socializare în evenimentele ce au avut loc în 2009 şi 2010, fără a avea în vedere exploatarea tuturor informaţiilor disponibile în cadrul *social media*.

Astfel, depăşite de caracterul de noutate, precum şi de rapiditatea cu care informaţiile s-au răspândit prin intermediul reţelelor de socializare, departamentele de culegere a informaţiilor din cadrul Poliţiei Metropolitane din Marea Britanie s-au văzut nevoite să preia în aria lor de competenţă şi acest spaţiu virtual, asumându-şi misiunea de a preveni şi contracara ameninţările provenite din mediul *on-line*. Cu toate că mulţi au privit la început cu scepticism acest lucru, nepunându-se un accent deosebit pe această nouă disciplină de culegere de intelligence, ea a început să joace un rol important pe fondul emergenţei erei informaţionale şi a societăţii cunoaşterii.

Şeful Departamentului de Surse Deschise al poliţiei londoneze, Umut Ertogral, declara că pentru OSINT-ul pe care îl conduce „*social media* se comportă precum CCTV în spaţiul terestru" (*Financial Review*), făcând referire la sistemul de supraveghere stradală cu camere, disponibil la nivelul Angliei. Conform site-ului Wired UK, Scotland Yard-ul ar fi recunoscut existenţa unei echipe care să monitorizeze reţelele de socializare şi postările aferente ce fac referire la tensiunile politice. Echipa ar fi compusă din 17 ofiţeri şi ar purta numele de *SocMint*, având misiunea de a monitoriza Facebook-ul, Twitter-ul, YouTube-ul, precum şi alte servicii de *social media*. Acest lucru se realizează cu o continuitate de 24 de ore pe zi, 7 zile pe săptămână, precizându-se totodată faptul că această echipă de ofiţeri dezvoltă noi mijloace şi metode pentru a-şi îmbunătăţi activitatea de intelligence. Ca unitate componentă a Poliţiei Metropolitane, echipa are jurisdicţie de acţiune la nivelul tuturor districtelor Marii Britanii, precum şi în Ţara Galilor (Wright, 26 iunie 2013).

Cu toate că în presa *on-line* au fost vehiculate aceste informaţii, recunoscute tacit chiar de către directorul OSINT din cadrul poliţiei londoneze, Urmut Ertogral, există încă neînţelegeri şi incertitudini privind ce este *social media intelligence* sau de ce este necesară abordarea SOCMINT în rândul serviciilor de informaţii.

Aşadar, întrucât disciplina este caracterizată de noutate, nu există o terminologie clară, încă, a fenomenului, dar încep să apară o serie de lucrări ce abordează în mod direct problematica, pe de-o parte, iar pe de altă parte, lucrări care studiază conex fenomenul. În acest sens, în lucrarea sa *Introducing*

Social Media Intelligence, lucrare considerată pilonul de bază al abordării SOCMINT, Sir David Omand defineşte noua disciplină ca „existenţa unor capabilităţi prin care autorităţile accesează datele de comunicare şi accesează sub mandat, atunci când acesta este necesar, conţinutul comunicaţiilor din Internet, în speţă din *social media*" (Sir Omand, Bartlett şi Miller, 2012, p. 802). Tot el susţine că utilizarea capabilităţilor SOCMINT poate contribui într-un mod decisiv la asigurarea securităţii publice prin identificarea activităţilor criminale, asigurarea unei avertizări timpurii cu privire la existenţa unor stări de tensiune sau ameninţări publice sau crearea unei avertizări operative, atunci când evenimentele evoluează într-un ritm alert (Sir Omand, Bartlett şi Miller, 2012, p. 9). Astfel, Sir David Oman, împreună cu echipa sa, pune bazele a ceea ce înseamnă culegerea de informaţii din cadrul reţelelor de socializare, care în esenţă se poate rezuma la culegerea de informaţii disponibile din comunicarea realizată *on-line via social media*, totodată oferind şi câteva exemple de domenii de asigurare a securităţii, fie ea naţionale sau internaţionale, precum şi modalităţi prin care SOCMINT poate contribui în mod direct la realizarea acestui lucru.

Alte încercări de definire a ceea ce înseamnă *social media intelligence* fac referire la „culegerea de informaţii din surse deschise de către specialişti în tehnica de supraveghere *on-line* de pe site-urile de socializare, chat-uri, site-uri web şi Internet" (*Use of Internet for Terrorist Purposes*, 2012, p. 68) sau particularizează ceea ce înseamnă SOCMINT, ca fiind un domeniu subsecvent culegerii de informaţii din surse deschise, pornind de la ideea că *social media intelligence* reprezintă o ramură a OSINT, dar care are un domeniu de acţiune specific, în speţă, reţelele de socializare (SOCMINT, 31 octombrie 2012). Aşadar, se poate considera faptul că se vorbeşte despre o nouă disciplină a intelligence-ului, aflată, însă, încă într-o faza incipientă de dezvoltare şi introducere în activitatea serviciilor de informaţii. Cu toate acestea, se observă şi materializează, chiar dacă pentru moment sub forma unor lecţii învăţate, oportunităţile pe care *social media intelligence* le-ar putea oferi, odată cu implementarea acesteia în cadrul agendei de lucru a activităţii de informaţii, oportunităţi ce nu sunt deloc de neglijat, datorită contribuţiilor pe care acestea le-ar putea aduce în vederea asigurării climatului de securitate.

Social Media Intelligence – oportunităţi pentru serviciile de informaţii

Lecţiile învăţate după revoltele din Londra din anul 2011 au condus către necesitatea introducerii conceptului de *social media intelligence* ca o nouă disciplină de culegere a informaţiilor, alături de cele clasice HUMINT sau TECHINT, înscriindu-se în acelaşi timp în rândul celor moderne, de natura

CYBERINT. Cercetările întreprinse asupra evenimentelor din Londra şi a modului de propagare a informaţiilor în cadrul reţelelor de socializare au relevat faptul că o analiză întocmai şi la timp a faptelor ce au fost expuse în cadrul reţelelor de socializare s-ar fi dovedit o bună avertizare timpurie pentru Poliţia Metropolitană, care ar fi putut în acest sens să combată timpuriu violenţele din Londra şi să evită escaladarea conflictului.

Astfel, a fost conturat contextul introducerii SOCMINT pe agenda de lucru a serviciilor de informaţii, acest INT dovedind o serie de oportunităţi de care ar trebui profitat în vederea completării instrumentelor ce pot ajuta, în primă instanţă, la obţinerea unor date primare de cunoaştere cu privire la o anumită problematică, iar mai apoi la sporirea climatului de securitate prin valorificarea acestora prin analiza realizată de analiştii serviciilor de informaţii.

Vorbind de oportunităţile aduse de utilizarea *social media intelligence*, se vorbeşte de fapt despre plusurile pe care acestea le oferă pe de-o parte activităţii de informaţii, iar pe de altă parte serviciilor de informaţii, care uneori îşi pot uşura munca, culegând cu o mai mare uşurinţă date, locaţii sau ore de desfăşurare a unor evenimente sau persoane ce iau parte la acestea. Pe lângă cele menţionate, există o serie de concepte cheie ce fac obiectul studierii oportunităţilor pe care activitatea de *social media intelligence* le aduce.

În acest sens, vorbind despre oportunităţile aduse de fenomenul *social media intelligence*, se poate vorbi despre utilitatea conceptului de *crowd sourcing*. James Surowiecki, repurtat jurnalist al publicaţiei *The New Yorker*, vorbeşte despre inteligenţa mulţimilor şi, implicit, despre culegerea informaţiilor din rândul unei mulţimi. El îşi asociază teoriile cu cele ale lui Gustave Le Bon în ceea ce priveşte ideea de mulţime. Totodată, el susţine faptul că mai mulţi oameni ce abordează o problematică, vor oferi o soluţie mult mai bună spre rezolvarea ei, decât dacă aceasta ar fi rezolvată de una sau două persoane. În cartea sa, *Wisdom of Crowds*, el întregeşte ce înseamnă de fapt *crowd sourcing*-ul (culegerea de informaţii din cadrul unor mulţimi), insistând însă asuprea unui aspect esenţial, şi anume că atunci când se vorbeşte despre inteligenţa mulţimilor nu se vorbeşte despre mai multe minţi puse la un loc, ci despre descentralizare, mai multe persoane abordând subiectul de interes în cadrul unei colectivităţi extinse, dar în mod individual, fiecare oferind propria soluţie de rezolvare a problematicii. Astfel, susţine el, va apărea o persoană cu cea mai bună ideea de a rezolva subiectul abordat (Surowiecki, 2005).

Acelaşi fenomen poate fi observat şi în rândul platformelor de socializare. Încă din prezentarea principalelor reţele de socializare, a fost stabilit faptul că utilizatorii diseminează conţinut şi informaţie în cadrul unei

pagini *social media*. Spre exemplu, în cazul revoltelor din Londra, în anul 2011 şi al zvonurilor apărute pe Twitter, fiecare utilizator al platformei a putut să posteze propriile informaţii cu privire la ce se întâmpla, de fapt, în realitatea tangibilă. În acest context, se poate vorbi despre *crowd sourcing* în cadrul reţelelor de socializare, Poliţia Metropolitană având posibilitatea să fi analizat toate aceste zvonuri (culegere), să le verifice pentru a putea stabili veridicitatea lor (verificare), să le analizeze pentru a stabili direcţiile de acţiune (analiză), iar în final să aleagă cea mai bună cale de acţiune în baza unei informaţii provenite din *social media*, pentru a preveni sau contracara violenţele stradale (operaţionalizare şi valorificare). Astfel, poate fi demonstrată utilitatea activităţii de *crowd sourcing* chiar pe baza unui instrument cheie al activităţii de informaţii, în speţă ciclul de intelligence.

O altă dimensiune a acestui fenomen, ca oportunitate SOCMINT pentru serviciile de intelligence, este dată de Sir David Omand, care susţine faptul că atunci când se vorbeşte despre *crowd sourcing*, din punct de vedere instituţional, se poate vorbi despre asigurarea unui flux mai bun de informaţii între guvern şi proprii cetăţeni, mai ales atunci când se vizează situaţii de criză. El porneşte de la teoria conform căreia persoanele ce asistă la producerea unui eveniment se pot transforma în *jurnalişti de ocazie*, având posibilitatea să posteze în *social media*, informaţii din teren, ce ar putea fi ulterior verificate şi valorificate de către ofiţerii de informaţii. Prin facilităţile oferite de reţelele de socializare, mai ales prin posibilitatea diseminării de conţinut multimedia, aceşti *jurnalişti de ocazie* pot posta fotografii sau filmuleţe de la faţa locului, pe care mai apoi, instituţiile abilitate le pot folosi pentru a deschide noi operaţiuni sau în cadrul celor deja existente. Conexând conceptul de *crowd sourcing* cu ideea de *wisdom of crowds* în ceea ce priveşte activitatea serviciilor de intelligence, a fost elaborată o platformă web, denumită Ushahidi, unde cei interesaţi puteau posta informaţii de orice natură, „de la cutremurul din Haiti, până la blocajele rutiere din Washington, DC" (Sir Omand, Bartlett şi Miller, 2012, p. 805). Astfel, încet, dar sigur, se pun bazele unor noi tehnologii în acest sens, pentru a oferi publicului posibilitatea de a contribui activ la asigurarea climatului de securitate.

O altă oportunitate a emergenţei *social media intelligence* poate consta în cercetarea şi înţelegerea survenită din analiza reţelelor de socializare. Studierea platformelor *social media* poate ajuta serviciile de informaţii să înţeleagă anumite fenomene emergente în cadrul WEB 2.0. Acestea pot face referire la o serie de aspecte esenţiale, precum indicatori ai violenţei, căile promovate pentru auto-radicalizarea teroriştilor islamişti sau praguri şi indicatori ai criminalităţii survenite din cadrul reţelelor de socializare. Astfel, acest lucru poate contribui la înţelegerea modalităţilor prin care se formează

şi se schimbă anumite idei şi la investigarea „intersecţiei socio-tehnologice" dintre persoana *off-line* şi persoana *on-line* (Sir Omand, Bartlett şi Miller, 2012, p. 805), în vederea asigurării unui palier de cunoaştere integrat asupra fenomenelor, dar şi asupra celor care le generează.

Aparte de cele menţionate, în cazul oportunităţilor oferite de SOCMINT, se vehiculează conceptul de cunoaştere operaţională în timp real a activităţilor ce se desfăşoară în spaţiul virtual al reţelelor de socializare. Analiza statisticilor Twitter a relevat faptul că există postări, atât *pre*, cât şi *post* apariţiei unui fenomen. Astfel, prin realizarea unei evaluări a traficului platformelor de socializare, se poate facilita identificarea fenomenelor emergente, acest lucru realizându-se poate mult mai uşor decât dacă ar fi folosite tehnici investigative tradiţionale. Spre exemplu, dacă s-ar realiza o geo-localizare a evenimentelor promovate în *social media*, analiştii de intelligence ar putea obţine hărţi de evoluţie ale posibilelor noi locaţii fizice de realizare ale unui protest, revolte sau de ce nu, chiar act criminal (Sir Omand, Bartlett şi Miller, 2012, p. 805).

Conex cunoaşterii activităţilor desfăşurate şi promovate în cadrul reţelelor de socializare, se poate vorbi despre cunoaşterea persoanelor şi a grupurilor care desfăşoară astfel de activităţi. Adesea, grupări teroriste sau extremiste îşi creează pagini de Facebook sau Twitter pentru a-şi promova ideologia, mesajul sau valorile proprii. Astfel, ofiţerii de intelligence pot pătrunde în cadrul acestor grupuri, dobândind astfel o cunoaştere mult mai bună a mentalităţii şi a modalităţilor de acţiune a acestora. Pentru aceasta se poate studia nivelul nemulţumirilor sociale existente în cadrul unui grup, a stării de nervozitate a membrilor acestuia sau a principalelor motive ce animă activitatea utilizatorilor. De asemenea, SOCMINT poate fi folosit de către serviciile de intelligence pentru identificarea intenţiilor criminale, extremiste sau teroriste, prin realizarea unor operaţiuni de amploare de monitorizare a reţelelor de socializare, de către ofiţeri tehnici specializaţi, aceştia având posibilitatea să monitorizeze activitatea grupurilor şi a persoanelor cunoscute a desfăşura acţiuni ce pot aduce atingere securităţii naţionale (Sir Omand, Bartlett şi Miller, 2012, p. 806).

Totuşi, nu doar grupările teroriste sau extremiste se organizează în *social media* pentru a-şi recruta noi membrii. După emergenţa fenomenului reţelelor de socializare şi serviciile de intelligence au început puternice campanii de recrutare din acesta spaţiu. Aceste campanii capătă două direcţii de dezvoltare. Pe de-o parte se poate vorbi despre promovarea instituţiilor de securitate şi a transparenţei acestora şi de atragerea de personal către acestea, după modelul companiilor private care prin campanii de marketing îşi promovează imaginea şi urmăresc recrutarea de personal pentru interviuri.

Pe de altă parte, în ceea ce privește intelligence-ul, există un aspect particular, în speță recrutarea unor noi agenți și atragerea la colaborare a persoanelor cu posibilități în mediile de interes. Astfel, prin îmbinarea unui INT clasic, HUMINT, cu un INT modern, SOCMINT, se poate întregi palierul de intelligence în vederea asigurării securității.

În acest sens, serviciile de informații britanice (MI6 și SIS), spre exemplu, au apelat la aplicația Facebook pentru a-și recruta personalul, prin completarea unor chestionare cu scopul de a atrage către servicii oameni ce provin din medii sociale diferite. Și CIA și-a creat o pagină Facebook destinată exclusiv recrutării candidaților, rețeaua lui Mark Zuckerberg fiind acuzată în diverse medii că ar reprezenta chiar un mijloc al Central Intelligence Agency în activitatea sa, serviciul american investind sume enorme în tehnologie destinată supravegherii *social media* (Ciupercă, Ciupercă, Niță, Stoica, 2010, pp. 124-125). În acest sens, „modul de recrutare și dirijare a agenturii ca metodă și mijloc specific activității de intelligence respectă aceleași reguli de conspirativitate, având marele avantaj al unei mai bune conspirări și a unui grad mai mare de operativitate" (Ciupercă, Ciupercă, Niță, Stoica, 2010, pp. 126-127), deoarece totul se realizează la distanță, fără ca ofițerii de intelligence să fie expuși în mod direct, aceștia putând acționa din spatele unui calculator.

Astfel, serviciile de intelligence pot acționa în *social media* sub profiluri conspirate, simulând acoperirea din viața reală pentru a putea stabili legăturile cu viitorii agenți sau pentru a pătrunde în mediul relațional al vectorilor, care și ei la rândul lor, bazându-se pe anonimatul oferit de rețelele de socializare pot fi mult mai deschiși în vederea cooperării cu serviciile de informații. Totodată, prin intermediul acestor platforme, ofițerii de intelligence pot „verifica alibiul unor persoane prin compararea variantelor oferite de aceștia" (Ciupercă, Ciupercă, Niță, Stoica, 2010, pp. 126-127) cu activitatea lor din cadrul rețelelor de socializare. Totuși, în cazul în care se dorește totuși o viitoare recrutare a unor posibile surse sau agenți, dar în spațiul real, tangibil, despre care se cunoaște că sunt activi în cadrul rețelelor de socializare, ofițerii de intelligence pot recurge la culegerea unor date de cunoaștere primară despre aceștia, urmărind câteva criterii standard, disponibile spre exemplu, pe Facebook, realizându-se astfel *profiling*-ul agentului sau sursei.

Astfel, un prim pas în activitatea de cunoaștere îl poate constitui poza sau pozele de profil, precum și alte poze postate pe pagina personală a utilizatorului. Atunci când, ofițerul de intelligence deține doar numele unei persoane (sau numele de utilizator al acesteia) aflată în cercul relațional al unor suspecți și despre care anterior au fost obținute date primare ce o indică

în vederea selecționării și recrutării, fără a avea posibilitatea la acel moment de a obține alte date de cunoaștere, acesta poate trece la verificarea acestei persoane pe Facebook. În cazul în care a fost găsit un profil sau mai multe, ce corespund numelui deținut, ofițerul va avea posibilitatea de a documenta persoana respectivă prin compararea datelor înscrise în Registrul de Evidență al Populației și a celor regăsite pe Facebook, în vederea confirmării corespondenței dintre nume real sau cel de utilizator deținut și profilul de Facebook (în acest sens, se poate face referire aici, spre exemplu, la compararea datei de naștere înscrisă la Evidența Populației cu cea ce se regăsește în cadrul profilului, facilitându-se astfel corespondența mai sus amintită și identificarea persoanei vizate). Astfel, ofițerul serviciului de intelligence poate avea acces la poza sau pozele de profil ale utilizatorului, devenind astfel facilă cunoașterea acestuia și identificarea lui. Aparte de aspectele fizice, ofițerul mai poate documenta, prin prisma fotografiilor postate, cercul relațional al utilizatorului, având posibilitatea să observe atent mediul în care acesta își petrece timpul liber sau persoanele cu care se afișează, identificând astfel pasiuni sau chiar vulnerabilități, posibile a fi exploatate în viitor. Toate acestea vin în sprijinul ofițerului care va avea astfel posibilitatea să cunoască anterior realizării unei întâlniri reale persoana, beneficiind deja de câteva detalii pe care le poate aborda în cadrul discuțiilor pe care le poate purta cu aceasta în vederea recrutării.

Mergând mai departe, în vederea realizării profilului persoanei vizate spre recrutare, ofițerul de intelligence poate urmări datele cu caracter personal afișate în cadrul paginii personale a acesteia. În acest sens, tot în sprijinul cunoașterii necesare a fi dobândite de către ofițerul de intelligence ce are în lucru realizarea profilului persoanei, vine expunerea datelor cu caracter personal, date pe care anumiți utilizatori aleg să le facă publice în cadrul profilului lor. Vorbim aici de date cu privire la data și locul nașterii, studii absolvite sau în curs de absolvire, loc de muncă, precum și detalii privind starea civilă, domiciliul, rude și alte date de contact (uneori chiar e-mail sau telefon). De asemenea, în cadrul acestei secțiuni există două subsecțiuni ce fac referire la posibilitatea utilizatorului de a adăuga o scurtă descriere cu privire la propria persoană și la posibilitatea de a adăuga anumite citate favorite aparținând unor diverși autori. Cele mai sus menționate ajută ofițerul serviciului de intelligence să stabilească acele detalii privind nivelul de educație, situația familială și materială, precum și surprinderea acelor trăsături psiho-socio-comportamentale pe care în urma unei atente analize le poate valorifica în vederea stabilirii și a unui profil psihologic al persoanei vizată în sensul recrutării.

Prietenii sau legăturile pe care utilizatorul le-a stabilit în cadrul paginii personale pot constitui următorul aspect esenţial ce trebuie avut în vedere de către ofiţerul de intelligence în stabilirea profilului persoanei în cauză. Astfel, persoana ce realizează *profiling*-ul, prin analiza relaţiilor de prietenie ale utilizatorului şi a altor legături stabilite în *social media*, îşi completează datele de cunoaştere cu privire la cercul relaţional al persoanei aflată în atenţia recrutării. Atenta observare a persoanelor adăugate ca prieteni în cadrul profilului utilizatorului, precum şi analiza legăturilor strânse pe care acesta le păstrează cu anumite persoane poate conduce la determinare unui anumit mediu relaţional şi stabilirea unor caracteristici cu privire la acesta, identificându-se starea socială a persoanei, cercurile sociale în care îşi desfăşoară activitatea, precum şi cele în care se simte cel mai comod. Aşadar, se pot obţine date de cunoaştere importante cu privire la motivaţia recrutării sau cu privire la crearea unui context favorabil recrutării.

Opţiunea de *check-in*, împreună cu serviciile de localizare oferă o mare oportunitate celui care analizează profilul utilizatorului vizat. Acesta are posibilitatea de a observa, chiar în timp real, locul în care persoana se află la un moment dat, în cazul în care aceasta aflându-se într-un anumit loc şi apelând la funcţia de *check-in* marchează prezenţa sa în locul respectiv. Astfel, ofiţerul poate şti cu exactitate locul în care se află persoana, beneficiind de coordonatele GPS oferite de Facebook, dar şi de numele unor locaţii publice sau private ce se regăsesc în cadrul *check-in*-ului. Astfel, în cazul unei postări se poate observa zona, cu aproximaţie, din care s-a făcut postarea, ofiţerul având posibilitatea să verifice prezenţa persoanei într-un anumit cartier, sector, într-o anumită localitate sau regiune.

Astfel, în acest sens, ofiţeri ai serviciilor de intelligence pot apela la această metodă de *profiling* prin intermediul *social media*, obţinând prin analiza unor elemente cheie ale reţelei Facebook, date de cunoaştere primară cu privire la viitori candidaţi la recrutare, care coroborate şi verificate prin comparaţia cu alte informaţii obţinute prin intermediul altor surse pot oferi o imagine de ansamblu asupra recrutării noilor surse de informaţii, a calităţilor acestora, precum şi a trăsăturilor psihologice care cu condus la demararea procesului de recrutare.

Dacă pe palierul informativ operativ al activităţii de intelligence se poate vorbi despre realizarea unui profil cu date primare de cunoaştere a candidaţilor pentru recrutare culese prin intermediul reţelelor de socializare, în ceea ce priveşte partea tehnică a acestei activităţi, căci a fost susţinut faptul că şi în acest spaţiu activitatea de informaţii se desfăşoară după aceleaşi norme, mijloace, metode şi principii, *social media* se bucură de un aport al oportunităţilor, adus prin intermediul programelor informatice de analiză

a reţelelor de socializare, de care pot beneficia cu uşurinţă analiştii serviciilor de intelligence.

În acest sens, a fost elaborată o serie de *soft*-uri a căror utilitate pentru realizarea analizei reţelelor de socializare constă în uşurinţa cu care acestea realizează o serie de reprezentări grafice, sub forma unei pânze de păianjen, în vederea oferirii unei imagini puternice şi bine conturate a reprezentării reţelei din spaţiul 2.0, în realitatea tangibilă.

Pornind de la ideea că în mod succint, o reţea socială reprezintă un set finit sau seturi finite de actori care realizează conexiuni unul cu celălalt, analiza reţelelor sociale implică detectarea şi interpretarea unor tipare sociale a caracteristicilor ce leagă actorii între ei (Everton, 2013, p. 9), toate acestea redate într-o formă grafică, prin intermediul programelor informatice mai sus amintite.

Un exemplu de un astfel de soft este reprezentat de *soft*-ul UCINET, creat de către Linton Freeman, pe vremea când acesta era la Universitatea din California, Irvine, fiind ulterior îmbunătăţit în mai multe rânduri. Acesta este unul dintre cele mai cunoscute programe de analiză a reţelelor sociale, fiind totodată şi cel mai folosit, deoarece oferă o serie de instrumente de măsurare a datelor provenite din platformele de socializare, precum şi alte instrumente de management al datelor. Toate acestea contribuie la măsurătorile estimative ale topografiei reţelei, oferind informaţii despre actorul central al reţelei, identificând subgrupurile şi estimând valorile de măsurare ale echivalenţei structurale a platformei vizate. Mai mult decât atât, UCINET oferă o serie de instrumente prin care se pot selecta subseturi de date din cadrul reţelei şi prin care se pot importa şi exporta date sub orice format, toate acestea făcând din UCINET un redutabil program folosit în realizarea analizei reţelelor de socializare (Everton, 2013, p. 50).

Concluzii

Aşadar, se poate concluziona cu faptul că utilizarea unui intelligence axat pe o dimensiune 2.0, prin intermediul radiografierii *social media*, poate conduce la o serie de oportunităţi, care exploatate de către cadrele serviciilor de intelligence, acestea pot oferi o serie de date de cunoaştere suplimentare cu privire la o anumită problematică investigată, iar uneori pot chiar oferi aspecte de noutate, ce nu au putu fi culese de către cei ce îşi desfăşoară activitatea în teren. În acest sens, se justifică abordarea unor INT-uri 2.0, care odată exploatate pot oferi chiar piesele lipsă ale unui puzzle după care îşi ghidau activitatea serviciile de informaţii. Totuşi, trebuie avut în vedere un fapt simplu şi anume că şi cei ce folosesc *social media* în scopuri care nu deservesc valorilor şi intereselor naţionale pot cunoaşte toate aceste

oportunităţi şi pot chiar ei să fie primii care beneficiază de acestea, astfel, reţelele de socializare şi Internetul rămânând un spaţiu de tatonare, un teritoriu „demilitarizat" unde activează atât grupările ce doresc a prejudicia climatul de securitate, cât şi serviciile de intelligence, lupta fiind una pentru dobândirea puterii digitale. Întrebarea care survine se poate rezuma în următoarea propoziţie, cât va fi fiecare dispus să rişte pentru a putea cuceri spaţiul virtual? Vor fi gata serviciile de intelligence să ducă o nouă activitate de cercetare şi cunoaştere pentru a înţelege noile fenomene sau aceste grupări îşi vor proteja atât de bine liderii, simpatizanţii şi metodele încât comunitatea internaţională de informaţii nu va reuşi să culeagă datele necesare?

Pe fondul acestor oportunităţi amintite anterior şi pe fondul emergenţei activităţilor grupărilor ce pot aduce atingere securităţii naţionale, regionale sau internaţionale, precum şi valorilor şi intereselor actorilor statali sau chiar non-statali şi pe fondul luptei continue între structurile comunităţii de intelligence şi a acestor grupări, nu trebuie totuşi pierdute din vedere, nicio clipă, limitele la care poate fi supusă activitatea de culegere a informaţiilor, întreprinsă prin intermediul *social media intelligence*.

Referinţe bibliografice:

1. Ciupercă, Ella, Ciupercă, C., Niţă, C, Stoica, M., (2010), *Rolul reţelelor de socializare pe internet în modelarea comportamentelor*, Bucureşti: Editura ANI.
2. Everton, Sean, (2013), *Disrupting Dark Networks*, Cambridge University Press.
3. *Financial Review*, accesibil pe www.afr.com/p/technology/ google_glass_and_social_media_to_R5en8jIWOeVUjasiJqsaIL.
4. *How riot rumours spread on Twitter*, (7 decembrie 2011), în *The Guardian* accesibil pe www.theguardian.com/uk/interactive/2011/dec/07/ london-riots-twitter.
5. Lesidrenska, Rada, Bancheva, Vessela, (2012), *Adaptation of Intelligence and Security Services to Contemporary Challenges* în Proceedings of the XVIIIth International Conference – Intelligence in the Knowledge Society.
6. Lewis, Paul, (7 august 2011), *Tottenham riots: a peaceful protest, then suddenly all hell broke loose*, în *The Guardian* accesibil pe www.theguardian.com/uk/2011/aug/07/tottenham-riots-peaceful-protest.
7. Maior, George Cristian, *Mesajul directorului Serviciului Român de Informaţii* în *SRI în era informaţională, Viziunea strategică 2011-2015*.
8. *Mark Duggan inquest and reaction*, BBC News accesibil pe www.bbc.com/news/uk-england-london-25648913.

9. *Pagina oficială de facebook R.I.P. Mark Duggan* accesibilă pe www.facebook.com/pages/RIP-Mark-Duggan/200659976657547, accesat la 03.03.2014.
10. Philips, Richard, Frost, Diane, Singleton, Alex, (2012), *Researching the riots* în the Geographical Journal.
11. Sir Omand, David, Bartlett, Jamie, Miller, Carl, (2012), *Introducing Social Media Intelligence,* în *Intelligence and National Security*, Vol. 27, Nr. 6.
12. Sir Omand, David, Bartlett, Jamie, Miller, Carl, (2012a), *A Balance between Security and Privacy Online Must Be Struck*, în Demos.
13. Social Media Intelligence (SOCMINT), (31 octombrie 2012), Same Song, New Melody?, accesibil pe www.osintblog.org/2012/10/31/social-media-intelligence-socmint-same-song-new-melody.
14. Surowiecki, James, (2005), *The Wisdom of Crowds*, Anchor Books.
15. *Use of Internet for Terrorist Purposes*, (2012), Oficiul Națiunilor Unite pentru Droguri și Criminalitate.
16. Wright, Paul, (26 iunie 2013), Meet Prism's little brother: Socmint, accesibil pe www.wired.co.uk/news/archive/2013-06/26/socmint.