RRSI Nr. 14 /2015

REVISTA ROMÂNĂ DE STUDII DE INTELLIGENCE

Nr. 14
Decembrie
2015

Revistă cu prestigiu științific recunoscut
de *Consiliul Național de Atestare a Titlurilor, Diplomelor și Certificatelor Universitare*
(CNADTCU), indexată în bazele de date internaționale CEEOL și EBSCO

București
2015

Colegiul Editorial

Eduard HELLVIG
- director al Serviciului Român de Informaţii
George Cristian MAIOR
- prof. univ. dr. Academia Naţională de Informaţii *„Mihai Viteazul”* şi Şcoala Naţională de Studii Politice şi Administrative
Christopher DONNELLY
- senior fellow Defence Academy din Regatul Unit, director al Institute for Statecraft and Governance, Oxford, Marea Britanie
Mark PHYTHIAN
- professor, University of Leicester, Marea Britanie
Ioan Mircea PAŞCU
- prof. univ. dr. Şcoala Naţională de Studii Politice şi Administrative
Vasile DÂNCU
- prof. univ. dr. Universitatea din Bucureşti, Universitatea Babeş-Bolyai
Michael ANDREGG
- professor, St. Thomas University, SUA
Elaine PRESSMAN
- senior fellow Patterson School of International Affairs, Carleton University, Canada
Jan GOLDMAN
- professor, Tiffin University, SUA
Gheorghe TOMA
- prof. univ. dr. Academia Naţională de Informaţii *„Mihai Viteazul”*
Sergiu MEDAR
- prof. univ. dr. Universitatea „Lucian Blaga” din Sibiu
Niculae IANCU
- conf. univ. dr. Academia Naţională de Informaţii *„Mihai Viteazul”*
Cristiana MATEI
- lecturer Center for Civil-Military Relations din Monterey, SUA
Iulian CHIFU
- conf. univ. dr. Şcoala Naţională de Studii Politice şi Administrative
Iulian FOTA
- conf. univ. dr. Academia Naţională de Informaţii *„Mihai Viteazul”*
Marian SEBE
- prof. univ. dr. Academia Naţională de Informaţii *„Mihai Viteazul”*
Irena CHIRU
- prof. univ. dr. Academia Naţională de Informaţii *„Mihai Viteazul”*
Valentin FILIP
- lect. univ. dr. Academia Naţională de Informaţii *„Mihai Viteazul”*

Colectivul de redacţie

Redactor-şef:	*drd. Valentin NICULA*
Redactor-şef adjunct:	*dr. Mihaela TEODOR*
Redactori:	*dr. Irena CHIRU*
	dr. Karin MEGHEŞAN
	dr. Cristina IVAN
	dr. Aitana BOGDAN
	dr. Cristian NIŢĂ
	dr. Codruţ LUCINESCU
	dr. Valentin STOIAN
	drd. Daniela BACHEŞ
	Teodora DOBRE
Tehnoredactor:	*Alina-Rodica PETRA*
Coperta:	*Valentin NICULA*

CUPRINS

MEDIUL INTERNAŢIONAL DE SECURITATE 5

Michael ANDREGG
Criza globală emergentă și fluxul curent de migranți/refugiați care se îndreaptă către Europa 7
Michał WOJNOWSKI
Terorismul servind scopuri geopolitice. Conflictul ruso-ucrainean ca exemplu al doctrinei lui Aleksandr Dugin și conceptului lui Evgeny Messner de „Război Rebel" 17

PARADIGME DE SECURITATE ÎN SECOLUL XXI 61

Raisa Gabriela ZAMFIRESCU
Mediul de securitate informațional. Atacul cibernetic – amenințarea modernă a secolului XXI 63
Teodora DOBRE, Virginia ANDREI
Lumea văzută de Vladimir Putin 77

STRATEGII ŞI POLITICI DE SECURITATE 91

Elaine PRESSMAN
Analiză de risc contrainformativ: infrastructuri critice, structuri militare și de intelligence 93

CULTURĂ DE SECURITATE ȘI DIPLOMAȚIE PUBLICĂ 119

Iulian DICULESCU
Diplomație publică și intelligence - O perspectivă pragmatică asupra unei intersectări sensibile 121

INTELLIGENCE ÎN SECOLUL XXI 131

Florian COLDEA
Noi provocări în linia întâi a activității de intelligence – perspectiva unui practician 133
Loredana IVAN
Sistemul francez de intelligence economic 145

ANALIZA DE INTELLIGENCE 159

Cristina POSAŞTIUC
Teorie şi practică în intelligence: driveri ai cunoaşterii 161

Mircea MOCANU
Dileme și soluții pentru modelul ciclului de intelligence 171

OSINT 185

Rareș-Adrian RAICU
Emergența fenomenului social media intelligence 187

ISTORIE ȘI MEMORIE ÎN INTELLIGENCE 205

Ioan Codruț LUCINESCU, Valentin STOIAN
Motivații ale trădării. Cazuri istorice prin perspectiva modelelor de analiză contemporane 207

RECENZII ȘI NOTE DE LECTURĂ 225

Publicații românești de Business Intelligence. Recenzie de **Oana Puie** 227
Philip Davies și Kristian Gustafson editori, (2013), *Intelligence elsewhere: spies and espionage outside the anglosphere*, Georgetown University Press, *W*ashington D.C. Recenzie de **Cosmina-Elena Epure** 230

FOCUS ACADEMIC 233

Ediția a XII-a a Conferinței Internaționale Anule a Asociației Internaționale pentru Educație în Intelligence (IAFIE), Breda, Olanda, 22-24 iunie 2016 235
Ediția a III-a a Programului „Security in the Black Sea Region. Shared Challenges, Sustainable Future" (SBSR), București-Sibiu, 30 mai–4 iunie 2016 237
Ediția a XXII-a a Conferinței Internaționale Intelligence in the Knowledge Society, București, 13-14 octombrie 2016 239
CITYCOP Citizen Interaction Technologies Yield Community Policing, iunie 2015 – mai 2018..... 241
CARISMAND Culture and Riskmanagement in Man-made and Natural Disasters, octombrie 2015 -septembrie 2018 243
SAFFRON Semantic Analysis against Foreign Fighters Recruitment Online Networks, 2015-2018 245
REACT PN-II-RU-TE-2014-4-1669. Percepție socială și strategii comunicaționale privind riscurile de securitate națională, octombrie 2015 – septembrie 2017 246
Invitație la contribuții - RRSI nr. 15/2016 248

MEDIUL INTERNAŢIONAL DE SECURITATE

CRIZA GLOBALĂ EMERGENTĂ ȘI FLUXUL CURENT DE MIGRANŢI/REFUGIAŢI CARE SE ÎNDREAPTĂ CĂTRE EUROPA

Michael ANDREGG*

Abstract

A "Developing Global Crisis" is unfolding today that reflects synergistic interactions among demographic pressures, authoritarian politics, militant religion, corruptions of governance and other factors worldwide. All of these four and several other relevant factors are complex, and many interact synergistically (e.g. non-linear interactions) so they will be illustrated by the case of Syria here.

Keywords: global crisis, migrant, Syria, demographic pressure.

Introducere

O „Criză Globală Emergentă" caracterizează la momentul actual scena internaţională, fapt ce reflectă sinergia interacţiunilor care au loc la nivelul presiunilor demografice, politicilor autoritare, religiei militante, actelor de corupţie de la nivel guvernamental și alţi factori. Toţi aceşti patru factori, alături de alţi factori relevanţi, sunt caracterizaţi de complexitate, un număr mare interacţionând de-o manieră sinergetică (de exemplu, interacţiuni non-lineare), motiv pentru care am ales prezentarea lor prin prisma situaţiei din Siria. Cele mai multe comentarii cu privire la această criză se concentrează asupra personalităţilor lui Bashar al-Assad și a preşedintelui rus Vladimir Putin. Alţi observatori se axează asupra forţelor emergente ale răului, precum ISIS, considerat un cult al morţii (denumit și ISIL, Daesh sau Statul Islamic – dar numele nu mai contează) și nici liderii săi.

Aceste aspecte sunt relevante în încercarea de a răspunde la mai multe întrebări, dar pot, în acelaşi timp să eclipseze cauze relevante care pot declanşa un război, cum ar fi presiunile demografice care generează numeroase probleme globale, sau corupţia omniprezentă la nivel guvernamental care face dificilă găsirea soluţiilor. De exemplu, înainte de declanşarea actualei crize, populaţia statului sirian înregistra o creştere de 2,4%/an, conducând la dublarea numărului de locuitori în mai puţin de 30 de ani (CIA World FactBook, 2010). Acest lucru pune o presiune foarte mare asupra resurselor naturale precum terenurile agricole sau rezervele de apă.

---

* Michael Andregg este profesor în cadrul Departamentului de Studii de Pace și Justiție al Universităţii St. Thomas din St. Paul, Minnesota, SUA.

Schimbarea climatică este un factor derivat, determinat de creşterea populaţiei şi dezvoltarea industrială. Siria a experimentat cea mai mare perioadă de secetă din ultimii 150 de ani (potrivit istoriei înregistrate cu privire la ploile care au avut loc acolo), care a durat 4 ani de zile înainte de izbucnirea conflictului. Conform rapoartelor Băncii Mondiale, cel puţin 1,5 milioane de cetăţeni sirieni (8% din populaţia Siriei) au părăsit zonele rurale neproductive şi s-au mutat în oraşe deja supraaglomerate cu milioane de şomeri tineri (Liverani, 2015). Surse locale mi-au putut oferi chiar mai multe informaţii, conform acestora, migranţii interni au blocat oportunităţile pentru adolescenţii din oraşele în care s-au stabilit. Un alt efect al ratelor crescute ale natalităţii este reprezentat de distribuţia piramidală a vârstelor, cu o discrepanţă foarte mare între tineri (majoritari) şi bătrâni.

Assad a rezervat cele mai bune oportunităţi pentru alegătorii săi Alawiţi şi pentru minoritarii aliaţi, precum creştinii. Proteste paşnice s-au declanşat în oraşele lipsite de oportunităţi sau caracterizate de un nivel ridicat al fenomenului corupţiei. Răspunsul instituţiilor de securitate a fost unul exagerat, acest lucru transformând represiunile în război civil. Chiar dacă Bashar al-Assad a fost considerat un înger al lui Dumnezeu (sau un prizonier al *status-quo-ului*), acesta a trebuit să se confrunte cu o problemă primejdioasă din punct de vedere moral.

Prinşi, pe de o parte, între bombe improvizate, atacuri cu arme chimice şi recrutări forţate, şi între ISIS sau Al Qaeda pe de altă parte, milioane de cetăţeni sirieni au plecat în ţări precum Turcia, Liban sau Iordania, exercitând o presiune foarte mare asupra acestora: peste 4 milioane, iar alte 8 milioane erau dislocate intern (UNHCR, 29 August 2015). În timp, cei mai bogaţi, mai educaţi şi cu simţ antreprenorial au decis că o viaţă în tabăra de refugiaţi nu este potrivită pentru copiii lor. Aşa că ceea ce era un pârâu de migranţi în Europa s-a transformat într-un râu. Atunci când Angela Merkel a anunţat că Germania va primi sute de mii de refugiaţi, râul a devenit un flux (Wagstyl, 2015). Situaţia nu se va termina curând, iar aceasta nu este doar o problemă a Germaniei sau a Europei. Pentru o perioadă lungă de timp, America de Nord s-a confruntat cu valuri mari de imigranţii proveniţi din regiunile de sud, motiv pentru care politicile SUA în acest domeniu au fost înghețate.

Următoarele secţiuni ale lucrării vor furniza mai multe detalii cu privire la câţiva dintre aceşti factori. Însă ideea principală trebuie menţionată încă de pe acum şi se referă la soluţii. Este vorba de „soluţii" la crize de acest gen, pentru care nu avem o confirmare foarte bună a cauzelor determinante cum ar fi:

a) presiunea populaţiei;

b) schimbările climatice;
c) legile autoritare;
d) religie militantă;
e) actele de corupţie la nivel guvernamental;
f) inegalităţi la nivelul și între naţiuni în termeni de câștiguri salariale și
g) puterea specială a demagogilor de a mobiliza, în asemenea condiţii, populaţia disperată prin direcţionarea mâniei acestora asupra altor persoane ușor identificabile;
și care nu vor înregistra succes.

Această situaţie va fi o problemă generaţională cu consecinţe considerabile asupra întregii lumi. La toate acestea se adaugă armele de distrugere în masă și tabuurile în ceea ce privește discuţiile legate de majoritatea acestor factori, în final obţinându-se ceea ce poate fi numit o problemă „primejdioasă”[1].

Creșterea populaţiei, presiunea populaţiei și schimbările climatice

Creșterea populaţiei și presiunea populaţiei sunt două noţiuni diferite, însă ambele conduc la o competiţie mai accentuată asupra resurselor. Dacă resursele se împuţinează, unii oameni tind să intre într-o luptă pentru a obţine acces la acestea. Dacă resurse critice se împuţinează considerabil, majoritatea persoanelor se vor implica în războaie împotriva celorlalţi alături de grupul din care fac parte. Dacă foametea este iminentă, chiar și persoanele „civilizate” și sofisticate ar putea lupta pentru pâine, sau ar fura-o de la vecinii mai bogaţi. Schimbările climatice sunt un factor derivat, o consecinţă a secolelor caracterizate de creșterea populaţiei și a folosirii cu preponderenţă a combustibililor fosili pentru funcţionarea sectorului energetic al societăţilor. A devenit foarte clar că nivelurile ridicate de dioxid de carbon din aer, precum și a altor produse secundare obţinute prin arderea petrolului, cărbunelui, gazelor și pădurilor cauzează creșteri semnificative ale temperaturilor globale, care au alte consecinţe asupra populaţiilor marginale și chiar asupra sistemelor care susţin întreaga omenire.

Numărul de persoane care pot prospera pe un anumit teritoriu depinde de tehnologia de care acele persoane dispun și de calitatea acelui pământ. Creșterea populaţiei este aritmetică simplă, numere absolute ce caracterizează populaţia, ratele natalităţii, ratele mortalităţii, ratele fertilităţii, dublarea timpului, migraţia netă și alte asemenea numere (Andregg, 2014). O societate

[1] Pentru mai multe detalii privind termenul de „problemă primejdioasă” vezi https://en.wikipedia.org/wiki/Wicked_problem.

high-tech stabilită pe un pământ fertil poate susţine mult mai multe persoane care pot fi hrănite pe un pământ identic, dar cu o agricultură specifică secolului al XIX-lea. Astfel, **presiunea populaţiei** implică factori economici, tehnici şi culturali printre mulţi alţii. Indiferent cât de fertil este, fiecare tip de pământ are limitele sale şi nu poate susţine productivitatea la nesfârşit. Dar societăţile rezistă, de obicei, în faţa acestei legi de bază a naturii. Dacă o societate continuă să crească o dată ce aceste limite au fost atinse, atunci există o creştere a presiunii unor persoane aparţinând societăţii de a se extinde pe terenurile vecine, sau pur şi simplu să se mute acolo. Deşi este vast, pământul are un sfârşit. Şi fiecare cultură de pe pământ se teme să nu fie copleşită de migranţi, deoarece acest lucru s-a mai întâmplat de multe ori în istorie.

Schimbarea climatică joacă un rol important astăzi deoarece există deja un număr de 60 de milioane de refugiaţi permanenţi, majoritatea dintre care au plecat ca urmare a conflictelor violente în desfăşurare în ţările lor de origine (Mocanu, 17 Octombrie, 2015). Sute de milioane de oameni se află acum în mişcare, migranţi de un fel sau altul. Rapoarte precum raportul anual al Grupului Interguvernamental privind Schimbările Climatice (IPCC, 2014) arată că pe măsură ce seceta şi inundaţiile se vor manifesta la nivelul mai multor state, furtunile vor deveni, în medie, din ce în ce mai puternice, iar oceanele nu doar se vor acidula ca urmare a absorbţiei de dioxid de carbon, ci vor creşte pe măsură ce gheţarii şi gheaţa polară se vor topi. Aceste lucruri au un impact vast asupra securităţii internaţionale. Siria este un exemplu.

Legi autoritare şi religie militantă

Legea autoritară nu este acelaşi lucru cu religia militantă, dar ambele contribuie la creşterea probabilităţii declanşării unui conflict armat în diverse moduri. Cel mai important, acestea reacţionează sinergetic, astfel că în combinaţie sunt mult mai periculoase decât separat. Am tratat acest subiect în detaliu într-o carte despre cauzele războiului din 2001 (Andregg, 2001, cap. 13, pp. 74-83), dar esenţa este reprezentată de faptul că legea autoritară oferă mijloacele necesare pentru represiunea politică sau cucerirea, cu sau fără justificare, în timp ce religia militantă oferă raţiuni „morale" pentru utilizarea violenţei statale împotriva altora. În acest sens poate fi folosit drept exemplu curent şi extrem gruparea teroristă ISIS. Dar au existat în istorie multe alte cruciade morale împotriva altor grupuri desemnate, bazate pe o teorie religioasă (de exemplu, islamiştii adesea subliniază „cruciadele" medievale „de eliberare" a Ierusalimului care au avut loc în secolele XI-XIII.

În cazul crizei din Siria, guvernul lui Bashar al-Assad a fost autoritar tot timpul (tatăl său Hafez a omorât în mod infam aproximativ 20 000 de persoane

în Hama în luna februarie a anului 1982, deoarece s-au opus legii impuse de acesta). Acea legea autoritară a legitimat violenţa și a contribuit la finanţarea poliţiei înarmate și a soldaţilor care au reprimat protestele din 2011. După ani de abuz, ISIS și-a făcut apariţia pe baza principiului religiei militante, afirmând că regimul a reprezentat un agent al Shaytan (diavolului) și că „musulmanii buni" au responsabilitatea de a ataca acel regim. Iar dacă tu eşti musulman, dar nu eşti de acord, atunci tu devii un musulman „rău", condamnat la execuţie. Nu există o cale de mijloc pentru ISIS; eşti fie cu ei, fie împotriva lor, dar nu poţi fi neutru. Actualul lider al ISIS, Abu Bakr al-Baghdadi, duce acest obiectiv și stil la extrem, afirmând că a primit de la „Dumnezeu" misiunea de a conduce pe oricine de pe pământ sub un „nou Califat".

Oricare dintre aceşti doi factori este periculos. Dacă sunt puşi împreună, se vor obţine reacţii intense, ca atunci când amesteci sodiu și apă, deoarece atât legea autoritară, cât și religia militantă tind să fie **unicul** utilizator legitim al metodelor violente. Aceşti doi factori nu se pot tolera, iar persoanele care trăiesc pe teritoriul unor state conduse de oameni cu asemenea convingeri sunt mereu în pericol. Cea mai periculoasă dintre toate este situaţia în care fanatismul moralei religioase și puterea politică autoritară fuzionează. Acei dictatori consideră că sunt trimişii lui Dumnezeu pentru a conduce pământul. Astfel de persoane nu cunosc ruşinea în a-i abuza pe alţii pentru „a îndeplini voia lui Dumnezeu".

Acest lucru creează un mediu propice pentru apariţia aşa-numiţilor „demagogi", un tip periculos de personalitate politică. Voi acoperi acest subiect pe scurt în secţiunea care urmează după capitolul referitor la actele de corupţie la nivel guvernamental.

Acte de corupţie la nivel guvernamental și inegalitatea veniturilor

Actele de corupţie de la nivelul guvernelor se manifestă încă de la începutul timpului, dar se află printre cele mai puţin studiate cauze primare ale unui război. Motivul principal pentru care se întâmplă acest lucru este reprezentat de faptul că majoritatea fondurilor destinate cercetării în ştiinţele sociale provin de la guverne, ai căror membri nu sunt încântaţi de faptul că oamenii studiază corupţia de nivel guvernamental. În contextul subiectului tratat de acest articol, acest factor este important deoarece împiedică multe guverne să rezolve problemele evidente și uneori chiar letale pentru propriul popor.

Inegalitatea veniturilor este de asemenea o problemă globală și continuă, specifică, în mod evident războaielor civile care predomină astăzi. Cazul Siriei este, de fapt, un exemplu minor al unei probleme globale. În general, probabilitatea izbucnirii unui conflict creşte direct proporţional cu creşterea

inegalităţii veniturilor, în interiorul şi între naţiuni. Aceste subiecte sunt complexe pentru a fi doar trecute în revistă, motiv pentru care le voi ilustra pe scurt pentru a scoate în evidenţă modul în care ambii factori influenţează actorii externi, prin analizarea răspunsului Statelor Unite la criza siriană.

Pe măsură ce războiul civil din Siria a escaladat şi a intrat în metastază, Statele Unite s-au întrebat ce ar trebui să facă. Însă cadrul său de referinţă pentru a înţelege conflictul a trebuit să fie de natură militară. Şi ca urmare a propriilor dinamici ale politicii interne, a trebuit să se concentreze mai degrabă asupra personalităţilor lui Bashar al-Assad şi Abu Bakr al-Baghdadi, decât asupra forţelor impersonale precum creşterea populaţiei, schimbările climatice sau corupţia sistemică de la nivel guvernamental. Astfel, în locul abordării acelor probleme scumpe şi dificile, întrebarea practică a fost dacă trebuie bombardate ţintele, şi dacă da, atunci care dintre ele?

De fapt, negarea realităţii referitoare la schimbările climatice (încurajată de investiţiile unor mari sume de bani şi influenţată de companiile producătoare de combustibili fosili) a ajuns la un nivel foarte ridicat în momentul în care lucrurile s-au destrămat în Siria, astfel încât majoritatea membrilor din cadrul unuia dintre cele două partide politice principale nu considerau schimbările climatice ca fiind o problemă, în ciuda unui raport al Pentagonului din anul 2003 care menţiona faptul că schimbările climatice vor avea consecinţe dramatice asupra securităţii naţionale şi internaţionale (Schwartz & Randall, Octombrie 2003). Astfel de parlamentari au preferat să creadă că Siria este o problemă de natură militară cauzată de unul sau mai mulţi lideri diabolici din ţări străine. Aceştia nu au luat în considerare faptul că răspunsurile militare, în special bombele, nu au niciun efect pozitiv asupra schimbărilor climatice şi nicio evaluare terapeutică atunci când sunt folosite asupra valurilor mari de migranţi sau guvernelor corupte. Ei preferă poveştile simple despre bine şi rău. Între timp, eşecul politicii Statelor Unite se adaugă la statele eşuate din Orientul Mijlociu, pe când forţe ale rebeliunii tribale împotriva guvernelor corupte capătă din ce în ce mai multă putere. Zeci de milioane de bărbaţi adolescenţi care nu au beneficiat de o educaţie corespunzătoare se maturizează acum în circumstanţe disperate, demagogii fiind nerăbdători în a le îndrepta ura în direcţia pe care ei o doresc.

Demagogi, psihopaţi şi arme de distrugere în masă (ADM)

La fel ca în cazul secţiunilor precedente, conceptul de demagog nu este identic cu cel de psihopat, însă ambii factori sunt comuni politicilor de vârf şi reprezintă un risc pentru societatea politicoasă, deoarece ei se manifestă de-o manieră veritabilă asemeni unor paraziţi pentru o societate. Ambii factori sunt adepţii manipulării oamenilor creduli şi nemiloşi în metodele pe care le

utilizează. Nu produc nimic de valoare prin acţiunile lor, dar, de regulă, îndreaptă furia persoanelor disperate asupra unor alte „persoane" uşor identificabile, de cele mai multe ori fie asupra unei minorităţi etnice, fie asupra unui grup religios. În statele în care guvernele sunt corupte, acestea devin cele mai bune ţinte. În momentul în care un demagog sau un psihopat acaparează puterea unei naţiuni majoritare, ţintă devin naţiunile vecine sau ceea ce poate fi numit simbolic „cea de-a cincea coloană", așa cum au fost evreii pentru Germania lui Adolf Hitler.

Cea mai bună referinţă pe care o cunosc în domeniul răului psihologic în politicile de vârf este foarte dificil de lecturat, dar o voi cita, totuși, datorită caracterului special al sursei înseși. Lucrarea a fost redactată de sociologii și psihiatrii din Polonia care au supravieţuit nu doar ocupaţiei naziste, ci și procesului de „liberare" și ulterior de subjugare desfășurat de forţele sovietice la sfârșitul celui de-al doilea Război Mondial. Din acest motiv, aceştia au fost extrem de motivaţi în a înţelege modul în care forţe malefice pot ocupa naţiuni întregi. Titlul acestei lucrări este „Political Ponerology", iar autorul este Andrew M. Lobaczewski, care a murit în anul 2007 (Lobaczewski, 2008)[2].

Armele de distrugere în masă sunt, așa cum spune și titlul, arme și nu oameni. Însă joacă un rol foarte important în acest context, deoarece orice psihopat din lume și-ar dori să aibă la dispoziţie arme de distrugere în masă. Una dintre caracteristicile principale ale persoanelor într-adevăr malefice, indiferent de modul în care acestea sunt numite sau clasificate, este reprezentată de dorinţa necumpătată de a obţine mai multă putere (Peck, Simon & Schuster, 1983). Nu există nicio limită naturală pentru acest apetit. Așa cum afirmă Kevin Dutton (2012), psihopaţii dezvoltă cariere de succes atât în domeniul politicilor de vârf, cât și în cel industrial, datorită capacităţii lor de concentrare, gradului ridicat de inteligenţă, abilitatea dezvoltată de a manipula oameni „obișnuiţi" și a indiferenţei generale vizavi de normele morale, în special interdicţiile cu privire la acţiuni care afectează individul. Psihopaţii clinici tind să nu manifeste empatie, să fie lipsiţi de compasiune și posibil chiar și de conștiinţă.

---

[2] Lucrarea originală a apărut în limba poloneză, în 1984, fiind tradusă în engleză în 1985 de Alexandra Cheiuk-Celt și corectată chiar de autor în 1998. Patocraţie este un termen folosit pentru a descrie un stat-naţiune intrat sub influența, și în genere distrus, de un lider psihopatic. Lobaczewski a susținut întotdeauna că acest volum a fost scris împreună cu alți colaboratori, specialiști în științe sociale și psihiatrie din Polonia, care, fiind treptat reabilitați de sistemul sovietic, încercau să-și exprime ideile.

În cazul Siriei, nu poate fi nicio îndoială că Abu Bakr al-Baghdadi este un demagog, posibil un lider psihopat al unui cult al morţii, care a ajuns la putere pe baza haosului general ce caracterizează statul eşuat Irak şi a situaţiei similare din Siria, care a devenit principala lui sursă de putere. Bashar al-Assad a răspuns la acţiunile întreprinse de ISIS, însă cine a fost primul dintre cei doi care au omorât primii oameni nevinovaţi rămâne o problemă mai degrabă academică decât practică. Dacă fiecare lider ar avea arme nucleare sau alte tipuri de arme de distrugere în masă, atunci le-ar folosi împotriva inamicilor. Acest aspect a atras atenţia acelor entităţi care au arme nucleare și alte arme de distrugere în masă.

Concluzii

În opinia mea, fluxul curent de migranţi/refugiaţi care se îndreaptă către Europa nu este temporar și nu se va sfârși nici dacă, teoretic vorbind, condiţiile din Siria s-ar îmbunătăţi miraculos peste noapte. Ar fi extraordinar dacă s-ar putea stabili pacea în acea regiune, la fel ca în orice altă regiune caracterizată de conflict, dar problema este că situaţia din Siria este un fenomen global determinat, în mod fundamental, de rata crescută a natalităţii la nivelul populaţiei care locuieşte în regiuni care sunt în cea mai mare parte deşertificate. De fapt, sute de milioane de tineri sunt exploataţi de demagogi care le promit o răsplată fantastică pentru a lupta, iar uneori le oferă salarii semnificative pe care le vor primi doar dacă mai trăiesc. Aceste condiţii nu se aplică doar asupra Siriei, ci și în regiuni întinse din Africa de Nord și Orientul Mijlociu, pe lângă multe alte locuri. Toate aceste regiuni generează migranţi care se mută în funcţie de oportunităţile oferite de fiecare zonă la gândul unui viitor mai bun.

Să ne gândim pentru un moment că America de Nord s-a confruntat, de asemenea, cu două generaţii de migraţii legale și ilegale din Mexic și America Centrală. Aceste migraţii nu au nicio legătură cu situaţia actuală din Siria, iar majoritatea migranţilor provin din regiuni care nu s-au transformat încă în deșerturi neproductive, deoarece pământul de obicei reuşeşte să facă faţă unei suprapopulări pentru o perioadă lungă de timp. Însă toţi migranţii sunt în căutarea oportunităţilor, iar cei mai mulţi fug din regiuni caracterizate de violenţă, corupţie sau asuprire.

Doresc astfel să atrag atenţia lumii asupra acestor factori mult mai dificili: presiunea populaţiei, legile autoritare, religia militantă și corupţia la nivel guvernamental, demagogi sau lideri psihopaţi, precum și asupra varietăţii de factori derivaţi, precum schimbările climatice și inegalitatea veniturilor.

În domeniul medical, dacă sunt căutate tratamente pentru probleme majore, este necesară o distincţie clară între conceptul de „simptom" şi „cauză". Da, simptomul este un apel pentru ajutor. Dar dacă un doctor tratează doar simptomul și neglijează cauza, cum ar fi o febră cauzată de o infecţie, poate stabiliza pacientul și îi poate reduce durerea, însă, în acelaşi timp, îl va urmări cum moare. Migrarea în masă din Siria din anul 2015 este similară cazului descris mai sus, fiind un simptom al unei probleme mult mai complexe. Mai mult, să nu uităm că zecile de milioane de persoane care se află astăzi în mişcare nu provin doar din Siria.

Aşadar, Europa, asemeni Americii de Nord, poate absorbi în mod productiv un număr mare de migranţi și poate ajuta mult mai mulţi refugiaţi din motive umanitare, lucru pe care îl susţin. Dar nu trebuie pierdute din vedere cauzele fundamentale ale crizei specifice regiunilor de provenienţă ale migranţilor, deoarece niciun stat nu poate absorbi un număr nelimitat de migranţi fără a suferi efecte adverse. Ajutorul oferit acum refugiaţilor nu face nimic altceva decât să cumpere timpul necesar pentru tratarea cauzelor fundamentale. Dar dacă acest timp nu este folosit eficient, iar statele eşuează în a recunoaşte și încerca să trateze cauzele principale, ajutorul va fi doar temporar, în timp ce ţările de origine ale migranţilor vor fi distruse de haosul care continuă să le macine.

Referinţe bibliografice:

1. CIA World FactBook, 2010, demographics of Syria retrieved from https://www.cia.gov/library/publications/download/download-2010.
2. Liverani, Andrea, 21 October, 2015, accessible at: http://blogs.worldbank.org/ peoplemove/syrian-refugee-cop21.
3. *United Nation High Commissioner for Refugees, 29 August 2015,* retrieved from *UNHCR Syria Regional Refugee Response/Total Persons of Concern".*
4. Wagstyl, Stefan, 14 September 2015, *Merkel's Welcome to Refugees Comes Back to Bite Her*, in „Financial Times", accessible at: http://www.ft.com/intl/cms/s/0/ 60264684-5af4-11e5-a28b-50226830d644.html#axzz3rDj8NNF.
5. Andregg, Michael (2001) *On the Causes of War*, 3rd edition, published by Ground Zero Minnesota.
6. Andregg, Michael, (2014) *Seven Billion and Counting: The Crisis in Global Population Growth*, Twenty-First Century Press (an imprint of Lerner Books).
7. Mocanu, Mircea, (17 October 2015), *Valuing Migration: Benefits and Challenges*, in a paper presented at the 21st annual Conference

Information in the Knowledge Society, at Romania's „Mihai Viteazul" National Intelligence Academy, Bucharest.

8. The UN affiliated Intergovernmental Panel on Climate Change Report (2014), available at: http://www.ipcc.ch/report/ar5/syr/.
9. Schwartz, Peter, Randall, Doug (October 2003) The "Marshall Report" or "An Abrupt Climate Change Scenario and Its Implications for United States National Security", commissioned by Pentagon Strategic Forecasting guru Andrew Marshall available at: http://www.climate.org/PDF/clim_change_scenario.pdf. A good summary of this report's implications can be found at the History Commons, accessed on 11 November, 2015 at: http://www.historycommons.org/context.jsp?item= PentagonClimateChangeReport.
10. Lobaczewski, Andrew M. (2008) *Political Ponerology: A Science on the Nature of Evil Adjusted for Political Purposes*, Red Pill Press, Edmonton Canada, Peck, Scott M., Simon & Shuster (1983) *People of the Lie: The Hope for Healing Human Evil*.
11. Dutton, Kevin, (2012), *The Wisdom of Psychopaths: What Saints, Spies, and Serial Killers can teach us about Success*, Scientific American Press/Farrar, Straus and Giroux.

TERORISMUL SERVIND SCOPURI GEOPOLITICE. CONFLICTUL RUSO-UCRAINEAN CA EXEMPLU AL DOCTRINEI LUI ALEKSANDR DUGIN ŞI CONCEPTULUI LUI EVGENY MESSNER DE „RĂZBOI REBEL"

Michal WOJNOWSKI*

Without geopolitics it is not possible to understand the events in Ukraine – every attitude excluding that is doomed to an immediate failure.

(Aleksandr Dugin, 14 martie 2014)

Every man, whether a serviceman or a civilian, takes part in the information warfare no matter of its form.

(Gen. Vladimir Markomienko, 2000)

Abstract

Defining the interests of the state in reference to its geographical location is the key element to understanding political actions being taken by the Russian Federation in an international domain.

The geographical location of Russia has been influencing for centuries the way of perceiving the world by the Moscow leadership elites. Starting in the 16th century they have been forced to pursue their policy in three main directions: The Western one (from the Baltic Sea to theCarpathian Mountains), The Southern one (from the Danube River to Persia) and The Eastern one (from the Volga River to the Altai Mountains).

Keywords: state interest, geographical location, Dugin, geopolitical doctrine.

Introducere

Definirea intereselor unui stat, în raport cu localizarea sa geografică, este elementul cheie necesar înţelegerii deciziilor şi acţiunilor politice ale Federaţiei Ruse în mediul internaţional. Esenţa acestui fapt este subliniată de viziunea filosofului ortodox Nikolai Bedryaev (1874-1947), care vorbea despre „puterea spaţiului asupra sufletului rus". Acesta afirma că ruşii nu posedă limitarea Europei, care îşi concentrează energia într-un spaţiu restrâns al *sufletuluilor, nici nu posedă prudenţă, economia spaţiului şi timpului şi intensitatea culturii* (Бердяев, 1990, p. 64). Aşezarea geografică a Rusiei a influenţat de secole modul în care elita rusească percepe lumea. Începând cu secolul 16 au fost forţaţi să urmărească atingerea obiectivelor politice proprii pe trei direcţii principale: zona occidentală (de la Marea Baltică la Munţii Carpaţi), zona sudică (de la Dunăre la Persia) şi zona estică (de la fluviul Volga la Munţii Altai). De aceea au încercat în permanenţă să rămână activi în toate

* Serviciul Intern de Securitate Polonia.

cele trei regiuni simultan, fapt ce solicită atât un grad ridicat de consolidare internă a statului, cât și centralizarea autorităţilor guvernamentale (Le Donne, 2004, pp. 15-38; Nowak, 2008, pp. 13-24). Mai mult decât atât, localizarea în areale geografice deschise a generat o frică constantă faţă de pericolul extern ce a determinat o tendinţă de garantare a securităţii prin implementarea de acţiuni preventive și ofensive. Este necesar să subliniem că actuala politică externă a Rusiei relevă o activitate intensificată în următoarele regiuni geostrategice: din Balcani, prin bazinul Mării Negre (Transnistria, Crimeea), prin Caucaz, bazinul Mării Caspice, până la Asia Centrală și Sakhalin și zona Arctică (*Russia between East and West*, 2003; Grachev, 2005, pp. 255-275; Wiśniewski, 2013, pp. 365-385). Conform afirmaţiilor unor membri ai elitei ruse, noua reconfigurare a graniţelor, urmare a dizolvării Rusiei Sovietice, nu este favorabilă, prin comparaţie cu perioadele istorice precedente. Reflecţiile asupra acestor consecinţe geopolitice ale evenimentului sunt încă actuale la nivelul opiniei elitei politice conducătoare din Rusia, dar și la nivelul mentalului colectiv al societăţii civile ruse. De aici și sloganele politice ce fac referire la reconstruirea imperiului pierdut au avut un impact semnificativ în formularea politicii externe a Federaţiei Ruse, ceea ce înseamnă că probabilitatea de încălcare a legii internaţionale pentru raţiuni geopolitice și geostrategice este una destul de ridicată (Grabowski, 2011, pp. 21-22; Кириллов și Крючков, 2008, pp. 10-21). Implicarea Rusiei în conflictele armate ce au avut loc după 1991 vine să confirme această ipoteză. Este necesar să menţionăm că aceste conflicte au fost condiţionate, inter alia, de locaţiile geografice ale teritoriilor vecine statelor ex-sovietice, în special acelea cu structuri etnice, sociale și religioase variate, acest aspect având o semnificaţie deosebită în cazul anexării Crimeei și a evenimentelor ce au avut loc în vestul Ucrainei (Grabowski, 2011, p. 38; Эллисон, 2005, pp. 147-191).

Prin urmare, nu este surprinzător că geopolitica în Rusia este înţeleasă ca strategie politică aplicată și în relaţiile internaţionale (Колосов, 1996, p. 86; Колосов și Мироненко,, 2001, pp. 9-29). Mai mult, geopolitca în Rusia actuală a căpătat statutul unei viziuni generale asupra lumii, un concept universal pe baza căruia se formulează viziuni globale și atitudini la nivel internaţional (Косолапой, 1996, pp. 57-61; Marciniak, 2004, pp. 4-13; Mäkinen, 2008, pp. 34-49; Isakova, 2005, pp. 10-23). Un exemplu relevant în acest sens, ce confirmă această opinie, este oferit de Valery Korovin – Directorul Centrului pentru Expertiză Geopolitică, ce oferă sprijin Șefului Dumei rusești, un activist proeminent al mișcării neo-eurasianistă. Afirmaţiile sale, publicate în jurnalul „Izwiestija" (rusă:«Известия») conţin informaţii precise referitoare la scopurile și metodele politicii externe rusești în raport cu Ucraina, dar și în context global. Valery Korovin s-a distanţat de moștenirea ideologică a Rusiei

Sovietice, criticându-i liderii pentru *ideologizarea politicii externe*. A subliniat faptul că *metoda geopolitică* aplicată pentru a stopa colapsul rusesc a fost recunoscută ca bază a strategiei de securitate doar după ce Vladimir Putin a venit la putere în Federația Rusă. Potrivit lui Korovin, principalul obiectiv al politicii externe ruseşti ar trebui să fie limitarea influenței „Blocului Atlantic" (Statele Unite ale Americii și Uniunea Europeană) prin crearea unui model de securitate globală, regională și subregională. Acest scop ar trebui să fie atins prin includerea statelor și naţiunilor ce au făcut în trecut parte din spaţiul rusesc (apropiate Rusiei la nivel de civilizaţie și cultură) pe orbita polului geopolitic eurasianist.

Conform lui Korovin, acest proces ar trebui realizat într-o manieră similară procesului de anexare a Crimeei, pe care acesta l-a interpretat ca fiind *susținerea soluționării pașnice a conflictelor regionale și locale.* Mai mult, în opinia lui Korovin, *metoda geopolitică* ar trebui să reprezinte baza tuturor acţiunilor viitoare ale Ministerului Apărării, Ministerului de Interne și Serviciului Federal de Securitate, pentru a neutraliza orice ameninţare de natură a prejudicia securitatea naţională (Коровин, 24 IV 2014; Пустошкин, 1976, pp. 521-522; Grygajtis, 2011, pp. 10-18). Afirmaţia citată relevă faptul că acest conflict ruso-ucrainean reprezintă o etapă a implementării doctrinei politice extinse ce vizează reintegrarea strategică a spaţiului post-sovietic și în perspectivă, construirea așa-zisei lumi multipolare. Autorul acestui concept este Aleksandr Dugin – un intelectual reprezentativ și teoretician al geopoliticii ruse și euroasianismului. Baza mișcării eurasianiste, renăscută graţie lui Dugin, este o luptă constantă pentru putere asupra spaţiului dintre state, blocuri politico-militare, organizaţii internaţionale și civilizaţii (Vezi detalii la Kerr, 1995, pp. 977-988; Smith, 1999, pp. 481-494; O'Loughlin, Toal, Kolossov, 2005, pp. 322-335). Aleksandr Dugin a pretins întotdeauna că ideologia eurasianistă anti-occidentală și geopolitica academică servesc obiectivele imperialiste ruse importante, pe termen lung. Din punctul său de vedere, geopolitica este:

> (...) viziunea globală asupra puterii, educaţia despre putere și pentru putere (...). Geopolitica este disciplina elitelor politice, atât a celor reale, cât și a celor alternative; istoria sa demonstrează că este în apanajul exclusiv al oamenilor implicaţi activi în guvernarea naţiunilor și statelor sau a celor ce se pregătesc în acest sens (...). În prezent, reprezintă cartea puterii, ce ar trebui luată în considerare când se discută despre decizii globale (importante), precum alianţe, războaie, reforme, restructurări ale societăţii, aplicarea de sancţiuni economice și politice pe scară largă (Дугин, 1997, pp. 13-14).

Interpretarea definiţiei de mai sus, dată de Dugin, relevă faptul că geopoliticareprezintă o viziune subiectivă asupra spaţiului, împământenită în conştiinţa unei anumite societăţi sau a anumitui mediu politic. Este rezultatul unui calcul al intereselor şi scopurilor politice, raţional şi subiectiv, dar şi al factorilor culturali (experienţa istorică, miturile naţionale etc.). Aceste elemente influenţează semnificativ activitatea unui anumit subiect, care în speţa de faţă este practica politică (Potulski, 2010, pp. 9-10; Tuathail, 1998, pp. 16-39; Lashchenova, 2013, pp. 110-118; Ambrosio, Vandrovec, 2013, pp. 435-466).

Conform cercetătorilor contemporani, Aleksandr Dugin este reprezentativ pentru mediile politice în care se susţine ideea restaurării Imperiului Rus. Această idee a devenit motivul primordial al activităţii sale politice, ştiinţifice şi jurnalistice. Poziţia înaltă pe care o ocupă în cadrul elitei politice apropiate a lui Putin este general cunoscută. Dugin a afirmat oficial că a pregătit o serie de proiecte geopolitice acreditat de către autorităţi (Дугин, 2014). Este deseori ilustrat în mass-media ca fiind un expert sau un comentator al evenimentelor politice curente. Un factor important în biografia lui Aleksandr Dugin îl reprezintă relaţia pe care o are cu reprezentanţii de nivel înalt şi ai instituţiilor cu rol de implementare a legii. Pare evident că aceste legături i-au influenţat în mod semnificativ evoluţia profesională. Mai mult decât atât, iniţiativa sa a determinat crearea unor organizaţii politice şi sociale precum: Mişcarea Internaţională Eurasianistă (Международное Евразийское движение, МЕД), Uniunea Euroasiană de Tineret (Евразийский союз молодёжи, ЕСМ) şi „Clubul Izborski" (Изборский клуб). Aceste organizaţii reunesc experţi din diferite zone, precum şi persoane notabile din mediul politic şi cultural rus ce împărtăşesc viziunea lui Dugin (Dunlop, 2001, pp. 91-127; Umland, 2010, pp. 144-152; Wojnowski, 2014, pp. 11-38).

Principalul scop al cercetării de faţă este acela de a prezenta ipotezele referitoare la doctrina rusească faţă de Ucraina şi identificarea metodelor sale de implementare. În primul rând, este necesară evidenţierea relaţiei dintre doctrina geopolitică a lui Aleksandr Dugin şi anumite aspecte din ideologia politicii externe a Kremlinului – atât la nivel global, cât şi regional. Acesta este subiectul primei părţi a prezentei lucrări. În al doilea rând, este crucială definirea modalităţilor de realizare a politicii externe, la care, având în vedere opiniile lui Korovin, ne putem referi ca fiind „metoda geopolitică". În baza afirmaţiilor sale, putem considera că metodă geopolitică trebuie înţeleasă ca o serie de activităţi diverse de natură a sprijini atingerea doctrinei politice. Aşa cum am menţionat anterior, Korovin sugerează că „metoda geopolitică" ar

trebui aplicată prioritar de către instituţii de aplicare a legii. Aşadar ar trebui avansată teza potrivit căreia „metoda geopolitică", dincolo de aspecte exclusiv militare, reprezintă totodată o paletă extinsă de activităţi asimetrice. Această definiţie face referire la metodele neconvenţionale ale războiului, precum activităţile teroriste, războaie de tip economic, informaţional şi psihologic (Wejkszner, 2009, pp. 120-121; Arreguin-Toft, 2005, pp. 1-48; Katz, 2013, pp. 77-85). De aceea, intenţia noastră este de a prezenta conceptul rus asupra activităţilor asimetrice, în care ar trebui inclus conceptul de „război rebel" (мятежевойна), fiind în prezent un element constitutiv al conceptului mai amplu „război informaţional" (информационная война). Una dintre întrebările care se ridică este în ce grad Rusia îşi îndeplineşte obiectivele geopolitice în Ucraina utilizând metodele şi mecanismele războiului rebel. Pentru a răspunde la această întrebare este necesară analogia dintre aspectele teoretice ale acestor activităţi şi practică, aspecte ce fac subiectul celei de-a doua părţi a acestui articol.

Teritoriul Ucrainei în doctrina geopolitică a lui Aleksandr Dugin şi a promotorilor săi

Punctul de pornire pentru înţelegerea importanţei acordate Ucrainei în doctrina geopolitică a lui Aleksandr Dugin se regăseşte în lucrarea fundamentală a acestuia intitulată „Bazele geopoliticii. Viitorul geopolitic al Rusiei". Această carte remarcabilă, atât sub aspectul formei, cât şi al conţinutului, a fost publicată în 1997. Merită subliniat că generalii şi strategii Academiei Militare a Centrului Forţelor Militare ale Federaţiei Ruse (Военная академия Генерального штаба Вооружённых сил Российской Федерации) au participat la crearea ei. Cartea prezintă doctrina geopolitică, prin care se urmăreşte reconstrucţia imperiului pierdut, comparabil Rusiei Sovietice. În prezent, cartea reprezintă poziţia geopolitică primordială, fiind obligatorie în universităţile şi academiile militare. A obţinut popularitate atât pe teritoriul Rusiei, cât şi în afară, devenind o doctrină ce nu poate fi ignorată în analiza relaţiilor inter-statale. Ideile propuse de autor sunt susţinute de un număr mare de cetăţeni ruşi. Mai mult decât atât, conţinutul cărţii constituie fundamentul pentru următoarele scrieri ale lui Dugin, precum şi pentru programele partidelor politice şi organizaţiilor înfiinţate la iniţiativa sa (Dunlop, 2001, pp. 93-94; Eberhardt, 2010, p. 236; Дугин, 2011 şi 2012).

Cea mai importantă sarcină stabilită de Dugin pentru naţiunea rusă este crearea unui imperiu continental puternic. Primul pas pentru obţinerea supremaţiei globale ar trebui să fie integrarea strategică a teritoriilor exsovietice şi crearea unei Uniuni Eurasiatice, care ar deveni echivalentul

geopolitic al Rusiei Sovietice (Дугин, pp. 170-175; Дугин, 2002, pp. 781-787). Una dintre condiţiile de bază pentru atingerea acestui obiectiv este, inter alia, extinderea controlului strategic asupra teritoriului descris de Dugin ca „Sudul Rusesc" (русский Юг), și anume teritoriile localizate în partea de nord a Peninsulei Balcanice din Serbia în Bulgaria, Moldova, sudul și estul Ucrainei, Rostov, Krasnodar Krai, Caucazul, estul și nordul coastei Mării Caspice, Asia Centrala (Kazakhstan, Uzbekistan, Kirgistan, Tajikistan), precum și Mongolia, Tibet și Manciuria. Dominaţia asupra acestor teritorii reprezintă doar o fază intermediară a expansiunii teritoriale către sud și către „ape calde". Conform lui Dugin, întreprinderea unei asemenea acţiuni este crucială pentru securitizarea frontierelor ruseşti. Din punctul său de vedere, abandonarea acestor teritorii într-un „vid geopolitic" ar putea crea posibilitatea ca acestea să fie incluse în zona de influenţă Atlantică. Teritoriul „de sud al Rusiei" este abordat de Dugin ca fiind principala platformă de confruntare între Federaţia Rusă și lumea „Atlantică", locul în care este hotărât destinul viitorului imperiu (Дугин, pp. 340-345). Cu toate acestea, stabilirea unei noi ordini geopolitice în această parte a lumii nu este posibilă fără reglementarea situaţiei statalităţii Ucrainei. Din punctul său de vedere, preluarea controluui asupra Ucrainei va permite Moscovei o expansiune continuă către vest și sud. Controlul asupra zonei de sud-est a Ucrainei ar asigura Rusiei o graniţă inviolabilă, și anume coasta de nord a Mării Negre. Acest fapt ar limita influenţa Turciei „Atlantice", al cărui principal obiectiv este, în concepţia lui Dugin, realizarea unui proiect geopolitic turanist – ideea de reunire a naţiunilor turce, în mod special a celor din Kazakhstan, Tatarstan și Republica Sakha (Yakutia), care ar fi o ameninţare evidentă la adresa Uniunii Eurasiatice (Дугин, pp. 347-349, 356; Сотниченко, 2011, pp. 4-14; Сотниченко, 2011a, pp. 141-149; Telkin și Williams, 2011, pp. 145-186).

Obţinerea controlului asupra Ucrainei de Vest va constitui primul pas pentru decompunerea așa-zisei „staţiei sanitare" (санитарный кордон). Această sintagmă, conform lui Dugin, se referă la statele localizate în partea estică a unei mici peninsule europene situată între Marea Baltică, Marea Adriatică și Marea Neagră. Această zonă are o importanţă strategică pentru securitatea Federaţiei Ruse. Pe de o parte o acestei zone de graniţă se află periferiile occidentale ale continentului Eurasian, iar pe celalaltă se află capătul podului operaţional al Atalnticului, subordonat imperiului atlantist – SUA. Diferenţele culturale accentuează diversitatea geopolitică a regiunii, având în vedere că „staţia sanitară" reprezintă însăși demarcaţia longitudinală etnico-religioasă între statele latine și moștenitoarele Imperiului Bizantin (Eberhardt, 2010, pp. 167-187).

„Staţia sanitară" include în principal Polonia, dar și Lituania, Letonia, Estonia, Ucraina de Vest, Ungaria, România, Republica Moldova, Republica Cehă și Slovacia. Dugin subliniază că principala caracteristică a politicii externe a acestor state este ostilitatea faţă de Rusia și Germania și serviabilitatea faţă de Statele Unite ale Americii. Existenţa acestei „staţii sanitare", care din perspectiva lui Dugin este o producţie geopolitică atlantistă, implementată la nivelul sistemului internaţional după sfârșitul Primului Război Mondial, este sursa conflictelor dintre Germania și Rusia. Mai mult decât atât, acest produs geopolitic împiedică realizarea unei uniuni între Imperiul Eurasian și așa-zisa Europa continentală, identificată de geopoliticieni ca fiind sub influenţa Germaniei. De asemenea, caracterul cultural diferit al statelor aflate în „zona sanitară" reprezintă un impediment pentru integrarea lor totală atât cu Estul, cât și cu Vestul. De aceea, este necesar ca Rusia să lichideze „staţia sanitară" printr-o reorganizare totală a graniţelor statelor din Europa Centrală și de Est. Noua ordine geopolitică nu ar trebui stabilită prin anexări teritoriale; în schimb, Dugin sugerează crearea mai multor federaţii alcătuite din regiunile caracterizate printr-o orientare geopolitică uniformă, ceea ce relevă abilitatea lor de a se integra sub aspectreligios, cultural, etnic și economic în Imperiul Eurasiatic sau în Europa continentală, aflată sub influenţa Germaniei (Дугин, pp. 368-370; Савин, 2011, pp. 225-235)[1]. Luând în considerare contextul religios (predominanţa influenţelor catolice și protestante), geopoliticianul rus consideră că următoarele state se află sub influenţa Germaniei: Polonia, Lituania, Letonia, Estonia, Republica Cehă, Slovacia, Ungaria, România, Slovenia, Croaţia, Bosnia și Herţegovina și partea Ucrainei cu majoritate greco-catolică, unde predomină un naţionalism ucrainian puternic. Celelalte teritorii ale Ucrainei ar trebui integrate în Federaţia Rusă. Alte state ale Europei de sud-est, unde majoritatea populaţiei aparţine cultului creștin ortodox, precum Serbia, Macedonia, România, Bulgaria, Republica Moldova, Grecia, precum și Albania majoritar musulmană, ar trebui, din punctul său de vedere, incluse în zona de influenţă rusă, care se întinde până la Marea Ionică (Дугин, pp. 219-228 și 224-226; Бовдунов, 2011, pp. 4-18; Eberhardt, pp. 228-232).

Divizarea Ucrainei, așa cum este sugerată de Dugin, este strâns corelată cu scenariul geopolitic mai sus-menţionat. Din punctul său de vedere, existenţa Ucrainei este inexplicabilă în sens geopolitic, iar soarta sa este determinată de numele statului, sinonim pentru graniţa regiunii de frontieră,

[1] Dugin susține că Belarus aparține acestei „stații sanitare" din cauza minorității catolice cu atitudine nefarorabilă Imperiului Euroasiatic.

zona tampon între Est şi Vest. De asemenea, Dugin subliniază faptul că nicio civilizaţie unică nu s-a format pe teritoriul Ucrainei. Potrivit lui Dugin, Dunărea şi Niprul, două dintre cele mai mari fluvii de pe teritoriul Ucrainei, au restricţionat cu eficienţă de-a lungul timpului posibilităţile integrative ale statului ucrainian. Geopoliticianul susţine că un teritoriu vast al statului ucrainian este locuit de diferite „etnos"/„societăţi" (этнос), cu scopuri geopolitice diferite. Locuitorii etnici ai Rusiei Mari şi Rusiei Mici au civilizaţii similare, cu rădăcini comune, orientate către spaţiul rusofon/rusofil, în timp ce „etnos"-urile diferite prezente în teritoriul Ucrainei manifestă o tendinţă de apropiere şi integrare cu zona culturală vest-europeană (Дугин, pp. 376-377; Дугин, 2011, pp. 8-25; Багдасарян, 2012, pp. 138-143). De aceea Ucraina de astăzi nu poate fi integrată total nici în blocul Eurasian, nici în Europa Centrală, aflată sub influenţa Germaniei. Într-un asemenea aranjament geopolitic, Ucraina – o păpuşă în mâinile politicienilor americani – poate exista doar ca o parte a „staţiei sanitare", fiind sursa destabilizărilor politice din Europa de Est şi factor emergent pentru un potenţial conflict armat în regiune. Acestea sunt motivele pentru care o Ucraina suverană, aşa cum este astăzi, reprezintă o ameninţare la adresa intereselor şi securităţii Federaţiei Ruse, pe care Dugin o identifică ca fiind sinonimă cu o invazie a teritoriului Federaţiei Ruse (Дугин, pp. 347-349; 378-379). De aceea, ca şi în cazul altor state aparţinând „zonei sanitare", este necesară împărţirea Ucrainei în patru teritorii omogene din punct de vedere al contextului geopolitic în care sunt plasate, cum ar fi:

- Ucraina de Est, regiunea aflată pe malul drept al Dunării, de la Chernihiv la Marea Azov, care de secole a fost apropiată de Rusia în sens politic, religios şi etnic. Dugin nu exclude posibilitatea acordării unei autonomii extinse acestei regiuni, dar nu specifică limitele acesteia. In viitor, susţine Dugin, regiunea ar trebui anexată Federaţiei Ruse.
- Peninsula Crimeea, care ar trebui plasată sub controlul strategic al Rusiei. Având în vedere caracterul etnic complex al acestei părţi a Ucrainei, ar trebui să i se acorde autonomie, luând în considerare interesele tuturor „etnos"-urilor existente şi anume locuitorii Rusiei Mari, Rusiei Mici şi tătarii din Crimeea.
- Ucraina Centrală, care se întinde de la Chernihiv la Odessa (incluzând Kiev-ul), apropiată de Ucraina de Est prin prisma contextului cultural comun, fapt ce justifică plasarea acesteia sub influenţa eurasiană.

- Ucraina de Vest, incluzând Volhynia, Galicia, Transcarpatica și partea de est a Basarabiei. Această parte a Ucrainei are cel mai semnificativ impact asupra politicii statale, fiind punctul de sprijin pentru forţele anti-ruse și pro-occidentale. De aceea, scopul Rusiei în ceea ce privește acest teritoriu nu ar trebui să fie anexarea, ci obţinerea controlului permanent asupra regiunii prin stabilirea unei „Federaţii a Ucrainei de Vest", a cărei integritate ar putea fi reglementată în funcţie de nevoi. Graniţa strategică a Federaţiei Ruse ar trebui să mutată cât mai spre vest (în partea estică a Europei Centrale). Pe de altă parte, graniţa cultural-religioasă, ar trebui localizată între Ucraina Centrală și Ucraina de Vest. O asemenea soluţie ar trebui implementată pentru a proteja Rusia ortodoxă împotriva influenţei catolicismului și bisericilor unite și unificatoare (Biserica Unitariană). (Дугин, pp. 376-383; Коваленко, 2010, pp. 15-22; Корнев, pp. 25-32; Савин, 2011, pp. 51-64).

Pentru a elimina posibilitatea utilizării Ucrainei ca instrument al politicii americane în Europa Central-Estică este necesară decompunerea politică. O realizare de succes a acestui proces în perioada ce urmează (având în vedere că acest concept apare în cartea publicată în anul 1997) ar trebui să fie principalul imperativ al politicii externe ruse în această regiune. Federaţia Rusă nu poate deveni un imperiu strategic, politic și demografic fără integrarea Ucrainei și a Belarusiei (Дугин, pp. 382-383).

„Revoluţia portocalie" a fost principalul motiv pentru radicalizarea lui Dugin și a adepţilor săi în privinţa Ucrainei. Revoluţia a fost percepută ca o creaţie artificială, sprijinită de Statele Unite cu un singur scop – crearea unui guvern la Kiev care va rupe orice legătură cu Rusia. De aceea succesul revoluţiei portocalii a fost tratat, din motive evidente, ca o ameninţare la adresa imperiului eurasian (Максимов, 2010, pp. 19-23; 27-43; 86-104; Черемных și Восканян, 2013, pp. 60-94; Стариков, 2013, pp. 88-94). Este necesar să menţionăm că una dintre consecinţele acestui eveniment a fost nu doar stabilirea unui concept de integrare a Ucrainei în Rusia, ci și a unor metode de atingere a obiectivului. De exemplu, a fost postulată provocarea unor revolte sociale în anumite regiuni ale Ucrainei, care în contextul actual capătă o importanţă sporită. Pe 26 aprilie 2006, la Russian Exhibition Centre, localizat în partea de nord-est a zonei administrative a Moscovei, a avut loc cea de-a doua convenţie a Eurasian Youth Union. Organizaţia a fost înființată de către Dugin și este activă atât pe teritoriul Rusiei, cât și pe teritoriile statelor asociate cu Comunitatea Statelor Independente. Pe durata convenţiei,

s-a hotărât că Rusia și Ucraina aparţin unui spaţiu geopolitic uniform. A fost subliniată necesitatea menţinerii relaţiilor dintre Rusia și Ucraina pentru a garanta statusul de Imperiu Eurasian al Federaţiei Ruse; în absenţa acestora, Rusia devenind un alt stat asiatic. Pe de altă parte, Ucraina este predestinată marginalizării economice și politice, în situaţia ruperii legăturilor cu Rusia. Guvernul pro-occidental de la Kiev, stabilit ca urmare a „revoluţiei portocalii", a fost recunoscut ca fiind un regim ce ocupă teritoriul Ucrainei. Leonid Savin – moderatorul fracţiunii ucrainiene în cadrul convenţiei și Valery Korovin – liderul organizaţiei la momentul respectiv, ambii prezenţi la a doua convenţie a evenimentului, au postulat stabilirea Mișcării Eurasiatice și a Armatei Revoluţionare Eurasiatice în Ucraina. Baza pentru aceste iniţiative a fost Eurasian Youth Union, care activează în multe orașe ucrainiene și structuri regionale ale Partidului Bolșevic Naţional (Национал-большевистская партия, НБП). Principalul obiectiv al armatei emergente ar fi coordonarea unui război de guerilla și eliminarea invadatorilor din teritoriile ocupate (Публичная интернет-библиотека Владимира Прибыловского, Съезд ЕСМ объявил повстанческую войну Украине [online]).

În anii care au urmat, Aleksandr Dugin și-a promovat viziunea, tratând Ucraina ca un stat deteriorat, suspendat într-un vid geopolitic între Est și Vest. El a postulat, de asemenea, în multiple ocazii, ideea de divizare a Ucrainei, așa cum apare în cartea sa *Bazele geopoliticii* (Dugin, 13 August 2008; Eberhardt, p. 236; Dugin, *The fate of Ukraine is settled. An interview given to the Russian state television in 2009*; Darczewska, 2014, pp. 20-22). Interpretarea evenimentelor ce au avut loc în Euromaidan a condus la recurgerea lui Dugin la argumente de ordin geopolitic și escatologico-filosofice. Din punctul său de vedere, de secole, lumea a fost martora unei lupte planetare între „supercivilizaţiile mării" (întruchipate de SUA, Regatul Unit, Australia și aliaţii lor) și „supercivilizaţiile continentale" (Rusia, Europa continentală, excluzând Regatul Unit, statele arabe, statele din Asia Centrală, China, India, Japonia). Dugin asociază „supercivilizaţiile mării" cu individualismul, conformismul, materialismul, modernismul și capitaluri, pe când „supercivilizaţiile continentale" sunt asociate cu tradiţia, ierarhia, personalismul și colectivismul. Din punct de vedere mitologic, simbolizează lupta Leviatanului, spre exemplu SUA, cu Behemoth, spre exemplu civilizaţia eurasiană (Дугин, 2012, pp. 15-22; Дугин, pp. 14-19, 466-471). În prezent această confruntare are loc atât la nivel ideologic și informaţional, cât și la nivel economic, militar și politic (Дугин, 2005, pp. 486-493; Gołąbek, 2014, pp. 95-100).

Un alt punct al rivalităţii geopolitice, în afară de Transnistria, Caucaz, Abhazia și Osetia de Sud și Georgia, este Ucraina. Conform lui Dugin,

principalul obiectiv al SUA este punerea în practică a strategiei dezvoltate de Zbigniew Brzezinski, care presupune separarea Ucrainei de civilizaţia eurasiană, concomitent cu diminuarea statutului Rusiei la rolul de superputere regională. Din perspectiva sa, primul pas în implementarea acestei strategii l-a constituit răsturnarea autorităţilor legale de la Kiev cu ajutorul naţionaliştilor ucrainieni, sprijiniţi de SUA și instaurarea unui guvern anti-rus, care a început exterminarea rușilor din Ucraina. Anexarea Peninsulei Crimeea este modalitatea prin care Rusia a oferit un „răspuns simetric" „provocării" lansate de Atlantic în Kiev, sprijinită de etnicii ruși și armata Federaţiei Ruse. Mai mult decât atât, criza ucrainiană, ca rezultat al evenimentelor din Euromaidan, a fost percepută de Dugin ca un motiv pentru reevaluarea integrităţii ucrainiene. Următorul pas pentru „protejarea graniţelor ruse" a devenit aplicarea scenariului Crimeei în părţile estice ale Ucrainei (Brzezinski, 1997, pp. 30-48; 87-118). Este necesar de menţionat faptul că Aleksandr Dugin, pentru care situaţia din Ucraina este și o problemă personală (mama sa fiind originară din Ucraina), s-a implicat activ în conflict (http://evrazia.org/article/2469). Rolul său în conflictul ruso-ucrainian pare a fi mult mai extins decât simpla coordonare a informaţiilora sprijinului financiar și logistic oferite separatiștilor de către organizaţiile sale.

Aleksandr Dugin se presupune a fi unul dintre autorii soluţiei finale oferite problemei ucrainiene și creatorul modelului geopolitic în baza căruia s-a acţionat, și în urma căruia s-au stabilit organisme statale pro-ruse pe teritoriul Ucrainei. Pentru această afirmaţie există dovezi. În timpul conflictului ruso-georgian, el se afla în Osetia de Sud, oferind consiliere pentru obţinerea controlului asupra Tbilisi și răsturnarea președintelui Mihail Saakashvili. Următorul pas a fost preluarea Peninsulei Crimeea, care, așa cum susţine Dugin, reprezintă *oricum o parte din Rusia* (Ньюман, [online]). Într-un interviu, a admis că liderii Republicii Populare Donetsk și Luhansk sunt prietenii săi apropiaţi, care în anii '90 au participat la cursurile sale de geopolitică. A subliniat faptul că aceștia au o pregătire solidă și că susţin cu tărie ideea neo-eurasianistă. De asemenea, a confirmat faptul că a menţinut legăturile cu liderii mai sus-menţionaţi. Mai mult, Dugin a afirmat că Republica Populară Donetsk reprezintă etapa finală a unui proiect politic, care a fost conceput ca răspuns la „revoluţia portocalie" în timpul unei sesiuni de training organizate de către International Eurasian Movement lângă Volodymyr, în 2006 (Дугин, *Вводить войска в Новороссию* [online]). În contextul afirmaţiillor lui Dugin, este notabil faptul că în 2006 a apărut ideea unei școli de gândire geopolitică neo-eurasianiste și ideea de crearea a unei Armate Revoluţionare Eurasianiste în Ucraina. Mai mult, Dugin a afirmat că fiul său,

Artur, un activist marcant al Eurasian Youth Union, a luat parte la operaţiunile din Crimeea, asemenea multor activişti neo-eurasieni, ce s-au alăturat iniţiativei „Crimean Self-Defence" (auto-apărarea Crimeei). În timpul operaţiunilor, acesta a executat sarcini ce au presupus blocarea clădirilor guvernamentale ucrainiene pentru a evita scurgerea de informaţii sensibile (se spune de asemenea că a participat la acţiunea de împiedicare a guvernului ucrainian în încercarea sa de a divulga informaţii în exterior sau de a manipula informaţiile ce urmau a fi transmise astfel încât să fie favorabile partidului rus). Ulterior, acesta s-a hotărât să devină jurnalist pentru Russia Today, pentru a lua parte la războiul informaţional (Дугин, *Это моя война!* [online]). Unul dintre activiştii „veterani" ai Eurasian Youth Union a fost Aleksandr Prosiolkov, care până la moartea sa din data de 31 iulie 2014, a fost Adjunct al Ministrului Afacerilor Externe în cadrul Republicii Populare Donetsk. Este necesar să menţionăm că principalii lideri ai administraţiei de stat în republicile auto-desemnate şi forţele armate aferente – Denis Puszylin, Igor Strielkov, Aleksandr Borodaj, Pawel Gubariev şi Valery Bolotov – au luat parte la o adunare specială a „Clubului Izborski" la Donetsk. De notat este faptul că organizaţia în sine reuneşte cele mai influente personalităţi din mediul politic rusesc şi se constituie într-o pepinieră intelectuală pentru Kremlin. Aleksandr Prochanov – scriitor, politician şi director al „Clubului Izborski", împreună cu Aleksandr Dugin, Valery Korovin şi alţi experţi au pregătit proiectul unui nou stat, localizat în partea de sud-est a „fostei Ucraina". Noul fenomen geopolitic, incluzând Republica Populară Donetsk (http://rossia3.ru/proselkov3107) şi Republica Populară Luhans, a fost proclamat la 12 mai 2014. Aceasta este modalitatea în care un nou stat, Statul Federal al Novorossyia (Федеративное государство Новороссия, Ukrainian: Федеративна держава Новоросія) a fost creat (http://novorossia.su/ru/node/2386 şi http://novorossia.su/ru/node/2783). Numele statului nu este întâmplător – este ales astfel încât să indice că teritoriul actual a aparţinut în trecut Imperiului Rus şi Federaţia Rusă, ca succesor legitim al acestuia, are dreptul de a-l anexa (Краснов, 1863). Dugin subliniază faptul că districtele Donetsk şi Luhansk au fost mereu părţi integrante ale Rusiei şi locuitorii teritoriilor, care au fost în permanenţă conectaţi la Biserica Catolică Ortodoxă, ar trebui trataţi ca partea sud-vestică a civilizaţiei eurasiene. Aceşti oameni au recunoscut întotdeauna conexiunea puternică cu Rusia. Pământurile Novorosia au devenit o parte a Ucrainei din întâmplare – în 1991, după colapsul Uniunii Sovietice. Aceste teritorii pot fi o parte a Ucrainei, doar în situaţia în care Ucraina este integrată în Federaţia Rusă. Din perspectiva lui Dugin, identitatea istorică a „etnos"-urilor din Novorosia derivă din trecutul ruso-soviet, influenţat de Imperiul Rus, Biserica

Catolică Ortodoxă şi Marele Război Patriotic. Conform autorilor Novorosia, acest teritoriu trebuie să se subordoneze „autorităţilor suverane" şi să se elibereze de influenţele oligarhilor, a căror bogăţie ar trebui naţionalizată (Дугин, *Время Новоросии*; Дугин, *Крым в России. Что дальше?* şi Дугин, *Новороссия часть Русского мира*). Aceste idei s-au reflectat de asemenea în programul politic al Mişcării Social-Politice Partidul Novorosia (Общественно-политическое движение «Партия Новороссии») înfiinţat pe 13 mai 2014 de Pawel Gubariev (http://novorossia.su/ru/node/1753).

Trebuie menţionat că anumite concepte geopolitice proclamate de Dugin şi conectate cu mişcarea neo-eurasianistă sunt puternic vizibile în activitatea Kremlinului şi declaraţiile preşedintelui Vladimir Putin. În primul rând, elementul cheie în politica rusă în raport cu noile autorităţi ucrainiene este solicitarea reformei constituţionale, care ar modifica statusul ţării din stat unic în federaţie, privilegiind semnificativ regiunile din est şi sud. Acest fapt poate fi confirmat de declaraţia ministrului de externe rus din data de 17 martie 2014, prin care Moscova solicită ca Verkhovna Rada din Ucraina să stabilească o adunare constituţională cu o reprezentare echitabilă a tuturor regiunilor din Ucraina. Acest organ ar urma să pregătească şi aprobe proiectul constituţional. Conform conceptului rus, Ucraina va fi „un stat democratic federal", ale cărui regiuni separate vor avea dreptul de a-şi alege independent autorităţile legislative şi executive, care vor avea puteri extinse care să le reflecte caracteristicile istorice şi culturale specifice. Recurgerea la asemenea soluţii ar garanta Rusiei controlul asupra politicilor Kievului prin controlarea politicilor regiunilor din estul Ucrainei. Asta ar presupune transformarea Ucrainei într-o formă federativă diluată, fără omogenitate la nivelul politicilor economice, culturale şi sociale, iar regiunile cu propriile autorităţi legislative nu ar fi obligate să urmeze direcţiile trasate date de autorităţile centrale, fapt ce preocupă în special regiunile estice (Olszański, 2014, pp. 1-2; Moshes, 2014, pp. 2-3). Mai mult, declaraţiile preşedintelui referitoare la proiectele geopolitice pe termen lung reflectă conceptul de neo-eurasianism. Într-una dintre declaraţiile sale, Vladimir Putin a subliniat faptul că Rusia devine centrullumii ruse, alcătuite dintr-un nucleu ruso-ucraineano-belarus. Principalul spaţiu al acestei lumi va consta în teritoriile post-sovietice locuite de rusofoni (Menkiszak, 2014, pp. 1-7; Panov, 2010, pp. 85-94). Apartenenţa la lumea rusă va fi garantată de aspecte culturale precum limba, Biserica Ortodoxă şi valori comune, indiferent de naţionalitate şi origine etnică. Aşadar, viziunile preşedintelui Putin sunt echivalente definiţiei date de Valery Korovin asupra polului geopolitic eurasian ca fiind parte integrată a lumii multipolare (Bieleń, 2013, p. 110; Дугин, 2009, pp. 16-17. Sykulski, 2013, pp. 349-365).

Aşadar, anexarea Crimeei la Rusia şi activităţile separatiştilor în partea de sud-est a Ucrainei nu ar trebui să fie tratate ca o aspiraţie la libertate autentică a locuitorilor săi, aşa cum este descrisă de propaganda de la Kremlin – „Primăvara rusă". Se pare că este mai degrabă un proiect geopolitic creat artificial şi implementat prin intermediul controlului social tehnologic şi al agresiunilor informaţionale şi militare. Proiectul a fost creat de geopoliticieni ruşi sprijiniţi de Kremlin şi conexaţi mediului eurasian, aşa cum este acesta descris de Aleksandr Dugin. Adevăratul obiectiv, ce sprijină realizarea doctrinei geopolitice a lui Dugin, este în primul rând o legătură profundă accentuată a regiunilor ucrainiene sud-estice de Rusia, care în perspectivă are potenţialul de a priva Ucraina de suveranitate. Posibilitatea reală de concretizare a unui astfel de scenariu este relevată de analizele realizate de principalii geopoliticieni ruşi, care au proiectat o viziune de dezvoltare viitoare a acestei situaţii. În acest context, este de interes prognoza realizată de către gen.col. Leonid Iwaszov. În opinia sa, evenimentele din Euromaidan au iniţiat procesul de prăbuşire al Ucrainei. În următorul an sau doi, noi referendum-uri – similare celui care a avut loc în Crimeea pe data de 16 martie 2014 – sunt foarte probabile. Rusia ar trebui să sprijine într-o manieră activă activităţile ce au ca scop este returnarea regiunilor sud-estice la ţara „mamă". După „stabilizarea" situaţiei socio-politice în aceste regiuni, mai trebuie adoptată o măsură, sub foma unui „război rebel" (sintagmă în rusă). Ar afecta regiunile vestice ale Ucrainei, în special în zona de graniţă religios-culturală, ceea ce înseamnă limita de demarcaţie între Ucraina Centrală şi de Vest. Aşadar, este necesară provocarea de proteste puternice. Acest obiectiv poate fi atins prin utilizarea, inter alia, de dispute cu fundament religios, activităţi represive ale noilor autorităţi şi scăderea standardelor de trai ale locuitorilor în comparaţie cu locuitorii din Novorossyia, teritoriu anexat Federaţiei Ruse.

Datorită unor asemenea operaţiuni, prin procesul de federalizare al Ucrainei, va fi posibilă stabilizarea situaţiei. Patru republici federale vor fi astfel înfiinţate: o republică occidentală cu capitala la Liov, una centrală cu capitala la Kiev, una esticăcu capitala la Kharkiv şi una sudică cu capitala la Dnipropetrovsk. Conform generalului, un alt scenariu este de asemenea posibil: organele statale menţionate să fie independente, totuşi criza economică şi disputele dintre puterile aspirante şi oligarhii influenţi vor genera o situaţie de criză. În asemenea circumstanţe, anumite state „independente" pot aspira la un proces integraţionist mai profund în raport cu Rusia. Ucraina de Vest (Lvov) ar fi privată de o asemenea posibilitate. Conform afirmaţiilor lui Iwaszov, pentru ca această idee să fie implementată este necesară o activitate intensă a instituţiilor şi organizaţiilor sociale ruse. Această declaraţie enigmatică ar trebui desigr înţeleasă ca fiind echivalentă cu „războiul informaţional" (Ивашов, 2014, p. 11).

Aleksandr Dugin ia în calcul un scenariu similar pentru Ucraina. Din punctul său de vedere, partea vestică a Ucrainei și regiunile vecine Mării Negre ar trebui să rămână sub control rusesc. Graţie acestei configurări va fi posibilă acordarea de sprijin împotriva mişcărilor centrale de tip „junta", în speţă guvernul de la Kiev, evitând o intervenţie militară directă (Дугин, *Крым в России. Что дальше?* [online]). Și Valery Koronin nu ia în calcul o existenţă viitoare a Ucrainei, prezicând scindarea acesteia între cele două bloocuri – Atlantic și Eurasiatic (Коровин, 2014, pp. 19-21).

Planul geopolitic al Rusiei faţă de Ucraina pare a fi evident – subordonare permanentă a Ucrainei prin obţinerea controlului rusesc asupra politicii sale externe, politicii interne și asupra proceselor din zona securităţii și economiei. Astfel, menţinerea unei situaţii instabile în Donbas este doar un instrument menit să menţină controlul asupra întregii Ucraine.

„Războiul rebel" al lui Evgeny Messner ca un element al războiului informaţional rus reliefat în exemplul conflictului ruso-ucrainean

Potrivit generalului Leonid Iwaszov, principala metodă de atingere a scopurilor geopolitice ale Federaţiei Ruse pe teritoriul Ucrainei este așa-numitul „război rebel". Elementele teoretice de bază ale acestui fenomen au fost decrise de către Evgeny Messner (1891-1947)[2], colonel în cadrul Cartierului General al Armatei Ţariste și veteran al ambelor conflagraţii mondiale, care și-a petrecut ultimii ani din viaţă ca om de știinţă în cadrul academiilor militare din Argentina. Acesta a avertizat lumea cu privire la era războaielor neconvenţionale, denumite astăzi conflicte asimetrice sau neregulate[3]. Interesele ştiinţifice ale lui Messner vizau aspectele psihologice ale artei războiului, moralul soldaţilor și al ofiţerilor și diferitele forme de conflict (Месснер, 1999, pp. 363-404). Bazându-se pe experienţa sa personală și pe cunoștinţele erudite, completate de cunoașterea câtorva limbi străine, Messner a publicat numeroase monografii, articole și studii, dintre care o atenţie deosebită trebuie să fie acordată lucrării intitulate *World Rebel War* (în rusă: *Всемирная Мятежевойна*), publicată la Buenos Aires în 1971. O parte componentă a acestei lucrări este reprezentată de un studiu intitulat „Revolta, sau numele celui de-al Treilea Război Mondial" (în rusă:

---

[2] Bibliografia detaliată a lui Evgeny Messner poate fi găsită în: И.В. Домнин, *От Первой мировой до «Третьей Всемирной». Жизненный путь Генерального штаба полковника Е.Э. Месснера*, w: *Хочешь мира, победи мятежевойну! Творческое наследие Е.Э. Месснера*, И.В. Домнин (ed.), Москва 2005, pp. 18-51; К. Александров, *Армия генерала Власова 1944-1945*, Москва 2006, pp. 26, 41-42, 182, 248, 507; И.В. Домнин, *Краткий очерк военной мысли Русского Зарубежья*, in: *Военная мысль в изгнании. Творчество русской военной эмиграции*, И.В. Домнин (ed.), Москва 1999, pp. 448-527.

[3] Vezi nota 16.

Мятеж – имя Третьей Всемирной), publicat în 1960 în capitala Argentinei sub forma unui studiu independent[4].

Revoluţia din Rusia, filozofia artei războiului a lui Sun Tzu, ambele conflagraţii mondiale și numeroasele conflicte regionale sunt considerate a fi surse de inspirație pentru cercetările lui Evgeny Messner cu privire la geneza unei noi metode de purtare a războiului. În urma unor observaţii amănunţite, Messner a concluzionat că lupta obișnuită a soldaţilor se împletește deseori cu revolte de ordin politic, social sau economic sau cu atacurile teroriste și activităţi desfășurate de organizaţii secrete, grupuri de sabotaj și indivizi. Aceste activităţi sunt dificil de clasificat. Este de asemenea dificil de identificat originea lor. El a denumit acest nou fenomen „lupta împotriva unei rebeliuni" (în rusă: борба мятежом), pe scurt „război rebel" (мятежевойна, din rusescul мятеж – rebeliune, revoltă). Din punctul de vedere al lui Messner palierul psihologic a fost utilizat rareori în războaiele anterioare, însă în cazul „războiului rebel" este conisderat a fi instrument principal. Acesta este motivul pentru care „războiul rebel" este unul de natură psihologică. Messner subliniază faptul că pe viitor acesta va fi modul predominant de purtare a războaielor și studiul său menţionat anterior este unul incomplet, neacoperind întreaga problematică.[5].

Principala regulă în purtarea unui „război rebel" este reprezentată de folosirea mișcărilor naţionale, rebeliunilor etc., ca subiect al revoluţiei (Месснер, 2004, pp. 15-23, 332-340.). Potrivit lui Messner revoluţia este mai presus de toate un fenomen psihologic, care trebuie să fie înţeles ca o schimbare rapidă și radicală a conștiinţei oamenilor. Arta revoluţiei se bazează pe crearea și separarea unui grup activ condus de lideri revoluţionari,de societate sau de naţiune. Revoluţia este caracterizată de procese psihologice care au loc la nivelul maselor stimulate de grupuri active.

---

[4] Nici cercetătorii polonezi, nici cei occidentali nu au recunoscut lucrările academice ale lui Evgeny Messner. Trebuie amintit faptul că monografiile sale nu au fost traduse în limba engleză încă. Un om de știință care a devenit interesat de această problematică din țara noastră este Kazimierz Kraj. Vezi: K. Kraj, *Wojny asymetryczne czy miatieżewojna Jewgienija Messnera zagrożeniem dla bezpieczeństwa w XXI wieku*, „Bezpieczeństwo. Teoria i praktyka" 2012, issue 3, pp. 33-41; idem, *Мятежевойна Jewgienija Messnera*, „E-Terroryzm" 2012, issue 2, pp. 16-18.

[5] Trebuie să fie menționat faptul că războaiele în care sunt desfășurate activități asimetrice au fost subiectul unui studiu aprofundat al filozofului nazist Carl Schmitt. În una din lucrările sale el a sugerat că astfel de activități ar trebui să fie legal legitimate în dreptul international. Vezi:C. Schmitt, *Theorie des Partisanen Zwischenbemerkung zum Begriff des Politischen*, Berlin 1975; T. Kochi, *The Partisan: Carl Schmitt and Terrorism*, „Law Critique" 2006, issue 17, pp. 267-295. Opiniile lui Schmitt au devenit baza afirmațiilor lui Dughin, care susține că grupurile de gherilă care utilizează tehnici teroriste de luptă reprezintă principalul instrument în lupta dintre „ Supercivilizația Mării" și „ Supercivilizația Uscatului" și Rusia, care ca urmare a tradițiilor sale din războaiele napoleoniene și Marele Război Patriotic, este considerat un imperiu de gherilă. Opiniile lui Dughin sunt așadar un process (chiar dacă numai unul ideologic pentru moment) pentru a legitima activitățile asimetrice applicate în cadrul politicii ruse. Vezi: А.Г. Дугин, *Философия войны*, Москва 2004, pp. 96-100.

Se bazează pe instincte ale legii și psihologia maselor, al cărei rezultat este reprezentat de transformarea unui om civilizat într-un barbar. În conformitate cu conceptul lui Messner, psihologia „maselor rebele" reprezintă instrumentul principal care poate conduce către victorie sau către eșec. Scopul unui război nu se limitează doar la neutralizarea forţelor armate ale inamicului, ci include și destabilizarea întregii ţări prin utilizarea factorilor psihologici: demoralizarea, frica și sentimentul de incertitudine fiind rezultatul activităţilor grupărilor teroriste și de gherilă (Schmid, 2005, pp. 137-146). De aceea „războiul rebel" este descris adesea de către Messner ca fiind un „război parţial", care trebuie înţeles ca o etapă de tranziţie între pace și activităţile specifice războiului convenţional.

„Războiul rebel" este de asemenea caracterizat de imposibilitatea determinării cu precizie a părţilor aflate în conflict, care se ascund în spatele și desfășoară activităţi prin intermediul grupurilor „non-statale" neregulate (Месснер, 2004, pp. 46-59). Este de asemenea dificil de identificat care este punctul de pornire și finalul unui astfel de război, în cazul căruia termeni precum teatru de operaţiuni sau linie de front nu pot fi utilizaţi în sens propriu.

Principalul scop al unui „război rebel" – potrivit lui Messner – este acela de a obţine *controlul asupra sufeltului* inamicului. De aceea, pentru a învinge este necesară realizarea profilului psihologic nu doar la nivelul individului ci, mai ales, la nivelul întregului grup, societăţi sau naţiuni. Acest fapt implică provocări majore pentru noua formă de intelligence – așa-numitul intelligence psihologic (în rusă: психоразведка) (Месснер, 2004, pp. 105-116). Activităţile sunt derulate nu doar în spaţiile tradiţionale (uscat, apă, aer), dar și (preponderent, de fapt) la nivelul psihicului uman. Conceptul de linie de front în ceea ce privește „războiul rebel" se referă la sferele individuale ale activităţilor derulate de societate, precum economia, politica, cultura etc. Un obiectiv important al unui „război rebel" este reprezentat de procesul de integrare al propriei naţiuni și atragerea sprijinului unei părţi componente a naţiunii adverse. Această sarcină a fost atribuită jurnaliștilor, sabotorilor, instigatorilor și propagandiștilor. Toate grupurile sociale inamice ar trebui puse sub presiune psihologică. Potrivit lui Messner, un rol important în acea activitate este jucat de către partidele politice și organizaţiile sociale. Secretul păstrării controlului psihologic asupra maselor rebele se bazează pe definirea nevoilor acestora și modelarea noii lor conștiinţe (neo-conștiinţă) astfel încât aceștia să creadă că își exprimă propria lor voinţă de fapt (Месснер, 2004, pp. 59-64; Зелинский, 2008; Кириллов, 2012, pp. 71-74).

După descrierea generală a genezei, definiţiilor și scopurilor unui „război rebel" Messner prezintă principalii actori participanţi. Acesta îi împarte în patru grupuri:

1. „mase rebele" (în rusă: мятежные массы) semnificând acei cetăţeni neobedienţi sau mulţimi care se revoltă, reprezentând partea cea mai numeroasă și cel mai dezorganizat grup care ia parte la un conflict. Acest grup este caracterizat de imprevizibilitate și atitudine radicalistă, trecând de la pasivitate la activitate și vice versa, aspect care reprezintă o mare provocare pentru comanda operaţională, fiind comparabile în arta tradiţională a războiului trupelor de coaliţie.
2. „coloanele rebele" (în rusă: мятежные колонны), numite de asemenea drept „cripto-armată" sau „poliţie secretă", se referă la indivizii sau grupurile alese din rândul „ maselor rebele" ale căror sarcini principale sunt reprezentate de activităţi teroriste și subversive. Membrii unor astfel de grupuri pot fi descrişi drept ideologişti care deservesc ideea pentru care luptă. „Coloanele rebele" sunt alcătuite cu preponderenţă din sabotori, terorişti și instigatori.
3. „miliţia rebelă" (în rusă: мятежное ополчение) se referă la grupuri neregulate, voluntare de gherilă sau la armate de insurgenţi. Acest grup se limitează doar la naţiunea sau grupul etnic din care provine. „Miliţia rebelă" este teritorială, lucru care înseamnă că este activă în zona din care provin membrii săi și beneficiază de regulă de sprijinul populaţiei locale.
4. „armata într-un război rebel" (în rusă: войско в мятежевойне) care constituie unh element la fel de important în timpul unui conflict. Activităţile „maselor rebele", „coloanelor rebele" și grupurilor de gherilă ar trebui să fie coordonate după modelul unei armate regulate. În conceptul lui Messner armata regulată joacă doar un rol de susţinere a grupurilor de gherilă, a „miliţiei cetăţenilor", a grupurilor sociale revoltate sau minorităţilor naţionale (Месснер, 2004, pp. 65-73; Beckett, 2001; Arquilla, 2012; Larson, Eaton, Nichiporuk, Szayna, 2008; Svete, 2009, pp. 381-399).

Cooperarea între cele patru grupuri anterior menţionate ar trebui să vizeze atingerea unor obiective definite cu precizie, pe care Messner le defineşte drept:

- dezintegrarea moralului naţiunii ostile/inamice;
- dezintegrarea unor elemente active ale ţării (armata, grupurile de gherilă, mişcările sociale);
- preluarea sau dezactivarea obiectelor cu valoare psihologică;
- preluarea sau dezactivarea obiectelor cu valoare materială;
- desfăşurarea de activităţi cu scopul de a căştiga aliaţi sau de a slăbi aliaţii inamicului;

- protejarea moralului propriei naţiuni;
- economisirea propriilor forţe armate;
- securizarea propriilor obiecte cu valoare psihologică şi materială,
- neutralizarea factorilor care ar putea conduce la reacţii din partea unos ţări neutre (trebuie luat în considerare faptul că nu doar guvernele, ci și grupurile sociale pot reacţiona) (Месснер, 2004, pp. 110-116 și 212).

Trebuie menţionat faptul că conceptul lui Evgeny Messner de „război rebel" a fost evidenţiat la începutul anilor '90 ai secolului trecut pe parcursul dezvoltării doctrinei Federaţiei Ruse cu privire la activităţi asimetrice, integrată în conceptul extins de „război informaţional". Operaţiunea din Crimeea și escaladarea conflictului ruso-ucrainean a creat oportunitatea de a evalua conceptul rus de „război informaţional", care a devenit subiectul unui studiu aprofundat realizat de Jolanta Darczewska (2014). Aceasta a recunoscut faptul că teoreticienii ruși interpretează conceptul de război informaţional drept influenţarea conștiinţei maselor în contextul rivalităţii internaţionale dintre sistemele de civilizaţii în mediul informaţional, care poate fi realizată prin utilizarea unor metode speciale de exercitare a controlului asupra resurselor informaţionale, folosite drept „arme informaţionale". Conceptul rus de „război informaţional" se referă la războiul psihologic și propaganda utilizate în perioada Rusiei Sovietice. Autorul subliniază faptul că dimensiunea tehnologică a războiului informaţional în Rusia a fost marginalizată și eliminată de la nivelul spaţiului public, făcând loc factorilor culturali și ideologici. Principala sarcină a „războiului informaţional" este aceea de a atinge obiective precise în politica externă, regională și internă, precum și de a asigura avantajul geopolitic. Astăzi, în Rusia, există două școli ale „războiului informaţional" înființate de Igor Panarin și Aleksandr Dughin – principalii reprezentanţi ai conceptului de geopolitică și lideri ai opiniei publice, având legături cu serviciile secrete. Autorul susţine că ei încearcă să sensibilizeze propria societate la ameninţările informatice din exterior, dezvoltând în acelaşi timp sistemul rusesc de contracarare informativă. Ei tratează conceptul de „război informaţional" atât în plan teoretic, cât și practic (Месснер, 2004, pp. 11-18).

Trebuie amintite numeroasele studii ale lui Igor Panarin, Aleksandr Dughin, Valery Korovin și Leonid Savin, care au funcţii de popularizare, dezinformare și propagandă, analizând în detaliu preponderent conceptul de război informaţional al americanilor. Scopul acestui război, după cum subliniază autorii, este dezintegrarea Rusiei și destabilizarea spaţiului post-sovietic. Aceiași autori fac referire, de asemenea, la presupusa slăbiciune a

Rusiei şi la necesitatea de a-şi construi propriul concept de „război informaţional", cu scopul de a se opune agresiunii occidentale, care a determinat în trecut prăbuşirea Uniunii Sovietice (Дугин, 2007, pp. 321-347; Савин, 2011; Савин, 2012; Коровин, 2014, pp. 177-309; Коровин, 2009; Панарин, 2010). Comparând studiile autorilor menţionaţi mai sus cu teze ale teoreticienilor americani, se ajunge la concluzia că definiţiile şi metodele de implementare ale „războiului informaţional", presupuse a aparţine ruşilor, au fost preluate din lucrări ale unor autori americani (nu departe de definiţiile menţionate mai sus) şi au fost ajustate la scopurile propagandei ruseşti. Acest fapt poate fi confirmat de activitatea jurnalistică a lui Dughin, în care acesta a recunoscut conceptul american de purtare a războiului centrat pe reţea (Network Centric Warfare) şi o parte componentă a acestuia – formula C4ISR (Comandă, Control, Comunicaţii, Calculatoare, Intelligence, Supraveghere şi Recunoaştere), drept principale instrumente de iscare a „revoluţiilor florale" în teritoriile post-sovietice. Inspirându-se din literatura americană, acesta a creat modelul „reţelei euroasiatice", care se presupune că este un răspuns la „provocarea americană reprezentată de războiul centrat pe reţea" (Дугин, pp. 333-347; Дугин, 2008, pp. 2-10; Дугин, 2013, pp. 38-68; Ferris, 2004, pp. 199-225; Kipp, 2014, p. 36; Бедрицкий, 2008, pp. 54-86).

Un concept similar a fost de asemenea formulat de Igor Panarin, care a adoptat teoria americană denumită noopolitik la nivelul la nivelul statului rus (Панарин, 2006, pp. 163-172; Arquilla, Ronfeldt, 1999; Grau, Thomas, 1996, pp. 508-511; Thomas, 1996-1997, pp. 81-91; Heickerö, 2010, pp. 13-15; Лебедев, Лютов, Назаренко, 1991, p. 14).

Astfel, conceptul de „război informaţional", în accepţiunea autorilor de mai sus, care are ca bază de inspiraţie conceptul original american, cu greu poate fi acceptat ca fiind o reflexie reală a practicii aplicate la nivelul Federaţiei Ruse. În acest context, se pune întrebarea cu privire la autenticitatea ipotezelor teoretice referitoare la războiul informaţional rus şi punerea sa în practică. Analizând această problemă trebuie luate în considerare şi realizările armatei în acest domeniu. Aspectele teoretice şi practice ale acestui tip de război au fost studiate de către forţele armate ale Federaţiei Ruse de la începutul anilor '90 ai secolului trecut. Aceste activităţi au fost stimulate de realizările SUA în zona de operaţiuni, desfăşurate pe baza informaţiilor, în timpul Războiului din Golf, indiferent de asemănarea pe care acestea o aveau cu conceptul lui Evgeny Messner de război rebel, bazat pe factori informaţional-sociologici (Grau, Thomas, 1996, pp. 508-511; Thomas, 1996-1997, pp. 81-91; Heickerö, 2010, pp. 13-15; Лебедев, Лютов, Назаренко, 1991, p. 14). Definiţiile „războiului rebel" formulate de militarii

ruşi au mai degrabă un caracter universal şi se referă la activităţi derulate atât în perioadă de pace, cât şi în perioadă de război.

Trebuie semnalat faptul că aceste definiţii nu se regăsesc în studiile formulate de geopoliticieni, specialişti în ştiinţe politice sau politologi şi lideri de opinie. La nivelul nomenclaturii militare, termenul de „război informaţional" nu este utilizat. În Rusia termenul este rezervat jurnaliştilor, oamenilor de ştiinţă şi analiştilor civili. În mediul militar, sunt preferaţi termenii de „confruntare informaţională" (în rusă: информационное противоборство) sau „luptă informaţională" (în rusă: информационная борьба). Ambii termeni sunt utilizaţi alternativ şi diferenţa dintre ei nu este suficient de clară (Grau, Thomas, pp. 516-517; Воронцова, Фролов, 2006, pp. 3-5.).

Astfel, trebuie menţionate câteva definiţii selective spre exemplificare. În anii '90 ai ultimului secol unul dintre teoreticienii pionieri ai acestei forme de conflict, Col. Sergey Komov, a definit războiul informaţional ca fiind contracararea informaţiilor, concomitent cu protejarea propriilor surse prin utilizarea informaţiilor în conformitate cu un plan uniformizat, care are ca scop obţinerea şi menţinerea avantajului faţă de inamic. El susţine că aceasta trebuie să fie doar una dintre diversele acţiuni întreprinse împotriva inamicului (Комов, 1996, pp. 76-80; Комов, 1994, pp. 16-17; Комов, 1997, pp. 18-22). Un ofiţer al Academiei Militare a Sediului Forţelor Armate ale Federaţiei Ruse, citat de Timothy Loyd Thomas, oferă o definiţie similară a confruntării informaţionale. În opinia sa, este doar una din numeroasele forme de soluţionare a conflictelor dintre părţi, al cărui scop este acela de a câştiga şi menţine avantajul informaţional asupra adversarului. Acest lucru poate fi atins prin utilizarea unor metode tehnico-informaţionale şi psihologico-informaţionale, prin influenţarea factorilor de decizie, sistemelor de comandă şi control, cetăţenilor şi surselor informaţionale ale unei anumite ţări (Thomas, 2003, pp. 208-210; Clogg, 1997, pp. 425-430).

Opinia lui Vladimir Cymbal – analist în Ministerul rus al Apărării, care abordează definiţia războiului informaţional atât în sens extins, cât şi mai restrâns, este la fel de semnificativă. Conform acestuia, războiul informaţional, în sens larg, este un set de activităţi întreprinse de către o ţară împotriva cetăţenilor unei alte ţări sau unui grup de ţări, pe timp de pace. Aceste activităţi vizează influenţa asupra conştiinţei societăţii prin intermediul educaţiei, artei, culturii, sistemului educaţional, administraţiei etc., care ar trebui să fie desfăşurate de către servicii speciale civile – Serviciul Federal de Securitate şi Serviciul de Informaţii Externe. Sarcina principală a celui din urmă ar trebui să fie aceea de a obţine controlul asupra surselor de informaţii ale altor ţări, de a sabota dezvoltarea tehnologiilor informaţionale în ţările considerate ostile şi de a neutraliza sistemele de comunicaţii şi reţelele informatice ale adversarului. O altă sarcină importantă a acelui serviciu este aceea de a dezvolta şi implementa sistemele care să garanteze securitatea informaţională a Rusiei. Pe de altă parte, „războiul informaţional", în sens

restrâns, se referă la activităţi militare care au scopul de a obţine un avantaj informaţional asupra inamicului, în vederea transmiterii, utilizării şi prelucrării informaţiilor, precum şi a implementării unor decizii eficiente, care să permită obţinerea avantajului pe câmpul de luptă. Realizarea acestui domeniu al războiului informaţional ar trebuie să fie în responsabilitatea Ministerului Apărării şi a forţelor armate (Thomas, 2000, pp. 338 şi 342-343; Blank, 2013, p. 41; Giles, 2011, pp. 45-60.)[6].

Definiţiile prezentate aici implică faptul că „războiul informaţional" rus este un set de activităţi diverse, coordonate, desfăşurate atât de forţele militare, cât şi serviciile speciale civile, în numeroase domenii cu scopul de a neutraliza inamicul prin utilizarea instrumentelor tehnologico-informaţionale şi psihologico-informaţionale. Colonelul american Timothy Loyd Thomas, care a tratat acest subiect timp de două decenii, a încercat să clasifice aceste activităţi. Bazându-se pe un material substanţial confruntat cu declaraţiile (pe care le ştia din propriile sale experienţe) reprezentanţilor mediului militar rus, care au luat parte la conferinţe în Washington şi Moscova în 1996, a creat o structură detaliată a „războiului informaţional", diferită radical de cea promovată de tehnologii militari ruşi.

Conform lui T. L. Thomas „războiul informaţional" rus este caracterizat de diversitatea de mijloace şi de flexibilitatea activităţilor în sfere diverse, care se aplică chiar şi astăzi. Presupune existenţa următoarelor elemente:

- aspectul filozofic al „războiului informaţional";
- securitatea informaţiilor ca aspect al securităţii naţionale şi globale;
- surse informaţionale ca potenţial guvernamental;
- definiţia războiului informaţional;
- computerizarea conflictelor armate:
  - instrumente electronice pentru conflictele armate;
  - automatizarea conflictelor armate;
  - utilizarea roboţilor în conflictele armate;
  - instrumente intelectuale ale conflictelor armate (arme inteligence care permit lovituri precise);

[6] Trebuie subliniat faptul că primele definiţii oferite de către V. Cymbal se referă la conceptul rus de „sabotaj ideologic" sau „rebeliune ideologică". Vezi: *Контрразведывательный словарь*, Москва 1972, pp. 90-91. Un volum mare de informaţii despre „sabotajul ideologic" a fost dezvăşuit de către ofiţerul KGB şi corespondentul RIA Novosti, Jurij Bezmienow, vel Thomas Schuman. În opinia sa, „sabotajul ideologic", pe care l-a asociat cu războiul psihologic, agresiunea ideologică şi războiul propagandistic, este un process pe termen lung (care se desfăşoară pe parcursul ultimilor 15-25 de ani) fiind divizat în patru etape: „Demoralizarea", „Destabilizarea", „Criza" and „Normalizarea". Scopul acelui process este acela de a subjuga o ţară anume fără a fi necesară pornirea unui conflict armat deschis. Vezi: T.D. Schuman (J. Bezmienov), *Love Letter to America*, Los Angeles 1984, pp. 17–46. Compare: idem, *No „Novosti" is Good News*, Los Angeles 1985; *idem*, *World Thought Police*, Los Angeles 1986.

- computerizarea luptelor (pregătirea operaţiunilor);
- computerizarea câmpului de luptă (digitalizarea câmpului de luptă);
- război psihologico-informaţional:
  - educaţie militar-patriotică a cetăţenilor autohtoni;
  - pregătirea morală și psihologică a personalului militar;
  - operaţiuni psihologice împotriva personalului civil și militar al ţării ostile;
- război tehnico-informaţional:
  - utilizarea unor sisteme de comunicaţii și control într-o confruntare;
  - rolul și locul intelligence în războiul informaţional,
  - utilizarea unor programe speciale cu scopul de a:
    1) distruge sursele de informaţii;
    2) redistribui sursele de informaţii;
    3) asigura protecţia surselor de informaţii;
- pregătirea personalului care va lua parte la războiul informaţional,
- aspecte ale dreptului internaţional cu privire la războiul informaţional (Thomas, 1996, p. 34; Thomas, 1998, pp. 40–62; Thomas, 2009, pp. 465–491).

Trebuie menţionat faptul că la începutul anilor ’90 ai secolului trecut a fost creată o structură de tip reţea alcătuită din servicii speciale civile (FAPSI, FSB, SWZ) și o parte a forţelor armate. Aceasta avea responsabilităţi în domeniul războiului informaţional și al perfecţionării metodelor specifice, care includeau atât elemente psihologice, cât și tehnologice (Thomas, 1998, pp. 156–172). Acestea se raportau la modelul rus al „sabotajului ideologic” și la conceptul de „război rebel” al lui Evgeny Messner. Așadar, trebuie evidenţiat faptul că promovarea imaginii Federaţiei Ruse ca victimă a agresiunii Occidentului și complet nepregătită să facă faţă „războiului informaţional”, este doar parte a unui proces de dezinformare, care are scopul de a justifica „războiul împotriva «războiului informaţional» desfășurat împotriva Rusiei”.

Conceptul rus de „război informaţional” evoluează și este în mod continuu ajustat la situaţia geopolitică curentă (Thomas, 2010, pp. 265-301; Goble, 2009, pp. 181–196.). Acest aspect poate fi confirmat de constatările a doi distinși teoreticieni, asociaţi ai Centrul de Studii Strategice de Război al Sediului Forţelor Armate ale Federaţiei Ruse (în rusă: Центр военно-стратегических исследований Генерального штаба Вооружённых Сил Российской Федерации): col. Sergey Czekinov și gen. lt. rez. Sergey Bogdanov (Main, 2000, pp. 47-62; Чекинов, 2010 pp. 3-5; Giles, 2014, p. 21). Ei au utilizat termenul de „activităţi asimetrice” (în rusă: асимметричные действия) la nivelul societăţii ruse, definindu-l ca activităţi complexe și sistematice de ordin politic, diplomatic,

economic, informaţional şi militar. Ei demonstrează că o confruntare informaţională ar trebui să joace un rol important în procesul de dezintegrare al sistemului de management şi control al unei anumite ţări. Ar trebui, de asemenea, să influenţeze opinia publică, având ca rezultat, spre exemplu, demonstraţii anti-guvernamentale şi destabilizarea unei anumite ţări sau a altei entităţi care este ţinta acelor operaţiuni, a căror esenţă este utilizarea avantajului intelectual. În acest context,operarea sistemelor care prezintă lumea, oamenii, esenţa civilizaţiei şi direcţiile de dezvoltare ale acesteia, precum şi cele mai importante valori, ar trebui să fie recunoscute drept „războiul informaţional" contemporan (în rusă: информационное оружие).

În afară de factorii tehnico-informaţionali şi psihologico-informaţionali, ar trebui utilizate şi instrumente tehnico-ştiinţifice şi politico-psihologice. Aceste tehnologii ajută la influenţarea subiecţilor „războiului informaţional". Principalul obiectiv al acelui tip de război este acela de a manipula conştiinţa unei societăţi sau a unei naţiuni cu viziuni false asupra lumii înconjurătoare şi, prin direcţionarea şi stimularea activităţilor desfăşurate de către aceştia. Subiectul confruntării informaţionale va fi, atunci, sistemul de valori tradiţionale, idealuri şi mituri, care constituie baza culturală a unui anumit stat, precum şi baza sa de identificare. Scopul final este acela de a face victima să accepte forma de agresiune şi să considere că modul de gândire şi acţiunile impusesunt proprii. Din acest motiv geopolitica este atât de importantă în cazul „războiului informaţional" deoarece oferă argumentaţia ştiinţifică care serveşte drept o armă în purtarea acestui tip de război. Pe de altă parte, semnificaţia activităţilor asimetrice în sfera militară ar trebui să fie aceea de a atinge scopul fără un conflict armat. Acest lucru poate fi atins prin intimidarea duşmanului şi prin determinarea acestuia să realizeze, prin demonstrarea pregătirii militare într-un teritoriu strategic sau distrugerea celor mai periculoase entităţi ale sale, că un posibil conflict armat este inutil (Чекинов şi Богданов, 2010, pp. 13-22; Thomas, 2014, pp. 105-106; Короход, 2013, p. 302; Бухарин, Цыганов şi Бочкарева, 2013, pp. 14-21; Цыганов, Васин, Бухарин, 2007, pp. 25-30; Бухарин, Матвиенко, 2008, pp. 2-9; Rothstein, 2007, pp. 160-187; Лайнбарджер, 2013).

Evenimentele curente din Ucraina reprezintă un exemplu de model al utilizării aspectelor teoretice ale activităţilor asimetrice ruseşti prezentate anterior. De aceea este esenţial studiul fiecărei etape a conflictului în parte, prin comparaţie cu teoria. Pe 28 februarie 2014 o operaţiune a fost lansată în Crimeea cu scopul de a prelua controlul militar asupra peninsulei de către Federaţia Rusă. La operaţiune au participat forţele locale „de apărare ale Crimeei", sprijinite de formaţiuni neidentificate ale armatei ruseşti. Ei au preluat controlul asupra majorităţii instituţiilor strategice, precum aeroporturile, nodurile d transport şi pasajele, precum şi clădirile care aparţineau armatei ucrainene şi

Serviciului Secret ucrainean. Într-o săptămână, întreaga peninsulă era ocupată. Deşi unele clădiri au rămas sub conducerea armatei Ucrainei, acestea au fost incapacitate de a desfăşura activităţi militare prin tăierea curentului electric, a apei şi a celortalte utilităţi. Cel mai semnificativ amănunt este acela că întreaga operaţiune a fost desfăşurată fără declanşsarea unui conflict direct între cele două părţi. Autorităţile auto-proclamate din Simferopol au început să formeze forţele armate autonome pe baza trupelor de auto-apărare locale și a clădirilor pe care le-au ocupat de la armata ucraineană. Soldaţi înarmaţi cu feţele acoperite și purtând uniforme fără emblemă, numiţi „omuleţii verzi" sau „oamenii blânzi" au luat prin suprindere mass-media mondială și analiștii care comentau în mod ironic conflictul. Ei au preluat controlul asupra aeroportului din Sevastopol, susţinând că au venit să îl apere împotriva „trupelor Bandera din Kiev". Cu toate acestea, ei nu au informat pe nimeni cu privire la cine sunt și din ce ţară provin. Când a fost clar că presupusele trupe nu reprezintă un pericol pentru aeroport, ei au fost retraşi. În clipa în care informaţiile au devenit publice, aceste trupe s-au întors şi au preluat din nou controlul asupra aeroportului (Wilk, *Rosyjska interwencja wojskowa na Krymie* [online]; Iwański, Rodkiewicz, Wierzbowska-Miazga, Wilk, *Rosja wobec Ukrainy: nie tylko Krym* [online]).

Aceste activităţi sunt suficient de evidente pentru a fi considerate aşa-numite operaţiuni psihologice speciale, (în rusă: психологические специальные операции) aflându-se în competenţa trupelor de operaţiuni speciale ale GRU. Unul dintre foştii membrii ai acestei formaţiuni, Col. Vladimir Kvaczkov, a explicat că scopul acestor operaţiuni este acela de a manipula conştiinţa şi emoţiile oamenilor (ofiţerilor şi civililor) prin acţiuni de instaurare a confuziei şi demoralizării, pentru a-i face să empatizeze cu armata rusă (Квачков, 2010, p. 376). Acest lucru a putut fi realizat prin îndepărtarea emblemelor de pe uniformele soldaţilor, făcând în acest sens imposibilă identificarea ţării (aşa-numită cripto-operaţiune) şi a formaţiunii din care fac parte, precum şi prin interzicerea relaţionării, sub orice formă, cu civilii. Toate aceste au condus la numeroase interpretări contradictorii ale „omuleţilor verzi", „soldaţilor în uniforme" sau „oamenilor blânzi" şi la incapacitatea de a defini inamicul şi de a lua măsuri oportune. Mai mult, se poate afirma că elementul-supriză a fost asigurat, ceea ce a permis Rusiei să dea o interpretare proprie evenimentelor: pe parcursul demonstraţiilor paşnice din Maidan peste 100 de oameni au murit, în timp ce pe durata intervenţiei militare din Crimea nicio persoană nu a fost rănită. Această operaţiune a fost de asemenea descrisă drept o *operaţiune strategică de instigare bazată pe informaţii* (în rusă: стратегическая наступательная информационная операция) care a avut scopul de a preceda intervenţia militară, cu pregătiri bazate pe utilizarea informaţiilor (Почепцов, *Информационные операции и Крым: базовые*

причины для манипуляций și *Информационные операции и Крым: причины и следствия. Часть 2* [online])[7].

Astfel, activităţile ruse din Crimeea au confirmat una din regulile unui „război rebel" – cea care se referă la utilizarea unor mase rebele care au fost supuse de-a lungul anilor unei presiuni psihologico-informaţională adecvată (așa numita intoxicaţie) indusă de armata regulată (Darczewska, 2014, p. 20; Nord, 2004, pp. 87-111). Pentru atingerea acestui obiectiv au fost iniţiate activităţi multidirecţionale și în masă: canale radio și TV federale, ziare și resurse Internet. Acestea au fost sprijinite de diplomați, politicieni, politologi, experţi, precum și elitele din domeniul cultural și științific. Au fost aduse argumente conform cărora adevărata ameninţare la adresa Crimeei este reprezentată de „trupele Bandera care invadează peninsula", „trupele NATO care preiau controlul asupra Flotei de la Marea Neagră" sau „procesul de derusificare a cetăţenilor ucraineni". S-a afirmat, de asemenea, că guvernul de la Kiev a fost stabilit de serviciile speciale străine, în special cele americane și poloneze, ale căror reţele de spionaj (aflându-se sub apanajul Serviciului Militar de Informaţii,WSI) au fost pentru mulţi ani instrumentul intereselor americane în Ucraina, în special în sectorul energetic și petrolier (Савин, 2008, pp. 50-51). Așa cum a mai fost menţionat înainte, participarea activiștilor membri ai Uniunii Tineretului Eurasiatic în cadrul operaţiunii din Crimeea a fost confirmată, aspect care se raportează la definiţia „coloanelor rebele". Așa cum a anticipat Evgeny Messner, armata a jucat un rol secundar. Prima linie a aparţinut „maselor rebele" și „coloanelor rebele" care au preluat controlul asupra clădirilor și utilităţilor. Scopurile au fost atinse prin intermediul presiunii informaţional-psihologice, sabotajului și sancţiunilor economice, fără declanșarea unei lupte armate, prin preluarea controlului asupra unei infrastructuri intacte și evitarea înregistrării de victime în rândul soldaţilor și activiștilor, precum și în rândul locuitorilor peninsulei. Un element important a constat în atitudinea președintelui Vladimir Putin, care a rămas calm și care a dezinformat liderii occidentali (Cimbala, 2014, pp. 359-379; Berzins, 2014, pp. 1-7; Darczewska, pp. 5-6; 31-32; Vázquez Liñán, 2009, pp. 137-159).

Scenariul din Crimeea a fost repetat în următoarele luni. Pe 6 aprilie 2014 în Doneţk, Kharkiv și Lugansk, grupuri formate din câteva sute până la 2000 de activiști pro-ruși au pornit o rebeliune, care s-a încheiat cu preluarea controlului asupra clădirilor guvernamentale. În Kharkiv și Doneţk clădirile guvernamentale locale și cele aparţinând SBU au fost, de asemenea, ocupate.

---

[7] Pentru reglementări cu privire la dreptul internaţional asupra purtării uniformelor și emblemelor militare în timpul conflictelor armate, vezi: W. Hays Parks, *Special Forces' Wear of Non-Standard Uniform*, w: *International Law Studies. Issues in International Law and Military Operations*, J.B. Jaques (ed.), Newport 2006, pp. 69-121.

Activiştii au făcut cereri politice similare, ceea ce confirmă faptul că acţiunile au fost planificate înainte şi că au fost coordonate şi, în consecinţă, orchestrate, de către Rusia. Pe site-ul Uniunii Tineretului Eurasiatic pot fi regăsite instrucţiunile pentru „propria organizare" şi preluarea clădirilor de către grupuri (*Молот Правды. Жителям Юго – Востока: инструкция по самоорганизации* [online]). A fost proclamată înfiinţarea Republicii Populare Doneţk şi Republicii Populare Kharkiv, iar în Lugansk populaţia a refuzat să se supună guvernului ucrainean. Pe 11 mai 2014 a fost organizat un referendum cu privire la suveranitatea districtelor Doneţk şi Lugansk. Pe 12 mai 2014 a fost aprobată o rezoluţie cu privire la suveranitatea Republicii Populare Doneţk şi Republicii Populare Lugansk şi au fost demarate negocieri cu privire la înfiinţarea Novorossiyei. Acesta a fost un moment cheie care a marcat trecerea la un alt nivel al conflictului în momentul în care autorităţile celor două republici auto-proclamate au înfiinţat miliţii armate cu aportul semnificativ al unor instructori din Rusia (Iwański, Menkiszak, *Prorosyjski „separatyzm" narzędziem przymuszenia Ukrainy do federalizacji* [online:]).

Exemplul lui Igor Strielkov vel Girkin este relevant în acest context. Pe 15 aprilie 2014 Serviciul de Presă al SBU a anunţat că unul dintre liderii grupului subversiv de separatişti care ocupă clădirile guvernametale din Sloviansk a fost identificat. Se pare că acesta era sus-menţionatul Igor Strielkov care, potrivit SBU, a fost soldat al GRU Spetsnaz, ceea ce a făcut evident faptul că separatiştii erau instruiţi şi sprijiniţi de serviciile de informaţii militare ruse. Strielkov a devenit în scurt timp subiect al războiului informaţional dintre părţile implicate în conflict: Ucraina a expus conexiunile pe care acesta le avea cu serviciile speciale ruseşti pentru a demonstra implicarea acelor servicii în activităţile separatiste, în timp ce propaganda rusească l-a înfăţişat pe Strielkov drept un erou al luptei naţionale pentru libertate. Astfel, un pasionat de istorie şi reconstituiri istorice a devenit un soldat în lupta pentru libertatea Novorossiyei – voluntar, din considerente patriotice (Скоморохов, 20.V.2014). Strielkov însuşi admite că el nu a fost niciodată un membru al GRU, ci al FSB. Numele său real este Girkin şi „Strielkov" este numele său fals (Виноградов, 5.VII.2014). Aleksandr Czerkasov, Preşedintele Fundaţiei pentru Drepturile Omului „Memoriał", a expus detalii interesante cu privire la adevăratele activităţi desfăşurate de Igor Girkin. Bazându-se pe declaraţiile martorilor, el a arătat că în anul 2001 Girkin a participat la omorârea şi răpirea cetăţenilor ceceni, la acel moment fiind membru al Regimentului Independent 45 pentru Operaţiuni Speciale al Forţelor Armate Aeriene ale Federaţiei Ruse (în rusă: 45-й Отдельный полк

специального назначения Воздушно-десантных войск Вооружённых Сил Российской Федерации) (Черкасов, 21 mai 2014).

Principala sarcină a formaţiunilor militare de acel tip era reprezentată de desfășurarea de acţiuni de intelligence speciale (în rusă: специальная разведка) prin utilizarea tuturor mijloacelor specifice – de la observare, la acţiuni de luptă vizând prinderea persoanelor sau ocuparea clădirilor desemnate, la intelligence radio-tehnic (Министерство обороны РФ, *Разведывательная Подготовка Подразделений ВДВ*, pp. 5-10, 56-71.). O parte importantă a activităţii lor este de asemenea constituită de *operaţiunile speciale care vizau formarea, sprijinul și utilizarea în luptă a forţelor neregulate* (Russian: специальные операции по формированию, поддержке и боевому применению иррегулярных сил). Potrivit lui Kvaczkov astfel de operaţiuni vizează înfiinţarea unor formaţiuni neregulate care să desfășoare activităţi specifice forţelor armate, aspect de care Federaţia Rusă este deosebit de interesată. Acestea includ sarcini în domeniul intelligence pentru grupurile de gherilă și trupele de insurgenţi, precum și pentru organizaţiile implicate sau care sunt susceptibile de a se implica într-un anumit conflict. Includ, de asemenea, orice formă de ajutor, în special în domeniul logistic și al pregătirii, precum și utilizarea a numeroase mijloace de protecţie operaţională cu ajutorul reţelei de spionaj avută la dispoziţie (Квачков, 2010, p. 376). Așadar, se poate concluziona că exemplul lui Strielkov este o confirmare vie a sprijinului oferit de Federaţia Rusă miliţiilor și sepratiștilor din regiunile Doneţk și Lugansk, atât pe parcursul pregătirilor, cât și pe parcursul desfășurării conflictului. SBU l-a acuzat pe Strielkov că a directat activităţile operaţionale din Crimeea cu scopul de a pregăti penetrarea și lichidarea reţelei ucrainene de spionaj dinSloviansk și Kramatorsk (Скоморохов, 20.V.2014). Cu toate acestea, trebuie subliniat faptul că linia de front a activităţilor armate aparţine miliţiei, forţele speciale ruse jucând doar un rol de susţinere. Un exemplu interesant al acestui fapt este telegrama de la Strielkov în care acesta raportează că sursa sa personală de informaţii din Kiev l-a informat cu privire la o încercare a postului de televiziune ucrainean de realizare a unui reportaj. Reportajul urma să trateze tema „presupuselor crime ale soldaţilor ruși". Apoi Strielkov îi cere lui Dughin să publice acele informaţii pe Internet, fapt care i-ar conferi Federaţiei Ruse un avantaj și care ar discredita încercarea Ucrainei (*Сводки от Стрелкова Игоря Ивановича. Сообщение от ополчения* [online]).

Așadar, acesta este un exemplu elocvent al sprijinului informativ acordat separatiștilor de către forţele speciale ale Federaţiei Ruse. Miliţia este formată din mai multe grupuri de oameni care desfășoară activităţi de gherilă. Conducătorii acestor grupuri provin din mediul militar, adesea din Rusia, sau au fost antrenaţi în această ţară. Trebuie avut în vedere faptul că ei au cunoștiinţe precise cu

privire la teatrul de activităţi armate și caracterul acestuia, din moment ce majoritatea veteranilor din forţele speciale, care au lucrat în Ucraina, au plecat în Federaţia Rusă după prăbușirea Uniunii Sovietice (Козлов, 2010, pp. 151-161). După declanșarea unui foc deschis împotriva armatei ucrainene, acele trupe se retrăgeau de cele mai multe ori pentru a atrage armata în lupte de stradă. De asemenea, au pus la cale capcane care erau foarte eficiente. Un bun exemplu și o confirmare a acestui fapt este operaţiunea desfășurată pe 22 mai 2014 asupra orașului Wolnovacha, în care separatiștii au distrus cea de-a 55-a Brigadă Mecanizată a Forţelor Armate ucrainene, omorând 18 soldaţi și rănind alţi 32, aceasta fiind pierderea cea mai mare suferită de armata Ucrainei în istoria sa de 23 de ani. Separatiștii au fost sprijiniţi de civili, aceștia blocând coloanele ucrainene. Așadar, acesta este un exemplu evident al cooperării dintre „masele rebele" și „miliţia rebelă" descrise de Evgeny Messner (Żochowski, Wilk, și Konończuk, *Konflikt w Donbasie – wymuszona deeskalacja?* [online]).

Un element la fel de important al unui „război rebel" este reprezentat de activarea „coloanelor rebele". Definiţia pe care Messner a atribuit-o acestora se poate aplica grupurilor de mercenari și voluntari care provin nu doar din Federaţia Rusă, ci de pe întreg teritoriul post-Sovietic și chiar din Balcani. Este cunoscut faptul că printre „apărătorii Novorossiyei" există și un grup de aproximativ 250 de sârbi cunoscuţi sub numele de „Jowan Szewicz". Numărul în creștere al mercenarilor este însoţit de livrările de echipamente militare și alte provizii de pe teritoriul Federaţie Ruse. Se pare că, cu ajutorul Moscovei, mercenarii au preluat controlul asupra grupurilor separatiste locale[8].

---

[8] Aleskandr Matjuszyn poreclite „Warjag", unul dintre liderii forţelor armate ale Republicii Populare Donețk, poate fi un exemplu excelent al atitudinii ideologice caracterizate de Messner in definiția oferită „ coloanelor rebele". Acesta a oferit un interviu în care a dezvăluit din culisele activităţilor sale în Ucraina, unde obiectivul său principal a fost acela de a pregăti o revoltă. După ce a absolvit facultatea, a începută să își desfășoare activitatea politică în rândul skinhead-ului din Moscova, participând la revolte și la lupte de stradă. Apoi s-a alăturat Partidului Național Bolșevic al lui Dughin, condus de Eduard Limonov. După ce s-a întors de la Moscova, acesta s-a ocupat de stabilirea structurilor de partid din districtul Donețk. Cu toate acestea, el a părăsit partidul după ce „ Limonov s-a vândut liberalilor". În timpul „ revoluției portocalii" el a fost unul dintre fondatorii campaniei intitulate „ Ucraina fără Iușcenko". După ce a părăsit partidul s-a alăturat unei noi mișcări numite Republica Donețk (în rusă: движение «Донецкая Республика»). El și-a desfășurat activitățile în orașul Makiejevka. A fost arestat de către SBU. Din moment ce s-a ocupat de pregătirea grupurilor tinere din Republica Donețk în 2007, a fost acuzat de conducerea unor grupuri armate ilegale. Aleskandr Matjuszyn subliniază rolul imens al cooperării sale cu suporterii mișcării eurasiatice a lui Dughin și cu naționaliștii ruși la acel moment. El a declarat că înființarea Republicii Populare Donețk nu a fost una accidentală – a fost un plan pe termen lung al activiștilor. Declarațiile sale au evidențiat fapătul că aceștia au fost sprijiniți de Moscova. După ce Republica Populară Donețk și-a declarat independența, el a fost numit comandantul Batalionului de Voluntari „ Warjag" (în rusă: Добровольческий батальон «Варяг»), aflat în subordinea Ministerului Securității de Stat al acelei republici.

Activităţile ruse pe teritoriul Ucrainei au scos în evidenţă eficienţa organizaţiilor de tip nou. Un exemplu elocvent poate fi Eurasian Youth Union, ai cărei activişti i-au sprijinit în mod evident pe separatişti, prin organizarea referendumurilor în Moscova şi oferindu-le sprijin informativ, dar în principal prin coordonarea ajutorului umanitar (Публичная интернет-библиотека Владимира Прибыловского, *Евразийский Союз Молодежи* [online]). Pe 14 mai 2014, pe site-ul oficial al organizaţiei putea fi observat anunţul referitor la recrutarea de *echipe de voluntari care să lupte împotriva mercenarilor americani naziști și oligarhilor de pe teritoriul Novorossiyeii* (Евразийский Союз Молодёжи, *Помощь Донбассу, записаться добровольцем!* [online]). Pavel Karnishev, actualul lider al organizaţiei, a declarat că un grup de aproximativ 1000 de voluntari a fost înfiinţat. Organizaţiaparamilitarănumităeurasian Youth Union este o facţiune de tineret a International Eurasian Movement. Eurasian Youth Union a fost înfiinţată în timpul convenţiei care a avut loc pe 26 ianuarie 2005 şi la care au participat 600 de persoane. Numărul actual al membrilor săi este necunoscut. Structurile Uniunii sunt active nu doar în Rusia, ci şi în alte ţări care aparţin Comunităţii Statelor Independente, precum și în Germania, Italia și România. Conducerea sa restrânsă îi include pe Karnishev, Dmitri Jefremov, Arthur Dughin și Aleksey Bielajev-Gintovt – „stylist-ul" organizaţiei. Uniunea are structuri similare celor militare în plan central, cât şi local (Публичная интернет-библиотека Владимира Прибыловского, *Евразийский Союз Молодежи*…).

Principalii lideri sunt numiţi moderatori. Profilul ideatic al Uniunii se caracterizează prin atitudinea radicală anti-americană și atitudinea ostilă față de Occident. Cu toate acestea, profilul ideatic creat de Aleksandr Dughin este de asemenea modelat de referinţe oculte[9]. Principalul scop al Uniunii este

---

Principalul obiectiv al acelui batalion, în afară de lupta de pe front, este acela de a lupta împotriva și de a elimina „ sabotorii" și „ hoții". M. Учитель, *Александр «Варяг» Матюшин: нам нужна республика нового типа* [online], http://rossia3.ru/politics/vatjag_matyushi [availability: 31 VII 2014].

[9] Este de menționat faptul că emblema Uniunii Tineretului Eurasiatic este o „ Stea a Haosului" stilizată, simbolul renașterii magice în Occident. Simbolul, preluat de Dughin din lucrările ocultistului Aleister Crowley, se referă la „ magia haosului". Din moment ce pentru Dughin termenul de „haos" este un sinonim al termenului diferit, opus culturii occidentale, de „ordine", se crează noi posibilități de acțiune pentru atingerea scopurilor geopolitices. Dughin a avut o atitudine pozitivă vizavi de lucrările lui Crowley (care, apropo, a fost un agent MI6) și a scris că *trendurile revoluționare radicale au fost percepute de Crawleyca realizarea furtunii echinocțiului cu ajutorul puterilor haosului pentru a șterge rămășițele civilizațiilor putrede, apropiindu-se, astfel, de sfârșitul logic și ciclic.*Vezi: L. Sykulski, *Koncepcja Radykalnego Podmiotu i „czwarta teoria polityczna" Aleksandra Dugina w kontekście bezpieczeństwa Polski i Unii Europejskiej,*

acela de a stabili o armată eurasianistă și de a purta o revoluție eurasianistă. Eurasian Youth Unionare o structură de tip rețea; încearcă să influențeze mediul tineretului înțeles în sens larg, prin utilizarea arsenalelor caracteristice războiului informațional. În acest caz, cel mai important rol este jucat de Divizia Analitico-Informațională, așa-numita celulă informațională a a KGB, care a fost condusă de Valery Korovin (Публичная интернет-библиотека Владимира Прибыловского, *Коровин Валерий Михайлович* [online]; *Катехизис члена Евразийского Союза Молодежи* [online]; Arquilla, Ronfeldt, 2001, pp. 1-25). Fără dubii acea organizație este un sprijin informațional pentru Kremlin. Membrii săi tratează războiul informațional din perspectiva științifică. În anul 2007, activiștii uniunii au desfășurat un atac cibernetic la adresa site-ului prezidențial ucrainean. După acest incident, structurile ucrainene ale organizației au fost controlate cu stricteţe de către SBU, fapt care a determinat părăsirea uniunii de mulți dintre membrii săi (*Евразийские боевики из Восточного Казахстана?* [online]).

Cu toate acestea, trebuie subliniat faptul că Eurasian Youth Union este doar una din multele „coloane rebele". Aleksandr Dughin și adepții acestuia au adoptat cu rapiditatea ideea de „război informațional". Conceptul a fost preluat de Dughin de la ideologii așa-numitei mișcări Noua Dreaptă. Obținerea puterii politice (în regiune, țară sau la nivelul întregului continent) ar trebui să fie însoțită de impunerea propriei culturi, propriului mod de gândire și a propriului sistem de valori. Pentru a putea realiza acest lucru, trebuie desfășurată o îndoctrinare cultural-ideologică a mediului universitar și a reprezentanților unor profesii precum cea de doctor sau avocat, care au capacitatea de a influența opinia publică. O asemenea idee a fost postulată de Alain de Benoist, care este respectat de către eurasiatici și care spijină „A Patra Teorie Politică" a lui Aleksandr Dughin. Eurasian Youth Unioneste doar o parte a unei organizații mai mari, cu caracterul unei rețele, care este o „bandă rulantă" a ideologiei care provine direct din Moscova[10].

Pentru a concluziona, trebuie subliniat faptul că Rusia a prezentat propriul său concept de „război informațional" întregii lumi. În acest caz putem vorbi despre diversificarea și sincronizarea multor activități.

„Przegląd Geopolityczny" 2014, issue 8, p. 236; A. G. Dugin, *The Multipolar World and the Postmodern*, „Journal of Eurasian Affairs" 2014, issue 2, pp. 11-12.

[10] Un exemplu al rețelei este o altă organizație numită Alianța Revoluționară Globală, GRA, înființată de Dughin. Aceasta este un nou tip de organizație care nu este legată în mod oficial de centrul pentru care funcționează. Asemenea organizații realizează așa-numita strategie de rezistență non-directată. Vezi: L. Sykulski, *Koncepcja Radykalnego Podmiotu*..., p. 238. Compare: J. Tomasiewicz, *Strategia oporu niekierowanego w wojnie asymetrycznej*, „Przegląd Geopolityczny" 2009, issue 1, pp. 161-191.

Caracteristica lor comună este utilizarea și prelucrarea informaţiei ca principală armă bazată pe factori psihologici, sprijiniţi de utilizarea soluţiilor tehnologice moderne. Războiul informaţional presupune desfășurarea de activităţi asimetrice, care sunt direcţionate cu îndemânare. Toţi factorii menţionaţi mai sus creează un concept unic de provenienţă rusească, de „război hibrid", care constituie o ameninţare reală la adresa securităţii Occidentului. Modelul rus de purtare a unui conflict, în genealogia sa, se raportează la filosofia de război a lui Sun Tzu și la patrimoniul militar al populaţiei din Est, bazându-se pe conceptul de slăbirea maximă a adversarului cu cele mai mici pierderi. Luând în considerare specificaţiile activităţilor ruse și posibilele scenarii ale evoluţiei situaţiei, se poate considera că în cazul dezacordului exprimat de Kiev cu privire la federalizarea Ucrainei, războiul, indiferent de forma sa, poate dura ani de zile. Este posibil ca diviziunile dintre părţile care poartă acest război civil, ca urmare a numărului mare de victime, să se aprofundeze, iar „ocuparea" constantă a districtelor din partea de est a statului de către forţele guvernamentale să fie inevitabilă pentru a putea stabiliza acea parte a Ucrainei.

Ocuparea, pe de altă parte, ar însemna cheltuirea unor sume de bani pe baze militare imense, echipate cu tehnologie militară de ultimă oră și protejarea operaţională maximă a acelei regiuni de către serviciile speciale ucrainene, aspect care ar putea fi foarte costisitor pentru acea ţară. Într-o perspectivă viitoare, această situaţie poate conduce la escaladarea conflictului, care este purtat nu numai sub forma luptei regulate, ci și sub forma activităţilor tipic teroriste desfășurate pe teritoriul întregului stat, destabilizându-l. Situaţia poate fi comparată cu Ulster[11].

Diferenţa este aceea că în cazul ucrainean, conflictul este la o scală mai largă. Raportările presei internaţionale cu privire la atacurile teroriste din

---

[11] Conflictul din Ulster (Irlanda de Nord) este cel mai cunoscut și mai descris conflict european, în care au fost utilizate metode teroriste. Principalul motiv al acestui conflict a fost reprezentat de dorința naționaliștilor irlandezi și republicanilor (majoritatea catolici) de a alipi provincia guvernată de Marea Britanie la Republica Irlanda. Acest lucru a fost împotriva unioniștilor (majoritatea protestanți) care își doreau integritatea cu Marea Britanie. Conflictul a luat o formă atât militară, cât și politică, cu implicarea simultană a politicienilor, organizațiilor paramilitare și teroriste, precum și a forțelor de securitate ale Marii Britanii și Irlandei. Activitățile au fost desfășurate cu precădere pe teritoriul Irlandei de Nord. Din când în când, acestea escaladau pe teritoriile Angliei, Irlandei și Europei continentale. A durat până la sfîrșitul anilor '60 ai secolului trecut, până la semnarea Acordului din Vinerea Bună la Belfast în 1998. Chiar dacă acordul a fost semnat, au mai avut loc atacuri ocazionale. Vezi pe larg: J. Loughlin, (2010), *The Ulster Question Since1945*, London–New York 2003; J. Muller, *Language and Conflict in Northern Ireland and Canada: A Silent War*, London–New York; L.A. Smithey, (2011), *Unionists, Loyalists, and Conflict Transformation in Northern Ireland*, Oxford.

Ucraina vor deveni la fel de banale ca cele referitoare la explozia unei alte bombe în Irak sau Palestina. Cu toate acestea, există un singur posibil scenariu. Separatiştii vor primi sprijini (uman şi tehnologic) care le va permite nu numai să îşi menţină controlul asupra Donbass-ului, dar şi să desfăşoare activităţi ofensive în partea de vest a ţării. Potenţialul unor asemenea activităţi este semnificativ: în Odessa, Kharkiv, Zaporizhia sau Dnipropetrovsk mii de separatişti aşteaptă ordine şi armament. Criza economică şi emergenţa unor mişcări anti-guvernamentale în Ucraina favorizează un asemenea scenariu. O chestiune diferită este reprezentată de mişcările separatiste din Zakarpattia Oblast, care se pare că escaladează odată cu problemele interne ale Republicii Moldova. În acest caz intervenţia militară oficială a Rusiei poate fi considerată ca fiind una dintre posibilităţi.

Referinţe bibliografice:

1. Dugin, A.G., (14 martie 2014), *Geopolityka znaczenia. Semantyczna wojna wokół Ukrainy* accesibil pe http://xportal.pl/?p=13003.
2. Бердяев, Н.А., (1990), *Судьба России. Опыты по психологии войны и национальности. Репринтное воспроизведение издания 1918 г.*, Москва 1990.
3. Le Donne, J.P., (2004), *The Grand Strategy of the Russian Empire, 1650–1831*, Oxford.
4. Nowak, A., (2008), *History and Geopolitics. A Contest of Eastern Europe*, Warsaw.
5. *Russia between East and West: Russian Foreign Policy on the Threshold of the Twenty-First Century,* (2003), G. Gorodetsky (ed.), London.
6. Grachev, A., (2005), *Putin's Foreign Policy Choices,* w: *Leading Russia: Putin in Perspective Essays in Honour of Archie Brown,* A. Pravda (ed.), Oxford.
7. Wiśniewski, R., (2013), *Przemiany terytorialne państwa rosyjskiego – aspekt historyczno-polityczny,* in: *Studia nad geopolityką XX wieku,* P. Eberhardt (ed.), Warszawa.
8. Grabowski, T.W., (2011), *Rosyjska siła. Siły Zbrojne i główne problemy polityki obronnej Federacji Rosyjskiej w latach 1991–2010,* Częstochowa.
9. Кириллов, В.В., Крючков, Ю.Н., (2008), *Влияние войны на развитие и международное значение России в мире,* în „Военная мысль", issue 2.
10. Р. Эллисон, (2005), *Россия, региональные конфликты и применение военной силы*, in: *Вооруженные силы России: власть и политика*, С.Э. Миллер, Д. Тренин (red.), Кембридж–Лондон.
11. Колосов, В. А., (1996), *Российская геополитика: традиционные концепции и современные вызовы*, „Общественные науки и современность", issue 3.

12. Колосов, В. А., Мироненко, Н.С., (2001), *Геополитика и политическая география: Учебник для вузов*, Москва.
13. Косолапой, Н.А., (1996), *Геополитика как теория и диагноз (метаморфозы геополитики в России)*, „Бизнес и Политика", isuue 4.
14. Marciniak, W., (2004), *Przestrzeń jako kategoria dyskursu politycznego w Rosji współczesnej*, Warsaw.
15. Mäkinen, S., (2008), *Russian Geopolitical Visions and Argumentation. Parties of Power, Democratic and Communist Opposition on Chechnia and NATO, 1994–2003*, Tampere.
16. Isakova, I., (2005), *Russian Governance in 21th Century. Geostrategy, Geopolitics and Governance*, London–New York.
17. Ištok, R., Plavčanová, D., (2013) *Russian Geopolitics and Geopolitics of Russia. Phenomenon of Space*, „European Journal of Geopolitics", issue 1.
18. Sykulski, L. (2014), *Geneza rosyjskiej geopolityki*, w: *Studia nad rosyjską geopolityką*, L. Sykulski (ed.), Częstochowa.
19. Коровин, В., (24.IV.2014), *Геополитика вместо идеологии*, „Известия" [online], http://izvestia.ru/news/569829 [availability: 20 VI 2014].
20. Пустошкин, В.В., (1976), *Геополитические теории войны*, in: *Советская военная энциклопедия. Том 2: Вавилон – Гражданская война в Северной Америке*, А.А. Гречко (red.), Москва.
21. Grygajtis, K., (2011), *Józef Stalin oraz sowiecka geopolityka i geostrategia lat 1924–1953*, Nysa.
22. Kerr, D., (1995), *The New Eurasianism: The Rise of Geopolitics in Russia's Foreign Policy*, „Europe-Asia Studies", issue 47.
23. Smith, G., (1999) *The Masks of Proteus: Russia, Geopolitical Shift and the New Eurasianism*, „Transactions of the Institute of British Geographers. New Series", issue 24.
24. O'Loughlin, J., Toal, G., Kolossov, V., (2005), *Russian Geopolitical Culture and Public Opinion: The Masks of Proteus Revisited*, „Transactions of the Institute of British Geographers. New Series", issue 30.
25. Дугин, А.Г., (1997) *Основы геополитики. Геополитическое будущее России*, Москва.
26. Potulski, (2010), *Współczesne kierunki rosyjskiej myśli geopolitycznej: między nauką, ideologicznym dyskursem a praktyką*, Gdańsk.
27. Tuathail, G.Ó., (1998), *Postmodern Geopolitics? The Modern Geopolitical Imagination and Beyond*, w: *Rethinking Geopolitics*, Ó Tuathail, S. Dalby (ed.), London–New York.
28. Lashchenova, E. (2013), *National Archetypes of Russia's Foreign Policy*, „International Affairs. A Russian Journal of World Politics, Diplomacy and International Relations" 2013, issue 2.

29. T. Ambrosio, G. Vandrovec, *Mapping the Geopolitics of the Russian Federation: The Federal Assembly Addresses of Putin and Medvedev*, „Geopolitics" 2013, issue 18, no. 2.
30. Г. Дугин, *Стратегические выводы Прямой Линии Путина* [online], http://evrazia.org/article/2505 [availability: 20 VI 2014].
31. В. Иванов, *Дугин – политический Мерлин России* [online], http://www.evrazia.info/article/4377 [availability: 20 VI 2014].
32. J.B. Dunlop, *Aleksandr Dugin's "Neo-Eurasian" Textbook and Dmitrii Trenin's Ambivalent Response*, „Harvard Ukrainian Studies" 2001, issue 25.
33. A. Umland, *Aleksandr Dugin's Transformation from a Lunatic Fringe Figure into a Mainstream Political Publicist, 1980–1998: A Case Study in the Rise of Late and Post-Soviet Russian Fascism*, „Journal of Eurasian Studies" 2010, issue 1.
34. M. Wojnowski, *Aleksandr Dugin a resorty siłowe Federacji Rosyjskiej. Przyczynek do badań nad wykorzystaniem geopolityki przez cywilne i wojskowe służby specjalne we współczesnej Rosji*, „Przegląd Bezpieczeństwa Wewnętrznego" 2014, issue 10.
35. A. Wejkszner, *Wojny XXI wieku. Istota współczesnych konfliktów asymetrycznych*, in: *Zagrożenia asymetryczne współczesnego świata*, S. Wojciechowski, R. Fiedler (ed.), Poznań 2009.
36. I. Arreguin--Toft, *How the Weak Win Wars: A Theory of Asymmetric Conflict*, Cambridge 2005.
37. D.J. Katz, *Waging Financial War*, „Parameters" 2013, issue 43.
38. P. Eberhardt, *Koncepcje geopolityczne Aleksandra Dugina*, „Przegląd Geograficzny" 2010, issue 82.
39. А.Г. Дугин, *Геополитика: Учебное пособие для вузов*, Москва 2011.
40. А.Г. Дугин , *Геополитика России: Учебное пособие для вузов*, Москва 2012.
41. *Политсовет ОПОД «Евразия», Евразия превыше всего (манифест Евразийского движения)*, in: *Евразийский взгляд. Основные принципы доктирнальной евразийской платформы*, Н. Мелентьева (ed.), Москва 2001.
42. А.Г. Дугин, *Россия может быть или великой, или никакой*, in: *Основы евразийства*, А.Г. Дугин (ed.), Москва 2002.
43. А.А. Сотниченко, *Турция: геополитическая ось Евразии*, in: *Геополитика. Информационно-аналитическое издание. Выпуск IX: Турция*, Л.В. Савин (ed.), Москва 2011.
44. *Геополитика Турции*, w: *Левиафан: Материалы семинаров по проблемам геополитики и многополярности*, А.Г. Дугин (ed.), Москва 2011.

45. A. Telkin, P.A. Williams, *Geo-Politics of the Euro-Asia Energy Nexus. The European Union, Russia and Turkey*, London 2011.
46. P. Eberhardt, *Koncepcja granicy między cywilizacją zachodniego chrześcijaństwa a bizantyńską na kontynencie europejskim*, „Przegląd Geograficzny" 2010, issue 76.
47. А.Г. Дугин, *Основы геополитики*…, pp. 368–370. Compare: Л.В. Савин, *Россия–Украина–Польша: геополитические императивы*, in: *К геополитике*, Л.В. Савин (red.), Москва 2011.
48. А.Л. Бовдунов, *Политико-географические образы Центральной и Восточной Европы и геополитическая организация региона*, in: *Геополитика. Информационно-аналитическое издание. Выпуск X: Восточная Европа*, Л.В. Савин (ed.), Москва 2011.
49. А.Г. Дугин, *Этносоциология*, Москва 2011, pp. 8–25; В.Э. Багдасарян, *Этнос и проблема цивилизационной идентичности*, w: *Этноцентрум: Сборник материалов по проблемам этносоциологии и социальной антропологии*, А.Г. Дугин, А.Л. Бовдунов (ed.) Москва 2012.
50. *Czekam na Iwana Groźnego. Rozmowa z Aleksandrem Duginem. Rozmawiał Grzegorz Górny*,Moscow 1998, „Fronda. Pismo poświęcone" 1998, issue 11–12.
51. А.А. Коваленко, *Перспективы федерализации Украины*, w: *Геополитика. Информационно-аналитическое издание. Выпуск II: Украина*, Л.В. Савин (ed.), Москва 2010.
52. А.Ю. Корнев, *Государственно-правовые аспекты развития крымского регионализма*, w: *Геополитика. Информационно-аналитическое издание*…, pp. 25–32; Л.В. Савин, *Национально-политическая идентификация в Украине и формы репрезентации власти*, w: *К геополитике*, Л.В. Савин (ed.), Москва 2011.
53. И.В. Максимов, *Цветная революция-социальный процесс или сетевая технология?* Москва 2010.
54. К. Черемных, М. Восканян, *Анонимная война*, „Изборский клуб" 2013, issue 6.
55. Н. Стариков, *„Оранжевая кровь"*, „Изборский клуб" 2013, issue 10.
56. Публичная интернет-библиотека Владимира Прибыловского, Съезд ЕСМ объявил повстанческую войну Украине [online], http://www.anticompromat.org/esm/esm02.html [availability: 29 VII 2014]:
57. A.G. Dugin, *The fate of Ukraine is settled. An interview given to the Russian state television in 2009* [online], http://geopolityka.net/prof-dugin-kwestia-podzialu-ukrainy-jest-juz-przesadzona/ [availability: 29 VII 2014].

58. А.Г. Дугин, *Евразийский проект и его украинская проблема* [online], http://www.odnako.org/magazine/material/evraziyskiy-proekt-i-ego-ukrainskaya-problema/ [availabilty: 29 VII 2014];
59. J. Darczewska, *Anatomia rosyjskiej wojny informacyjnej. Operacja krymska – studium przypadku,* Warsaw 2014.
60. А.Г. Дугин, *Геостратегический контекст противоборства морских и континентальных держав*, in: *Геополитика. Информационно-аналитическое издание. Выпуск XIV: Евразийский Союз*, Л.В. Савин (ed.), Москва 2012.
61. А.Г. Дугин, *Попкультура и знаки времени,* Санкт-Петербург 2005, pp. 486–493; B. Gołąbek, *Runet jako extra territorium byłego ZSRR – wokół rosyjskiej cybergeopolityki,* in: *Studia nad rosyjską geopolityką,* L. Sykulski (ed.), Częstochowa 2014.
62. А.Г. Дугин, *О Новороссии и вводе войск. Геополитический анализ* [online], http://novorossia.su/ru/node/3321 [availability: 29 VII 2014].
63. Группа экспертов во главе с Сергеем Глазьевым, *Украина: между Западом и Россией*, „Изборский клуб" 2014, issue 4.
64. Z. Brzezinski, *The Grand Chessboard. American Primacy and Its Geostrategic Imperatives*, New York 1997.
65. А.Г. Дугин, *Украинцев я очень люблю, я сам – украинец* [online], http://evrazia.org/article/2469, [availability: 29 VII 2014].
66. Д. Ньюман, *Кто придумал аннексировать украинский Крым? Многие россияне симпатизирует новому виду милитаристского патриотизма авторства Александра Дугина* [online], http://evrazia.info/article/4839 [availability: 31 VII 2014].
67. А.Г. Дугин, *Вводить войска в Новороссию* [online], http://dynacon.ru/content/articles/3314/ [availability: 31 VII 2014].
68. А.Г. Дугин, *Это моя война!* [online], http://dynacon.ru/content/articles/3274/ [availability: 31 VII 2014].
69. А.Г. Дугин, *В Крыму надо ввести духовную цензуру…* [online], http://crimea.mk.ru/articles/2014/06/04/aleksandr-dugin-v-krymu-nado-vvesti-dukhovnuyu-cenzuru.html [availability: 31 VII 2014].
70. Евразийский союз молодёжи, *Убит лидер ЕСМ по ЮФО Александр Просёлков* [online], http://rossia3.ru/proselkov3107 [availability: 31 VII 2014].
71. *Александр Проханов разработает идеологию Новоросии* [online], http://novorossia.su/ru/node/2386, [availability: 31 VII 2014].
72. *В Донецке состоялось первое заседание филиала Изборского клуба – Новороссия*, http://novorossia.su/ru/node/2783 [availability: 31 VII 2014].

73. *Идеология Новороссии. Изборцы предлагают своё видение идейной основы для нарождающегося на юго-западных рубежах РФ государства*, „Изборский клуб" 2014, issue 5.
74. *Россия. Географическое описание Российской Империи по губерниям и областям с географическими картами*, Санкт-Петербург 1913.
75. Н. Краснов, *Материалы для географии и статистики России, собранные офицерами Генерального штаба. Земли Войска Донского*, Санкт-Петербург 1863.
76. А.Г. Дугин, *Время Новоросии* [online], http://dynacon.ru/content/articles/3309/ [availability: 31 VII 2014].
77. *Крым в России. Что дальше?* [online], http://dynacon.ru/content/articles/2864/ [availability: 31 VII 2014].
78. idem, *Новороссия часть Русского мира* [online], http://dynacon.ru/content/articles/3419/ [availability: 31 VII 2014].
79. *Программа Общественно-политического движения „Партия Новороссии"* [online], http://novorossia.su/ru/node/1753 [availability: 31 VII 2014].
80. T.A. Olszański, *Ukraina: suwerenna decentralizacja czy niesuwerenny federalizm*?, „Komentarze OSW" 2014, issue 134.
81. A. Moshes, *More Stick, Less Carrot: Russia's Policy Towards Ukraine Following Recent Events*, „Russian Analytical Digest" 2014, issue 146.
82. M. Menkiszak, *Doktryna Putina: Tworzenie koncepcyjnych podstaw rosyjskiej dominacji na obszarze postradzieckim*, „Komentarze OSW" 2014, issue 131.
83. P. Panov, *Nation-building in Post-Soviet Russia: What Kind of Nationalism is Produced by the Kremlin?* „Journal of Eurasian Studies" 2010, issue 1.
84. S. Bieleń, *Erozja monocentryzmu w stosunkach międzynarodowych*, w: *Studia nad geopolityką XX wieku*, P. Eberhardt (ed.), Warszawa 2013.
85. А.Г. Дугин, *Четвертая политическая теория. Россия и политические идеи XXI века*, Санкт-Петербург 2009.
86. Zob. А.Г. Дугин, *Теория многополярного мира*, Москва 2013.
87. L. Sykulski, *Integracja polityczna Eurazji we współczesnej rosyjskiej myśli geopolitycznej*, in: *Studia nad geopolityką XX wieku*, P. Eberhardt (ed.), Warsaw 2013.
88. Л.Г. Ивашов, *Будущее Украины и Россия*, „Изборский клуб" 2014, issue 5.
89. А.Г. Дугин, *Крым в России. Что дальше?* [online], http://dynacon.ru/content/articles/2864/ [availability: 31 VII 2014].
90. В. Коровин, *Гибель Украины*, „Изборский клуб" 2014, issue 5.
91. Е.Э. Месснер, *Лик современной войны*, în: *Военная мысль в изгнании. Творчество русской военной эмиграции*, И.В. Домнин (ed.), Москва 1999.

92. K. Kraj, *Wojny asymetryczne czy miatieżewojna Jewgienija Messnera zagrożeniem dla bezpieczeństwa w XXI wieku,* „Bezpieczeństwo. Teoria i praktyka" 2012, issue 3.
93. idem, *Мятежевойна Jewgienija Messnera,* „E-Terroryzm" 2012, issue 2.
94. C. Schmitt, *Theorie des Partisanen Zwischenbemerkung zum Begriff des Politischen*, Berlin 1975.
95. T. Kochi, *The Partisan: Carl Schmitt and Terrorism*, „Law Critique" 2006, issue 17, pp. 267–295. А.Г. Дугин, *Философия войны*, Москва 2004.
96. Е.Э. Месснер, *Всемирная мятежевойна*, Москва 2004.
97. A. Schmid, *Terrorism as Psychological Warfare*, „Democracy and Security" 2005, issue 1.
98. С.А. Зелинский, *Информационно-психологическое воздействие на массовое сознание. Средства массовой коммуникации, информации и пропаганды — как проводник манипулятивных методик воздействия на подсознание и моделирования поступков индивида и масс*, Санкт-Петербург 2008.
99. А.В. Кириллов, *Информационно-психологическое воздействие на массовое сознание посредством СМИ (на примере операций по информационному обеспечению «MISO» военных конфликтов начала XXI в.)*, „Армия и общество" 2012, issue 2.
100. I.F. Beckett, *Modern Insurgencies and Counter-Insurgencies: Guerrillas and Their Opponents since 1750*, London–New York 2001.
101. J. Arquilla, *Insurgents, Raiders, and Bandits: How Masters of Irregular Warfare Have Shaped Our World*, Lanham 2011.
102. M. Kennard, *Irregular Army: How the US Military Recruited Neo-Nazis, Gang Members, and Criminals to Fight the War on Terror*, New York 2012.
103. E.V. Larson, D. Eaton, B. Nichiporuk, T.S. Szayna, *Assessing Irregular Warfare.*
A Framework for Intelligence Analysis, Santa Monica 2008.
104. U. Svete, *Asymmetrical Warfare and Modern Digital Media: An Old Concept Changed by New Technology?* w: *The Moral Dimension of Asymmetrical Warfare, Counter-terrorism, Democratic Values and Military Ethics*, Th.A. van Baarda, D.E.M. Verweij (ed.), Leiden–Boston 2009.
105. А.Г. Дугин, *Геополитика постмодерна. Времена новых империй. Очерки геополитики XXI века*, Санкт-Петербург 2007.
106. Л.В. Савин, *Сетецентричная и сетевая война. Введение в концепцию*, Москва 2011.
107. *От шерифа до террориста. Очерки о геополитике США*, Москва 2012; В.М. Коровин, *Третья мировая сетевая война*, Санкт-Петербург 2014.

108. Idem, *Главная военная тайна США. Сетевые войны*, Москва 2009; И.Н. Панарин, *Первая мировая информационная война. Развал СССР*, Санкт-Петербург 2010.
109. А.Г. Дугин, *Теоретические основы сетевых войн*, „Информационные войны" 2008, issue 1.
110. J. Ferris, *Netcentric Warfare, C4ISR and Information Operations: Towards a Revolution in Military Intelligence?* „Intelligence and National Security" 2004, issue 19.
111. J.W. Kipp, *'Smart' Defense From New Threats: Future War From a Russian Perspective. Back to the Future After the War on Terror*, „Journal of Slavic Military Studies" 2014, issue 27.
112. А.В. Бедрицкий, *Информационная война: концепции и их реализация в США*, Москва 2008.
113. И.Н. Панарин, *Информационная война и геополитика*, Москва 2006.
114. J. Arquilla, D.R. Ronfeldt, *The Emergence of Noopolitik: Toward an American Information Strategy*, Santa Monica 1999.
115. L.W. Grau, T.L. Thomas, *A Russian View of Future War: Theory and Direction*, „The Journal of Slavic Military Studies" 1996, isuue 9.
116. T.L. Thomas, *Deterring Information Warfare: A New Strategic Challenge*, „Parameters" 1996–1997, issue 26.
117. R. Heickerö, *Emerging Cyber Threats and Russian Views on Information Warfare and Information Operations*, Stockholm 2010.
118. Ю.В Лебедев, И.С. Лютов, В.А. Назаренко, *Война в зоне Персидского залива: уроки и выводы*, „Военная мысль" 1991, issue 11–12.
119. Л.В. Воронцова, Д.Б. Фролов, *История и современность информационного противоборства*, Москва 2006.
120. С.А. Комов, *Информационная борьба в современной войне: вопросы теории*, „Военная мысль" 1996, issue 3.
121. *О концепции информационной безопасности страны*, „Военная мысль" 1994, issue 4.
122. T.L. Thomas, *Information Warfare in the Second (1999–) Chechen War: Motivator for Military Reform?*, in: *Russian Military Reform 1992–2002*, A.C. Aldis, R.N. Mc Dermott (ed.), London–Portland 2003.
123. R. Clogg, *Disinformation in Chechnya: An Anatomy of a Deception*, „Central Asian Survey" 1997, issue 16.
124. T.L. Thomas, *The Russian View of Information War*,in: *The Russian Armed Forces at Dawn of the Millennium 7–9 February 2000*, M.H. Crutcher (ed.), Carlisle 2000.
125. S. Blank, *Russian Information Warfare as Domestic Counterinsurgency*, „American Foreign Policy Interests: The Journal of the National Committee on American Foreign Policy" 2013, issue 35.

126. K. Giles, „ *Information Troops" – a Russian Cyber Command?*, w: *Third International Conference on Cyber Conflict*, C. Czosseck, E. Tyugu, T. Wingfield (ed.), Tallinn 2011.
127. *Контрразведывательный словарь*, Москва 1972.
128. T.D. Schuman (J. Bezmienov), *Love Letter to America*, Los Angeles 1984.
129. T.L. Thomas, *Russian Views on Information – Based Warfare*, „Air and Space Power Journal" 1996, issue 115.
130. T.L. Thomas, *Russia's Information Warfare Structure: Understanding the Roles of the Security Council, FAPSI, the State Technical Commission and the Military*, „European Security" 1998, issue 7.
131. T.L. Thomas, *Russian Information Warfare Theory: The Consequences of August 2008*, in: *The Russian Military Today and Tomorrow. Essays in Memory of Marry Fitzgerald*, S.J. Blank, R. Weitz (ed.) Carlisle 2010.
132. P.A. Goble, *Defining Victory and Defeat: The Information War Between Russia and Georgia*, in: *The Guns of August 2008: Russia' War in Georgia*, S.E. Cornell, S. Frederick Starr (ed.), New York–London 2009, M.E. Sharpe.
133. S.J. Main, *The 'Brain' of the Russian Army: The Centre for Military-Strategic Research, General Staff (TsVSI GSh), 1985–2000*, „Journal of Slavic Military Studies" 2000, issue 13.
134. С.Г. Чекинов, *Центр военно-стратегических исследований Генерального штаба Вооруженных Сил Российской Федерации. История и современность*, „Военная мысль" 2010, issue 1, pp. 3–5; K. Giles, A. Monaghan, *Russian Military Transformation. Goal in Sight?*, Carlisle 2014, p. 21.
135. С.Г. Чекинов, С.А. Богданов, *Асимметричные действия по обеспечению военной безопасности России*, „Военная мысль" 2010, issue 3.
136. T.L. Thomas, *Russia's Information Warfare Strategy: Can the Nation Cope in Future Conflicts?*„Journal of Slavic Military Studies" 2014, issue 27.
137. Я.Д. Короход, *Информационно-психологические войны – оружие XXI века*, „Актуальні проблеми політики" 2013, issue 50.
138. С.Н. Бухарин, В.В. Цыганов, Ю.Г. Бочкарева, *Провокации в информационном противоборстве*, „Информационные войны" 2013, issue 1.
139. В.В. Цыганов, В.В. Васин, С.Н. Бухарин, *Интеллектуальные механизмы информационных войн*, „Проблемы управления" 2007, issue 1.
140. С.Н. Бухарин, Ю.А. Матвиенко, *Информационно-психологическая война как одна из форм разрешения социально-политических противоречий в современном обществе*, „Информационные войны" 2008, issue 4.

141. H.S. Rothstein, *Strategy and Psychological Operations*, w: *Information Strategy and Warfare. A Guide to Theory and Practices*, J. Arquilla, D.A. Borer (ed.), New York 2007.
142. П. Лайнбарджер, *Психологическая война. Теория и практика обработки массового сознания*, Москва 2013.
143. A. Wilk, *Rosyjska interwencja wojskowa na Krymie* [online], http://www.osw.waw.pl/pl/publikacje/analizy/2014-03-05/rosyjska-interwencja-wojskowa-na-krymie [availability: 16 VIII 2014];
144. T. Iwański, W. Rodkiewicz, A. Wierzbowska-Miazga, A. Wilk, *Rosja wobec Ukrainy: nie tylko Krym* [online], http://www.osw.waw.pl/pl/publikacje/analizy/2014-03-12/rosja-wobec-ukrainy-nie-tylko-krym [availability: 16 VIII 2014].
145. В.В. Квачков, *Применение Войск Специального Назначения в современных условиях*, in: *Спецназ ГРУ. Очерки истории. Кн. V: Новейшая история 1999–2010 гг.*, С.В. Козлов и др. (ed.), Москва 2010.
146. *Некоторые положения теории специальной операции и необходимость Сил Специального назначения в составе ВДВ*, in: *Спецназ ГРУ. Очерки истории. Кн. V: Новейшая история 1999–2010 гг.*, С.В. Козлов и др. (ed.), Москва 2010. Compare: И.Н. Воробьёв, *Информационно-ударная операция*, „Военная мысль" 2007, issue 6.
147. Г. Почепцов, *Информационные операции и Крым: базовые причины для манипуляций* [online:], http://psyfactor.org/psyops/infowar_krym.htm [disponibilitate: 16 VIII 2014].
148. W. Hays Parks, *Special Forces' Wear of Non-Standard Uniform*, w: *International Law Studies. Issues in International Law and Military Operations*, J.B. Jaques (ed.), Newport 2006.
149. P. Nord, *L'intoxication par une intoxicateur*,w: *La désinformation: Arme de guerre*, V. Volkoff (ed.), Lausanne 2004.
150. Л.В. Савин, *Украина в сетевой войне*, „Информационные войны" 2008, issue 3.
151. S.J. Cimbala, *Sun Tzu and Salami Tactics? Vladimir Putin and Military Persuasion in Ukraine, 21 February–18 March 2014*, „Journal of Slavic Military Studies" 2014, issue 27.
152. J. Berzins, *Russia's New Generation Warfare in Ukraine: Implications for Latvian Defense Policy*, Riga 2014.
153. M. Vázquez Liñán, *Putin's Propaganda Legacy*, „Post Soviet Affairs" 2009, issue 25.
154. *Молот Правды. Жителям Юго - Востока: инструкция по самоорганизации* [online], http://rossia3.ru/quotes/all/9007 [availability: 16 VIII 2014].

155. T. Iwański, M. Menkiszak, *Prorosyjski „separatyzm" narzędziem przymuszenia Ukrainy do federalizacji* [online:], http://www.osw.waw.pl/pl/publikacje/analizy/2014-04-09/prorosyjski-separatyzm-narzedziem-przymuszenia-ukrainy-do [availability: 16 VIII 2014].
156. Р. Скоморохов, *Портреты века: Игорь Стрелков*, „Военное обозрение" dated 20 V 2014 [online], http://topwar.ru/48026-portrety-veka-igor-strelkov.html [availability: 16 VIII 2014].
157. Д. Виноградов, *Боевые заслуги: кто научил воевать Игоря Стрелкова*, „Свободная Пресса" dated 5 VII 2014 [online], http://svpressa.ru/society/article/89194/?rss=1 [availability: 16 VIII 2014].
158. А. Черкасов, *Игорь Стрелков в Чечне. 2001 год, Веденский р-н,* Радиостанция «Эхо Москвы» от 21 мая 2014 [online], http://www.echo.msk.ru/blog/shalommani/1324504-echo/ [availability: 16 VIII 2014].
159. Министерство обороны РФ, *Разведывательная Подготовка Подразделений ВДВ*, Москва 1995.
160. *Сводки от Стрелкова Игоря Ивановича. Сообщение от ополчения* [online], http://vk.com/strelkov_info?w=wall-57424472_5439 [availability: 16 VIII 2014].
161. С.В. Козлов, *Противостояние*, w: *Спецназ ГРУ. Очерки истории. Кн. IV: Безвременье. 1989–1999гг.*, С.В. Козлов и др. (ed.), Москва 2010.
162. Żochowski, P., Wilk, A., Konończuk, P. *Konflikt w Donbasie – wymuszona deeskalacja?* [online], http://www.osw.waw.pl/pl/publikacje/analizy/2014-06-11/konflikt-w-donbasie-wymuszona-deeskalacja [availability: 16 VIII 2014].
163. *Noworosja: „Jowan Szewicz" rośnie w siłę* [online], http://xportal.pl/?p=15319 [availability: 16 VIII 2014].
164. Учитель, М. *Александр «Варяг» Матюшин: нам нужна республика нового типа* [online], http://rossia3.ru/politics/vatjag_matyushi [availability: 31 VII 2014.
165. Публичная интернет-библиотека Владимира Прибыловского, *Евразийский Союз Молодежи* [online], http://www.anticompromat.org/esm/esm_spr.html [availability: 31 VII 2014].
166. Евразийский Союз Молодёжи, *Помощь Донбассу, записаться добровольцем!* [online], http://rossia3.ru/news/2014/05/14/12:37:24 [availability: 31 VIII 2014].
167. Sykulski, L., (2014), *Koncepcja Radykalnego Podmiotu i „czwarta teoria polityczna" Aleksandra Dugina w kontekście bezpieczeństwa Polski i Unii Europejskiej*, „Przegląd Geopolityczny", issue 8.
168. Dugin, A.G., (2014), *The Multipolar World and the Postmodern*, „Journal of Eurasian Affairs", issue 2.

169. Публичная интернет-библиотека Владимира Прибыловского, *Коровин Валерий Михайлович* [online], http://www.anticompromat.org/esm/korovbio.html [availability: 31 VIII 2014].
170. *Катехизис члена Евразийского Союза Молодежи* [online], http://www.rossia3.ru/katehizis.html [availability: 31 VIII 2014].
171. Arquilla, J., Ronfeldt, D., (2001), *The Adwent of Netwar (Revisited)*, in: *Networks and Netwars: The Future of Terror, Crime, and Militancy*, J. Arquilla, D. Ronfeldt (ed.), Santa Monica.
172. *Евразийские боевики из Восточного Казахстана?* [online], http://z001.kz/news/view?id=1700 [availability: 31 VIII 2014].
173. Tomasiewicz, J. (2009), *Strategia oporu niekierowanego w wojnie asymetrycznej*, „Przegląd Geopolityczny", issue 1.

PARADIGME DE SECURITATE ÎN SECOLUL XXI

MEDIUL DE SECURITATE INFORMAŢIONAL. ATACUL CIBERNETIC – AMENINŢAREA MODERNĂ A SECOLULUI XXI

Raisa Gabriela ZAMFIRESCU*

„The new century risks being overrun by both anarchy and technology. The two great destroyers of history may reinforce each other."
(Cooper, 2007)

Abstract

The 21st century began with remarkable discoveries in countless fields, it has brought along a technological evolution unheard of but together with the positive aspects the negative ones have appeared, the latter being defined by specialists as pervert aspects. Certainly one of the greatest challenges is the one in computing where, according to Eric Schmidt, CEO of Google, starting of 2010, in 48 hours there is produced as many information as before 2010, but it is not knowledge what it is being produced, most of the registered data being noise, reason for which, generally speaking, information services and security structures must reevaluate the paradigm, the operating mode, the working methodologies and instruments. This evolution had and it still has a powerful contribution in transforming and modernizing the risks and threats to the security of a state, asymmetry being presently a success feature for the malware attacks of the new century; most times it is this feature that succeeds in ensuring the necessary strategic advantage.

Keywords: security, intelligence, Digital Age, hybrid warfare, cyber-attack.

Introducere

Una din teoremele cunoscute ale sociologiei atunci când vine vorba de societate şi comunitate aparţine omului de ştiinţă Herbert Spencer care, în activitatea sa de cercetare atât în biologie cât şi în sociologie, a emis teoria conform căreia, societatea este asemeni unui organism biologic, anume aceasta se naşte/se formează, creşte/evoluează, se maturizează iar apoi moare/dispare (Enciclopedia Britannica, 2014).

Societatea este într-o continuă evoluţie şi schimbare, fapt pe care nu îl putem stopa ori înlătura nerămânându-ne decât să acceptăm, să înţelegem

* Academia Naţională de Informaţii „Mihai Viteazul".

şi să lucrăm pentru a preveni ceea ce se poate şi a menţine securitatea naţională, dar şi pentru a fi îndeplinit rolul pe care îl are statul nostru în parteneriatele bilaterale, alianţele şi structurile internaţionale din care este membru. Ceea ce a fost înainte de 1990 ne-a ajutat să înţelegem ameninţările convenţionale, să le putem clasifica şi defini, să formăm un cadru de bază şi un model de analiză la care să ne raportăm în prezent, în această încercare de a cataloga şi eticheta atipicul şi imprevizibilul. Nu este un pattern uşor de realizat însă este cert că se încearcă reactualizarea sa constantă, completându-se periodic prin cotidianul pe care îl definim ca stare de stabilitate şi prin acţiunile întreprinse ce nu se încadrează în constructul securităţii cu toate ramificaţiile sale.

Odată cu această evoluţie constantă a tehnologiei, societatea s-a văzut pusă în faţa unor noi provocări, mediul academic începând a studia şi dezvolta noi ramuri precum netnografia[1], cybercultura, etnografia digitală, în timp ce sectorul securităţii ia contact din ce în ce mai des cu atacuri maliţioase de natură cibernetică. Un bun exemplu îl poate constitui atacul cibernetic la adresa SONY Pictures Entertainment, întreprins la sfârşitul anului 2014, un caz ale cărui ramificaţii s-au extins dincolo de industria entertainment-ului şi de impactul asupra celor în cauză prin invadarea corespondenţei şi publicării informaţiilor cu caracter personal, ajungându-se treptat până la administraţia prezidenţială a Statelor Unite ale Americii, a semnării unui acord trilateral şi nu în cele din urmă la o serie de declaraţii ameninţătoare din partea Coreei de Nord.

Scopul acestui demers este de a puncta evoluţia mediului de securitate în secolul al XXI-lea şi noile ameninţări cu care ne confruntăm atât individual cât şi colectiv ca societate, punctând de asemenea elementele definitorii şi repercusiunile atacului de la SONY Pictures, o anchetă ce este încă în curs de desfăşurare şi un moment considerat critic, un moment ce a schimbat Hollywood-ul modern.

Mediul de securitate

Securitatea unui stat „este un drept imprescriptibil care derivă din suveranitatea deplină a poporului, se fundamentează pe ordinea constituţională (...) are ca domeniu de referinţă valorile, interesele şi

[1] Netnografia este ramura etnografiei care analizează comportamentul internauţilor în exprimarea online a acestora, considerându-se că prin gradul ridicat de anonimitate şi de accesibilitate, toate interacţiunile care se petrec în câmpul virtual sunt catalogate ca fiind mai profunde şi mai complexe decât cele reale, aspecte datorate în special lipsei de consecinţe. Termenul a fost utilizat prima dată de Robert V. Kozinets şi defineşte o metodă mai rapidă şi mai accesibilă pentru cercetători, mai naturală şi mai discretă decât multe alte metode de cercetare, oferind informaţii despre limbaj, comportament, obiceiuri, simboluri, sensuri şi varii perspective culturale.

obiectivele naţionale." (Strategia de Securitate Naţională a României, 2007, p. 7) Pe scurt, aceasta poate fi definită ca protecţie a valorilor, intereselor şi obiectivelor existenţei unui stat, însă, înainte de a o fixa în categoria drepturilor fundamentale, securitatea poate fi definită, pe scurt, ca o situaţie dependentă de structura fiecărui sistem, având un set de particularităţi şi o serie de paradigme care au rămas neschimbate în faţa evoluţiei umane şi a tranziţiei societăţii post-industriale la cea modernă, evoluând ulterior la cea informaţională, actualmente trecând la o societate a cunoaşterii – cu o serie de paradigme ce se regăsesc la nivelul întregii materii vii deoarece nu doar statul necesită securitate ci chiar şi individul, la nivel biologic.

La rândul său, mediul de securitate poate fi definit ca ansamblul de activităţi, acţiuni şi preocupări care evidenţiază starea de securitate, al cărui principal factor de influenţă este globalizarea, proces ce a condus şi încă conduce la evoluţia şi inovaţia riscurilor şi ameninţărilor naţionale şi internaţionale. În ultimii 25 de ani ameninţările din mediului de securitate contemporan şi-au modificat atât caracterul – posibilitatea unui atac din partea altor state democratice este una redusă motiv pentru care trebuie să luăm în considerare ameninţări venite din partea unor actori non-statali ori transfrontalieri –, cât şi forma de manifestare, aceasta din urmă fiind definită în special de inovaţie prin evenimente de tip Lebădă Neagră – evenimente neaşteptate şi neprevăzute din viaţa socială care să fie rare, să aibă un impact deosebit prin consecinţele ulterioare, dar şi un grad de predictibilitate scăzut (Taleb, 2010, pp. 5-17).

Unul din cele mai întâlnite exemple pentru acest tip de evenimente este reprezentat, cu siguranţă de atacurile de la 11 septembrie (9/11). Ceea ce s-a întâmplat pe 11 septembrie 2001 a generat numeroase urmări de proporţii pe toate palierele şi sectoarele societăţii americane şi, într-o lume modernă interconectată, schimbarea paradigmei de securitate la nivel mondial. De asemenea, difuzarea atentatelor în direct de către mass-media a condus la o expunere continuă a fenomenului atacurilor teroriste, provocând instabilitate atât în plan intern pentru Statele Unite ale Americii cât şi în plan extern, în relaţiile şi parteneriatele diplomatice şi strategice. Astfel, 9/11 a devenit un eveniment mediatic care a adus în lumina reflectoarelor Islamul alături de vulnerabilitatea epicentrului capitalismului mondial, ziua fatidică a Americii urmând a fi definită de unii experţi ca ziua în care civilizaţia occidentală s-a ciocnit cu cea musulmană. Prin expunerea excesivă şi agresivă, mass-media a reuşit să creeze noi prejudecăţi şi stereotipuri la nivel social, iar panica şi teroarea răspândită de teroriştii Al-Qaeda prin atentatele din 11 septembrie, dar şi prin alte acţiuni similare ulterioare, au condus la

catalogarea acestora de către John Graz drept „simbol al modernităţii şi un simptom al globalizării" (Barna, 2010, p. 9).

Aceste noi ameninţări atipice şi asimetrice nu pot fi combătute ori prevăzute de state doar în mod individual, iar dacă înainte de 1990 se cunoşteau caracteristicile unui atac armat convenţional, în prezent un stat poate fi atacat mult mai uşor prin lansare unor acţiuni care să vizeze infrastructura naţională economică şi/sau informaţională, acţiune care ar necesita doar achiziţionarea unor sisteme computerizate performante, costuri mult mai reduse decât ar necesita echiparea unei armate. Acesta este unul din motivele pentru care majoritatea ţărilor aderă şi se îndreaptă către alianţe şi parteneriate economice, politice şi/sau militare, formându-se astfel o nouă ordine mondială caracterizată prin fluidizarea graniţelor statale.

Mediul de securitate a evoluat, iar asimetria a devenit o trăsătură de succes pentru atacurile cibernetice ale noului secol şi mileniu, uneori chiar această caracteristică asigurând rezultatul scontat. Asimetria ori iregularitatea unui atac, indiferent de domeniul la care ne referim, oferă un avantaj strategic pentru cel care îl declanşează, elementul de noutate nefiind încadrat în niciunul din pattern-urile deja monitorizate.

Secolul XXI a deputat cu descoperiri remarcabile în nenumărate domenii, a adus cu sine o evoluţie tehnologică fără precedent însă o dată cu aspectele pozitive au apărut şi cele negative, ori cum le numesc specialiştii, efecte perverse. Una din cele mai mari provocări este cea din domeniul informaţional, unde, conform spuselor lui Eric Schimdt, CEO Google, începând cu 2010, în 48 de ore se produc tot atâtea informaţii câte s-au produs până în 2010, însă aceasta nu este cunoaştere, majoritatea datelor fiind zgomot, motiv pentru care serviciile de informaţii şi structurile de securitate în general trebuie să îşi reevalueze paradigma, modul de operare, metodologiile şi instrumentele de lucru, cele patru câmpuri de luptă devenind în prezent cinci: aer, apă, terestru, spaţiu şi cyberspaţiu.

O altă dimensiune a acestei evoluţii este redată de faptul că în prezent, securitatea nu mai este una pur militară, de tipul celei din trecut, când exista o relaţie de egalitate între securitate şi puterea militară, astfel că în prezent, când aducem în discuţie protejarea obiectivelor, valorilor şi intereselor naţionale evidenţiem un sistem amplu de procedee şi măsuri de apărare din care rezultă o clasificare a securităţii la nivel politic, militar, societal, economic, alimentar, informaţional, chiar şi la nivel de mediu înconjurător, biosfera fiind scena tuturor acţiunilor. Pare o modalitate eficace de a evidenţia tipurile de securitate, reuşind a se stabili elementele unei astfel de analize pentru fiecare clasă, având un obiect de referinţă şi o serie de actori implicaţi şi funcţionali la fiecare nivel, însă ele sunt elemente inseparabile ale

constructului securităţii naţionale, motiv pentru care nici atacurile nu mai sunt cele de altădată care să respecte reţeta de atac ori război convenţional, vorbind astfel de acţiuni hibride cu implicaţii la fiecare nivel şi pe fiecare palier al societăţii.

Chiar dacă nu este o modalitate nouă, acceptarea termenului de hibrid şi a unui cumul de acţiuni complexe ce aduce două state ori entităţi în conflict, fără a mai exista neapărat o declaraţie ori o întâlnire militară pe un câmp de luptă, a dat startul unor noi divergenţe. Taxonomia termenului este amplu dezbătută pentru a se putea stabili ce anume include acest nou termen, hibrid, pentru a se putea afla care sunt limitele permise şi de unde anume putem vorbi de încălcarea regulilor.

Până în momentul de faţă, războiul hibrid[2] este definit ca un tip de război fără limite, complex, cu acţiuni pe multiple dimensiuni şi tehnologie modernă ce încearcă a surclasa pregătirea militară, care îmbină războiul convenţional cu regulile şi limitele sale cu asimetria tipică secolului XXI, o formă modernă ce cuprinde mijloace de acţiune care îi permite agresorului să evite atribuirea/însuşirea acţiunilor, ele putând să devină atacuri clandestine (Hunter şi Pernik, 2015, p. 3).

Războiul hibrid se duce pe toate palierele societăţii, prin acţiuni şi sancţiuni economico-financiare (embargo, restricţionarea comerţului, amânarea ori anularea anumitor contracte, blocarea conturilor bancare), politice (excluderea din anumite organizaţii şi alianţe), diplomatice, militare şi nu în ultimul rând la nivel informaţional, **dimensiunea cyber reprezentând unul din punctele forte ale acestei noi forme de conflict.** Cu o societate din ce în ce mai tehnologizată şi mai dependentă de sistemele informaţionale era de aşteptat să apară şi ameninţările la acest nou stil de viaţă ales şi totodată impus.

Secolul XXI – o eră digitală

Sfârşitul Războiului Rece împreună cu globalizarea au dus la o revoluţie informaţională, conducând astfel la diversificarea paletei de riscuri şi de ameninţări pe care orice stat trebuie să le prevină şi să le combată, secolul XXI forţând mediul de securitate la o schimbare de paradigmă, la o îmbinare armonioasă şi eficientă a tradiţionalului cu modernul. Eric Hrovat (2001) a evidenţiat foarte bine că „războiul convenţional (tancuri, avioane, trupe la sol, submarine, rachete, sisteme de apărare) a început să fie înlocuit de *tirurile cifrelor binare*, într-un câmp de luptă diferit. Războiul informaţional

[2] Hibrid – entitate provenită din încrucişarea a doi indivizi de specii, de soiuri, de genuri sau de rase diferite.

este noua artă de subminare a adversarului în noile bătălii. Nu este nevoie să te afli pe câmpul de luptă" (Hrovat, 2001, p. 2), De remarcat este faptul că în trecut a apela la mijloace neconvenţionale de luptă te cataloga ca fiind un oponent slab ce luptă murdar, profitând de vulnerabilităţile adversarului, însă în prezent, tocmai ceea ce ducea la propria denigrare acum se consideră o strategie inteligentă.

Secolul în care trăim este unul digital iar informaţia este o armă ce poate ucide, puterea fiind de partea celui ce o deţine. Trăim într-o societate informaţională în care totul se face online, după noul rit modern, avem conexiune *wi-fi* oriunde ne-am deplasa, tabletele şi/sau smartphone-urile deja sunt un *must have* şi chiar dacă nu le utilizăm la adevărata lor capacitate, tot sunt nişte instrumente de nădejde atunci când vine vorba de reţelele de socializare şi de lipsa privaţiunii auto-indusă odată cu *check-in*-urile, ori cu pozele postate pentru a putea vedea prietenii (şi nu numai) cât de bine te distrezi, cum te plictiseşti, pe unde călătoreşti, care îţi sunt hobby-urile sau orice alt lucru mai mult sau mai puţin insignifiant la care te gândeşti. Unii ar spune că Internetul este un cadou de la Dumnezeu pentru psihopaţi şi persoane cu intenţii rele (criminali şi/sau hărţuitori), această evoluţie uşurându-le cu siguranţă *munca.* Pe baza acestor fapte se poate afirma că evenimentele din 11 septembrie 2001 au demonstrat cum aspectele pozitive ale globalizării, cu tot ceea ce prezintă Occidentul ca fiind evoluţie şi tehnologie modernă, pot fi folosite în sens negativ şi în mod distructiv de către teroriști pentru propria cauză. De asemenea, este de menţionat că una din strategiile lor de recrutare constă în prezentarea materialelor găsite în mediul online în care se regăsesc elemente de violenţă, corupţie, abuzuri, privarea de libertate a cetăţenilor în numele securităţii naţionale, distrugeri, oameni săraci lipsiţi de ajutor ori de vreun sprijin material, pe scurt, „imagini ale disperării" (Barna, 2010, pp. 7-20).

Piraţii Internetului: #GOP şi atacul SONY Pictures

Ultimul sfert de secol a condus la o dezvoltare tehnologică fără precedent, fapt ce a contribuit la formarea unei comunităţi cibernetice ce activează într-un spaţiu fără graniţe geografice/fizice, cyberspaţiul, al cărui câmp de luptă este reprezentat de Internet iar arsenalul, frecvent reactualizat, este redat de New Media (Ghidul OSINT, 2012). Dacă după atacurile din 11 septembrie 2001 presa a fost invadată de articole avându-i în centru pe piraţii aerului, în ultimii ani şi ca urmare a războiului global dus împotriva terorismului, notorietatea acestora a scăzut iar în lumina reflectoarelor au păşit piraţii Internetului, atacurile cibernetice înmulţindu-se considerabil.

Pentru acest nou domeniu s-a structurat rapid o taxonomie a termenilor cyber pentru a se încadra acţiunile *soldaţilor* noului câmp de luptă, astfel că majoritatea tehnicilor convenţionale au primit prefixul „cyber", creându-se astfel termeni precum cyberintelligence, cyberwarfare, cyber manipulation, cyber infiltration, cyber assault, cyber crime, cyber raid, cyber attack (Alford, 2000, p. 105).

Există, totuşi, o confuzie în definirea şi catalogarea atacurilor informaţionale şi a celor cibernetice de tip terorist, astfel că, chiar dacă ambele tipuri se desfăşoară pe acelaşi câmp de luptă, între ele există o serie de diferenţe considerabile, cea mai importantă fiind redată de caracteristica principală a unui atac terorist şi anume, producerea de victime umane. O definiţie completă pentru cyberterorism ce poate fi cotată ca principală distincţie între această formă modernă de terorism şi atacurile cibernetice este furnizată chiar de Biroul Federal de Investigaţii (FBI) care descrie cyberterorismul ca fiind „atacul premeditat, motivat politic împotriva informaţiei, sistemelor informatice, programelor informatice şi datelor, rezultând în violenţa împotriva ţintelor necombatante, de către grupuri subnaţionale sau agenţi clandestini" (Alford, 2000, p. 105).

Atacul cibernetic este una din cele mai grave ameninţări informaţionale ce vizează realitatea virtuală a acestui univers on/offline al secoului XXI, atac ce poate fi întreprins cu mijloace de software, cu produse specifice de atac al parolelor, codurilor de identificare, poştei electronice, acţiuni fără reguli prestabilite ce au ca scop modificare şi/sau distrugerea bazelor de date ori a diferitelor produse prin depistarea vulnerabilităţilor de sistem, a breşelor de securitate şi a furtului de date. Astfel, de atacuri cibernetice pot viza site-urile prezidenţiale (Ucraina, octombrie 2007)[3], bursiere, bancare, ale ambasadelor (august 1997)[4], ori pagini oficiale ale instituţiilor publice şi nu numai, atacuri ce pot escalada cu uşurinţă de la activism şi hacktivism, la cyberterorism dacă ar ataca infrastructuri critice, iar apoi ar bloca serviciile de urgenţă, dacă ar sabota reţelele informaţionale, financiare, electrice, de transporturi ş.a.m.d. De asemenea teroriştii se pot folosi de cyberspaţiu pentru a-şi amplifica efectele atacurilor convenţionale. Avantajele atacurilor cibernetice se pot regăsi în anonimatul atacatorului, în lipsa unor frontiere geografice, în accesibilitatea şi în costurile reduse ale aparaturii şi, nu în ultimul rând, în popularitatea care poate fi dobândită

---

[3] Ucraina, octombrie 2007: atacul cibernetic asupra site-ului preşedintelui Viktor Iuşcenko de către ramura tânără a Mişcării pentru Eurasia, atac ce a blocat website-ul timp de 3 zile.

[4] August 1997: blocarea site-urilor mai multor ambasade din Sri Lanka timp de două săptămâni de către Gruparea Tigrii Negrii, grupare legată de Tigrii Eliberării din *Tamil Eelam*, supraîncărcând poşta electronică cu peste 800 de e-mail-uri.

cu uşurinţă prin asigurarea unui public martor, o audienţă ce poate fi transformată rapid în ţintă.

Soldaţii noului *câmp de luptă* se împart în diferite categorii de genul hackerilor black hat/white hat[5], crackerilor[6], au un limbaj propriu (*leet*)[7], tehnici de luptă personalizate domeniului în care activează – phishing[8], spoofing[9], juice jacking[10] ş.a.m.d., şi nu în ultimul rând, instrumentele/armele necesare pentru atacul de malware – botnets, viruşi ori viermi informaţionali care profită de acele zero-day[11] din aparatura utilizată la nivel mondial. Deep Web ori Dark Web au devenit termeni cunoscuţi de majoritatea chiar dacă pătrunderea în aceste zone ale internetului necesită cunoştinţe în domeniu.

Unul dintre atacurile cibernetice care au ţinut prima pagină a ziarelor în Statele Unite ale Americii este cel la adresa Sony Pictures Entertainment de la sfârşitul anului 2014, la nici trei ani de la atacul Sony PlayStation, care a provocat serioase pagube financiare şi de imagine. Menţionam că astfel de atacuri s-au înmulţit, motiv pentru care trebuie amintit că, în septembrie 2014, Apple a fost ţinta unui atac cibernetic asupra contului deţinut de companie în sistemul iCloud, făcându-se publice mai multe poze (în mare parte nud) cu vedete celebre din cetatea filmului. Ameninţările au continuat, iar după ce, în data de 24 noiembrie, sistemul informatic SONY Pictures din Cluver City a fost blocat şi închis ulterior pentru motive de siguranţă şi investigaţii, angajaţii revenind la lucrul cu foaia şi creionul, de Crăciun, o altă entitate a atacat serviciul Playstation, dar şi consolele Xbox de la Microsoft. Stabilit fiind deja faptul că cele două atacuri au avut autori diferiţi, cele întâmplate în luna noiembrie 2014 au fost revendicate de grupul intitulat #GoP aka Guardians of Peace, iar în decembrie 2014 de Lizard Squad, o entitate virtuală despre care nu se cunoaşte pentru moment dacă este un

---

[5] Black hat hacker: persoană care pătrunde ilegal şi cu intenţii maliţioase în software-ul unor device-uri. White hat hacker: persoană care pătrunde legal în software-ul unor device-uri fiind un expert în securitatea informaţională.

[6] Cracker: persoană care se ocupă exclusiv cu spargerea parolelor şi/sau schimbarea ulterioară a acestora.

[7] Noul alfabet *leet* folosit de comunitatea închisă de gameri şi de hackeri în spaţiul virtual pentru ca activitatea lor să fie mai greu de depistat.

[8] Phishing: acţiunea de a trimite e-mail-uri frauduloase pentru a infecta device-urile de pe care sunt accesate cu scopul de a fura informaţiile stocate.

[9] Spoofing: acţiunea prin care un program ori un device este manipulat să arate şi să se comporte ca un altul în scop fraudulos.

[10] Juice jacking: intruziune frauduloasă prin folosirea unui cablu de alimentare de tip USB, acţiune prin care se poate instala un malware şi/sau accesa, copia informaţii. Dispozitivele vulnerabile sunt cele de tip smart (telefon, tabletă) .

[11] Zero-Day: vulnerabilitate în soft-ul device-urilor necunoscută de producător, ce poate fi exploatată de hackeri.

grup ori un singur individ, însă se poate spune că este de cuvânt deoarece acesta a anunţat încă de la începutul lunii că urmează *un cadou* de Crăciun.

Pe scurt atacul de la Sony Pictures Entertainment, considerat ca cel mai mare atac informatic, a început în data de 24 noiembrie 2014, când angajaţii Sony Pictures din Culver City au primit un mesaj ce le-a blocat sistemul informatic (telefoanele, poşta electronică, computerele), pe desktop-ul calculatoarelor afişându-li-se o poză cu un schelet şi titlul „Hacked by #GOP" (fig. 1). Pentru moment aceştia nu au precizat motivul atacului, însă pagubele estimate s-au ridicat la furtul a aproximativ 10 TB (terabiţi) de date secrete şi strict secrete de pe serverele Sony Pictures.

Figura nr. 1 – mesajul primit de angajaţii Sony Pictures în 24.11.2014
Sursa: https://pmcdeadline2.files.wordpress.com/2014/11/hacked-by-gop-sony-pictures-under-attack.png?w=970

După trei zile de tăcere, a urmat o nouă acţiune din partea hackerilor, GoP urcând pe hub-urile online, aka Torrente cinci filme noi ale studioului – acestea au fost extrase la atacul din 24 noiembrie, fiind versiuni de DVD de tip promoţional. Din cele cinci producţii Sony, doar unul a fost lansat până la acea dată, mai precis filmul cu Brad Pitt „Fury", producţia devenind rapid al doilea

cel mai piratat film cu peste 1 milion de download-uri cu adrese unice de IP. Alături de acesta au mai fost postate şi versiuni complete a patru filme în curs de apariţie: „Annie", „Mr. Turner", „Still Alice" şi „To Write Love On Her Arms".

În 28 noiembrie au apărut primele speculaţii conform cărora în spatele atacului cibernetic întreprins de gruparea intitulată Guardians of Peace s-ar afla chiar Coreea de Nord, făcându-se legătura cu premiera comediei „The Interview", iar pe 1 decembrie, Internetul a fost încă o dată bombardat de informaţii confidenţiale sustrase de pe serverele companiei Sony Pictures: bugete de producţie, parole, protocoale de securitate, informaţii despre vedete, pseudonime ale acestora pentru rezervări, date de naştere, adrese, numere de asigurare socială ale angajaţilor şi nu numai, salariile celor mai bine plătiţi 17 oficiali ai companiei, dar şi ale altor 47.000 de angajaţi şi colaboratori şi, nu în ultimul rând, o serie de e-mail-uri din cadrul unor conversaţii cu caracter ofensator la adresa unor nume celebre de la Hollywood, dar şi la adresa preşedintelui Barack Obama (potrivit Mediafax.ro).

După această acţiune, şefii Sony Pictures, Michael Lynton şi Amy Pascal, au făcut primele declaraţii oficiale catalogând atacul ca fiind unul maliţios, implicând totodată şi FBI-ul. Lucrurile au escaladat treptat, iar investigaţiile sunt în curs de desfăşurare, însă chiar dacă Coreea de Nord a continuat să nege vehement implicarea sa în atacul cibernetic întreprins de GoP, anchetatorii au reuşit să urmărească o serie de reziduuri virtuale identificându-le ca aparţinând strict de sistemele şi serverele accesibile doar în Coreea de Nord – informaţii furnizate la sfârşitul lunii decembrie într-o declaraţie a directorului FBI, James Comey (Agerpres.ro, 07.01.2015).

Piesa centrală a întregului atac cibernetic este producţia Sony Pictures, „The Interview", o comedie cu un buget de 44 milioane dolari SUA, ce prezintă o tentativă fictivă de asasinare a liderului nord-coreean Kim Jong-un. Filmul a fost unul controversat încă de la început, Phenianul solicitând încă din luna iunie a anului 2014 să fie blocat. Neacceptând cenzura impusă, Sony a amânat totuşi premiera din octombrie 2014, făcând o serie de modificări ale finalului privind moartea dictatorului. După patru variante modificate şi chiar acordul preşedintelui japonez Sony, Kazuo Hirai, producătorul şi actorul Seth Rogen a considera, într-un e-mail adresat co-preşedintei Sony, Amy Pascal, conversaţie făcută publică de GoP, că „acesta este acum povestea americanilor care schimbă filmul pentru a-i face fericiţi pe nord-coreeni. Este o poveste condamnabilă"(Mediafax.ro).

Decizia studioului de a nu amâna premiera a dus la o nouă serie de ameninţări din partea hackerilor, în urma cărora FBI a avertizat cinematografele de posibile atacuri şi astfel lansarea oficială a filmului a fost

anulată, acţiune ce a provocat un val de nemulţumiri la Hollywood dar şi în rândul administraţiei prezidenţiale, considerându-se un act de predare: ***„În curând, lumea va vedea ce film prost a făcut Sony Pictures Entertainment. Lumea va fi plină de temeri (...) Aduceţi-vă aminte de 11 septembrie 2001. Vă recomandăm să vă ţineţi la distanţă de acele locuri (în care va fi proiectat filmul). Iar dacă locuinţa voastră este în apropiere, ar trebui să plecaţi de acasă. Tot ce se va petrece în zilele viitoare va fi din vina SPE. Lumea întreagă va denunţa Sony*" (Mediafax.ro).**

Concluzii

Chiar dacă se credea că totul este pierdut, toată publicitatea şi controversa au pornit un adevărat război pentru libertatea de exprimare într-un stat democrat, iar filmul a reuşit să fie proiectat în peste 500 de săli de cinema independente din Statele Unite ale Americii. La 8 ianuarie 2015, acesta înregistra încasări din vânzarea biletelor de aproximativ 5 milioane dolari SUA şi era pus la dispoziţia publicului în mediul online pe cele mai cunoscute platforme, pentru închiriere ori achiziţionare. Site-urile care s-au înscris la streaming au fost GooglePlay, YouTube Movies, Xbox Video Microsoft şi pagina oficială www.seetheinterview.com, acestora adăugându-li-se în 28 decembrie Apple cu serviciul iTunes. Din difuzarea online, filmul a reuşit să strângă (prin preţurile de 5,99 dolari SUA şi 14,99dolari SUA), pînă la data de 8 ianuarie 2015, 31 de milioane dolari SUA, având încasări finale de 38 milioane dolari SUA. Astfel, „The Interview" devenea filmul online numărul unu al Sony Pictures.

Consecinţele nu au întârziat să apară, iar o serie de coincidenţe nu fac decât să întărească suspiciunile unora că totul a fost planificat. Chiar dacă mai sunt conspiraţionişti care plasează atacul ca pe o strategie de marketing Sony pentru promovarea unui film de mâna a doua (şi care a reuşit să împartă lumea criticilor în două tabere), escaladarea tensiunilor dintre Statele Unite şi Coreea de Nord, ca de altfel şi implicarea FBI, par a contrazice această ipoteză. În cadrul Sony Pictures Entertainment a avut loc o serie de demiteri, iar mai mulţi angajaţi au depus o plângere comună pentru că nu li s-au protejat informaţiile cu caracter personal şi confidenţial – mesaj postat pe site-ul oficial de către Sony (www.sonypictures.com).

La nivel oficial şi diplomatic au fost făcute o serie de declaraţii, preşedintele Barack Obama catalogând atacul cibernetic ca pe un act de vandalism care va aduce represalii pentru vinovaţi (luându-se în calcul chiar reincluderea pe lista statelor ce sprijină terorismul, listă de pe care Coreea de Nord a fost scoasă în 2008, după ce în ianuarie 2002 preşedintele de la acea vreme, George W. Bush, a nominalizat statul pe axa răului, alături de Iran şi

Irak), în timp ce liderul Kim Jong-un şi administraţia sa a declanşat o serie de ameninţări şi jigniri, motiv pentru care unii specialişti consideră că acesta este începutul unui război cibernetic între cele două naţiuni: *«Contraatacul nostru cel mai dur va viza Casa Albă, Pentagonul și continentul american, fosa septică a terorismului, și va depăși cu mult „contraatacul simetric" anunțat de Obama».* – Comisia Națională de Apărare nord-coreeană (NDC) (Agerpres.ro, 21.12.2014).

O primă acţiune din partea SUA a fost întreruperea masivă a conexiunii la Internet şi reţele 3G dintre Coreea de Nord şi celelalte state, represalii nerecunoscute oficial însă acceptate chiar prin declaraţia purtătorului de cuvânt Maria Harf: „(...) printre răspunsurile noastre, unele vor fi vizibile, altele nu" (Agerpres.ro, 26.12.2014). Acestea au continuat cu semnarea unui acord trilateral între Statele Unite ale Americii, Japonia şi Coreea de Sud, acord privind schimbul de date confidenţiale la adresa proiectului nuclear al Phenianului, care prevede că orice informaţie cu caracter confidenţial să fie transmis celor două ţări asiatice prin intermediul Washington-ului (Agerpres.ro, 26.12.2014). O altă decizie luată de preşedintele Barack Obama, de această dată cu aplicabilitate internă, este revizuirea şi consolidarea strategiei cibernetice a Statelor Unite.

Investigaţiile continuă, Sony Pictures încearcă să remedieze ce se poate, lupta ducându-se acum la nivel de administraţii prezidenţiale. Este cert că atacurile cibernetice au devenit o mare problemă pentru societatea actuală, atacuri ce pot escalada în adevărate probleme globale, mai ales că mijloacele care pot fi utilizate ca principale arme de către piraţii Internetului sunt dispozitive indispensabile în viaţa cotidiană a secolului XXI, a erei digitale.

Referinţe bibliografice:

1. *Agerpres – Actualizează lumea. Sony Pictures.* http://www.agerpres.ro/views/site/pages/content/searchResults.html?q=sony+pictures [Online] (accesat în perioada 6-8.04.2015).
2. Agerpres.ro: http://www.agerpres.ro/externe/2014/12/21/phenianul-meninta- washingtonul-cu-represalii-daca-sua-vor-sanctiona-rpdc-in-scandalul-sony-18-47-42 .
3. Agerpres.ro: http://www.agerpres.ro/externe/2014/12/26/acord-sua-japonia- coreea-de-sud-pentru-schimb-de-date-confidentiale-vizand-programul-nuclear-nord-coreean-14-27-50.

4. Agerpres.ro: http://www.agerpres.ro/externe/2015/01/07/directorul-fbi-hackerii-au-fost-neglijenti-in-atacul-informatic-asupra-sony-si-au-folosit-servere-nord-coreene-20-39-27.
5. Alford JR., Lionel D. (2000). *Cyber Warfare: Protecting Military Systems.* [Online] http://www.dau.mil/pubscats/pubscats/AR%20Journal/arq2000/alford.pdf (accesat la 7.04.2015).
6. Antipa, Maricel (2010). *Triumviratul dezastrului global*, Bucureşti: Editura Monitorul Oficial.
7. *Analiza de intelligence.* (2013) Curs nepublicat, susţinut în cadrul prelegerilor de Analiza Informaţiilor: OSINT în cadrul Facultăţii de Sociologie şi Asistenţă Socială, Universitatea din Bucureşti.
8. Barna, Cristian (2010). *Terorismul, ultima soluţie? Mărirea şi decăderea Al-Qaīda*, Bucureşti: Editura Top Form.
9. Cooper, Robert (2007). *Destrămarea naţiunilor. Ordine şi haos în secolul XXI*, Bucureşti: Editura Univers Enciclopedic.
10. Deadline.com (22 decembrie 2014). *Sony Hack:A Timeline.* [Online] http://deadline.com/2014/12/sony-hack-timeline-any-pascal-the-interview-north-korea-1201325501/ (accesat la 6.04.2015).
11. Encyclopaedia Britannica (2014). *Herbert Spencer*. [Online] http://www.britannica.com/EBchecked/topic/559249/Herbert-Spencer (accesat la 10.04.2015, 10:17).
12. *Ghid OSINT*. (2012) [Online] http://www.sri.ro/upload/Ghid_OSINT.pdf (Accesat la 4.04.2015).
13. Hrovat, Eric (2001). *Information Warfare: The Unconventional Art in a Digital World*. [Online] http://www.sans.org/reading_room/whitepapers/warfare/information-warfare-unconventional-art-digital-world_787 (accesat la 6.04.2015).
14. Hunter, Eva şi Pernik, Piret (2015). *The Challenges of Hybrid Warfare.* [Online]http://www.icds.ee/fileadmin/media/icds.ee/failid/Eve_Hunter__Piret_Pernik_-_Challenges_of_Hybrid_Warfare.pdf (accesat la 7.05.2015).
15. Kozinets, Robert V. (2010) *Netnography: Doing Ethnographic Research Online*, London: SAGE.
16. Mediafax.ro. *Sony*. http://www.mediafax.ro/tags/sony [Online], (accesat în perioada 6-8.04.2015).
17. Mediafax.ro: http://www.mediafax.ro/cultura-media/sony-pictures-incearca-sa-diminueze-unda-de-soc-dupa-atacul-informatic-asupra-serverelor-sale-13718290.
18. Mediafax.ro: http://www.mediafax.ro/life-inedit/filmul-despre-kim-jong-un-scena-mortii-liderului-nord-coreean-considerata-inacceptabila-si-modificata-de-mai-multe-ori-video-13723225.
19. Mediafax.ro: http://www.mediafax.ro/externe/piratii-cibernetici-au-amenintat-studiourile-sony-evocand-atentatele-din-11-septembrie-2001-13725818.

20. Petrescu, Stan, coord. (2007). *Asimetriile prezentului – Contraterorism vs. Terorism. Terorismul cibernetic*, Bucureşti: Editura Academiei Naţionale de Informaţii.
21. http://www.sonypictures.com/corp/notification/SPE_Cyber_Notification.pdf?#zoom=100.
22. *The 2014 Counterterrorism Calendar. Modus Operandi – cyber attack*. (2014) Bucureşti: Serviciul Român de Informaţii, 2014.
23. Taleb, Nassim Nicholas [2007] (2010). *Lebăda Neagră. Impactul foarte puţin probabilului*, Bucureşti: Editura Curtea Veche.

LUMEA VĂZUTĂ DE VLADIMIR PUTIN

Teodora DOBRE*
Virginia ANDREI*

Motto
„Gentleman, the vote is 11 to 1, and the 1 has it!"
(Abraham Lincoln)

Abstract
At the strategic level, the psychological assessment of the political leader becomes primordial for a successful intelligence service, mostly because we often view a nation's foreign policy in terms of its leader's personality and we know that their decisions are influenced by their belief system (or operational code) and motivations. This paper is focused on shaping a connection between the operational code of Vladimir Putin and his actions, taken in the name of Russia, managing global crises like the American invasion in Iraq, the Iranian file, the missile defense problem, and the crisis in Syria and Ukraine. My attempt is meant to discover a pattern of action within the political behavior of the most controversial leader of the moment as well as to develop predictions, concerning his future approaches of global issues.
Keywords: Vladimir Putin, political behaviour, political lider, international crises, cognitive system.

Introducere

Înţelegerea fenomenelor de politică externă implică o cunoaştere aprofundată a intenţiilor, capabilităţilor altor state şi a relaţiilor existente între ele. Semnificaţia unui eveniment internaţional vine nu numai din analiza evenimentului în sine, ci şi a convingerilor relevante şi a valorilor individului cu atribuţii decizionale (Tetlock şi McGuire, 1986, p. 152). De exemplu, invazia sovietică din Afganistan capătă diferite semnificaţii în funcţie de presupunerile formulate cu privire la intenţiile sovietice. A fost acest act militar unul defensiv, în încercarea de a preveni o răspândire a islamiştilor în Asia Centrală? Sau a fost unul ofensiv, vizând o desfăşurare de forţe în Golful Persic pentru obţinerea supremaţiei? Posibile răspunsuri ale americanilor

* Academia Naţională de Informaţii „Mihai Viteazul".
* Serviciul Român de Informaţii.

definite în raport cu invazia sovietică sunt influenţate nu numai de motivaţiile şi capabilităţile sovietice, dar şi de raţionalitatea decidenţilor americani, cu privire la ceea ce reprezintă interese americane vitale şi ce politici pot fi folosite pentru protejarea acestor interese.

Aceste structuri cognitive pe care liderii se bazează în codarea informaţiilor noi, fie ele scenarii, coduri operaţionale, scheme cognitive, stereotipuri, prototipuri, au capacitatea de a oferi explicaţii intrinseci cu privire la scopul, cauza unui eveniment politic, adevăratele intenţii ale unui stat, ascunse în spatele unor acţiuni de politică externă, rolul lor fiind fundamental pentru gestionarea relaţiilor dintre state, întrucât evidenţiază centrul existenţei fiecărui actor naţional, şi anume, individul, liderul ce se află la conducerea arhitecturii statale.

Am ales să tratăm în următoarele pagini, într-o abordare complexă, sistemul cognitiv al liderului politic, şi anume, codul său operaţional, ce are rolul de a reuni informaţiile percepute de acesta asupra evenimentelor politice internaţionale, sub forma unor imagini cognitive proprii şi care, funcţionând pe baza unui proces de input-output, generează în urma interpretării informaţiilor deţinute, un răspuns, ca modalitate de gestionare a contextului politic confruntat. Studiul porneşte de la o abordare detaliată a conceptului de cod operaţional, iar apoi conturează, dintr-o perspectivă „cognitivă", crizele internaţionale gestionate de liderul Vladimir Putin, de la criza irakiană din 2003, disputa dosarului nuclear iranian, dilema scutului antirachetă, conflictul multidimensional sirian, până la criza ucraineană, cu scopul de a identifica *pattern*-ul comportamental, stilul cognitiv, motivaţiile unui lider aflat în spatele politicii externe ruse de mai bine de zece ani.

Cod operaţional – evoluţie, definire şi utilitate

Nathan Leites (1951) a fost primul care a introdus termenul de cod operaţional în cadrul arealului terminologic al psihologiei politice, ca fiind o serie de reguli standard urmate de membrii Biroului politic, considerate de aceştia ca fiind necesare pentru o conducere eficientă a statului. Studiul său se bazează pe scrierile lui Lenin şi Stalin şi tratează îndeosebi relaţiile stabilite între membrii Partidului Comunist şi lumea exterioară acestuia, scopul autorului fiind acela de a identifica un tipar al acestor reguli, aplicate în timpul ambilor lideri sovietici, şi mai ales de a prezice comportamentul bolşevic (Leites, 1951, p. 11).

Aceste reguli reprezintă un *pattern* al gândirii bolşevice, un set de norme de conducere a decidenţilor sovietici, ce sunt aplicate de moştenitorii comunismului prin comparaţie cu situaţiile ce au format istoria Partidului Comunist. Astfel, tiparul cognitiv bolşevic spune că toate evenimentele politice

semnificative sunt explicabile prin intermediul legilor marxist-leniniste, niciun astfel de eveniment nefiind accidental, iar cel care îl consideră ca fiind rezultatul altor forţe decât cele specifice tranziţiei de la capitalism spre comunism, este considerat un filistin politic (Leites, 1951, pp. 11-19).

Leites a identificat şi un *pattern* al gândirii bolşevice asupra puterii, a cărei lipsă creează o situaţie de real pericol pentru viitorul comunismului. Așa se explică și atitudinea agresivă a bolșevicilor față de puterile sistemului internaţional, chiar şi după revoluţia din 1917, când preluaseră puterea în plan intern. De asemenea, conform mentalităţii bolșevice, sentimentele individului trebuie controlate în întregime, întrucât ele îl pot domina, ceea ce produce o catastrofă. Leites afirma că „activitatea politică este un război ce trebuie tratat cu sânge rece" (Leites, 1951, p. 20). Mai mult decât atât, membrii partidului trebuie să menţină o linie politică clară, să îşi păstreze principiile în orice situaţie, dar în acelaşi timp să fie şi flexibili, în funcţie de traseul urmat de inamic, de schimbările venite din exteriorul statului, pentru a putea fi siguri de o victorie şi pentru a evita pericolele în alegerea strategiilor de acţiune greşite. Aceste trăsături definitorii ale organismului politic îi conferă atât elasticitatea, cât și rigiditatea în cadrul luptei de menţinere a supremaţiei, la nivel internaţional (Leites, 1951, pp. 32-35).

Tiparul cognitiv bolşevic susţine folosirea mijloacelor violente pentru dezvoltarea comunismului, concluziile lui Leites sugerând faptul că atunci când Partidul decide să nu folosească violenţa împotriva inamicilor săi, se expune singur în faţa violenţei adversarilor, neutilizarea violenţei fiind o eroare mult mai mare decât adoptarea unor mijloace prea violente în tratarea unei situaţii (Leites, 1951, p. 51). Ceea ce transcede graniţele preferinţelor pentru folosirea violenţei este concepţia bolşevică conform căreia orice grup care nu este controlat de partid, aflat în interiorul sau în exteriorul statului comunist, este considerat un inamic, aliatul cel mai potrivit fiind cel care este cel mai supravegheat de bolşevici. Astfel, într-un sens general, sovieticii cred că majoritatea politicilor conduse de guvernele statelor sunt concepute pentru a aduce atingere Uniunii Sovietice, întrucât scopul primordial al forţelor din exterior este anihilarea partidului, cu orice preţ (Leites, 1951, p. 57).

Alexander George a preluat câţiva ani mai târziu în cadrul lucrării sale *The Operational Code: A Neglected Approach to the Study of Political Leaders and Decision-Making* (1969) termenul de *cod operaţional* lansat de Leites şi a transformat normele standard care, conform opiniei sale, pot fi aplicate mecanic în alegerea unui curs de acţiune, într-o serie de premise, concepţii asupra universului politic.

Sensul central al operei lui Alexander George este cel de a examina sistemul conceptual dezvoltat de lideri veniţi din medii culturale şi

instituţionale diferite în abordarea *incertitudinii* şi *riscului* din cadrul procesului decizional, mai exact, atunci când ei se află într-un plin demers de alegere a obiectivelor, strategiilor corespunzătoare. Acest sistem conceptual, supranumit *cod operaţional*, este sintetizat de Alexander George sub forma unor răspunsuri date de lideri în faţa unor întrebări generale, ce urmăresc ilustrarea *convingerilor lor instrumentale,* precum şi a *convingerilor filozofice* (Alexander, 1969, p. 199).

Astfel, în ceea ce priveşte structura codului operaţional, Alexander George a creionat un set de întrebări asupra sensului politicii, care, împreună, acoperă multe dintre problemele principale legate de cunoaştere şi acţiune, cu care se confruntă un lider. Răspunsurile oferite de acesta ajută la definirea orientării sale fundamentale în faţa abordării universului politic.

În ceea ce priveşte conţinutul *filozofic* al codului operaţional, *referinţe externe formulate de lider asupra universului politic şi asupra celorlalţi actori ai sistemului internaţional*, au fost trasate întrebările:

1. Care este natura esenţială a vieţii politice? Universul politic, stilul oponenţilor politici este unul cooperativ sau conflictual?
2. Care sunt perspectivele liderului pentru îndeplinirea aspiraţiilor politice? Abordarea este una optimistă şi/sau pesimistă?
3. Este universul politic unul predictibil sau nu? În ce măsură şi în ce sens?
4. Cât de mult control poate avea un lider asupra dezvoltării cursului istoriei? Care este rolul liderului în transformarea şi remodelarea istoriei în direcţia dorită?
5. Care este rolul hazardului în viaţa omului şi în derularea cursului istoric?

Concepţiile *instrumentale, referinţe interne asupra celei mai bune abordări a liderului asupra acţiunii politice*, subsumate codului operaţional, reies din răspunsurile acordate întrebărilor:

1. Care este cea mai bună cale de alegere a scopurilor sau obiectivelor acţiunii politice?
2. Care este cel mai eficient mod de a ajunge la scopul politic urmărit (conflict/cooperare)?
3. Cum sunt calculate, controlate şi acceptate riscurile acţiunilor politice dorite a fi derulate?
4. Care este cel mai bun moment de acţiune pentru promovarea propriilor interese?
5. Care este utilitatea şi rolul diferitelor mijloace de promovare a intereselor proprii?

În încercarea de a dezvolta o formă mult mai rafinată a concepţiilor subsumate codului operaţional, Ole R. Holsti a formulat şase sisteme cognitive proprii liderilor, bazate pe întrebările filozofice şi instrumentale ale lui Alexander George. Unitatea de analiză a lui Holsti este comportamentul individual constrâns de sistemul cognitiv al decizionalului (apud Walker, 1990). Modelul preluat şi de succesorii săi este bazat pe *principiul consistenţei cognitive*, din cadrul căreia reies două propoziţii generale:

- convingerile se află într-o strânsă interdependenţă, tind să formeze un sistem cognitiv coerent şi sub impactul a unor condiţii specifice,
- convingerile constrâng gama de opţiuni alternative a decizionalului şi astfel influenţează decizia finală.

Astfel, ideea principală ce rămâne în urma studiului lui Holsti este faptul că deciziile unui lider sunt consistente cu convingerile restrânse în cadrul codului său operaţional (apud Walker, 1990, p. 409).

Walker şi Falkowski au aplicat versiunea lui Holsti în cadrul unor studii realizate asupra relaţiei dintre modalităţile de răspuns în faţa crizei derulate de administraţia americană şi codurile lor operaţionale (Walker, Falkowski, 1984). Analizând sistemele conceptuale ale unor personalităţi politice precum Truman, Marshall, Eisenhower, Dulles, Kennedy, Rusk şi Johnson şi încercând să realizeze o conexiune între rezultatele obţinute şi căile de acţiune ale guvernelor conduse de ei, autorii nu au putut încadra liderii studiaţi în niciuna din cele patru categorii ale codului operaţional (Walker, Falkowski, 1984). În schimb, ei au identificat diferite seturi de combinaţii între concepţiile filozofice şi cele instrumentale la fiecare din subiecţii analizaţi şi un *pattern* prezent în schemele cognitive, şi anume, o suprapunere a concepţiilor cu un ansamblu de motivaţii (Walker, 1990, p. 412).

Astfel, aceste studii au dus la crearea unei noi priorităţi în studiul codului operaţional al liderului, şi anume, stabilirea unei conexiuni între analiza codului operaţional şi psihologia motivaţională, ceea ce constă în surprinderea nevoilor de afiliere, de putere şi de realizare ale liderului. Ca dovezi atât ale dimensiunii cognitive, cât şi motivaţionale a analizei codului operaţional al liderului rămâne studiul realizat de Walker S. asupra codului operaţional al preşedintelui american, Woodrow Wilson, în contextul dezbaterii asupra ratificării Tratatului de la Versailles (Walker, 1990) şi studiul asupra schemei conceptuale a secretarului de stat american, Henry Kissinger, realizat de Starr H., prin care acesta încearcă să conexeze personalitatea cu percepţiile şi comportamentul de politică externă (Starr, 1984).

Deci, elementele cognitive, cât şi cele motivaţionale formează o personalitate coerentă, complexă a liderului, întrucât poate manifesta diferite

stări de spirit, în funcţie de problema abordată. Această perspectivă sugerează faptul că trasarea codului operaţional al liderului politic ar trebui să pornească „de jos în sus", prin alipirea concepţiilor asupra unor probleme specifice, decât printr-o abordare „de sus în jos", ca o serie de deducţii, pornind de la un sistem cognitiv general. O astfel de strategie „de jos în sus" este metoda *VICS (Verbs In Context System)*, cu ajutorul căreia se pot realiza posibile predicţii asupra strategiilor, tacticilor adoptate de lider în viitor în gestionarea problemelor de politică externă (Schafer şi Walker, 2006, p. 27).

VICS – analiza codului operaţional „la distanţă"

Conform opiniilor specialiştilor Snyder, Bruck şi Burton, cei care doresc să înţeleagă deciziile de politică externă trebuie să aibă acces la „cutia neagră" a procesului decizional, adică asupra agenţilor implicaţi în acest proces. Metoda cea mai eficientă pentru a studia mecanismul din spatele fiecărei decizii politice este *analiza la distanţă*, bazată pe extragerea caracteristicilor psihologice ale liderului prin studierea comportamentului său verbal (Snyder, Bruck şi Burton, 2008).

Premisa de la care porneşte metoda VICS este cea conform căreia modul în care liderii vorbesc despre relaţiile de putere din universul politic relevă concepţiile lor referitoare la exerciţiul puterii. Metoda se axează asupra verbelor folosite de actorii analizaţi în cadrul interviurilor acordate presei. În funcţie de percepţiile asupra sistemului internaţional, ca fiind unul conflictual sau cooperativ, liderii folosesc verbe orientate spre una din aceste direcţii, distincţia între sine şi ceilalţi fiind foarte importantă pentru stabilirea arealului de cuprindere a afirmaţiilor decidentului (instrumental sau filozofic) (Schafer şi Walker, 2006, pp. 30-32).

Astfel, din cadrul afirmaţiilor publice ale liderului, unitatea de înregistrare pentru VICS este enunţul format din verb, subiect şi obiect sau subiect, nume predicativ şi adjectiv. Metoda extrage valori pentru şase atribuţii ale fiecărui enunţ înregistrat: subiect (el însuşi sau ceilalţi), categoria verbului (pozitiv sau negativ/de cooperare sau conflictual), timpul verbului, ţinta şi contextul.

Indicatorii luaţi în calcul de VICS sunt organizaţi sub forma celor zece întrebări formulate de George, calculul acestora trasând şi răspunsurile, în funcţie de valorile înregistrate în urma codării discursurilor actorului analizat (Schafer şi Walker, 2006, pp. 33-38). De exemplu, pentru primul indicator de ordin filozofic, P-1: *Natura universului politic*, cât şi pentru primul indicator de ordin instrumental I-1: Direcţia strategiei (conflict/cooperare), avem o scală de valori de la -1 (extrem de ostil) la +1 (extrem de prietenos),

cu o creștere graduală în intensitate (foarte ostil (-0,75), categoric ostil (-50), oarecum ostil (-0,25), mixt(0), oarecum prietenos(+0,25), categoric prietenos (+0,50), foarte prietenos(+0,75)). Pentru un lider care obţine un scor de -0,21 respectiv +0,41 se obţine următoarea interpretare: Individul consideră universul politic ca fiind unul oarecum ostil și crede că o direcţie de acţiune categoric de cooperare este cea mai buna strategie de urmat în universul perceput. Interpretarea celorlalţi opt indici ai codului operaţional urmează aceeași schemă de interpretare, deşi scala valorilor este diferită în unele cazuri (Schafer și Walker, 2006, pp. 38-40).

Codarea discursurilor publice ale liderului politic se poate face atât manual, cât și folosind *software*-ul *Profiler Plus*[1], destinat analizei psihologice la distanţă a subiecţilor. Încadrând convingerile liderului, atât pentru imaginea sa asupra celorlalţi (convingerile filozofice), cât și pentru propriul sistem cognitiv asupra abordărilor diferitelor probleme de politică externă (convingeri instrumentale), putem formula predicţii asupra căror tactici se aşteaptă liderul să fie folosite de ceilalţi actori ai relaţiilor internaţionale, dar și asupra propriilor tactici, strategii adoptate în negocierile purtate cu ceilalţi (Walker, 2007, p. 20).

Codul operaţional al liderului politic Vladimir Putin

Vladimir Putin este o figură emblematică a statului rus, care a promovat pe lângă politicile de dezvoltare a statului rus în plan intern, prin reformele economice, sociale și politice, o politică externă destul de controversată, prin afișarea de fiecare dată a unei poziţii congruente cu interesele naţionale ale Rusiei, indiferent de riscurile generate prin opunerea viziunilor fundamentale ale celorlalte state. Ce se ascunde însă în spatele acţiunilor liderului rus, a justificărilor oficiale oferite în cadrul afirmaţiilor sale publice?

Răspunsul este oferit de studierea îndeaproape a sistemului cognitiv al preşedintelui de la Kremlin, altfel spus, de identificarea viziunii sale asupra lumii, a *pattern*-ului cognitiv urmat, motivaţiilor și percepţiilor sale, acestea dictând un curs preferat al evenimentelor, în cadrul crizelor globale care au afectat interesele Rusiei.

Vladimir Putin face politica externă a Rusiei, el planifică și îndeplinește obiective și împiedică derularea unor cursuri de acţiune nefavorabile, dominând în totalitate procesul decizional rus. Interesul sporit acordat

[1] Profiler Plus este un software dezvoltat de Social Science Automation, ce este folosit astăzi în analizele media, evaluările campaniilor electorale și profiling. Disponibil la http://socialscience.net/partners/academicusers.aspx.

de liderul rus problemelor de politică externă determină o personalizare a relaţiilor externe, un control strict asupra evenimentelor de pe scena internaţională, precum și o direcţie strategică dictată de o singură voce. Cei care ameninţă sau provoacă autoritatea sa, sunt eliminaţi, expresia definitorie a rolului jucat de Putin în cadrul dezbaterilor decizionale fiind următoarea: *„le consensus, c'est moi!".* Mai mult decât atât, o înţelegere a politicii externe ruse înseamnă o înţelegere a caracteristicilor sale individuale (Lo, 2003).

Preşedintele Federaţiei Ruse nu reprezintă un fenomen izolat, apărut de nicăieri, ci este un produs al mediului rus, instinctele și convingerile sale fiind modelate de experienţa personală, transformările masive ale societăţii ruse și ale statutului puterii ruse din cadrul sistemului internaţional, eșecurile și succesele deţinute de predecesorii săi și de biasurile și emoţiile care îl împiedică deseori să perceapă lumea înconjurătoare dintr-o perspectivă obiectivă și să renunţe la raţionalitate (Lo, 2003).

Întrucât crizele internaţionale sunt cele care reflectă cel mai bine elementele cognitive ale unui lider, acesta fiind forţat să acţioneze sub presiunea unor limite temporale, contextuale sau informaţionale, analiza elaborată în cadrul acestui capitol are ca scop identificarea codului operaţional al lui Vladimir Putin și validarea acestuia prin prisma deciziilor de politică externă adoptate în situaţii de risc, în care statul rus este implicat, precum invazia americană din Irak, gestionarea reacţiilor internaţionale negative cu privire la programul nuclear iranian, problemele impuse de apărarea antirachetă la nivel global, războiul civil din Siria și criza ucraineană.

Intrarea Crimeei sub autoritatea Rusiei și prezenţa trupelor ruse pe teritoriul provinciei au determinat reacţii negative din partea SUA și a altor state occidentale. Concluzia cancelarului german, Angela Merkel, asupra acţiunilor liderului rus, a fost următoarea: *„Putin trăiește într-o altă lume! A pierdut contactul cu realitatea!"* (Paterson, 2014). Această observaţie nu face altceva decât să confirme diferenţele de percepţie existente între liderii occidentali și Putin asupra aceleași probleme, realitatea însemnând pentru fiecare altceva, pentru că este trecută prin propriul filtru cognitiv, propriile viziuni, atitudini, concepţii, devenind o imagine, un produs al mecanismului de gândire individual. Declaraţia liderului Vladimir Putin, în faţa adunării generale a ONU, 12 dec 2013 confirmă acest fapt: „We have always been proud of our nation. But we do not claim to be any sort of superpower with a claim to global or regional hegemony; we do not encroach on anyone's interests, impose our patronage onto anyone, or try to teach others how to live their lives. But we will strive to be leaders, defending international law, striving for respect and national sovereignty and peoples' independence and identity."

(Presidential Address to the Federal Assembly, 2013) Aceste afirmaţii surprind elementele-cheie ale viziunii liderului Vladimir Putin asupra sistemului internaţional, aplicate în cadrul crizelor globale care au afectat interesele ruse. Astfel, abordarea crizei irakiene printr-un exerciţiu unilateral american este combătută constant de Putin, disputa dosarului nuclear este soluţionată datorită rolului de mediator jucat de Rusia lui Putin, programul de apărare antirachetă dezvoltat de SUA în Europa este perceput de liderul rus drept o ameninţare împotriva securităţii statului rus şi un instrument ce destabilizează balanţa strategică, criza siriană a evitat să devină un export de instabilitate datorită mijloacelor diplomatice şi soluţiei de distrugere a arsenalului chimic, propusă de liderul de la Kremlin, iar criza ucraineană, aflată în derulare, poate fi gestionată din perspectiva lui Putin, numai prin dialog şi cooperare şi prin acordarea şansei Kievului de a-şi gestiona instabilitatea din plan intern, fără o intervenţie nelegitimă din exterior, sau o dictare a viitoarelor mutări strategice.

Pattern-ul comportamental al liderului rus vine din sistemul cognitiv dezvoltat de acesta în traversarea fiecărui episod critic al politicii internaţionale şi oferă posibilitatea identificării unor elemente cu un caracter anticipativ asupra viitoarelor strategii urmate pe scena internaţională.

În abordarea crizei irakiene, Putin e moştenitorul dilemei precursorului său, Mihail Gorbaciov, de balansare a consensului internaţional privind condamnarea Bagdadului cu relaţiile apropiate deţinute cu statul irakian. Votul său în cadrul Consiliului de Securitate al ONU, împotriva folosirii atacurilor militare în Irak, ascunde motivaţii precum: stoparea unilateralismului american, conservarea intereselor economice din Irak şi o percepţie distinctă de gestionare a crizei, faţă de cea împărtăşită de comunitatea internaţională (Okhovat, 2011). Astfel, în timp ce majoritatea statelor considerau că apelul la mijloace militare este răspunsul optim în faţa suspiciunilor privind dezvoltarea armelor de distrugere în masă de guvernul irakian, Putin vedea o singură opţiune valabilă: continuarea inspecţiilor specialiştilor ONU (Okhovat, 2011).

Decizia liderului rus privind gestionarea crizei iraniene este cea de derulare a unei politici de balansare, între evitarea unui atac militar pe teritoriul Iranului şi continuarea relaţiilor economice dintre Moscova şi Teheran. Susţinerea Iranului la nivel internaţional atrage pentru Putin un conflict al opiniilor cu SUA şi UE, motivaţiile sale fiind legate de necesitatea statului rus de a menţine cooperarea economică cu Teheranul, dar şi de viziunea sa strict cooperativă, negocierile fiind percepute ca mijloc ideal de abordare a tensiunilor concentrate în jurul dosarului nuclear. Totuşi, sprijinul

acordat Iranului nu este unul constant, iar conformarea în faţa normelor internaţionale este considerată de administraţia de la Kremlin prioritară, ca dovadă fiind solicitările făcute în mod public iranienilor pentru alinierea la cadrul legal trasat de Agenţia Internaţională de Energie Atomică (AIEA).

Putin percepe amplasarea sistemului antirachetă american în Europa ca fiind o ameninţare la adresa securităţii ruse. Iniţial propune americanilor abordarea problemei apărării antirachetă dintr-o perspectivă cooperativă, dar întrucât aceştia refuză o conjugare a eforturilor pentru construirea unui sistem comun, el deviază de la *pattern*-ul comportamental politic înregistrat anterior, emite acuzaţii la adresa americanilor (Chastain, 2015). Problema percepţiilor diferite persistă şi în acest caz, în timp ce americanii susţin faptul că scopul sistemului antitrachetă dezvoltat în Europa este detectarea unui eventual atac cu rachete balistice lansat de Iran, Rusia nu vede o ameninţare viabilă în programul nuclear derulat de Teheran, fiecare dintre cele două părţi fiind convinse că cealălaltă nu doreşte cu adevărat stabilirea unei relaţii de cooperare în domeniul strategic.

În cadrul dezbaterilor asupra conflictului multidimensional sirian întâlnirii ale Consiliului de Securitate ONU, soluţia propusă de Vladimir Putin, şi anume, distrugerea arsenalului chimic al Siriei, este percepută de acesta ca o oportunitate de evitare a unei acţiuni militare în teritoriu, ca soluţie deţinută în faţa unei forme neconvenţionale de conflict, şi confirmă *pattern*-ul cognitiv al liderului rus îndreptat spre cooperare, compromis, dar şi principiile instrumentale care ghidează acţiunile politice ale acestuia în plan intern şi extern, axate pe respectarea legilor internaţionale, a suveranităţii statului şi eliminarea intervenţionismului ca modalitate de gestionare a unor crize interne. Ceea ce fundamentează însă susţinerea Damascului de către Moscova este substratul cognitiv al procesului decizional rus, ce pune accent asupra unor elemente precum identitatea celor două state, afinităţile istorice, asocierea opiniilor, viziunilor elitelor conducătoare ruse şi siriene.

Vladimir Putin percepe conflictul ucrainean ca fiind un conflict instrumentat de statele occidentale, îndreptat împotriva normelor constituţionale şi a dorinţelor populaţiei ucrainene (Pacer, 2014, Address by President of the Russian Federation, 2014). El neagă acuzaţiile Statelor Unite referitoare la prezenţa forţelor ruse armate pe teritoriul ucrainean şi propune ca soluţii pentru redresarea situaţiei mijloace diplomatice, democratice şi eliminarea violenţelor. De asemenea, liderul rus consideră că decizia de a acţiona militar în Ucraina este instrumentată de statul rus numai pe un fundament legitim, în deplină concordanţă cu normele internaţionale. Deşi *pattern*-ul cognitiv înregistrat anterior elimină utilizarea forţei ca mijloc

eficient de gestionare a crizelor internaţionale, este pentru prima dată când liderul de la Kremlin emite o astfel de declaraţie, ce contravine principiului intervenţionismului respectat în trecut, dar în acelaşi timp susţine spiritul legitim al stilului său de conducere a politicii externe ruse.

Concluzii

La nivel general, analiza codului operaţional al liderului politic Vladimir Putin relevă un lider îndreptat spre cooperare, un lider care percepe universul politic dintr-o perspectivă optimistă și care este capabil în acelaşi timp să folosească forţa, dar doar atunci când aceasta este ultima opţiune de care dispune. Nu se autointitulează ca fiind un lider ce deţine control semnificativ asupra evenimentelor scenei internaţionale și deţine o flexibilitate medie în ceea ce priveşte trecerea de la mijloacele cooperative la cele conflictuale. Disputa din jurul sistemului antirachetă relevă cele mai negative valori ale codului său operaţional, ceea ce înseamnă un risc mai mare de folosire a mijloacelor conflictuale în acest caz.

Acuzaţiile emise de Statele Unite la adresa Federaţiei Ruse, referitoare la modul de derulare a politicii externe și anume, la utilizarea resurselor ca instrumente de presiune prin care se vizează reconstruirea sferei de influenţă sovietică și revenirea la ideologia comunistă, au fost demontate de acţiunile și declaraţiile politice ale Moscovei, care au respectat de fiecare dată principiile multipolarităţii, pragmatismului, democraţiei și legitimităţii.

Tensiunile dintre SUA și Rusia se concentrează în jurul unui conflict al opiniilor, al suspiciunilor, intenţiilor ascunse și al motivaţiilor aflate în spatele unor decizii controversate, precum cea de invadare a unui stat-problemă, spre exemplu SUA și gestionarea crizei irakiene, sau de susţinere a unui regim în criză, spre exemplu Rusia și sprijinul acordat regimului de la Damasc. Cheia desluşirii acestor incertitudini stă tocmai în conştientizarea elementelor psihologice ale liderilor implicaţi, în înţelegerea unor fenomene din perspectiva celuilalt, în capacitatea de a empatiza cu „adversarul", aspect susţinut și de psihoterapeutul Gabrielle Rifkind în cartea *The fog of peace*.

În cadrul unui discurs ţinut de Putin în 18 martie 2014, după rezultatele referendum-ului organizat în Crimeea, liderul de la Kremlin a folost cuvântul *ruski* (ce denotă etnicitatea) în locul termenului *rosiski* (ce defineşte cetăţenia) de nenumărate ori, lucru ce nu a fost observat în discursurile anterioare Declaraţia preşedintelui Federaţiei Ruse, 2014. Dintr-o interpretare a istoricului Valery Solovei, acest detaliu, rezultat în urma unei analize verbale a discursurilor liderului rus, anunţă o unire a tuturor ruşilor

într-o singură comunitate, o inovaţie ideologică, ceea ce amplifică temerile americanilor (Piper, 2014).

Popularitatea liderului rus în plan intern, susţinerea afişată de opinia publică din Rusia, dar şi receptivitatea cetăţenilor ruşi din fostele state comuniste, reprezintă instrumentele la care va apela puterea de la Kremlin pentru a se apăra în faţa provocărilor americanilor, ca dovadă fiind cazul Crimeei, unde voinţa exprimată de cetăţenii regiunii, 58,5% din populaţie fiind de naţionalitate rusă[2], printr-un referendum organizat în martie 2014, a dus la intrarea republicii sub autoritate rusă. Nu o anexare teritorială impusă prin mijloace violente, fără consimţământul indivizilor, ci o uniune a ruşilor răspândiţi pe fostul teritoriu sovietic, poate fi viitoarea mutare strategică a Rusiei, în cazul în care NATO şi UE se vor extinde aproape de graniţele Federaţiei Ruse.

Imediat după ce Crimeea a intrat sub autoritatea Moscovei, Putin a explicat comportamentul Rusiei faţă de o regiune vitală pentru interesele statului rus: „They are constantly trying to sweep us into a corner because we have an independent position. If you compress the spring all the way to its limit, it will snap back hard. You must always remember this!"

Concluzia ce porneşte de la o astfel de afirmaţie este una singură şi exprimă, din punctul nostru de vedere, caracteristica principală a *pattern*-ului comportamental înregistrat de Rusia lui Putin în toate crizele sistemului internaţional analizate în această lucrare: Atât timp cât Putin se va afla la conducerea statului rus, nu va acţiona niciodată în mod ofensiv, nu va recurge la mijloace conflictuale pe scena globală din proprie iniţiativă, ci doar dacă statele occidentale vor intensifica presiunile asupra Moscovei, forţând o reacţie negativă semnificativă.

---

[2] Conform statisticilor realizate în 2001, disponibile la adresa: http://2001.ukrcensus.gov.ua/eng/results/general/nationality/Crimea/

Referinţe bibliografice:

1. Address by President of the Russian Federation, (18.03.2014) disponibil la http://en.kremlin.ru/events/president/news/20603
2. Alexander, G. (1969), *The Operational Code: A Neglected Approach to the Study of Political Leaders and Decision- Making*, *International Studies Quarterly*, nr. 13.
3. Chastain, M. (2015), *Vladimir Putin: U.S. Missile defense system threatens Russia* in *Breitbart*, disponibil la http://www.breitbart.com/national-security/2015/10/22/vladimir-putin-u-s-missile-defense-system-threatens-russia/
4. Leites, N. (1951), *The operational code of politburo*, New York: Mcgraw-Hill Book Company, Inc.
5. Lo, B. (2003), *Vladimir Putin and the Evolution of the Russian Foreign Policy*, London: Blackwell Publishing.
6. Meetings by UN Security Council on Syria, disponibil la http://www.un.org/apps/news/docs.asp?Topic=Syria&Type=Meeting.
7. Okhovat, S. (2011), *The United Nations Security Council: its Veto Power and Its Reform*, CPACS Working Paper, nr. 15/1.
8. Pacer, V. (2014), *Vladimir Putin's justification for Russian action in Crimea undermines his previous arguments over Syria, Libya and Iraq*, în The London School of Economics and Political Science, disponibil la http://blogs.lse.ac.uk/europpblog/2014/03/11/vladimir-putins-justification-for-russian-action-in-crimea-undermines-his-previous-arguments-over-syria-libya-and-iraq/.
9. Paterson, T. (03.03.2014), *Ukraine crisis: angry Angela Merkel questions whether Putin is 'in touch with reality'* in *The Telegraph* (online ed.), disponibil la http://www.telegraph.co.uk/news/worldnews/europe/ukraine/10673235/Ukraine-crisis-Angry-Angela-Merkel-questions-whether-Putin-is-in-touch-with-reality.html.
10. Piper, E. (2014, 06. 09), *'Patriot's handbook' may give insight into Putin's thoughts*, disponibil la Reuters: http://www.reuters.com/article/2014/06/09/us-russia-putin-ideology-insight-idUSKBN0EK09Y20140609, accesat la 06.08.2014.
11. Presidential Address to the Federal Assembly (12.03.2013), disponibil la http://en.kremlin.ru/events/president/news/19825.
12. Schafer, M., & Walker, S. G. (2006), *Beliefs and leadership in world politics*, New York: Palgrave Macmillan.
13. Snyder, R., Bruck, H., & Burton, S. (2008), *Decision-Making as an Approach to the study of International Politics* in S. Smith, A. Hadfield, & T. Dunne, *Foreign Policy, theories, actors, cases*, New York: Oxford University Press.

14. Starr, H. (1984), *Henry Kissinger: Perceptions of International Politics*, in *American Politics,* vol. 25.
15. Tetlock, P. E., & McGuire, C. J. (1986), *Cognitive Perspectives on Foreign Policy*, Boulder: Westview Press.
16. Walker, S. G. (1990), *The Evolution of Operational Code Analysis*, in *Political Psychology*, vol. 11, nr. 2.
17. Walker, S. G. (2007), *Coding and Scoring Operational Code Beliefs by Hand: The Verbs in Context System Manual*, New York: Arizona State University.
18. Walker, S. G., Falkowski, L. (1984), *The operational code of U.S. Presidents and Secretaries of State: Motivational foundations and behavioural consequences,* in *Political Psychology*, vol. 5.

STRATEGII ŞI POLITICI DE SECURITATE

ANALIZĂ DE RISC CONTRAINFORMATIV: INFRASTRUCTURI CRITICE, STRUCTURI MILITARE ȘI DE INTELLIGENCE

Elaine PRESSMAN*

Abstract

This paper reviews background information on insider threat and provides a rationale for the development of an evidence-based analytic tool to assess the individual risk for insider threat. This tool, referred to as the RAIT is of value to security and intelligence analysts in military settings, in critical structure settings and in organizations. The tool assists analysts in resolution of doubt decisions concerning the security status of individuals whose trust status is question. It is also applicable to routine re-assessments of individuals over time. Relevant risk indicators related to insider espionage, sabotage, unauthorized disclosures of classified information and violent extremism are structured into a standardized, systematic and reliable transparent tool to permit the assessment of individual risk and the threat that individuals may represent. This paper will identify some guidelines for use and the indicators in the RAIT tool. The RAIT is consistent with best practice for risk assessment and with other internationally recognized and validated risk assessment tools. The RAIT tool supports but does not replace the professional judgment of those mandated to provide these security decisions. This work was supported by the Canadian Department of National Defence but the author assumes full responsibility for all content and errors.

Keywords: risk assessment of insider threat, resolution of doubt for insider threat, intelligence analysis of insiders, individual risk and threat analysis of insiders.

Introducere

Amenințările rezultate în urma unor acțiuni de infiltrare și/sau trădare reprezintă o provocare majoră pentru structurile de contrainformații. Acest tip de amenințare este ubicuă și periculoasă, în special în Serviciile Armate, în care sunt localizate infrastructurile critice, în organizațiile de intelligence și în mediul industrial, în care proprietatea intelectuală impune o serie de măsuri de securitizare.

* Cercetător dr. în cadrul Centrului Canadian de Studii de Intelligence și Securitate, Universitatea Carleton Ottawa și cercetător asociat al Centrului Internațional pentru Contraterorism, Haga, Olanda.

Ameninţările interne de acest tip presupun derularea de acte de spionaj, sabotaj, terorism, furt, fraudă, diseminare neautorizată a informaţiilor clasificate şi acte fapte maliţioase şi criminale desfăşurate de personal considerat de încredere (Bronswill şi Brewster, 2013)[1]. Ameninţările interne reprezintă o preocupare principală, făptuitorii având acces la echipamente, documente şi instalaţii sensibile, ca urmare a încrederii pe care structurile de comandă şi management au investit-o în aceştia. Evaluarea acestora a existat în majoritatea cazurilor. Aceste analize însă nu au o rată de acurateţe ridicată sau nu răspund la toate semnalele din mediu, dacă nu pot identifica în avans pe acei indivizi care prezintă un risc de natură contrainformativă. Evaluările de risc ar trebui derulate periodic asupra angajaţilor care au acces la informaţii clasificate, pentru a determina nivelul de risc pe care aceştia îl prezintă pentru organizaţie la un anumit moment dat.

Evaluările individuale de risc, pe acest tip de ameninţări interne, se referă la analiza şi evaluarea nivelului de pericol sau prejudiciului pe care un angajat perceput ca fiind de încredere îl poate determina. Protocolul evaluării de risc presupune o serie de condiţii, necesare şi suficiente, adecvate tipului de risc evaluat, structurate pe indicatori cuantificabili. Acesta permite o evaluare atât pe fiecare indicator, cât şi realizarea unei imagini de ansamblu a riscului şi ameninţărilor potenţiale, în baza tuturor informaţiilor disponibile. În situaţia în care, pentru un anumit indicator, nu se cunosc date, câmpul aferent nu se completează. Marcând în acest fel informaţia lipsă, ea este luată în considerare în cazul evaluării, în termeni de importanţă critică pentru orice decizie de risc şi oferă direcţii utile pentru culegerea ulterioară de informaţii.

Organizaţia caută să elimine sau să reducă potenţialitatea acestui tip de ameninţări. Analiza de risc a fost dezvoltată astfel încât să permită evaluarea şi gestionarea potenţialului de risc. Riscul la care prezenta lucrare se raportează face referire la individ, mai degrabă decât la dezastre naturale, biologice sau fizice. Deşi metodologia a fost iniţial dezvoltată în criminalistică de psihologii interesaţi să prezică recidiva, a fost aplicată estimărilor de risc în cazuri de extremism violent, şi poate fi aplicată şi în cazul unor ameninţări interne privind scurgerea de informaţii.

Acest tip de ameninţare apare atunci când persoane cu acces la informaţii şi echipamente clasificate trădează încrederea pe care instituţia a investit-o în ele. Accesul la acest tip de informaţii se asigură în urma unei evaluări prin care se urmăreşte stabilirea nivelului de încredere şi loialitate al individului faţă de organizaţie. În cadrul structurilor militare şi

[1]Această definiţie este conformă cu cea oferită de Agenţia Canadiană de Securitate şi Intelligence (CSIS), informaţie regăsită în *The Threat Environment to 2025* – un document CSIS obţinut de CBC.

guvernamentale, expertului care realizează această analiză i se furnizează informaţii suplimentare de către organizaţiile de intelligence, dar şi de către alte instituţii relevante. Nivelul de încredere şi loialitate estimat pentru fiecare individ va diferi în funcţie de informaţiile livrate, comportamentul individului şi evaluarea finală.

Metodologia aplicată în prezent de către analişti şi factorii de risc utilizaţi pentru testarea de securitate a individului nu este transparentă total, obiectivă, riguroasă şi sistematică. Aceştia îşi pot baza deciziile pe informaţii disponibile, care sunt însă insuficiente, dar şi pe experienţele anterioare ale analistului. Experţii în analiza de risc au argumentat că o astfel de evaluare trebuie să se realizeze într-o manieră sistematică şi comprehensivă, care poate fi cuantificată, în concordanţă cu informaţiile disponibile, manifestând astfel un nivel de încredere ridicat, nefiind subiectivă, inconsistentă şi dependentă de analist. Rezultatele generate ar trebui să fie similare atunci când analiza este realizată de experţi diferiţi. Evaluările de risc, atunci când este utilizată o metodologie riguroasă, vor include şi vor aplica acelaşi set de indicatori relevanţi, într-o manieră sistematică, reducând în acest fel bias-urile cognitive şi subiectivitatea evaluatorului. Metodologia va fi suficient de riguroasă astfel încât să permită stabilirea unor criterii cuantificabile şi să faciliteze reiterarea măsurilor de risc care pot fi comparate (Pressman, 2009).

În cazuri de trădare, evaluarea de risc a fost fie eronată, fie inoportună, fie monitorizarea individului de către supervizori a fost insuficientă. Evaluările eronate sunt deseori rezultatul unei observări superficiale, datorate acordării anterioare a unor grade de încredere ridicate sau percepţiei subiective a colegilor şi supervizorilor. Identificarea timpurie a indicatorilor de risc permite acţiunea oportună de contracarare a acestor ameninţări (Johnston, f.a.).

Context. Ameninţări interne în Forţele Armate, organizaţii de intelligence: rolul implementării cadrului legal. Ameninţările interne sunt o prioritate pentru forţele armate şi serviciile de intelligence în orice stat (MOSID:00161şi MOSID:00214). Majoritatea ţărilor au trecut în ultimele decade prin procese de restructurare a forţelor armate şi a funcţiilor de securitate şi de intelligence, deseori subsumate comisiilor guvernamentale care au realizat evaluări şi au emis elaborări privind schimbarea organizaţională. În ciuda multiplelor reorganizări şi schimbări de politici în ultimele decenii, cele trei roluri fundamentale ale elaborării şi implementării de politici (ofiţerul de pacificare, ofiţerul de intelligence şi ofiţerul de implementare a legii) rămân elemente centrale în procesele de prevenţie, reducere şi detectare a ameninţărilor interne. În final, poliţia este cea care

aplică cadrul legislativ în situaţia apariţiei unor incidente de securitate interne. Aceştia sunt utilizatori ai instrumentelor de analiză de risc (MOSID:00161 şi MOSID:00214).

Într-un raport declasificat al Serviciului Canadian de Intelligence şi Securitate din 2013, ameninţări de genul acesta au fost identificate, devenind una dintre priorităţile agenţiei de intelligence (Bronswill şi Brewster, 2013). Cazul de spionaj al ofiţerului forţelor navale Jeffrey Delisle a devenit baza fundamentării unei tipologii a pericolului de acest fel în cadrul forţelor armate. În cazul lui Delisle, ameninţarea internă s-a extins dincolo de graniţele Canadei. A implicat aliaţii Canadei şi structurile lor de informaţii la care Delisle a avut acces. Delisle a fost condamnat în 2013 la 20 de ani de închisoare pentru faptele sale de spionaj, care au afectat Canada, SUA, Australia, Marea Britanie şi Noua Zeelandă. Acţiunile sale au fost descrise ca fiind „grave şi ireparabile" (Bronswill şi Brewster, 2013). Ce este clar e că aceste ameninţări interne sunt serioase şi credibile.

Experţii FBI au definit ameninţările interne ca „utilizatori autorizaţi care diseminează informaţii clasificate neautorizat în scopuri maliţioase" (Chickowski, 1 martie 2013). Intrusul este o persoană care şi-a pierdut în timp loialitatea faţă de organizaţia din care face parte, ca urmare a recrutării de către un stat sau o structură adversă. Asemenea trădări au, în cele mai multe cazuri, una dintre următoarele cauze:

(1) se produce o schimbare în sistemul de valori al individului;

(2) individul percepe o încălcare a încrederii investite în organizaţie , care cauzează alienare şi care auto-justifică lipsa de loialitate a individului;

(3) individul a reuşit să disimuleze cu eficienţă intenţiile sale, nepermiţând detecţia ameninţării.[2]

Detecţia trădării presupune o analiză asupra comportamentului individual, bazată pe indicatori relevanţi şi abordări care permit identificarea sistemului valoric, atitudini, credinţe, ideologii, revendicări, simpatii, prietenii, asocieri, vulnerabilităţi, intenţii şi capacităţi ale individului în cauză. Aşa cum a notat şi FBI, este o problema ce gravitează în jurul individului. Este de asemenea important să înţelegem indicatorii de risc utilizaţi în cadrul analizei. O astfel de analiză comprehensivă ar trebui să conţină atât elemente care favorizează apariţia riscurilor, cât şi cele care îl potenţează. Decizia privind riscul incumbat de o anumită persoană este luată în considerare după ce au fost evaluate ambele tipuri de informaţii şi toate celelalte variabile independente.

---

[2] Interviu personal nepublicat cu un agent special FBI din 3 martie 2014.

Perpetuatorii acestor acţiuni prejudicioase sunt de cele mai multe ori bine-educaţi şi experimentaţi şi deţin funcţii importante în cadrul organizaţiei. Foarte des, au funcţii cognitive normale şi deţin controlul asupra acţiunilor proprii. Acest tip de indivizi sunt capabili să ia decizii raţionale şi să schimbe natura acţiunilor proprii în timp, în baza a ceea ce consideră a fi motivant. Ca rezultat, indicatorii de risc pentru acest tip de ameninţări interne au o componentă dinamică. Diferă de instrumentele analitice care utilizează indicatori statici, precum sexul, vârsta, educaţia, istoricul criminal, abuzul în copilărie şi dorinţele şi acţiunile impulsive. Prezenţa unei afecţiuni mentale ar putea fi luată în considerare în evaluarea de risc, dar doar pentru a exclude angajaţii cu handicap mental. Pentru evaluarea eficientă a nivelului de risc, se porneşte de la premisa că individul a ales să se comporte neloial faţă de organizaţie sau violent, nu din cauza unor afecţiuni mentale, ci în baza unei decizii raţionale şi motivate.

Indivizii care comit acest tip de ameninţări sunt implicaţi în fapte de spionaj, sabotaj sau alte fapte înşelătoare din dorinţa de a obţine avantaje pecuniare, favoruri sexuale sau ca urmare a unui act de şantaj, traumă emoţională şi motive ideologice. Ca urmare a revizuirii literaturii de specialitate, experţii au identificat faptul că pentru o mare parte din acţiunile de dezinformare internă şi trădări se puteau identifica indicii concludente anterior comiterii faptei. Aceste semnale au fost însă ignorate pentru mai mulţi ani, din cauza incapacităţii colegilor de a accepta posibilitatea că un coleg sau prieten poate comite fapte de trădare (*The Insider Threat*). Descris în termeni militari, adversarul care face un atac frontal este mai uşor de anticipat şi de contracarat cu o forţă comparabilă decât cel care atacă din spate, întrucât acest individ nu este „anticipat sau învins exclusiv prin forţă" (Catrantzos, septembrie 2009). Pentru că acest tip de adversar este mai dificil de anticipat, evaluările de risc în ceea ce priveşte acest tip de comportament reprezintă o sarcină dificilă.

Elemente necesare evaluării de risc pentru ameninţări interne

Luând în considerare elementele prezentate anterior, o analiză de risc pentru acordarea certificatului de acces la informaţii clasificate ar trebui să includă următoarele elemente:

(1) explorarea atitudinilor relevante într-o manieră intensă pentru a identifica potenţialul de dezinformare;

(2) menţinerea constantă sub observaţie a indivizilor care au acces la informaţii clasificate, pentru a permite identificarea timpurie a schimbărilor dinamice ce au loc la nivel contextual şi valoric care ar putea afecta loialitatea şi;

(3) monitorizarea statusului individului în raport cu organizaţia din care face parte, incluzând nemulţumirea, lipsa anticipării unui progres profesional, sau alte dezamăgiri personale care ar putea fi percepute sau interpretate de individ ca o lipsă de încredere a organizaţiei în acesta. Evaluările de risc individuale necesită comprehensivitate şi eficacitate.

Verificările de cazier, ale situaţiei financiare, ale pregătirii profesionale permit selectarea acelor elemente care deşi utile pentru evaluarea nivelului de încredere al organizaţiei în individ, nu fac referire directă la loialitatea individului faţă de organizaţie, valorile sau ideologia care îl animă. De asemenea, nu iau în considerare schimbările dinamice ce ar putea apărea de-a lungul timpului în ceea ce priveşte elementele de risc. Evaluările privind acest tip de ameninţări interne, sunt multidimensionale şi angrenează o multitudine de factori, prin natura lor. Este o problemă complexă, ce necesită o analiză comprehensivă asupra motivaţiilor individuale, explorării emoţiilor morale, atitudinilor, valorilor, caracteristicilor de personalitate şi altor elemente psiho-sociale, precum şi o examinare a asocierilor individului. Cum toate infracţiunile pot fi conectate de motivaţii, personale, sociale, politice, economice, aşa şi un comportament ce generează ameninţări interne poate fi atribuit unei anumite categorii de motivaţie.

Este necesară implementarea unui set de măsuri proactive, pentru a detecta şi contracara riscuri potenţiale, înainte ca acestea să se concretizeze în acţiuni periculoase. Această acţiune preventivă trebuie să se realizeze în conformitate cu strategiile dezvoltate pe linia prevenirii ameninţărilor CIT (counter-insider-threat). La baza elaborării unei astfel de strategii stă o evaluare comprehensivă a riscului şi percepţiei acestuia. Evaluarea poate fi succedată de o intervenţie fixată asupra sursei de risc, în vederea reducerii sau eliminării acestuia. Acest tip de intervenţie este individualizată şi obiectivele pot fi identificate printr-o analiză a caracteristicilor distinctive ale riscurilor generate. Organizaţiile militare sunt în mod special vulnerabile la repercusiuni majore ale acestui tip de ameninţare internă, potenţialitatea de prejudiciere fiind cauzată de nivelul ridicat de pregătire militară şi instrucţie cu armament al individului, de abilitatea sa de a planifica atacuri strategice şi de capacitatea de a utiliza resurse militare eficient. Un alt risc indus de acest tip de ameninţare este cel de scurgere de informaţii sensibile şi de securitate naţională. În literatura de specialitate, care examinează cazuri în care indivizi au săvârşit acţiuni ilegale şi au încălcat normele interne pot oferi o bază de elaborare şi evaluare a indicatorilor de risc, astfel încât aceştia să fie incluşi într-un protocol de evaluare a nivelului de risc. Având în vedere limitarea de spaţiu a prezentului articol, sunt ilustrate mai jos trei exemple relevante.

Studii de caz și lecţii învăţate

„Intrusul" care reprezintă un risc de securitate. „Persoanele de încredere", care au acces la facilităţi sau resurse, pot să nu se implice în acţiuni de sabotaj, spionaj şi să nu comită atacuri violente, însă pot facilita sau permite accesul, neintenţionat, unor persoane cu intenţii maliţioase. Similar, diseminarea neautorizată de informaţii clasificate se poate produce neintenţionat.

Cu intenţie sau nu, actul în sine reprezintă o încălcare a legii, iar făptuitorul este pasibil de pedeapsă, fapt ce a fost recent demonstrat. Pe 7 februarie 2014, Stephen Jin Woo Kim, în vârstă de 46 ani, a fost judecat pentru scurgere de informaţii către mass-media. A pledat vinovat și a primit pentru fapta sa 13 luni de închisoare (Ingram, 7 februarie 2014). Kim este unul dintre cele 11 cazuri din istoria Statelor Unite, în care individul a fost pus sub acuzare pentru „scurgere neintenţionată de informaţii". Kim a declarat că nu a avut intenţii criminale, și a admis că a „lăsat garda jos", fapt ce a determinat o eroare în comportamentul său.

Kim era un contractor respectat al Departamentului de Stat la momentul arestării. A fost considerat „intrus", întrucât a lucrat pentru Centrul Naval de Analiză și pentru Comisia Politicii de Apărare. A fost consilier atât al lui Henry Kissinger, cât și al lui Dick Cheney pe probleme subsumate domeniului său de expertiză. A lucrat pentru Ministrul adjunct al Apărării (*Wall Street Journal*, 7 februarie 2014).

Canada, precum Statele Unite și alte naţiuni, nu este imună la ameninţări interne. Un an înaintea cazului Kim, Jeffrey Paul Delisle a fost condamnat la 20 ani de închisoare în februarie 2013, pentru diseminarea de informaţii clasificate serviciilor de informaţii ruseşti. Patrick Curran, prim-judecător al Judecătoriei Nova Scotia Provincial, a făcut un comentariu privind comportamentul lui Delisle începând cu anul 2007, numindu-l „rece și raţional"(*Globe and Mail*, 8 februarie 2013). Delisle a mărturisit că și-a trădat ţara și că a oferit informaţii din reţelele clasificate agenţilor serviciilor de informaţii ruseşti timp de 5 ani. El a fost supus evaluărilor de risc, de-a lungul timpului. În aceste evaluări a fost apreciat, de către responsabilii cu administrarea testelor, ca fiind loial și de încredere. Avea acces la informaţii clasificate de nivel înalt, iar poziţia sa ierarhică îi asigura accesul la informaţii sensibile, fiind analist de intelligence.

Asemenea evaluări de risc sunt dependente de timp și trebuie racordate la fiecare situaţie în parte. Delisle este un exemplu de individ evaluat ca fiind de încredere și loial la un anumit moment dat, dar care în timp și-a modificat comportamentul. Circumstanţele care determină un anumit tip de comportament și comportamentul individului se schimbă permanent,

aşa cum a fost şi în cazul lui Delisle. Acesta a luat o decizie conştientă şi raţională de a-şi trăda ţara.

Evaluările individuale de risc pentru obţinerea certificatelor de acces la informaţii clasificate de nivel înalt ar trebui administrate frecvent. Acestea ar trebui să fie standardizate şi să ofere un cadru de comparaţie privind comportamentul individual în două momente diferite în timp. Deşi acest tip de măsuri solicită resurse umane şi de timp, monitorizarea la intervale regulate este esenţială pentru a oferi o analiză corectă. Deşi evaluările individule nu identifică întotdeauna deviaţii de-a lungul timpului, orice generalizare a nivelului său de loialitate şi a gradului de încredere pe care îl prezintă este imprudentă şi nechibzuită, precum şi potenţial periculoasă. Prima evaluare de risc va genera datele de bază de la care se va porni în realizarea evaluărilor viitoare şi cu care acestea vor fi comparate.

Utilizarea elementelor cuantificabile în evaluare va permite identificarea rapidă a schimbărilor de comportament. Aplicarea unui set structurat şi obiectiv de indicatori de risc va oferi continuitate. Este vital ca protocoalele de evaluare de risc să utilizeze indicatori de risc pertinenţi. Aceşti indicatori includ elemente de personalitate, factori psiho-sociali şi circumstanţe economice. Informaţia asupra acestor elemente de interes este deseori oferită ca o listă evaluatorilor decât ca un instrument coerent şi structurat.

Acestea sunt lecţii importante de reţinut din cazuistica canadiană şi internaţională, privind „intruşii" care au determinat prejudicii securităţii naţionale. Aceste lecţii pot fi sumarizate, după cum urmează:

(1) la nivel organizaţional, există nevoia de elaborare a unui instrument de analiză dedicat identificării riscurilor interne;

(2) protocolul de evaluare ar trebui să fie realizat într-o manieră sistematică, care să utilizeze o metodologie behaviorală acceptată;

(3) este necesar un set de indicatori de risc pertinenţi;

(4) evaluările de risc ar trebui realizate la intervale regulate de timp, iar rezultatele obţinute de-a lungul timpului ar trebui supuse comparaţiei;

(5) alături de protocolul de evaluare, este necesară colectarea de cât mai multe informaţii privind subiectul, inclusiv prin observaţii informale, rapoarte, informaţii de intelligence, informaţii privind motivaţiile personale, valori şi alte informaţii accesibile pe durata derulării evaluării.

Aceste recomandări sunt confirmate de experţii FBI în domeniu, care au identificat că abordările behaviorale ale evaluărilor de risc „intern" sunt opţiunile cele mai bune pentru identificarea şi contracararea riscurilor de acest tip şi care sprijină persoanele concentrate asupra evaluării multidimensionale a riscurilor interne (Chickowski, 1 martie 2013).

Mai mulţi indivizi care şi-au trădat ţara au fost activi mai mulţi ani până să fie identificaţi şi prinşi. Datorită actualului nivel de tehnologizare şi accesului în reţea la informaţii clasificate, numărului ridicat de informaţii sensibile, acestea pot fi obţinute într-un timp semnificativ mai scurt decât înainte. Informaţiile pot fi extrase din reţea şi stocate pe discuri de memorie. Oficiul de Contrainformaţii al Statelor Unite a publicat o informaţie, conform căreia au fost mai multe informaţii pierdute în urma unor scurgeri interne „decât informaţii oferite inamicilor de-a lungul istoriei" (*Insider Threat*).

Cazuri recente de trădare au sprijinit necesitatea îmbunătăţirii protocoalelor de securitate şi utilizarea unor instrumente obiective de detecţie a ameninţărilor interne. Principalul obiectiv al analizei de risc este de a identifica potenţialitatea şi latenţa riscurilor, astfel încât să poată fi iniţiate măsuri de prevenire şi contracarare. Majoritatea structurilor guvernamentale au crescut numărul de elemente de protecţie fizică, au intensificat măsurile de securitate cibernetică şi au făcut o serie de îmbunătăţiri tehnice. Complementar, utilizarea analizei behaviorale şi evaluărilor individuale de risc vor spori măsurile de prevenire şi contracarare în ceea ce priveşte ameninţările din interior.

Studii de caz: Spionaj, sabotaj, violenţă, diseminare neautorizată

Exemplul nr. 1: Jeffrey Paul Delisle: Spionaj la o bază navală. Jeffrey Paul Delisle, fost sublocotenent în Armată Regală Canadiană, era la post la Centrul din Halifax, Noua Scoţie – Trinity Naval Intelligence Fusion, când a fost arestat pentru acte de spionaj, care au început în urmă cu 5 ani. El avea acces la reţeaua de informaţii clasificate „Stone Ghost", care era utilizată de „cei cinci ochi" şi pentru care era necesar un certificat de acces de nivel înalt. Delisle a transmis informaţii din reţeaua Stone Ghost serviciilor de informaţii ruseşti, GRU. Delisle a intrat în 2007 în Ambasada Rusiei din Ottawa pentru a-şi oferi serviciile voluntar. O mare parte din informaţia transmisă către GRU aparţinea serviciilor de informaţii ale Regatului Unit, Statelor Unite şi Australiei. În ceea ce priveşte informaţiile de intelligence militar aparţinând Canadei, Delisle a utilizat „SPARTAN", o reţea a Departamentului de Apărare Naţională şi se pare ca ar fi transmis date privind rapoartele de intelligence din mediul privat de la CSIS, RCMP, PCO, Agenţia de Transport şi a Serviciului de Graniţă din Canada (CBSA).

Delisle, care era ofiţer de intelligence la o bază militară navală şi analist de risc a afirmat, în urma arestării sale, că „spionăm pe toată lumea, toată lumea spionează". Aceasta a fost explicaţia oferită de el pentru faptul că a furnizat informaţii clasificate serviciilor ruseşti. „Am încercat să le dau informaţii care să le spună doar *Să ştiţi că acordăm atenţie*" (*RCMP full*

interview with Jeffrey Delisle). A declarat că o mare parte din informaţia pe care a diseminat-o în mod neautorizat provenea din SIGINT şi nu din surse umane.

În cadrul interogatoriului, Delisle a admis că a transmis Rusiei informaţii care provenea din Canada, Marea Britanie, Statele Unite şi Australia. A trimis conversaţii obţinute din supravegherea electronică, precum şi liste de contacte ale ofiţerilor de intelligence. A negat că ar fi devoalat vreodată identitatea spionilor sub acoperire. În octombrie 2012, în faţa instanţei juridice, Delisle a pledat vinovat pentru încălcarea încrederii investite de organizaţie şi două capete de acuzare pentru diseminarea neautorizată de informaţii clasificate unei entităţi străine, fapt ce contravine prevederilor Actului Canadian de Securitate a Informaţiilor. Pe 8 februarie 2013 el a fost condamnat la 20 ani de închisoare, minus timpul pe care l-a petrecut deja închis.

Acestea sunt exemple de lecţii învăţate din cazul Delisle. În primul rând, evaluarea şi monitorizarea atitudinilor indivizilor ce au acces la informaţii clasificate trebuie să se realizeze constant. Aceasta trebuie să observe orice deviaţie sau modificare a indicatorilor de la momentul obţinerii accesului la informaţii clasificate. Percepţia lui Delisle asupra informaţiilor provenite din SIGINT au devenit problematice mai târziu şi de asemenea, se consideră ca a devenit nemulţumit de poziţia sa în timp. În al doilea rând, este esenţial să fie monitorizat contextul personal al celor care au acces la informaţii clasificate pentru a determina modul în care se produc schimbări notabil în plan marital, financiar sau alte probleme. Acesta a fost un factor principal în cazul lui Delisle. În al treilea rând, este necesar să se observe şi să evalueze caracteristicile personale ale indivizilor cu acces la informaţii clasificate, pentru a putea determina caracteristicile personale sau de comportament precum narcisismul, lipsa de supunere, vicii. Delisle a raportat interogatorilor că a acţionat sub presiunea stresului emoţional cauzat de divorţ şi de legăturile extramaritale ale soţiei sale. Alte elemente, precum opiniile proprii, au avut o contribuţie la decizia sa de a trăda.

Exemplul nr. 2: Robert Philip Hanssen – Spionaj prin infiltrare (FBI). Robert Philip Hanssen este un caz recent de spionaj prin infiltrare în Statele Unite. Precum Jefffrey Delisle, prezentat anterior, Hanssen, care a fost agent special FBI, furniza un volum semnificativ de informaţii clasificate serviciilor ruse. La momentul arestării sale într-un parc din Viena, Virginia în 2001, Hanssen plasa, în mod clandestin, un pachet conţinând informaţii clasificate într-o „căsuţă poştală impersonală”, pentru a fi ridicat de ofiţerii de informaţii ruşi. Motivul aparent pentru trădarea sa a fost obţinerea de

avantaje financiare, iar Hanssen a primit anterior sume substanţiale din partea ruşilor (FBI declaraţie de presă despre cazul Robert Philip Hanssen, 20 februarie 2001).

Directorul FBI, Louis J. Freeh, a descris acţiunile lui Hanssen ca fiind „cea mai gravă încălcare a legii şi o ameninţare la adresa securităţii naţionale" şi a declarat că trădătorii sau persoanele infiltrate în organizaţii militare şi structurile civile de ordine publică sunt vinovate de „încălcări grave ale încrederii", întrucât sunt agenţi care au jurat să aplice legea şi să protejeze starea de securitate a naţiunii. Hanssen a minimizat amploarea acţiunilor declarând, la momentul arestării sale, că „Puteam fi un spion excepţional, cred, dar nu am vrut. Am vrut să câştig câţiva bani şi să ies." (FBI declaraţie de presă despre cazul Robert Philip Hanssen, 20 februarie 2001)

Hanssen a fost pus sub acuzare şi a pledat vinovat pentru spionaj şi complicitate pentru comiterea actelor de spionaj. În 2001 a fost condamnat la închisoare pe viaţă, fără posibilitatea eliberării condiţionate. Declaraţiile împotriva lui Hanssen au oferit o bază analitică pentru a identifica modul în care acesta s-a oferit voluntar să furnizeze informaţii clasificate ofiţerilor serviciilor de informaţii ruse aflaţi la ambasada rusească din Washington D.C. De asemenea, el a povestit transferul sistematic de diamante şi bani, în valoare de mai mult de 600.000 USD (estimate de alte surse la 1,4 milioane USD). Hanssen a plasat, în mod clandestin, pachete pentru ofiţerii din KGB şi din succesoarea sa instituţională, SVR, la locaţii predefinite în zona Washington de cel puţin 20 de ori şi a cauzat prejudicii majore, prin transmiterea către KGB/SVR a peste 2 duzini de dischete conţinând mai mult de 6.000 de pagini de informaţii importante. A compromis numeroase surse umane ale comunităţii americane de intelligence şi a furnizat Rusiei un volum semnificativ de documente clasificate, inclusiv documente „top secret" şi chei de criptare. De asemenea, a oferit informaţii importante privind operaţiunile tehnice.

Hanssen, similar cazului lui Delisle, a avut acces direct şi legitim la un volum impresionant de informaţii despre programe şi operaţiuni clasificate. Şi-a folosit experienţa, expertiza şi nivelul de instruire ca agent de contrainformaţii pentru a-şi menţine conspirate acţiunile de spionaj. Şi-a păstrat identitatea şi locul de muncă şi a evitat acţiunile şi călătoriile asociate de obicei cu acţiunile de spionaj. Nu a fost detectat prin evaluări de risc interne, ci ca urmare a obţinerii de către guvern a unor informaţii.

Exemplul nr. 3: David Sheldon Boon: Spionaj prin infiltrare în armată. David Sheldon Boon s-a înrolat în armată la vârsta de 18 ani şi a rămas în sistemul militar mai mult de 20 ani, până s-a pensionat, în 1991.

A lucra ca analist SIGINT pe comunicaţiile externe. De asemenea, el s-a ocupat de rapoartele de intelligence operaţionale, tactice şi strategice. A studiat limba rusă la Institutul Lingvistic al Forţelor de Apărare din Monterey, California şi în 1985, a fost numit analist senior de trafic criptologic la NSA, Fort Meade. Din această poziţie, pe care a ocupat-o timp de trei ani, a avut acces la informaţii privind capabilităţile şi mişcările forţelor sovietice şi armelor nucleare tactice ale sovieticilor şi a furnizat rapoarte pe operaţiunile de sprijin ale ruşilor. A fost transferat la o unitate americană din Germania, dar anterior transferului, a luat decizia de a deveni spion al Uniunii Sovietice şi s-a oferit voluntar la ambasada sovietică din Washington D.C. să furnizeze informaţii clasificate în schimbul avantajelor pecuniare.[3]

Boone a luat decizia de a-şi trăda ţara în 1988, înainte de a fi trimis în Germania. Căsătoria sa se destrămase, trebuia să acorde fostei soţii şi copiilor un sprijin financiar semnificativ, pe care nu şi-l putea permite, era nemulţumit de lipsa de echitate a NSA-ului în evaluările individuale şi era iritat de sistemul legal al Statelor Unite, a cărei decizie în cazul divorţului a pus o presiune financiară majoră asupra sa. Boone a admis „Aveam nevoie de bani. În plus, eram extrem de nervos".

Pentru o perioadă între trei şi şapte ani, înainte ca lui Boone să i se retragă certificatul de acces la informaţii clasificate, acesta a fost implicat în acţiuni de spionaj, fiind coordonat de un ofiţer rus, cu care se întâlnea de mai multe ori pe an. Sumele de bani primite au fost estimate la mai mult de 60.000 USD. Re-evaluările sale periodice necesare certificatului de acces la informaţii clasificate au relevat faptul că Boone avea probleme financiare şi datorii şi în 1990, certificatul său de acces a fost suspendat, ca urmare a lipsei sale de responsabilitate atât în plan personal, cât şi în plan profesional. A fost numit în funcţie la un spital militar, unde a rămas până la pensionare, în 1991, fapt ce a dus la sfârşitul carierei sale de spion şi relaţiei sale cu KGB. În 1998, Boone a fost contactat de un ofiţer FBI sub acoperire, care s-a recomandat ca fiind agent al SVR-ului (succesoarea instituţională a KGB-ului) şi care l-a contactat sub pretextul reactivării sale, din cauza unui eveniment recent ce a determinat o investigaţie asupra sa.

Boone a călătorit la Londra pentru a se întâlni de două ori cu „ofiţerul său de legătură", în timp ce era înregistrat. El a relatat în cadrul întâlnirilor

---

[3] Copie a dosarului despre David Sheldon Boone din 15 octombrie 1998, Procuratura Districtului Virginiei de Est Eastern District of Virginia; regarding See related court docket: http://jya.com/dsb101498.htm. Vezi şi *The Affidavit in Support of Criminal Complaint,Arrest, Warrant, and Search Warrantsfor David Sheldon Boon* accesibil pe http://cryptome.org/jya/dsb100998.htm şi Department of Energy, Hartford on Boon accesibil pe http://www.hanford.gov/c.cfm/oci/ci_spy.cfm?dossier=170.

în detaliu momentul în care s-a oferit voluntar şi cum a transmis informaţii clasificate ruşilor timp de 3 ani. Boone a acceptat să reia activităţile de spionaj şi să lucreze pentru SVR, acceptând un onorariu de 9.000 USD. Ulterior, a fost atras în SUA pentru o altă întâlnire cu agentul său de legătură în cadrul căreia, pe 10 octombrie 1998, a fost arestat la Hotelul Dulles International Marriott din Reston, Virginia.

Boone a fost acuzat de spionaj, a pledat vinovat pentru complicitate, ca parte a unui acord negociat, a reţinu 52.000 USD, inclusiv fondul său de pensionare şi a predat un scanner de mână pe care îl folosea pentru a copia documentele. Pe 26 februarie 1999, a fost condamnat la peste 24 de ani de închisoare (Davis, 1999).

Exemplul nr. 4: Theresa Squilacote – caz de spionaj la Pentagon. Theresa Marie Squillaco, în vârstă de 42 ani, un avocat al Pentagonului, a fost arestată şi acuzată de spionaj pentru Germania de Est şi Rusia pe 4 octombrie 1997. Ea a fost arestată împreună cu soţul său, Kurt Stand, în vârstă de 45 de ani, care era un sindicalist de stânga şi cu James Michael Clark, care era un detectiv privat. Clark a pledat vinovat şi a fost martor al procuratorii în procesul intentat împotriva lui Squillacote şi Kurt Stand. Cei trei au fost membri activi ai Mişcării de Tineret a Partidului Comunist la Universitatea din Wisconsin în anii 70. Squillacote şi soţul ei au fost condamnaţi în octombrie 1998 pentru complicitate la acte de spionaj, tentativă de spionaj şi alte capete de acuzare, conexe diseminării neautorizate de informaţii clasificate. Squillacote a fost condamnată în ianuarie 1991 la 21 de ani şi 10 luni de închisoare, iar Kurt Stand a fost condamnat la 17 ani şi 6 luni (*CBS news*).

Squillacote a absolvit Facultatea Catolică de Drept din Washington, D.C. şi a obţinut un loc de muncă la Consiliul Naţional privind relaţiile de muncă, ocupând ulterior poziţia de avocat în cadrul Comitetului Casei Armatei, iar mai târziu la Pentagon. Se crede că soţul lui Squillacote şi-a începu activitatea de spionaj în jurul anului 1972 şi el a recrutat-o prin 1980 în timpul căsătoriei. Activităţile de spionaj ale Squillacote şi a altora au fost documentate în dosarele STASI de către CIA după colapsul Germaniei de Est şi după cinci ani de luptă între agenţii, au fost în cele din urmă făcute publice de către FBI. După destrămarea Blocului Sovietic, în iunie 1996, Squillacote i-a trimis o scrisoare Oficialului Sud African şi Partidului Comunist admiţând că nu are niciun fel de admiraţie pentru democraţia parlamentară burgheză, sugerând o relaţie de lucru. Scrisoarea a fost transmisă FBI-ului. Squillacote a fost prinsă într-un flagrant al FBI-ului în care îi oferea unui ofiţer acoperit al FBI documente sensibile din cadrul Departamentului Apărării. Fostul său asociat Clarke a depus mărturie împotriva ei pentru transmitere de informaţii

către un spion al Germaniei de Est, Lothar Ziemer, cu care Squillacote şi Stand trebuiau să lucreze. Acest caz şi Squillacote nu au primit foarte multă atenţie, dar a generat o serie de controverse din cauza naturii dovezilor şi a flagrantului.

Acest caz diminuează nevoia unei evaluări relevante a riscului care să facă diferenţa între „libertatea" pe care un individ o are în conformitate cu legile Statului de a avea un punct de vedere politic care diferă de normă, de o evaluare a riscului privind existenţa unor astfel de opţiuni în anumite circumstanţe şi posturi. Accesul la informaţii clasificate la nivel înalt ar trebui să ia în considerare acest risc dincolo de libertăţile şi protecţiile existente în acest sens. Se identifică de asemenea rolul potenţial al factorilor psiho-sociali în evaluarea riscului[4].

Squillacote îndeplinea funcţia de analist de achiziţii pe zona de IT în rang superior în cadrul Biroului Adjunctului Sub-Secretarului Apărării pentru Reforma Achiziţiilor şi beneficia de un acces larg la informaţii până în momentul în care a fost arestată. Nu şi-a ascuns niciodată vederile politice sau diversele asocieri. S-a căsătorit cu fiul unui activist comunist. A călătorit în mod regulat în ţările Blocului Sovietic. Şi-a botezat copiii după numele unor „martiri" comuniști germani. În ciuda acestei povești și a opiniilor sale, a putut obţine un post ca jurist în cadrul House Armed Services Committee în timpul Războiului Rece şi a plecat să lucreze la Pentagon după primirea celui mai înalt certificat de acces la informaţii. Squillacote i-ar fi spus unui agent acoperit al FBI că „a început să desfăşoare acţiuni de spionaj pentru a sprijini mişcarea anti-imperialistă în dezvoltare". Urmărirea acesteia a fost „Spionaj în interiorul Departamentului Apărării". Acest caz reflectă o motivaţie de natură ideologică cu posibila implicare a vulnerabilităţii psihologice.

Exemplul nr. 5: Nidal Hasan: Acte violente în interiorul armatei (Terorism/Extremism violent). Pe 5 noiembrie 2009, la ora 1:34 p.m., Nidal Malik Hasan, cetăţean american şi ofiţer al Corpului Medical din cadrul Armatei Statelor Unite, a intrat în clădirea Soldier Readiness Center of Fort Hood din Killeen Texas şi a împuşcat mortal 13 oameni, rănind pe alţii 32. Acesta a folosit un pistol 5-7 semi-automat. Hasan s-a născut în Virginia, pe 8 septembrie 1970, avea 32 de ani şi era de profesie psihiatru în Statele Unite. Şi-a recunoscut pe deplin faptele. Există o controversă în ceea ce priveşte fapta lui Hasan: dacă aceasta, fiind motivată ideologic, a fost un act

---

[4] A se vedea discuţia în *American Psychological Association Monitor* privind monitorizarea conversaţiilor dintre Squillacote şi psihoterapeutul său şi rolul realizării profilului psihologic. Accesat pe 28 martie 2014 la http://www.apa.org/monitor/julaug02/jn.aspx.

terorist, sau este vorba despre violenţă la locul de muncă. A fost judecat de către 3 instanţe pentru crimă premeditată şi 32 de tentative de asasinat, fiind condamnat de un complet de 13 ofiţeri militari pentru toate învinuirile aduse (*O bombă cu ceas*, februarie 2011).

Investigatorii FBI şi ai Armatei SUA au determinat că Hasan a acţionat singur. Procesul său a fost amânat de o serie de probleme procedurale şi de reprezentare. Pe 3 iunie 2013, un judecător militar i-a permis lui Hasan să se reprezinte singur pentru crimă pe durata procesului. În prima zi a procesului, pe 6 iunie 2013, Hasan a recunoscut că el a fost cel care a tras focurile de armă de la Fort Hood. A mai spus juraţilor că a trecut de partea cealaltă şi că s-a considerat un Mujahedin care participă la „jihad-ul" împotriva Statelor Unite. Acesta îşi justifică actele prin faptul că militarii SUA duc un război împotriva Islamului. Hasan le-a transmis experţilor medicali care l-au evaluat în 2010 că va fi un martir dacă este condamnat şi executat de guvernul american. El nu şi-a chemat niciun martor în acest proces în care şi-a admis faptele şi poziţia ideologică puternică prin care îşi consideră faptele ca fiind justificate. A fost condamnat la pedeapsa cu moartea pe 28 august 2013. Şedinţa a fost contestată, statut ce se menţine.

Hasan este copilul unor Palestinieni emigraţi din Cisiordania. Acesta s-a alăturat Armatei Americane după terminarea liceului în 1988 şi a servit opta şi în calitate de soldat înrolat în timp ce urma facultatea. A absolvit Universitatea Virginia Tech în 1997 cu o licenţă în biochimie, iar apoi a studiat medicina la Uniformed Services University of the Health Sciences (USUHS), absolvind în 2003. A urmat această pregătire cu un internship şi apoi un rezidenţiat în psihiatrie în cadrul Walter Reed Army Medical Centre şi a obţinut acreditarea în psihiatrie în 2007. Aceasta a fost urmată de un master în Sănătate Publică la USUHS când a beneficiat de o bursa în domeniul Psihiatriei Preventive şi pentru cazuri de Dezastru în cadrul Centrului pentru Stres Traumatic al USUHS. A terminat acest program în 2009. În acelaşi an a fost promovat de la gradul de căpitan la cel de maior.

Au existat mai multe investigaţii guvernamentale privind focurile de armă de la Fort Hood Insider. Au fost identificate mai multe semnale de alarmă ignorate în cazul lui Hasan. Cea mai importantă întrebare cu privire la ameninţarea internă evidenţiată de acest caz este eşecul evident de a identifica riscul pe care Nidal Hasan îl reprezenta. Fie indicatori de risc incoerenţi au fost folosiţi în evaluarea riscului pe care Hasan îl reprezenta din perspectiva extremismului violent, fie nicio evaluare a riscului formală şi cuprinzătoare nu a fost realizată. Cu toate acestea, mai mulţi indicatori relevanţi cu privire la riscul de extremism violent au fost prezenţi.

Indicatorii de risc în cadrul VERA 2 (Versiunea revăzută a evaluării de risc în cazul extremismului violent) pot fi explorați cu privire la relevanța pentru Nidal Hasan și informațiile pe care ar fi putut să le furnizeze pentru a ajuta la identificarea unei potențiale amenințări din interior. Pentru a fi considerat un nivel de risc semnificativ (moderat sau mare) pentru extremismul violent, nu toți indicatorii reuniți în acest instrument de evaluare trebuie să fie identificați ca fiind prezenți și cu un grad mare de manifestare. Toți acești indicatori sunt luați în calcul și evaluați dacă informația este valabilă, iar dacă informația lipsește, informația este identificată în încercarea de a realiza evaluarea. Evaluarea finală a riscului nu este determinată de o metodă adițională. Este determinată printr-o evaluare profesională , asistată de folosirea unei metodologii sistematice și structurate care folosește întregul set de indicatori de risc în cazul extremismul violent. Fiecare indicator de risc este evaluat pe baza unor criterii pre-stabilite și cuantificabile, un nivel de risc pentru fiecare indicator fiind obținut în mod individual. Prin urmărirea acestui indicator complet printr-o analiză specifică, informația strânsă și structurată cu punctajele realizate este revizuită și analizată. O decizie asupra riscului obiectivă și de încredere este determinată ca urmare a acestei analize și reevaluări. Prezența unui număr limitat de indicatori de risc semnificativi evaluați ca fiind moderați către un nivel ridicat în manifestare în cadrul VERA2 (Evaluarea de risc în cazul extremismului violent) este suficientă pentru a ajunge la o evaluare a riscului care să identifice o preocupare serioasă a pericolului sau a potențialului hazard pe care îl reprezintă individul. În cazul lui Nidal Hasan, semnalele de alarmă erau prezente. Indicatorii VERA2 care ar fi documentat în mod cert pericolul intern sunt prezenți și descrişi mai jos. Dovada analizei de mai jos este valabilă în raportul Atacului Armat de la Fort Hood realizat de către Comisia Senatului Statelor Unite pe tema Securității Interne și Afacerilor Guvernamentale, publicat în februarie 2011 (*O bombă cu ceas*, februarie 2011).

Indicatorul de risc nr. 1: Victimă a nedreptății și nemulțumirilor. Nemulțumirile lui Hasan erau mereu exprimate public colegilor și supraveghetorilor săi. Acestea aveau legătură cu poziția SUA, trimiterea de trupe militare americane pe pământ musulman (Afganistan și Irak) și considera poziția Statelor Unite ca una de război împotriva Islamului. El și-a exprimat de asemenea nemulțumirea față de superiorii săi din Armata SUA care nu au reacționat la nemulțumirile exprimate privind acțiunile oamenilor pe care îi trata și care se întorseseră din Afganistan. Considera că acțiunile realizate de cei cu care discută cu ocazia ședințelor clinice ar fi trebuit considerate crime de război.

Indicatorul de risc nr. 2: Indentificarea persoanei, locului sau grupului responsabil pentru nedreptate și nemulţumire. Hasan a identificat deschis sursa nemulţumirilor sale, aceasta fiind Armata americană. A făcut remarci critice faţă de colegii săi în virtutea acestui punct de vedere și era cunoscut ca având remarci anti-americane cu ocazia prezentărilor sale de dinainte de evenimentul tragic. Unele dintre aceste remarci erau raportate superiorilor. Val Finnell, fost coleg de clasă la școala medicală s-ar fi plâns superiorilor despre afirmaţiile anti-americane ale lui Hasan. Acesta ar fi comentat că sistemul nu face ceea ce ar trebui să facă și că Hasan ar fi trebuit confruntat cu privire la atitudinile sale anti-americane (Passatino și Winter, 10 noiembrie 2009).

Indicatorul de risc nr. 3: Angajamentul faţă de o ideologie care justifică violenţa bazată pe o mai mare autoritate mai degrabă decât pe jurisprudenţa naţiunii. Deși Hasan nu era cunoscut ca practicând prozelitismul despre credinţa musulmană printre pacienţii săi și colegi în cel e-al treilea an la USUHS, un indicator de risc major în mod particular semnificativ era natura atitudinilor și convingerilor sale. Nu era capabil să facă diferenţa între opiniile sale politice și profesionale, iar poziţia ideologică a fost considerată primul factor determinant al viziunii sale asupra lumii încă înainte de atacul din 5 noiembrie 2009. Lui Hasan i s-a solicitat să ţină prezentări pe teme medicale ca parte din responsabilităţile sale. Studenţii și colegii care participau la aceste prezentări se așteptau ca acestea să cuprindă teme medicale, însă de multe ori vizau denunţarea infidelilor.

S-a arătat într-o prezentare US Army Physicians în cadrul Centrului Medical al Armatei Walter Reed că, pe durata bursei sale din ultimul an de rezidenţiat în psihiatrie, opiniile sale erau în contradicţie cu poziţia guvernului american și a Armatei SUA. În mod specific, o prezentare intitulată „Vederea lumii coranice din prisma musulmanilor din Armata SUA" a evidenţiat elemente prezente în atitudinea și ideologia sa. Aceasta a fost, de asemenea, un semnal de alarmă omis. Slide-ul 49/50 din prezentare afirmă că „Dumnezeu așteaptă deplină loialitate", că „Dumnezeu nu acceptă compromisuri" și că „lupta pentru stabilirea unui Stat Islamic pentru a-l bucura pe Dumnezeu, chiar și prin folosirea forţei, este tolerată de către Islam". Mai mult, Hasan a afirmat că soldaţii musulmani nu ar trebui să își îndeplinească atribuţiile în deplină capacitate, altfel riscă să îi rănească sau să îi ucidă pe credincioșii din rândul Islamului.

Lucrarea ar fi putut fi interpretată cu ușurinţă ca sugerând că:

(1) Hasan era în primul rând loial lui Dumnezeu, mai degrabă decât Armatei SUA sau Statelor Unite;

(2) Hasan credea că talibanii acţionau corect şi justificat în lupta lor de a crea un Stat Islamic în Afganistan;

(3) folosirea forţei de către „inamicul Americii" în Afganistan este aprobată religios de către Dumnezeu;

(4) musulmanii americani nu pot lupta în niciun pământ musulman din cauza riscului de a răni sau ucide alţi musulmani, chiar și pe terenul de luptă. Această ideologie susţinută de către dovada comportamentală, îl pune pe Hasan în conflict direct și în opoziţie cu politica SUA. El se află de asemenea în conflict cu activitatea militară stabilită prin lege pe care SUA o desfășoară.

Din punct de vedere minim, acești indicatori solicită o explorare serioasă printr-un protocol al evaluării riscului amănunţit. Hasan, în calitate de cetăţean, avea dreptul și libertatea de a avea propriile credinţe religioase, dar, după cum Dr. Finnell a precizat, ca militar, ai jurat să îţi aperi ţara de potenţialii inamici. Finnell își amintește că Hasan le spunea colegilor și profesorilor săi: „Sunt un musulman înainte de toate și respect Sharia, Legea islamică, înaintea Constituţiei americane." (Passatino și Winter, 10 noiembrie 2009).

Indicatorul de risc nr. 4: Contact personal cu extremiști violenţi. Între decembrie 2008 și iunie 2009, s-a știut că Hasan are legături cu Anwar al-Awlaki, cunoscut ca extremist violent. După cum a observat un singur indicator de risc, acest lucru ar fi considerat extrem de semnificativ din punct de vedere al evaluării potenţialului risc. Guvernul american cunoștea faptul că Hasan comunica pe email cu al-Awlaki, ideolog virulent anti-american care se manifestase în 18-20 de ocazii. Al-Awlaki (decedat în urma unui atac american) a fost un promotor influent și carismatic al atacurilor „jihadiste" din Statele Unite, responsabil în același timp cu recrutarea în cadrul Al-Qaeda. Hasan a fost investigat de către FBI după ce analiștii au interceptat schimbul de email-uri cu Anwar al-Awlaki. Al-Awlaki a apreciat atacul de la Ford Hood și i-a fost înregistrată mărturia conform căreia mai degrabă decât a-l convinge pe Hasan să comită violenţă, acesta din urmă a realizat un act de justiţie realizat în numele său. Se știa că investigatorii americani erau conștienţi că Hasan urma să contacteze Al-Qaeda și că avea alte „legături greu de explicat cu oameni care erau urmăriţi de către FBI" în afară de Anwar al-Awlaki (Raddatz, Ross, Abraham și El-Buri, 10 noiembrie 2009). Aceștia reprezintă indicatori de risc serioși.

Evaluarea realizată de D.C. Joint Task Force a arătat că email-urile și alte materiale interceptate nu au condus la solicitarea unei investigaţii amănunţite. Oficiali din cadrul Departamentului Apărării au afirmat că nu fuseseră notificaţi cu privire la aceste investigaţii dinaintea atacului armat (Raddatz, Ross, Abraham și El-Buri, 10 noiembrie 2009). Este greu de înţeles

cum s-a ajuns la o astfel de decizie de neurmărire în condiţiile importanţei acestui indicator însuşi pentru potenţiale acte de extremism violent. Natura dinamică a procesului de radicalizare ar fi putut justifica monitorizarea continuă. După cum afirma fostul ofiţer CIA Bruce Riedel, „corespondenţa prin e-mail cu un simpatizant al-Qaeda ar fi trebuit să tragă multe semnale de alarmă" şi chiar şi în cazul în care „ar fi schimbat reţete, biroul ar fi trebuit să intre în alertă" (Examiner, 2002).

Indicatorul de risc nr. 5: Căutător, Consumator al materialelor extremiste de violenţă. Se ştie că Hasan vizita website-uri de islamizare radicală. Deşi întregul conţinut al acestui comportament în lumea virtuală a fost determinat după examinarea computerului lui Hasan, lucru care a avut loc după împuşcături, orice investigaţie bazată pe indicatorii de risc anterior menţionaţi ar fi scos la iveală aceste căutări pe internet şi comportamentul online al lui Hassan de dinainte de atac.

Indicatorul de risc nr. 6: Sentimentul persecuţiei, alienarea şi izolarea. Hasan a fost descris de colegii săi ca fiind retras, izolat social şi stresat de către munca pe care o realiza. Acest stres la locul de muncă a crescut odată cu întoarcerea soldaţilor. S-a sugerat de asemenea că Hasan ar fi suferit de asemenea de pe urma hărţuirii religioase în armată şi ca aceasta ar fi dus la o alienare. Acesta a fost considerat ciudat din punct de vedere social, lipsit de pretenţii şi gânditor (*O bombă cu ceas*, februarie 2011). Nu i s-a cunoscut nicio prietenă. După atacul armat soldat cu doi morţi, angajaţi ai centrului de recrutare în cadrul Armatei din Little Rock, Arkansas de către Abdulhakim Mujahid Muhammad, care mai târziu şi-a recunoscut statutul de terorist al grupării Al-Qaeda, Hasan s-a arătat supărat din cauza acuzaţiei de crimă adusă făptuitorului.

Indicatorul de risc nr. 7: Expunerea timpurie la ideologia militantă în favoarea violenţei. Se ştie că Hasan venea dintr-o familie palestiniană care a părăsit Cisiordania când au decis să imigreze în Statele Unite. Deşi plecarea s-a realizat înainte de naşterea lui Nidal Hasan şi părea că acesta are o viaţă normală tipic americană, opiniile membrilor familiei sale şi a celor din anturajul avut pe durata copilăriei şi al adolescenţei ar fi trebuit exploatate în cadrul unei evaluări a riscului. Această exploatare ar fi trebuit să inclusă acele aspecte care sugerau legitimitatea acţiunii militante împotriva Statelor Unite şi a altor state care sprijineau statul Israel sau acele politici considerate anti musulmane. O evaluare a riscului reprezentat de Hasan ar fi trebuit să evidenţieze de asemenea expunerea anterioară în contextul întâlnirilor cu al-Awlaki la Moschea Dar al Hijrah din nordul statului Virginia unde acesta din urmă a fost imam din ianuarie 2001 până în aprilie 2002. Hasan ar fi putut fi influenţat într-o perioadă vulnerabilă de către al-Awlaki

după moartea mamei sale sau printr-o „radicalizare incipientă" în tinereţea sa care s-a dezvoltat pe măsura transformării în adult.

Indicatorul de risc nr. 8: Disponibilitatea de a muri pentru o anumită cauză sau ca martir. Disponibilitatea de a considera că poţi deveni un martir sau a muri pentru o anumită cauză este un indicator de risc important pentru extremismul violent. Acest indicator explorează „asasinatele sinucigaşe cu bombă" din prisma convingerilor subiectului de a se angaja într-o astfel de acţiune. Elementele specifice unei disponibilităţi de a se angaja sau de justifica acte de martiriu sunt explorate de asemenea în cadrul acestui indicator. În emailurile interceptate de către oficiali SUA trimise de Hasan lui Al-Awlaki, Hasanar fi scris: „De-abia aştept să mă alătur ţie în viaţa de apoi" şi l-a întrebat pe al-Awlaki când va fi adecvat jihadul şi dacă este permis în situaţia în care oameni inocenţi sunt ucişi într-un atac sinucigaş. Un email specific a fost cunoscut ca fiind problematic în mod particular în ceea ce priveşte justificarea atacurilor sinucigaşe cu bombă şi martiriul. În lunile de dinainte de împuşcături, se cunoştea că Hasan şi-a intensificat contactele cu al-Awlaki, lucru care trebuia să ridice semnale de alarmă asupra acestuia şi să susţină dovada comportamentală a unei schimbări cu potenţial de risc. Hasan, pe durata procesului s-a arătat deschis în a admite că va deveni un martir în cazul în care va fi executat de către guvernul SUA.

Indicatorul de risc nr. 9: Glorificarea Acţiunilor Violente. Hasan a intrat în atenţia autorităţilor federale cu cel puţin şase luni înainte de atacuri din cauza postărilor pe internet ce arătau că acesta ar fi discutat despre sinucideri cu bombă şi alte ameninţări (CBS News, 5 noiembrie 2009). Autorităţile nu au făcut o legătură directă între aceste postări şi el, deşi erau scrise în numele lui „Nidal Hasan". Postările făceau o comparaţie între un sinucigaş cu bombă şi un soldat care se aruncă în aer pentru a-şi salva colegii şi îşi sacrifică viaţa pentru o „cauză mai nobilă", aceasta nefiind „un act dispreţuit de Islam, ci mai degrabă este considerat o victorie strategică". Nicio investigaţie nu a fost începută. Indicatorul face referire la elementul de risc care îl motivează sau îl poate motiva prin „glorificarea acţiunii violente". Aceasta leagă o acţiune cu o cauză nobilă percepută care poate fi justificată sau care sprijină o autoritate mai înaltă precum o directivă a lui Dumnezeu.

Indicatorul de risc nr. 10: Planificarea şi pregătirea acţiunii violente ilegale. Din cauza antrenamentului militar, Hasan avea capacitatea de a folosi arme şi a plănui şi pregăti un atac. Acest indicator s-ar aplica „persoanelor din interior de încredere" din domeniul militar. Ca urmare, intenţia este un element critic în analiza riscului în cazul personalului militar.

Aceşti 10 indicatori reprezintă o situaţie de risc moderat spre risc foarte mare în ceea ce-l priveşte pe Hasan. Ei corespund unui număr de peste

50% dintre indicatorii de risc cuprinşi în VERA-2, adăugându-se indicatorilor ce explorează tipologia motivaţională şi factorii protectivi. Informaţia disponibilă cu privire la aceşti indicatori ar fi generat suficiente semnale de alarmă pentru a identifica în Hasan un risc relativ mare de ameninţare internă pentru zona militară dinainte de atacul produs. O astfel de evaluare ar fi asigurat monitorizarea îndeaproape a lui Hasan şi ar fi produs o oportunitate de acţiune în vederea reducerii riscului pe care îl reprezenta sau pentru o acţiune preventivă.

Deşi există incertitudine în orice evaluare a riscului privind extremismul violent, există informaţii de referinţă organizată sistematic şi de valoare care poate fi obţinută printr-un protocol transparent şi obiectiv. Acesta nu poate identifica doar riscurile potenţiale, dar poate de asemenea iniţia acţiuni care au scopul de a reduce aceste riscuri.

Lecţii învăţate din cazurile ameninţărilor interne

Indicatorii de risc pentru estimarea „ameninţării interne" pot fi extrase din examinarea acestor cazuri reprezentative. Elementele de risc au legătură cu factori economici, politici, sociali şi personali. Indicatorii de risc economic sunt cunoscuţi ca fiind un element puternic de motivare pentru multe situaţii de trădare, astfel încât orice abordare a evaluării riscului ameninţărilor interne trebuie să includă aspecte de evaluare a situaţiei financiare a subiecţilor. Mai mult, aspecte de natură psiho-socială a circumstanţelor financiare trebuie examinate. Acest lucru poate fi relaţionat cu existenţa unor aşteptări neîmplinite şi dorinţe ale unui individ care se adaugă datoriilor şi statutului financiar al individului.

Mai mult, factori economici pot fi afectaţi de alte cauze de stres personal precum divorţuri, solicitări financiare din partea copiilor sau a soţiei, sau alte comportamente vulnerabile (dependenţa de jocurile de noroc, alcool, droguri). Factorii de risc personal se raportează la factori de personalitate şi includ supraevaluarea, narcisismul şi instabilitatea emoţională, agresiunea şi alienarea. Factorii sociali se pot raporta la nemulţumirile legate de mediul social, printre aceştia numărându-se discriminarea percepută din cauza rasei, religiei, valorilor sociale, a beneficiilor anticipate sau a clasificărilor social. Factorii politici se raportează la ideologia politică şi atitudinile subiectului, poziţionarea politică asumată de guvern şi structurile legale care afectează voinţa politică.

Instrumentele de evaluare a riscului, pentru a furniza rezultate aplicabile şi folositoare trebuie să utilizeze indicatori care sunt relevanţi în mod specific tipului de risc evaluat (Pressman and Flockton, 2012). Prin urmare, se recomandă ca un instrument specific pentru evaluarea riscului să

fie dezvoltat, acesta fiind pertinent pentru ameninţarea internă. Acest instrument va include uns et complet de indicatori de risc identificaţi de pe urma lecţiilor învăţate ca urmare a studierii cazurilor cunoscute. Aceşti indicatori de risc se adresează de asemenea criminalităţii în general. Indicatorii de risc vor fi organizaţi într-un protocol de evaluare structurată profesionistă asemeni protocolului VERA-2 (Pressman and Flockton, 2012) prezentat mai înainte în acest articol. Cu toate acestea, spre deosebire de VERA-2, indicatorii de risc vor fi mai generali decât cei care se referă strict la extremismul violent.

Dezvoltarea instrumentului de Evaluare a Riscului pentru Ameninţarea din Interior

Prezentare conceptuală ar trebui folosită. Aceste lecţii învăţate din analiza diferitelor tipuri de cazuri din interiorul sistemului pot fi aplicate caracteristicilor cerute pentru dezvoltarea unui instrument relevant de o evaluare a riscului. Un astfel de instrument ar trebui să se aplice tuturor cazurilor prezentate mai sus şi să fie adecvat în estimarea persoanelor din interior care prezintă potenţial risc. VERA-2, un instrument de evaluare a riscului pentru extremiştii violenţi se va folosi în cazul aceloraşi persoane din sistem care, motivate ideologic, prezintă o ameninţare pentru agenţii. Totuşi, niciunul dintre aceşti indicatori ai instrumentului VERA-2 nu au legătură cu motivaţii de natură economică aşa cum s-a văzut în multe cazuri de spionaj ca cele identificate şi discutate în secţiunea precedentă a acestui raport. De asemenea, nu există indicatori în cadrul VERA-2 care să fie relevanţi pentru comportamente problematice şi tulburări de personalitate precum narcisismul, lipsa de conformitate cu regulile, neacceptarea culturii militare, respingerea valorilor militare, satisfacţia la locul de muncă, nemulţumirea faţă de avansarea la locul de muncă sau vulnerabilităţi personale. Nu există indicatori pertinenţi cu privire la dependenţa de droguri, jocuri de noroc sau alcool, ori alte probleme personale care necesită luarea în considerare a ameninţării interne. Se recomandă, astfel, ca un instrument de evaluare a riscului să fie dezvoltat specific, în conformitate cu derapajele de nerespectare a legii din interior. VERA-2 ar trebui folosită în acele cazuri în care motivarea ideologică este prezentă şi există riscuri potenţiale pentru dezvoltarea extremismului violent. În alte cazuri de ameninţare internă, evaluarea riscului pe care îl reprezintă indivizii ar trebui sa fie realizată cu ajutorul instrumentului dezvoltat în acest scop. Un astfel de instrument a fost dezvoltat cu acest scop şi este prezentat aici. Detalii despre folosirea acestui instrument pot fi puse la dispoziţie de către autor. Acest instrument, denumit RAIT

(Evaluarea Riscului pentru Ameninţări din Interior) va include elemente identificate în literatura de specialitate şi recenzii ale studiilor de caz. Indicatorii specifici sunt identificaţi mai jos. Instrucţiunile de evaluare sunt disponibile într-un document separat.

Evaluarea Riscului pentru Ameninţări din Interior (RAIT). Instrumentul RAIT este un instrument structurat de evaluare profesională care foloseşte aceeaşi metodologie sistematică şi de încredere folosită în cazul protocolului de evaluare a riscului VERA-2. Rapoartele de la utilizatorii VERA-2 precizează că această metodologie consistentă şi sistematică a fost benefică pentru aplicaţiile de securitate şi intelligence. Rapoartele de la profesionişti de pe patru continente din ultimii cinci ani (inclusiv din partea poliţiei, analiştilor de Intelligence, psihologilor, psihiatrilor şi avocaţilor au susţinut eficienţa şi relevanţa acestui instrument. Instrumentul RAIT foloseşte aceeaşi metodă comportamentală, dar include indicatori de risc specifici pentru ameninţarea din interior.

Instrumentul RAIT foloseşte 25 de indicatori de risc discreţi, fiecare dintre aceştia fiind evaluaţi pe o scară de până la 3 puncte (ce poate fi extinsă până la 5 puncte). Indicatorii de risc sunt grupaţi în cinci categorii adecvate fiecărui element de acţionare a ameninţării interne. Aceştia sunt de natură (1) politică, (2) socială, (3) economică şi (4) motivaţii personale. În unele cazuri, actorul poate fi motivat de mai mult de unul dintre aceste elemente. Conform opiniei experţilor din cadrul FBI, aceste patru motivaţii stau la baza a ceea ce motivează actele criminale[5].

Indicatorii de risc extraşi din literatura cu privire la ameninţările interne şi din analizele realizate pe baza unor cazuri cunoscute au fost organizate într-o evaluare profesionistă structurată (eng. SPJ), protocol consistent cu instrumentele SPJ. Clasamentele pe baza acestor criterii pentru fiecare indicator de risc sunt de natură să stabilească niveluri de risc pentru fiecare dintre aceşti indicatori. Factorii de risc sunt meniţi să fie cuprinzători. Aceştia se aplică celor din sistem angajaţi în activitatea de spionaj, sabotaj, dezvăluiri ilegale, extremism violent, furt şi alte infracţiuni. Indicatorii încorporează elemente de risc şi de reducere a riscului. Un manual preliminar RAIT cu instrucţiuni de folosire este disponibil din partea autorului.

RAIT: Indicatori Consultativi de Evaluare a Riscului (N=25)

A. FACTORI POLITICI – ATITUDINI ŞI VALORI

A1. Cauzele politice/ideologice/religioase au prioritate în faţa legilor naţionale şi militare;

---

[5]Acest model al motivației criminale se bazează pe o discuție personală și pe colaborarea cu un expert al FBI în materie de amenințări interne din cadrul Grupului de Răspuns la Incidente Critice al FBI și Academiei FBI din Quantico, VA.

A2. Perceperea nedreptăţii politice acasă şi/sau în străinătate, alte nemulţumiri percepute;
A3. Respingerea selectivă a valorilor societale;
A4. Conflict de identitate în ceea ce priveşte opiniile politice şi valorile militare;
A5. Furie faţă de decizii politice şi acţiuni ale ţării/armatei;
A6. Familie care trăieşte în străinătate în zone nedemocratice sau în care există conflict.

S. FACTORI SOCIALI

S1. Percepţia proprie sau a grupului ca victimă a nedreptăţii sociale;
S2. Considerarea rasei, religiei, culturii specifice ca fiind superioare celorlalte;
S3. Contact personal cu extremiştii, actorii violenţi în afara legii (membrii ai diferitelor grupări ilegale, infractori);
S4. Antecedente infracţionale/istoric violent;
S5. Antrenament paramilitar anterior, experienţă în utilizarea armelor;
S6. Lipsa respectării codului de conduită cultural/social, a regulilor militare.

P. FACTORI PERSONALI ŞI COMPORTAMENT

P1. Afişează tendinţe de agresiune, ostilitate şi furie morală;
P2. Afişează narcisism, supraevaluare;
P3. Se află sub influenţa stresului (divorţ, conflicte, copii);
P4. Nemulţumit de sarcinile de serviciu;
P5. Afişează instabilitate mentală, personalitate cu probleme, dezordine comportamentală;
P6. Existenţa frustrărilor în viaţa personală (relaţii, prietenii).

E. FACTORI ECONOMICI ŞI CÂŞTIGURI FINANCIARE

E1. Aşteptări financiare nesatisfăcute în carieră;
E2. Nemulţumiri în ceea ce priveşte avansarea în carieră;
E3. Probleme financiare;
E4. Dependent de: jocuri de noroc, alcool, droguri, sex.

M. FACTORI CE REDUC NIVELUL DE PROTECŢIE

M1. Supunere, participarea la şedinţe de diminuare a stresului, probleme financiare;
M2. Cursuri urmate pentru sprijinirea avansării în carieră;
M3. Modificarea opiniilor şi a nemulţumirilor, mai multă flexibilitate în atitudini.

Fiecare dintre aceşti indicatori este măsurat de către un ghid definitoriu de referinţă, iar o evaluare completă de risc est realizată. Evaluarea poate recomanda monitorizare suplimentară, interviuri, urmărirea îndeaproape a situaţiei sau intervenţia.

Concluzii

Ameninţarea interioară este ubicuă. Identificarea riscului este dificilă şi plină de provocări. Aceasta este în parte datorat decepţiei internaţionale a celui

care comite fapta și a caracteristicilor obișnuite ale agentului. Agenţii în domeniul securităţii și Intelligence cărora le-au fost încredinţate poziţii sensibile pot și schimbă în timp potenţialul de risc pe care îl reprezintă. Aceia din interior care sunt cu adevărat loial la un moment dat poat alege să trădeze într-un alt moment. Astfel de trădători din guvern, mediul militar și alte organizaţii pot conduce la dezastre semnificative și cu potenţial catastrofal de natură fizică, umană și de securitate naţională. Ameninţarea iniţială pe care un individ o reprezintă este dinamică. Este accidental în cazul unuia sau o combinaţie de atitudini și circumstanţe economice, sociale și personale. Deoarece ameninţarea internă poate fi identificată și construită într-un instrument, în timp ce indicatorii pot fi evaluaţi printr-o metodă standardizată și măsurată cu ajutorul unei metodologii de evaluare structurată profesional.

Aceasta oferă informaţii despre indicatorii de risc individuali, asistând în același timp evaluarea realizată de către evaluator într-o procedură completă de judecare a riscului. Un instrument în acest sens, cunoscut sub numele de Evaluarea Riscului pentru Ameninţări din Interior (eng. ARIT) a fost dezvoltată.

Referinţe bibliografice:

1. Bronswill, Jim, Brewster, Murray, (19 Septembrie 2013), *Declassified file list CSIS's worries over 'insider threat' to security*, în The Globe, accesibil la http://www.theglobeandmail.com/news/politics/declassified-file-lists-csiss-worries-over-insider-threat-to-security/article14431288/.
2. Chickowski, Erica, (1 Martie 2013), accesibil pe http://www.darkreading.com/insider-threat/5-lessons-from-the-fbi-insider-threat-pr/240149745 Retrieved March 19, 2014.
3. *The Insider Threat*, FBI accesibil pe http://www.fbi.gov/about-us/investigate/counterintelligence/insider_threat_brochure.
4. Catrantzos, Nicholas (Septembrie 2009), *No Dark Corners. Defending Against Insider Threats to Critical Infrastructure*, Naval Postgraduate School Thesis, Monterey, California, accesibil pe https://www.hsdl.org/?view&did=33503.
5. *FBI declaraţie de presă despre cazul Robert Philip Hanssen*, (20 februarie 2001), Washington D.C. accesibil pe http://www.fbi.gov/about-us/history/famous-cases/robert-hanssen.
6. CBS News, (23 octombrie 1998), accesibil pe http://www.cbsnews.com/news/couple-found-guilty-of-spying/.
7. *CBS News*, (5 noiembrie 2009), accesibil pe http://www.cbsnews.com/news/sources-hasan-web-posts-drew-fbi-interest/.
8. Davis, Patricia, (27 februarie 1999), *Ex-NSA worker get 24 years for spying*, în The *Washington Post*, accesibil pe http://www.jonathanpollard.org/1999/022799.htm.

9. Examiner (2002), accesibil pe http://www.examiner.com/article/cia-on-the-hunt-for-anwar-awlaki-san-diego-jttf-outraged-by-missed-chance-to-get-him-2002.
10. *Globe and Mail* (8 februarie 2013), accesibil pe http://www.theglobeandmail.com/news/national/canadian-spy-jeffrey-delisle-gets-20-years-for-selling-secrets-to-russia/article8390425/.
11. Ingram, David, (7 februarie 2014), *Update 2-Former U.S. Analyst Pleads Guilty in Leak to Reporter*, accesibil pe http://www.reuters.com/article/2014/02/07/usa-security-kim-idUSL2N0LC1D820140207.
12. Johnston, Roger, (f.a), *Mitigating the Insider Threat*, accesibil pe http://www.ne.anl.gov/capabilities/vat/pdfs/Insider%20Threat%20and%20Other%20Security%20Issues.pdf.
13. MOSID:00161 și MOSID:00214, documente ale Poliţiei Militare Canadiene accesibile pe http://www.forces.gc.ca/en/about-policies-standards-medical-occupations/mosid161-military-police.page.
14. *O bombă cu ceas*, (februarie 2011), Raport al Comisiei pentru Securitate Internă și Afaceri Guvernamentale din cadrul Senatului Statelor Unite, accesibil pe http://www.hsgac.senate.gov//imo/media/doc/Fort_Hood/FortHoodReport.pdf?attempt=2.
15. Passatino, Jonathan, Winter, Jana, (10 noiembrie 2009), *Raport pe Fox News*, accesibil pe http://www.foxnews.com/story/2009/11/10/fort-hood-suspect-warned-muslim-threat-within-military/.
16. Pressman, D. E., Flockton, J., (2012), *Calibrating risk for violent political extremists: The VERA 2 Structured assessment* in *The British Journal of Forensic Practise*, 14 (4).
17. Pressman, D.E., (2009), *Risk Assessment Decisions for Violent Political Extremism*, Report 2009-02 – Public Safety Canada, accesibil pe http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2009-02-rdv/index-eng.aspx.
18. Raddatz, M., Ross, B., Abraham, M-R, El-Buri, R. (10 noiembrie 2009), *Raport pe ABC News*, accesibil pe http://abcnews.go.com/Blotter/official-nidal-hasan-unexplained-onnections/story?id=9048590.
19. *RCMP full interview with Jeffrey Delisle,* accesibil pe https://archive.org/stream/564122-jeffrey-paul-delisle-rcmp-
20. U.S. Counterintelligence Executive, "Insider Threat" http://www.ncix.gov/issues/ithreat/ Retrieved March 24, 2014.
21. *Wall Street Journal*, (7 februarie 2014), *Devlin Barrett, Former State Department Contractor Pleads guilty in leak Case*, accesibil pe http://online.wsj.com/news/articles/SB10001424052702304450904579369153970706392.

CULTURĂ DE SECURITATE ŞI DIPLOMAŢIE PUBLICĂ

DIPLOMAŢIE PUBLICĂ ŞI INTELLIGENCE – O PERSPECTIVĂ PRAGMATICĂ ASUPRA UNEI INTERSECTĂRI SENSIBILE

Iulian DICULESCU[*]

Abstract

The approach assumed by this research study concerns namely the praxeological side of public diplomacy, found at the confluence with elements of state power, more specifically with those features characteristic to the Intelligence activity. The conceptual precariousness characterizing the field, both as an academic discipline and an effective instrument of power, is highly emphasized. Thus, the operational contextualization of public diplomacy, an approach enabled by emphasizing the role of information and by synthesizing a perspective specific to the Intelligence area, is an objective to be looked for. As a result, a comparative analysis is done between these two dimensions, with a focus on the fact that they are not completely separated, and there can be many common aspects, some of them transiting from one side to another.

Keywords: public diplomacy, intelligence, contextualization, comparative analysis, ethics.

Precaritatea umbrelei conceptuale

La început de drum. Diplomaţia publică se află la început de drum, atât ca disciplină de studiu şi cercetare de natură academică, cât şi ca instrument efectiv de putere (Hayden, 2013). Aceasta nu reprezintă un neajuns major pentru practicienii lipsiţi de preocuparea teoretizării sau pentru cei interesaţi de o perspectivă sumară asupra acestei noi stele a studiilor diplomatice (Melissen, 2011, p. 2), spre deosebire – trebuie subliniat – de cei care caută să ajungă la o cunoaştere structurată a domeniului. Pe ambele dimensiuni, unele state, printre care se remarcă SUA, sunt semnificativ mai avansate, mai ales raportat la situaţia pe care o regăsim în România, unde abia în ultimii ani au început să fie organizate forumuri ale diplomaţiei publice (ex: FEDP – Forumul European al Diplomaţiei Publice), să fie lansate lucrări de specialitate ale unor autori români (ex: Dima, 2013),

[*] Serviciul Român de Informaţii.

să fie încercată dezvoltarea unor filiere universitare de cercetare în domeniu etc. *Toate acestea reprezintă primii paşi, şi ei foarte necesari şi oportuni, pentru România.*

Până nu cu mult timp în urmă, şi nu doar în România, diplomaţia publică s-a caracterizat prin angajamente punctuale şi episodice, prin diverse „scurtături" şi „capricii" instituţionale, ca şi – în special – prin dependenţa excesivă de afinităţile şi abilităţile oarecum accidentale ale unor factori decizionali.

Nevoia unei viziuni credibile. Acest status incipient al diplomaţiei publice, atât ca disciplină de studiu, cât şi ca practică instituţională, contrastează puternic cu aşteptările majore legate de utilizarea acesteia pentru gestionarea provocărilor prezentului. Mai ales că a devenit tot mai evident că nici geografia şi nici capacităţile pur militare nu mai pot pretinde să justifice ori să acopere în întregime nevoile de securitate. Însă, pentru ca diplomaţia publică să poată fi considerată un real instrument de acţiune al statului, iar nu o simplă etichetă clamată din raţiuni de profil şi brand, ar fi necesară cumularea mai multor condiţii:

1) să cartografieze şi să impulsioneze conexiunile dintre actorii diferitelor tipuri de diplomaţii, cum ar fi cea publică, militară, de intelligence etc.;

2) să asigure nu doar „coordonarea" la suprafaţa ierarhiilor de putere, ci o reală orientare strategică;

3) să încurajeze implicarea şi creativitatea sectorului privat;

4) să ducă la o minimă instituţionalizare a ansamblului de activităţi.

Faptul că la nivelul diferitelor structuri ale statului, precum şi în rândul celor cu funcţii de decizie a început să se discute mai mult despre diplomaţia publică este o tendinţă clară şi direct observabilă, dar nu înseamnă că acestea şi reuşesc să dovedească o înţelegere comună sau măcar convergentă a subiectului. Unii actori recurg la strategii de diplomaţie publică pentru a-şi susţine politicile (CIR, 2001, referitor la războiul contra terorismului; Gilboa şi Muntean, 2014, referitor la relaţia cu diaspora etc.). Alţii arată că este necesară reformarea diplomaţiei publice (Miculescu, 2005) sau că trebuie măsurate performanţele diferitelor structuri sau politici specializate (CPD, 2010). O altă categorie face lobby pentru anumite priorităţi care – ni se spune – ar trebui implementate prin mijloacele diplomaţiei publice. În fine, câţiva pledează pentru o strategie de comunicare cuprinzătoare prin care să fie susţinute valorile şi interesele de securitate naţională.

Întrebări elementare. Tot acest mozaic şi varietatea relativ dezordonată a abordărilor indică faptul că orice stat care intenţionează să recurgă la diplomaţia publică trebuie, mai întâi, să răspundă coerent unor întrebări elementare:

1) care sunt actorii şi instituţiile diplomaţiei publice?
2) cum ar trebui integrate şi orientate eforturile acestora?
3) ce înseamnă, din punct de vedere operaţional, să fim deschişi către lume fără să compromitem securitatea?
4) cum putem face faţă unor campanii de propagandă denigratoare?
5) cum trecem de la conştientizarea problemelor la modalităţile potrivite de acţiune?
6) care priorităţi sunt mai relevante în contextul actualelor ameninţări şi oportunităţi?

Astfel, termenul de „diplomaţie publică" este acum parte a unei conversaţii globale, relativ polifonice, după o perioadă de folosire şi disputare între specialişti. Acesta pare a deveni acum o sintagmă umbrelă pentru comunicare strategică, afaceri publice, difuzare internaţională, operaţiuni deschise etc. Şi, adesea, acestea sunt dificil de separat din punct de vedere analitic: dacă, spre exemplu, un comandant militar face o declaraţie de presă difuzată de mass media globale, cu ce avem de a face? Diplomaţie publică, diplomaţie militară, afaceri domestice comunicate internaţional sau operaţiune de informaţii militară? *Branding*, propagandă sau management de percepţie? Este evident, în atare condiţii, că „a numi" este parte a luptei pentru „a da sens", acel sens pe care fiecare parte îl doreşte. Prin numire şi etichetare facem mai mult decât o simplă descriere: judecăm şi propunem perspective valorice, stabilim câmpuri semantice, propunem punţi de legătură sau linii de demarcare.

Contextualizări încrucişate

Rolul informaţiei. Informaţia rămâne resursa strategică cea mai valoroasă şi în mediul relaţiilor internaţionale (Eriksson şi Giacomello, 2006), un mediu modelat de capacitatea de înţelegere şi acţiune a actorilor. Însă evoluţia tehnologică şi emergenţa reţelelor sociale a modificat în profunzime felul şi viteza cu care circulă şi este consumată informaţia. În urmă cu un secol, un diplomat avea la dispoziţie zile sau chiar săptămâni pentru a pregăti răspunsul la o anumită acţiune sau solicitare. Diplomaţia „uşilor închise" reprezenta norma activităţii, iar scurgerile de informaţii erau mai rare.

Nu existau camere video care să monitorizeze constant şi să permită evaluarea prestaţiei diplomatului.

Diplomaţia operează acum într-un mediu radical diferit: deşi interacţiunea dintre state este încă marcată de un minim cod al confidenţialităţii, nu mai este secretă prin însăşi natura sa. Diplomaţia modernă include şi dimensiunea publică (Barston, 2014, p. 1), iar ceea ce se întâmplă în diferite părţi ale lumii poate deveni rapid chestiune de interes public/domestic şi majoritatea acestor situaţii trebuie gestionate prin mijloacele specifice diplomaţiei publice.

Perspectiva operaţională. Un exemplu rapid privind modul de „consumare" a informaţiei în cazul unor atacuri teroriste: „ţările democratice trebuie să ia teroriştilor oxigenul reprezentat de publicitatea pe care aceştia mizează" (Thatcher, 15.06.1985). Remarca privea două dimensiuni:

1) mass-media reprezintă o miză/un vector pentru fiecare atac terorist;

2) rolul pe care diplomaţia publică îl are în prevenirea şi contracararea fenomenului terorist, atât pe termen scurt, cât şi pe termen lung.

Practic, dincolo de pierderile directe de vieţi sau materiale ale unui atac, terorismul nu ar avea un impact semnificativ/de durată decât în raport cu modul în care societatea îi răspunde, iar aversiunea faţă de risc cuplată la reacţii alarmiste ce stârnesc temerile publice pot alimenta terorismul sau, în unele cazuri, chiar îl pot genera.

Dacă ar trebui sintetizat din perspectiva unei praxeologii specifice zonei de intelligence, diplomaţia publică apare tot mai des şi mai clar ca o formă de lucru, una care părea greu de imaginat sau de acceptat nu cu mult timp în urmă. Sigur că există motive convingătoare pentru a susţine necesitatea negocierilor diplomatice „de culise" sau „în spatele scenei", aşa cum arată şi Kissinger (1998, p. 484) exemplificând cu negocierile de pace dintre SUA şi Vietnamul de Nord, dintre 1970 şi 1972, în cadrul cărora canalul secret de dialog a jucat un rol esenţial.

Per ansamblu, însă, actorii acestui proces nu îşi mai pot duce activitatea în secret absolut, complet separaţi de observarea numeroaselor categorii de public interesat (parteneri, beneficiari, interlocutori etc.). În plus, audienţa „domestică", este mult mai conectată la diverse aspecte punctuale ale afacerilor interne şi externe şi împinge, astfel, către o mai mare transparenţă şi răspundere a reprezentanţilor săi, indiferent de însărcinările diplomatice sau de securitate formal atribuite. Ceea ce implică şi o dimensiune etică, astfel încât interacţiunea celor două domenii să nu îmbrace forma intruziunilor

manipulatorii, nici de o parte, nici de cealaltă – ambele fiind în egală măsură posibile (Pinkus, 2014).

Diplomaţia publică permite o evoluţie mai firească într-un mediu marcat de omniprezenţa mediatică, dar – în acelaşi timp – pretinde şi exersarea calităţilor de comunicatori, dobândirea unor noi competenţe profesionale, învăţarea unor noi tehnici de comunicare şi abilitatea de a reacţiona rapid la un mediu de lucru aflat în permanentă schimbare.

Paralele între intelligence şi diplomaţia publică

În acest context, apare şi întrebarea firească cu privire la rolul serviciilor secrete în domeniul diplomaţiei publice. Pentru a răspunde acestei nedumeriri se poate dovedi utilă o paralelă între intelligence şi diplomaţia publică, mai întâi **ca arii de studiu şi apoi ca aspecte ale puterii.**

Dimensiunea lipsă. *The missing dimension* (Andrew şi Dilks, 1984, lucrare ce ţine deja de istoria literaturii de intelligence) documentează o serie de motive pentru care istoricii nu au reuşit să observe felul şi măsura semnificativă în care dimensiunea secretă, anume activitatea de intelligence, a modelat politicile secolului XX. În mod similar, cred că există suficiente argumente pentru a considera că diplomaţia publică şi activităţile conexe acesteia reprezintă o altă „dimensiune lipsă".

Pe de o parte, această observaţie pare firească: pur şi simplu este greu să înţelegem nivelul şi rolul jucat de aceste activităţi în secolul trecut, ori de câte ori ambiţia comprehensivă nu se mulţumeşte cu luarea în considerare doar a reperelor consacrate ale diplomaţiei clasice, formale.

Pe de altă parte, chestiunea mai poate fi discutată: spre deosebire de istoricii specializaţi în activitatea de intelligence care, condiţionat de accesul la arhive, pot trasa o hartă a procesului şi pot face conexiunile necesare cu deciziile şi acţiunile strategice, dacă vrem să evaluăm impactul diplomaţiei publice vom constata că demersul este mult mai dificil. Adesea lipsesc legăturile directe de cauzalitate, lăsând loc unei marje foarte mari de apreciere subiectivă. Ceea ce nu înseamnă că efortul ar fi inutil sau irelevant, desigur.

Metafora maşinăriei. Aparatul de stat, în special după cel de-al doilea război mondial, a însemnat tot mai multe persoane şi instituţii/organizaţii, în tot mai multe locuri. Pe partea de intelligence, accentul nu a mai căzut pe gestionarea câtorva agenţi de mare clasă, ci pe „industrializarea" procesului de culegere a informaţiilor, iar mai apoi pe organizarea şi managementul cunoaşterii (Herman, 1996), cu procedurarea aşa-numitelor INT-uri (SIGINT, IMINT, HUMINT etc.), cu monitorizarea unor ramuri ale literaturii ştiinţifice, cu gestionarea unor operaţiuni complexe etc.

Pe partea diplomatică s-a înregistrat o evoluţie similară, către o maşinărie a diferitelor „complexe" de politică externă (Hook, 2014) în şi între care există tot mai multe conexiuni internaţionale. Şi se poate aprecia că miniştrii de externe au avut şi vor avea parte de o „competiţie" tot mai mare din partea altor actori, între aceştia numărându-se forţele armate, serviciile secrete, relaţiile directe şi personale ale unor înalţi funcţionari de stat sau chiar anonimi din afara „maşinăriei", dar în posesia unui *smartphone* şi aflaţi la locul şi momentul potrivit. Toate acestea indică o creştere exponenţială în complexitate a mediului diplomatic.

Decizie versus efecte. Fiecare, intelligence sau diplomaţie, ne oferă o perspectivă nuanţată cu privire la stat. Dacă discursul tradiţional cu privire la diplomaţie se referă la deciziile de politică externă luate de liderii naţionali, studiul activităţii de intelligence mută atenţia către faptul că la baza acelor decizii se află produsele informaţionale ale unor reţele complexe de culegere, procesare şi distribuire a informaţiei. Avem nenumărate studii de intelligence care tratează problema eşecurilor, a vulnerabilităţilor interne şi a motivaţiilor de acţiune. Prin contrast, diplomaţia publică este mai puţin interesată de *luarea deciziilor*, ci mai mult de *output*, de efecte, dar are şi ea de a face cu reţele complexe care caută să modeleze mediul în care evoluează şi se manifestă statul.

Un accent crescut pe partea de *produse/efecte* ale politicii externe diminuează atenţia tradiţional acordată *deciziei* ca element cheie al diplomaţiei şi *statului* ca actor unitar. Acesta este unul din motivele pentru care ar trebui acordată o atenţie mai mare teoriilor actori-reţele şi felului în care acestea sunt relevante pentru diplomaţia modernă (Gstohl, 2012). Dintr-o astfel de perspectivă chiar şi cele mai solide maşinării diplomatice tradiţionale par a fi structural inadecvate pentru a răspunde paletei tot mai largi de actori, cerinţe şi provocări.

Limitele surselor deschise. Cel mai adesea, atunci când trebuie gestionată relaţia cu grupuri sau societăţi relativ închise ori chiar opace (Iran, Coreea de Nord etc.), produsele furnizate de activitatea de intelligence reprezintă un element esenţial: fie şi doar pentru simpla comunicare, este indispensabil să ştii cu cine vorbeşti şi, mai ales, să şi ai subiecte comune de interes, chiar dacă perspectivele pot diferi substanţial.

Apoi, chiar şi în cazul relaţiei cu state/societăţi deschise, dar pe subiecte divergente sau de interes competitiv, nivelul de cunoaştere publică (TV, internet…) cu privire la acestea se poate dovedi destul de precar sau lipsit de structură – partea de intelligence fiind un reper important pentru înţelegerea şi alegerea diferitelor posibilităţi de abordare. Ca decident, nu

totdeauna poţi afla exact ceea ce ai nevoie, la timp şi oportun, urmărind televiziunile de ştiri.

Influenţarea percepţiilor. Chestiunea mai delicată a influenţării percepţiilor unui public mai larg ori a unor personalităţi cheie, prin acţiuni mai mult sau mai puţin discrete, nu poate fi evitată. Ea este abordată pe larg de o literatură de specialitate sau de vulgarizare deja extinsă, de la categoriile persuasive ale retoricii lui Aristotel în secolul IV, la dinamicile persuasiunii în secolul XXI descrise de Perloff (2003). Restrângându-ne, însă, la o perspectivă a pragmatismului analitic, am avea de câştigat dacă am gândi nu atât în termenii unei simple dihotomii *deschis* vs *acoperit*, ci mai degrabă la un *continuum* între 100% deschis („mesajul X a fost transmis prin grija guvernului Y") şi întreaga gamă de variaţiuni de la „sensibil", la „discret, dar nesecret", la „strict secret de importanţă deosebită" etc.

Este binecunoscut faptul că până şi unele ştiri, chiar şi în societăţi cât de poate de democratice, provin de la surse doar parţial dezvăluite. Auzim foarte des „surse apropiate ministerului X", cel mai adesea reprezentând o sintagmă surogat pentru a numi o scurgere de informaţii, uneori voită, alteori nu, transformată în ştire. Tipologia standard a propagandei – albă-gri-neagră – poate fi aplicată şi identificării surselor, iar simţul comun şi înţelepciunea clasicilor (argumentul platonician legat de mitul lui Gyges) arată că gradul de dezvăluire a surselor este adesea proporţional cu veridicitatea acestora. Totuşi, deşi e rezonabil să credem că o sursă „neagră" este mai probabil să dezinformeze decât una „albă", aceasta nu înseamnă neapărat că datele furnizate de aceasta sunt false.

Ideea de fond este că, asemenea ofiţerilor de informaţii şi alţi actori ai diplomaţiei publice trebuie să-şi evalueze mediul de acţiune din mai multe perspective, uneori cu metode împrumutate dimensiunii de intelligence.

Concluzii

Cele două dimensiuni nu sunt brutal separate şi pot exista mai multe puncte comune, unele chiar tranzitând dintr-o parte în cealaltă. Sunt cazuri în care calea diplomaţiei clasice este deschisă pe canale discrete ale diplomaţiei de intelligence, iar altele în care anumite segmente ale unor tratative publice au intrat în culise pentru a nu fi grevate de presiunea „jocului la scenă deschisă" – care îi poate face pe actorii negocierii mult mai puţin flexibili în dialogul reciproc.

În acest punct, practicienii autentici ai diplomaţiei de intelligence converg în a considera că una din regulile importante care face legătura între

negocierile publice şi cele discrete este aceea că trebuie să fii sigur că ceea ce spui în culise se aseamănă cu ceea ce este asumat şi în public – adică aprecierile şi angajamentele asumate în secret trebuie să aibă o substanţă şi un fond similare cu semnalele transmise în public. În caz contrar, dincolo de problema morală evidentă şi de riscul major de decredibilizare, se mai pot produce şi confuzii cu privire la intenţiile şi opţiunile reale.

Nu în ultimul rând, este necesară o anumită conduită etică menită să prevină şi riscul contrar, anume de manipulare, distorsionare ori politizare a rezultatelor activităţii de intelligence în scopuri de diplomaţie publică. Lipsa acestei dimensiuni etice conduce la afectarea consistenţei şi coerenţei procesului de decizie şi, suplimentar, la reducerea sau chiar pierderea încrederii publice – un element central atât pentru dimensiunea de intelligence, cât şi pentru cea de diplomaţie publică.

Mai departe, trebuie reflectat la felul în care diplomaţia de intelligence va evolua pe viitor, la schimbările care încă sunt necesare în ambele domenii, precum şi la strategiile prin care mijloacele unuia pot servi scopurile celuilalt, fără încălcarea limitelor etice şi afectarea încrederii cu care fiecare dintre ele este învestit de stat şi, mai ales, de cetăţean. În stadiul actual, par a fi încă insuficient valorificate studiile comparative. Însă, dat fiind că cercetarea în domeniul diplomaţiei publice este încă în curs de dezvoltare, astfel de problematizări situate la intersecţia dintre cunoaştere şi acţiune se pot dovedi utile, asigurând forţa motrice a unor dezvoltări ulterioare.

Referinţe bibliografice:

1. Andrew, C., Dilks, D., (1984), *The Missing Dimension: Governments and the Intelligence Communities in the 20th Century*, Basingstoke: Palgrave Macmillan.
2. Aristotel, (2004), *Retorica*, Univers Enciclopedic.
3. Barston, R.P., (2014), *Modern Diplomacy*, Routledge.
4. CIR – the US Committee on International Relations, (2001), *The role of public diplomacy in support of the anti-terrorism campaign,* audieri 10 octombrie 2001, accesibil la http://commdocs.house.gov/committees/intlrel/hfa75634.000/hfa75634_0.HTM.
5. CPD – the US Advisory Commission on Public Diplomacy, (2010), *Assesing US public diplomacy – a notional model*, accesibil la http://www.state.gov/documents/organization/149966.pdf.

6. Dima, Dan, (2013) *Noua practica diplomatică - Diplomaţia publică,* Euroinfo.
7. Eriksson, Johan şi Giacomello, Giampiero, (2006), *The Information Revolution, Security, and International Relations: (IR) Relevant Theory?*, în *International Political Science Review,* vol. 27, no. 3, 2006, pp. 221-244.
8. Gilboa, Eytan şi Muntean, Mihai, *Diplomaţia publică şi diaspora*, contribuţie la Forumul European pentru Diplomaţie Publică, Iaşi, 8-10 septembrie 2014.
9. Gstohl, Sieglinde, (2012), *Diplomacy in the 21st century is network diplomacy*, The Free Library, 01.04.2012, accesibil la http://www.thefreelibrary.com/Diplomacy in the 21st century is network diplomacy.-a0316796858.
10. Hayden, Craig, (2013), *Envisioning a Multidisciplinary Research Agenda for Public Diplomacy*, E-IR open acces, accesibil la http://www.e-ir.info/2013/01/11/envisioning-a-multidisciplinary-research-agenda-for-public-diplomacy/.
11. Herman, Michael, (1996), *Evolution and outline*, în *Intelligence in Peace and War*, capitolul I, Royal Institute of International Affairs, 1996.
12. Hook, Steven, (2014), *The Foreign Policy Bureaucracy, în U.S. Foreign Policy: The Paradox of World Power*, capitolul VI, Sage CQ Press 2014, pp. 171-208. http://college.cqpress.com/sites/hook/Home/chapter6.aspx.
13. Jones, Jeffrey B, (2005), *Strategic Communication: A Mandate for the United States*, Joint Force Quarterly, no. 39, 2005, pp. 108-113, accesibil la http://www.dtic.mil/doctrine/jel/jfq_pubs/1839.pdf .
14. Kissinger, Henry, (1998), *Diplomaţia,* Ed. ALL.
15. Melissen, Jan, (2011) *Beyond the New Public Diplomacy*, Netherlands Institute of International Relations 'Clingendael' Paper No. 3, October 2011, accesibil la http://www.clingendael.nl/sites/default/files/20111014_cdsp_paper_jmelissen.pdf.
16. Miculescu, Simona, (2005) *Relaţia dintre presă şi diplomaţie – război sau pace?*, accesibil la http://www.praward.ro/resurse-pr/articole/relatia-dintre-presa-si-diplomatie-razboi-sau-pace.html.
17. Perl, Raphael, (2006), *Combating Extremist Ideologies: Measuring Effectiveness – Considerations for Public Diplomacy*, Connections QJ, vol. V, no. 4, pp. 64-72, accesibil la http://www.pfpconsortium.org/file/combating-extremist-ideologies-measuring-effectiveness-considerations-for-public-diplomacy.
18. Perloff, Richard, (2003), *The dynamics of persuasion: Communication and attitudes in the 21st century*, LEA 2003, accesibil la

http://staff.uny.ac.id/sites/default/files/pendidikan/dwi-budiyanto-spd-mhum/e-book-dinamic-persuasive.pdf.

19. Pinkus, Jonathan, (2014), *Intelligence and Public Diplomacy: The Changing Tide*, în Journal of Strategic Security 7, no. 1, pp. 33-46.
20. Thatcher, Margaret, (15.06.1985), *Speech to American Bar Association*.

INTELLIGENCE ÎN SECOLUL XXI

NOI PROVOCĂRI ÎN LINIA ÎNTÂI A ACTIVITĂŢII DE INTELLIGENCE – PERSPECTIVA UNUI PRACTICIAN

Florian COLDEA*

Abstract

This century has come with different types of challenges in security matters that set a new security agenda for multiple fields, including intelligence. We all live in a growingly complex IT ecosystem, where the availability of the technology is pushed to lower levels, the security of information is fragile, and the citizens change the ways they communicate with one another and with states and governments. The technology-related change is affecting the intelligence agencies ability to deal with some of the most important threats, ranging or coming from the cyber arena, hybrid warfare, large scale migration flows, terrorism, counterespionage and other. Tackling these phenomena is not an easy task for the intelligence field requiring a comprehensive and reinforced cooperative approach, mutual support and assistance, doubled by the responsibility at state levels in decision making.

Keywords: challenges, gaps, security agenda, technology, innovation, way forward.

Introducere

Problema. Secolul al XXI-lea se caracterizează printr-o serie de provocări diverse în materie de securitate cărora trebuie să le facem față. Începând cu „vechea" problemă a Y2K din 2000, continuând cu ansamblul de comploturi teroriste de impact din mai multe orașe occidentale, seria de dezastre legate de diverse fenomene naturale sau migrația la scară largă, și până la problemele de securitate majore determinate de „lumea virtuală", toate acestea ne duc cu gândul la faptul că oamenii, statele și societățile se confruntă cu o nouă agendă de securitate, fundamental diferită față de ceea ce am experimentat în secolul al XX-lea, și caracterizată prin ceea ce numim setul de amenințări „înghețate".

Situaţii specifice. Noua agendă de securitate și provocările la care aceasta se raportează cunosc o serie de aspecte comune. În mare parte din

* Serviciul Român de Informații.

cazuri, amenințarea este direct legată de informație (Jouini, Rabai și Aissa, 2014), așa cum am văzut în toate cazurile de atacuri cibernetice împotriva statului sau a sistemelor informatice deținute de actori din mediul privat. Astfel, observăm că, printre altele, liderii sau responsabilii cu gestionarea crizelor au nevoie de informație critică pe care nu o pot obține în lipsa unei infrastructuri instituționale sau organizaționale solide (Suchan, 2002).

De asemenea, o altă categorie de provocări solicită un amestec complex de informații secrete (provenite fie din surse umane, fie din surse tehnice) și date deja disponibile, dar care nu au fost încă integrate într-un sistem de intelligence viabil (Delaforce, 2013).

Întâlnirea oamenilor și a administratorilor cu tehnologia

Avansul tehnologic din prima parte a secolului al XXI-lea a schimbat fundamental modul în care cetățenii comunică atât între ei, cât și cu statele și guvernele lor. Aceasta a determinat o schimbare evidentă a caracterului relațiilor sociale în societățile moderne, a modelelor de comerț, a relațiilor dintre cetățean și stat (Goldsmith & Crawford, 2014). Omniprezența și disponibilitatea tehnologiei transformă fața securității și a intimității, ceea ce solicită profesioniștilor din activitatea de intelligence să înțeleagă tendințele actuale dacă doresc să răspundă noilor provocări.

Dată fiind **facilitarea proceselor de colectare tehnică și stocare** la nivelul mai multor departamente guvernamentale, numărul bazelor de date privind populația a înregistrat o creștere în ultima vreme, punând la dispoziția agențiilor de informații și a agențiilor angajate în asigurarea securității sau în livrarea unui anumit serviciu în acest sens, o cantitate considerabilă de informații sensibile. **Aceste agenții nu sunt doar cele din domeniul informațiilor și al poliției** – așa cum majoritatea persoanelor cred, ci includ, de asemenea, administrația locală și autoritățile însărcinate cu colectarea taxelor. Aceasta reprezintă o extindere a puterilor oferite agențiilor fără atribuții în domeniul securității și activității polițienești.

Utilizarea datelor de către diverse autorități naționale a determinat îngrijorări considerabile în rândul multora dintre apărătorii dreptului la viața socială și intimă a persoanei, în cadrul informațiilor cu caracter privat aflându-se datele obținute cu ajutorul tehnologiei biometrice, imagini, transferuri de bani, istoricul medical, etc. Însă scurgerile de informații și colectarea acestor date de către sectorul privat (alături de utilizarea pe care o poate da acestor date), precum și numărul punctelor de acces de unde datele pot fi accesate ilegal de către adversari reprezintă o cauza diferită și de mare îngrijorare.

Pe scurt, dacă disponibilitatea și utilitatea tehnologiei sunt aduse tot mai aproape de individ, în mod contrar, cunoașterea necesară pentru securizarea informației nu urmează aceeași direcție, sau cel puțin nu cu aceeași viteză. În acest mod, securitatea informației este din ce în ce mai fragilă, direct proporțională cu utilitatea care îi este dată de către state și, implicit, de către sectorul privat.

Prezența întregii infrastructuri tehnologice creează ceea ce am putea numi un „ecosistem", în esență, un sistem de operare 24/7 în cadrul căreia servere, rețele și aplicații pe mobil trimit și primesc date către/de la alte servere, rețele și aplicații – sperând că toate sunt de interes pentru state, companii sau alte persoane și clienți pe care acestea îi servesc.

Statele pierd monopolul deținut asupra tehnologiei: provocarea decalajului

Ultimul deceniu s-a caracterizat prin trecerea la o paradigmă a tehnologiei, generată de creșterea exponențială a bugetelor pe care actorii privați le dedică progresului tehnologic – atât pentru dezvoltarea, cât și pentru integrarea acestuia în rândul activității zilnice de business – și astfel, lăsându-i în urmă pe cei care ocupau locul întâi cu ceva ani înainte: actorii statali. **A devenit clar că statele nu mai sunt principalele motoare ale dezvoltării tehnologice**, iar instituțiile trebuie să se adapteze pentru a putea ține pasul cu ritmul impus în prezent de către actorii privați și să răspundă la așteptările în schimbare ale societății. Această diferență între avansul tehnologic și capabilitatea statului reprezintă o vulnerabilitate nouă și strategică prin faptul că provoacă abilitatea instituțiilor de a folosi ultimele progrese în domeniul tehnologiei, chiar și în situații majore de criză.

Andrew Parker, directorul general al MI5, subliniază că „provocarea critică, și chiar cronică, am putea spune, căreia trebuie să-i facem față, vine din însăși schimbarea tehnologică" (Adresa din 8 ianuarie 2015). Altfel spus, schimbarea determinată de tehnologie ne afectează abilitatea de a trata corespunzător unele dintre cele mai importante amenințări.

Acest lucru nu este însă o surpriză: abilitatea de a accesa discuțiile purtate între teroriști este vitală pentru capacitatea agențiilor de intelligence de a menține nivelul de siguranță a țărilor ai căror cetățeni sunt. Internetul a schimbat și continuă să schimbe un număr foarte mare de aspecte din viața noastră – în foarte multe dintre aceste cazuri în bine, revoluționând comerțul și comunicațiile, lărgind gama de opțiuni în diverse domenii și facilitând accesul la informație pentru noi toți. Dar, în același timp, așa cum am arătat

în exemplele de mai sus, internetul a oferit de asemenea teroriștilor aceleași avantaje și oportunități (Weimann, 2004).

Toate virtuțile recunoscute ale internetului – accesul facil, absența reglementării sau prezența acesteia într-o formă minimală, potențiala audiența în creștere la nivel global sau fluxurile rapide de informații – au fost deviate astfel încât să poată lucra în avantajul grupurilor determinate să folosească teroarea asupra societăților pentru a-și putea atinge obiectivele. În aceste zile, toate grupările teroriste active și-au stabilit prezența pe Internet, de multe ori de-o manieră foarte dinamică prin intermediul unor site-uri web, grupuri și rețele au apărut deodată, acestea modificându-și frecvent forma și dispărând apoi dintr-o dată prin schimbarea adresei, dar păstrând conținutul similar sau membrii. Aceste canale sunt folosite pentru răspândirea propagandei, pentru radicalizarea indivizilor ușor impresionabili, pentru aranjarea călătoriilor, pentru transferul banilor. Dar cei mai mulți le folosesc pentru comunicare, pentru planificare și organizare; practic, folosesc aceleași instrumente de comunicare ca restul oamenilor.

Însă schimbările pe care tehnologia și piața le înregistrează riscă să ducă la închiderea zonelor în cadrul cărora ar trebui să avem acces pentru a opera. Locurile obscure din care aceia care doresc să ne facă rău, pot complota și planifica, se multiplică. Astfel, noi toți – statul, societățile și agențiile – avem nevoie să menținem același ritm și să nu permitem diferențelor tehnologice să devină noul teritoriu și o sursă de amenințări imposibil de abordat și contracarat.

Schimbarea tehnologică și cele mai importante amenințări

Arena cibernetică. În prezent, un stick USB stricat sau virusat poate provoca mai multe prejudicii decât o bombă sau o rachetă. Amenințarea cibernetică nu doar schimbă imaginea războiului, ci reprezintă, de asemenea, riscuri mari la adresa statelor și a cetățenilor.

Războiul cibernetic este un fenomen relativ nou, emergența sa justificându-se prin dependența crescândă față de infrastructura și dotările cibernetice, dar și prin costul scăzut al transformării acestui instrument menit să faciliteze munca și comunicarea într-o armă cu un potențial ofensiv ridicat. Există numeroase schimbări al paradigmei convenționale privind câmpul de luptă, iar această abordare cibernetică pare să opereze o trecere de la mijloace la scop (Sharma, 2009) – un foarte bun motiv pentru a înțelege și a fi în pas cu permanentele evoluții care au loc zilnic în domeniul IT.

Dintr-o perspectivă profesională, aceste evoluții în domeniul IT trebuie privite în raport cu o provocare deja existentă în domeniul securității,

iar în cadrul acestei perspective, este clar că acestea au devenit un nou declanşator atât pentru ameninţări vechi, cât şi pentru cele recent descoperite: spionaj, sabotare, dezinformare, energie etc. Există un consens clar că suntem martori la crearea unei noi „arene de confruntare" (Kostopoulos, 2008, pp. 165-169) – spaţiul virtual/cybernetic – caracterizat prin propriul tip de vulnerabilităţi, riscuri şi oportunităţi. Atacuri cibernetice au loc în fiecare minut peste tot în lume şi chiar dacă doar o mică parte au potenţialul de a aduce prejudicii securităţii naţionale, consecinţele lor deja s-au dovedit a avea potenţialul de a fi distrugătoare.

Pentru toate agenţiile de intelligence, este vital să ţină pasul cu transformările în această nouă arenă, să rămână competitive în abilitatea lor de a gestiona provocările ce se nasc chiar în acest nou context virtual. Serviciul Român de Informaţii şi-a extins cooperarea cu partenerii săi (atât la nivel naţional, cât şi internaţional) şi a creat Centrul Cyberint[1] pentru a creşte nivelul de protecţie şi pentru a facilita consolidarea rezilienţei necesare acestui nucleu de infrastructură critică al statului şi al societăţii deopotrivă, sisteme IT.

Dat fiind că doctrina în acest domeniu este într-o permanentă schimbare determinată de fiecare atac major sau „salt de broască" ce se înregistrează pe palierul tehnologiei, agenţiile de informaţii trebuie să acţioneze cu un set de norme flexibile şi adaptabile ce le conferă mai multă putere pentru a răspunde noilor ameninţări cibernetice, dar într-un cadru legal clar care nu expune cetăţenii, statele şi instituţiile.

Contraspionajul în era informaţională. Ritmul rapid înregistrat de avansul tehnologic a adus noi probleme şi oportunităţi pentru organizaţiile şi profesioniştii implicaţi în activităţi de contraspionaj. Există o cantitate incredibilă de informaţii deja disponibile pe internet şi relativ accesibile altor agenţii sau chiar indivizi „ambiţioşi", oferind posibilitatea de a accesa sau agrega informaţii secrete. Acum zece ani, un ziar a fost capabil de a crea o listă conţinând numele a mii de agenţi CIA, zeci de numere de telefon interne şi chiar mai multe facilităţi clasificate, adresele de domiciliu şi numele de acoperire, pur şi simplu prin scanarea bazelor de date comerciale disponibile on-line (Crewdson, 2006).

Dacă, de regulă, tehnologia se presupune că facilitează distribuirea la scară mai mare şi mai rapidă a informaţiilor, rolul pe care activitatea de contraspionaj îl are este acela de a bloca accesul la resursele statului sau

[1] Vezi detalii pe http://www.sri.ro/cyberintelligence-en.html.

a agenţiilor de informaţii. Astfel, este foarte important ca activitatea de contraspionaj să se adapteze rapid la noile condiţii operative pe care era informaţională le presupune. Dar această responsabilitate nu aparţine exclusiv ofiţerilor/agenţiilor de informaţii: pe de o parte pentru că unii dintre aceştia nu au pregătirea tehnică pentru a asigura un nivel ridicat de securitate împotriva hackerilor calificaţi din toată lumea sau armatelor de hackeri, pe de altă parte deoarece majoritatea informaţiilor şi a agenţilor sunt vulnerabili din motive independente de responsabilitatea acestora, cum ar fi indexarea în mai multe baze de date administrative, instrumente de recunoaştere facială, proiectarea deficitară a securităţii infrastructurii IT critice etc.

Toate aceste provocări trebuie abordate la un nivel mai larg, de către stat sau chiar prin politici aliate, articulate într-o viziune care implică abordări integrate în ceea ce priveşte oamenii, procesele şi infrastructurile, o viziune care să ia în considerare ameninţările clasice la adresa vieţii oamenilor, precum şi ameninţările tehnice care se multiplică într-un ritm accelerat. Un nou ansamblu de programe integrate de gestionare a resurselor şi de formare este necesar, scopul fiind acela de a depăşi obstacolele organizatorice şi culturale actuale, care încă mai despart activitatea de contraspionaj de cea de intelligence alături de alte tipuri de activităţi relevante pentru rezultatele dorite. Tehnologiile moderne (şi, adesea, scumpe) sunt necesare pentru a spori ansamblul de acţiuni specifice domeniului contraspionajului. Nu în ultimul rând, există o nevoie vitală în cadrul întregului proces vizat, şi anume de a obţine şi menţine încrederea cetăţenilor că politicile noastre de contraspionaj sunt structurate şi implementate într-un cadru strict legal, înlăturând astfel orice suspiciune şi teamă.

Războiul hibrid. Acesta poate fi considerat o *nouă provocare*, însă, în realitate, principalele sale elemente nu reprezintă ceva cu adevărat nou (Wilkie, 2009). Pentru noi toţi, este evident că securitatea energetică a fost folosită şi înainte în calitate de armă politică, la fel cum modul în care manevrele militare convenţionale în combinaţie cu atacuri cibernetice puternice şi o propagandă în expansiune s-au răspândit pe toate canalele de media de tip nou. Însă, din punctul meu de vedere, această idee, care deşi „nu este în totalitate nouă", ar trebui să fie dezbătută în rândul teoreticienilor militari, dat fiind că, în prezent, conflictele devin tot mai complexe.

Deşi nu există nicio definiţie unanim acceptată, putem considera cu uşurinţă războiul hibrid ca fiind un „cocktail" sau un „amestec" de forţe militare clasice, insurgenţe, terorism, crimă organizată şi tehnologii avansate. Acest tip de război poate include violări ale legilor internaţionale, de multe ori

de către actori „privaţi", sprijiniţi de către state cu agende puse la îndoială. Toate aceste aspecte se pot manifesta în diverse variante şi, mai mult, oricare ingredient poate fi prezent sau absent în diferite etape ale războiului hibrid. **Se impune astfel întrebarea: există un element de noutate în ceea ce priveşte acest război hibrid?**

Putem afirma că în ultima vreme am asistat la folosirea elementelor componente ale războiului hibrid pe o scară largă şi de-o manieră mai coerentă. Iată ce reprezintă de fapt elementul de noutate: **amploarea şi elementul central**.

Conflictul ucrainean reprezintă ceea ce am putea numi oportunitatea „unui studiu de caz" pentru aceia interesaţi de acest tip de război. După cum a observat Clausewitz (1989, p. 593): „fiecare perioadă are propriul său tip de război, propriile condiţii de limitare şi preconcepţii specifice". Astfel, se poate afirma că, deşi războiul hibrid nu este ceva nou, profesioniştii din domeniul informaţiilor şi al securităţii trebuie să ia în considerare că modalităţile de manifestare ale acestuia devin din ce în ce mai sofisticate şi fatale, necesitând un răspuns pe măsură.

Aceasta poate însemna că în cadrul efortului de a actualizare a principiilor şi teoriilor războiului, trebuie să identificăm acele aspecte care încă rămân constante. În acest domeniu nu există un „ciclu" care conduce la un nou panaceu revoluţionar cu fiecare deceniu care trece, dar se înregistrează schimbări permanente şi incrementale care sunt inerente activităţii de gestionare a securităţii în ansamblul său. „Schimbări revoluţionare ale paradigmei" sunt mai puţin susceptibile de a se produce spre deosebire de ceea ce cred mulţi dintre participanţii la conferinţe pe acest subiect.

La nivelul Alianţei Nord-Atlantice, aşa cum am evidenţiat într-o altă lucrare (Coldea, 2015) – luând în considerare atacurile cibernetice care au lovit Estonia în 2007 – subiectul a fost discutat pentru prima data în ianuarie 2008 şi dezbătut mai departe cu ocazia Summit-ului NATO organizat la Bucureşti în Aprilie 2008.

Terorismul. S-a dovedit a fi un fenomen foarte dinamic pe mai multe niveluri, rămânând una dintre principalele ameninţări la adresa securităţii naţionale şi internaţionale – în special din cauza curbei schimbării pe care o traversează. Ceea ce credem că ştim la un anumit moment despre acest fenomen s-ar putea să nu fie potrivit pentru contracararea sa în viitor, deoarece dacă rădăcina care duce la manifestarea terorismului rămâne constantă, modul de acţiune, tacticile, structura şi organizarea sunt într-o continuă evoluţie. În aceasta constă permanenta provocare pe care terorismul

o reprezintă și motivul pentru care acesta reprezintă principalul subiect de cercetare pentru mediul academic.

Evoluția constantă a terorismului a împins acest fenomen sub umbrela conceptuală a amenințării hibride, așa cum este cazul evident al grupării „Daesh" și al ambițiilor sale de a se comporta precum „un stat" – dând naștere unor noi provocări pentru toate instituțiile statului și pentru practicienii din domeniul securității. Un alt exemplu îl reprezintă numărul în creștere al luptătorilor străini și a celor care se reîntorc în/din zonele de conflict, în special în Irak și în Siria (*Addressing the Foreign Terrorist Fighters Phenomenon from a EU Perspective*, decembrie 2014) – un flux nu doar al persoanelor, ci și al abilităților militare și al ideilor radicale, al fluxului logistic și financiar, al celor care promovează terorismul și chiar al celor care practică terorismul.

Pentru a pune lucrurile în perspectivă, într-o anumită măsură de-o manieră similară cu problema războiului hibrid, trebuie spus că problema luptătorilor străini nu este un fenomen nou. În secolele al XIX-lea și al XX-lea, zeci de insurgenți și-au părăsit țările, alăturându-se grupărilor ostile în calitate de luptători străini în multe războaie civile moderne, multe voci dându-l drept exemplu pe poetul englez Lord Byron, luptător străin în Grecia în 1820 (Malet, 2010, p. 101). Ceea ce este nou în zilele noastre este amploarea amenințării pe care izbucnirea războiului civil și a violenței sectare din Siria, Irak, Libia și alte țări o reprezintă.

Abordarea acestor fenomene nu este ușoară, așa cum a devenit tot mai clar în ultimii ani. Este nevoie de o abordare cuprinzătoare și de cooperare, deoarece vorbim despre o problemă internațională, mai degrabă decât una națională, care poate fi abordată eficient numai prin eforturi comune ale mai multor țări și/sau agenții. Am văzut că, după fiecare atac major (Paris 2015 și 2016, Bruxelles 2015, etc.) normele juridice naționale respective sunt actualizate, în principal prin încadrarea de noi infracțiuni teroriste. Aceasta este o reacție comună și previzibilă la amenințarea tot mai mare, dar care poate crea, de asemenea, riscuri noi legate de lipsa unor standarde comune sau de diferențe în ceea ce privește unele incriminări și proceduri juridice în țări distincte, dar supuse aceleași amenințări.

În acest context, nevoia consolidării cooperării internaționale a devenit din ce în ce mai evidentă și poate fi consolidată în perioada următoare printr-o abordare multi-disciplinară (incluzând domeniul juridic, de intelligence etc.). Niciunul dintre noi nu poate face față singur acestei amenințări, astfel încât se impune nevoia cooperării strânse și concrete.

Fenomenul imigraţionist. Numărul imigranților și al refugiaților a crescut neașteptat de mult în 2015, devenind rapid o temă de importanță critică pe agenda europeană de politică și securitate, punându-i pe decidenţi în situația de a se confrunta cu probleme cheie precum: impactul asupra țărilor de tranzit și a destinațiilor finale (*Countries of transit* ..., 11 septembrie 2015), impactul asupra relațiilor și a solidarității între statele europene (Goldner Lang, 2015), măsura în care globalizarea acționează precum un catalizator pentru dinamica accentuată a populațiilor, rolul pe care instituțiile statului și societatea civilă ar trebui să și-l asume în acest context, etc.

Din perspectiva securității naționale, principala greșeală pe care o putem face este aceea de a gândi și de a aborda această problemă într-un cadru al securității ce intră exclusiv în competența statelor vizate, când de fapt avem de-a face cu o problemă pan-europeană cauzată de un ansamblu de conflicte și instabilităţi manifestate de-a lungul întregii regiuni și societăţi arabe.

Mai mult, dacă ținem cont că la nivelul țărilor europene, există probleme similare care fac obiectul politicilor și al dezbaterilor care transced elementele distincte ce privesc securitatea națională, identitatea și etnia, criza imigranților este cu atât mai mult o preocupare de interes comun la nivelul Uniunii Europene, necesitând solidaritatea în rândul statelor membre sub forma ajutorului și al asistenței reciproce. Dacă dorim să avem o perspectivă de viitor, ținând cont însă că nimeni nu știe care vor fi tendințele pe termen scurt sau mediu (fiind foarte probabil ca pe termen lung războaiele mici și urbanizarea populației la nivel global să mențină ridicat ritmul imigrației), trebuie să acceptăm că există o responsabilitate comună a statelor de a se ajuta pentru a gestiona această problemă și pentru a proteja securitatea națională și regională.

Perspectiva „valurilor mari" de imigranți generează noi riscuri, importante atât pentru instituțiile de implementare a legii, cât și pentru serviciile de informații și securitate. Aceste instituții trebuie să-și adapteze și să-și ajusteze resursele (umane și financiare), fiind nevoite să opereze într-un cadru legal actualizat.

Concluzii sau căi de urmat

În ultimele decenii, ritmul schimbării tehnologice și inovația au determinat neglijarea reglementărilor legislative. Acest decalaj se va adânci fără o serioasă actualizare a legislației care să reglementeze toate aceste progrese tehnologice și practicile asociate, și fără o dezbatere liberă și deschisă asupra gradului de supraveghere de către surse publice și private. State și societăți deopotrivă trebuie să-și adapteze reflexele la această lume

caracterizată de interdependenţă şi interacţiune în creştere inclusiv între domenii în aparenţă distincte precum terorismul şi sănătatea, precum şi între actori la prima vedere diferiţi precum indivizii, guvernul şi industria.

Provocarea centrală în acest context este înţelegerea modului în care putem construi capabilităţile statului, stabili şi sprijini existenţa şi acţiunea unor instituţii solide, bazate pe principii democratice, respectiv urmări îndeaproape profesionalismul, responsabilitatea şi integritatea acestora. Consider că este responsabilitatea noastră, în calitate de profesionişti în sfera activităţii de intelligence, să ţinem pasul cu aceste evoluţii rapide în cadrul actualului mediu volatil de securitate şi să propunem noi soluţii creative pentru a asigura şi a proteja securitatea cetăţenilor noştri.

Toate aceste provocări ar fi mai bine înţelese printr-un efort comun al decidenţilor, practicienilor, reprezentanţilor mediului academic astfel încât să putem dobândi o mai bună înţelegere a acestora, în vederea recomandării unor soluţii viabile. Această manieră de abordare a subiectelor dificile favorizează explorarea unei perspective şi a unor paradigme noi. Într-un moment în care cererea publică de informare şi transparenţă este mai mare ca oricând, trebuie să continue efortul nostru de căutare a unor noi modalităţi de gestionare a tuturor acestor interdependenţe.

Referinţe bibliografice:

1. Adresa din 8 ianuarie 2015 a directorului general al Serviciului de Securitate**,** *Andrew Parker, către Royal United Services Institute (RUSI) din Thames House*, accesibilă la https://www.mi5.gov.uk/home/about-us/who-we-are/staff-and-management/director-general/speeches-by-the-director-general/director-generals-speech-on-terrorism-technology-and-accountability.html**.**
2. *Addressing the Foreign Terrorist Fighters Phenomenon from a EU Perspective*, Global Center on Cooperative Security, Human Security Collective, and International Centre for Counter-Terrorism – The Hague, Policy Brief, December 2014.
3. Coldea, Florian, (2015), *Building national capabilities and countering hybrid threats: lessons learned*, Key Note Speech at NATO Advanced Research Workshop on *Countering Hybrid Threats: Lessons Learned from Ukraine*, Bucharest, 2015 September 28-29th.

4. *Countries of transit: meeting new migration and asylum challenges*, Council of Europe Committee on Migration, Refugees and Displaced Persons, Doc. 13867, 11 September 2015, accesibil la http://assembly.coe.int/nw/xml/XRef/X2H-Xref-ViewPDF.asp?FileID=22017&lang=en.
5. Crewdson, John, (March 12, 2006), *Internet Blows CIA Cover*, in Chicago Tribune, accesibil la http://articles.chicagotribune.com/2006-03-12/news/0603120396_1_agency-employees-or-operatives-cia-director-porter-goss-two-dozen-secret-cia.
6. Delaforce, Ruth, (2013), *Public and private intelligence: historical and contemporary perspectives*, în *Salus Journal*, Issue 1, Number 2, accesibil la http://www.salusjournal.com/wp-content/uploads/sites/29/2013/03/Delaforce_Salus_Journal_Issue_1_Number_2_2013_pp_21-39.pdf.
7. Goldner Lang, Iris, (2015), *The EU Financial and Migration Crises: Two Crises – Many Facets of EU Solidarity*, in E. Dagilyte & E. Küçük (eds.), *Solidarity in EU Law: Legal Principle in the Making*, Edward Elgar Publishing.
8. Goldsmith, Stephen, Crawford, Susan, (2014), *The responsive city. Engaging communities through data-smart governance*, San Francisco, Jossey-Bass.
9. Jouini, Mouna, Rabai, Latifa Ben Arfa, Aissa, Anis Ben, (2014), *Classification of Security Threats in Information Systems*, Procedia Computer Science, Volumul 32, pp. 489–496.
10. Kostopoulos, George K., (2008), *Cyberterrorism: The Next Arena of Confrontation*, Communications of the IBIMA 6(1), pp. 165–169, accesibil la http://www.ibimapublishing.com/journals/CIBIMA/volume6/v6n25.pdf.
11. Malet, David, (2010), *Why Foreign Fighters? Historical Perspectives and Solutions,* Published by Elsevier Limited on behalf of Foreign Policy Research Institute, Winter 2010**.**
12. **S**harma, Amit, (2009), *Cyber Wars: A Paradigm Shift from Means to Ends in The Virtual Battlefield: Perspectives on Cyber Warfare*, Proceedings 2009, NATO Cooperative Cyber Defence Centre of Excellence, accesibil la https://ccdcoe.org/sites/default/files/multimedia/pdf/01_SHARMA_Cyber_Wars.pdf.
13. Suchan, William, (2002), *The organizational information infrastructure maturity model*, AMCIS Proceedings, Paper 295, accesibil la http://aisel.aisnet.org/cgi/viewcontent.cgi?article=1654&context=amcis2002.
14. Von Clausewitz, Carl, (1989), *On War,* Princeton University Press.

15. Wilkie, Robert, (2009), *Hybrid Warfare: Something Old, Not Something New*, în Air & Space Power Journal – Winter 2009, accesibil la http://www.airpower.maxwell.af.mil/airchronicles/apj/apj09/win09/wilkie.html.
16. Weimann, Gabriel, (March 2004), *How Modern Terrorism Uses the Internet*, US Institute of Peace, Special Report 116, accesibil la http://www.usip.org/sites/default/files/sr116.pdf.

SISTEMUL FRANCEZ DE INTELLIGENCE ECONOMIC

Loredana IVAN*

Abstract

„Economic intelligence" or „State level competitive intelligence", a relatively new subject regarding international intelligence concerns, aims to augment economic competitiveness and to create synergy between state and private interest, for maximum efficiency and effectiveness in the competition for resources and markets. Information, as a production neo-factor, when it is properly processed and valued, has the potential to significantly contribute to the growth and consolidation of the national economy. France is one of the pioneers of the international scene, managed to obtain great results in the design and implementation of a national economic intelligence.

Key words: Economic intelligence, France, national interest, Risks.

Introducere

Mediul concurenţial este cel care permite pieţei să funcţioneze eficient, însă asigurarea performanţelor competitive la nivelul ansamblului economic impune monitorizarea relaţiilor economice şi ajustări prin politici publice. Statele sunt forţate să-şi adapteze permanent economiile, ceea ce generează nevoia permanentă de informaţie actualizată şi pertinentă. Pentru a preveni şi combate efectele nedorite ale concurenţei pe o piaţă devenită globală, statele avansate economic folosesc sisteme de creştere a competitivităţii propriilor economii, colectarea, procesarea şi analiza datelor şi informaţiilor fiind un instrument important.

Unele ţări precum Japonia, Franţa, SUA, Marea Britanie, Germania s.a au optat, în era postbelică, pentru dezvoltarea şi implementarea unor adevărate strategii de forţă, care să le permită să facă faţă provocărilor asociate competitivităţii economice la nivel global, iar, în acest spectru acţional, **modelul francez** s-a delimitat rapid şi în mod evident, mai ales, prin plasarea intelligence-ului economic la nivel de politică statală.

Astfel, la scurt timp după cel de-al doilea Război Mondial, Japonia a proiectat un sistem complex de culegere şi procesare a informaţiilor economice, în care punctul focal a fost Ministerul Industriei şi Comerţului

* Doctorand Academia Națională de Informații „Mihai Viteazul", București.

Exterior, reuşind, astfel, să recupereze decalajul faţă de alte state în multe domenii: construcţii navale şi de automobile, construcţii de maşini, computere, automatizări etc. În Franţa, începând cu anul 1994, odată cu raportul *Intelligence économique et stratégie des enterprises* (Martre, Clerc şi Harbulot, 1994), s-a acordat o importanţă majoră informaţiilor din domeniul economic, instituind un adevărat sistem naţional de colectare, procesare şi valorificare a informaţiilor utile operatorilor economici pentru implementarea propriilor strategii de afaceri. În SUA, din 1995, Strategia de Securitate (1995) se bazează pe trei piloni: componenta militară, cea economică şi cea culturală, astfel că administraţia de la Washington investeşte enorm în dezvoltarea capacităţilor proprii de „alimentare" a guvernului şi a întreprinderilor cu informaţie economică. În acelaşi timp, începând cu anul 1998, Marea Britanie a plasat problematica informaţiilor în centrul strategiei economice, definită în raportul *Our competitive future: building the knowledge driven economy* (1998), ce şi-a propus modificarea politicilor administraţiei pentru a veni în ajutorul companiilor britanice.

În acelaşi domeniu, Germania a reuşit, în anii '90, să coreleze interesele statului/landurilor cu cele ale operatorilor economici, de talie mare, medie sau mică, prin dialog sistematic pe subiecte legate de competitivitate prin informaţie, în final, rezultând un sistem puternic legat de doctrina economică ordo-liberală (Revista 22, nr. 304).

Alte ţări sunt în situaţia de a nu fi reuşit să armonizeze obiectivele companiilor cu cele oficiale la nivel de politică de stat, astfel că nu au încă definite strategii naţionale de intelligence economic, însă actori economici importanţi din aceste state precum Spania, Italia şi Portugalia au programe complexe de intelligence competitiv. Nici China nu dispune de o strategie naţională de intelligence economic, formalizată, în sens occidental, însă Beijing-ul a înţeles că spectrul competiţiei globale este preponderent economic, astfel că, încă de la finele anilor '90, guvernul chinez duce o politică bazată pe informaţie, care vizează preponderent controlul asupra tehnologiilor viitorului. Rezultatele sunt vizibile pentru oricine şi oriunde.

În schimb, statele din fostul bloc comunist nu au programe naţionale şi nici iniţiative semnificative pentru alinierea la practicile din domeniu ale statelor dezvoltate economic. Competiţia politică internă din aceste ţări a făcut imposibilă conturarea unor preocupări esenţiale care să direcţioneze resurse către crearea unor sisteme reale de creştere a competitivităţii economice. Mai mult, din cauza inexistenţei unei capacităţi administrative solide şi pe fondul tendinţelor către acte de corupţie ale unor segmente ale aparatului de stat, în ultimele decenii, au fost comise erori majore în plan economic intern, ceea ce a accentuat decalajul în raport cu ţările care au înţeles cu ce arsenal se cuceresc, în prezent, teritoriile şi minţile oamenilor.

Repere conceptuale

Intelligence-ul economic sau intelligence-ul competitiv la nivel de stat este un domeniu relativ nou în preocupările internaţionale de intelligence, cu o focalizare deosebită în cercurile de specialitate din Franţa. Conceptul s-a dezvoltat printr-un proces dual al standardizării practicilor, şi anume constituirea unei comunităţi ştiinţifice, fiind transformat în domeniu de studiu distinct în ultimii 20 de ani.

Henri Martre, coordonatorul Raportului Commisariatului Planului, denumit *l'Intelligence économique et la compétitivité des entreprises* (1994, pp. 16-17), defineşte intelligence-ul economic drept ansamblul acţiunilor coordonate de căutare, procesare şi distribuire a informaţiilor utile operatorilor economici pentru implementarea propriilor strategii de afaceri. Aceste diferite acţiuni se desfăşoară în mod legal, cu toate garanţiile de protecţie necesare pentru conservarea patrimoniului societăţii, în cele mai bune condiţii de calitate, timp şi costuri. Informaţiile utile sunt necesare diferitelor paliere de decizie ale societăţii sau comunităţii, pentru a dezvolta şi implementa în mod consecvent strategia şi tactica necesare pentru atingerea obiectivelor sale de a-şi îmbunătăţi poziţia în mediul său concurenţial. Aceste acţiuni, în cadrul companiei, sunt organizate în jurul unui ciclu nesfârşit, generând o viziune comună a obiectivelor companiei.

Potrivit lui Christian Harbulot (*Intelligence economique*), intelligence-ul economic este definit ca cercetarea și interpretarea sistematică a informațiilor accesibile tuturor, pentru a descifra intențiile competitorilor și a le cunoaște capacitățile. Include toate operațiunile de supraveghere a mediului concurențial (protecție, monitorizare și influență) și diferă de intelligence-ul tradițional prin (*Intelligence economique*):

- natura domeniului său de aplicare deoarece se referă la domeniul informațiilor deschise și, prin urmare, necesită conformitatea cu o etică credibilă;
- identitatea actorilor săi în măsura în care personalul și sistemul de încadrare – și nu numai experții – pot să participe la construirea unei culturi colective de informații;
- specificitățile culturale pentru că fiecare economie națională produce un model original de intelligence economic, al cărei impact asupra strategiilor comerciale și industriale variază de la țară la țară.

În Raportul *Intelligence économique, compétitivité et cohésion sociale,* prezentat premierului francez în 2003 (Carayon, 2003), deputatul Bernard Carayon a făcut din intelligence-ul economic o politică publică de competitivitate, de securitate economică, de influență, în special, în rândul

organizațiilor internaționale, precum și de formare. Intelligence-ul economic provine dintr-o grilă de lectură originală a globalizării, care ia în considerare caracteristicile cotidiene ale pieţelor, eludarea normelor, jocurile de putere și de influență. Este o nouă abordare, pe care autorul o consideră esenţială, așa cum au fost, la vremea lor, politicile cetăţii, dezvoltării durabile etc. Intelligence-ul economic este o politică publică de identificare a sectoarelor și tehnologiilor strategice, dar și de asigurare a convergenţei intereselor între sfera publică și cea privată. Este o politică publică prin definirea conținutului și sfera de aplicare a acesteia. Conținutul său este securitatea economică a statului. Ca urmare, intelligence-ul economic trebuie să definească activitățile ce trebuie protejate și mijloacele cu ajutorul cărora se poate atinge acest deziderat. În plus, raportul definește modul în care companiile sunt sprijinite pe pieţele globale, dar și maniera în care pot fi influențate organizațiile internaționale, care impun reglementări și standarde aplicabile statelor, întreprinderilor și cetățenilor (Carayon, 2003).

La rândul ei, Claude Revel (*Intelligence economique*) subliniază că intelligence-ul economic are scopul de a cunoaște mediul extern și, prin urmare, de a adapta comportamentul în prealabil. Identifică oportunitățile și factorii determinanți ai succesului, anticipează amenințările și previne riscurile, pentru a asigura, a acționa și a influența mediul exterior într-o perspectivă de competitivitate internațională. Claude Revel abordează intelligence-ul economic prin prisma a trei funcţii (*Intelligence economique*):

- gestionarea informaţiilor ce presupune colectarea, selectarea, validarea și prelucrarea datelor necesare și pertinente despre concurenţi, regulile și caracteristicile pieţelor;
- protejarea ce constă în asigurarea securităţii fizice și de orice altă natură, ceea ce înseamnă asigurarea capacităţii de a anticipa riscurile la adresa proprietăţii intelectuale, imaginii sau capitalului unei/unor firme;
- influenţarea concurenţei ce reprezintă capacitatea de a argumenta, convinge, negocia, de a face lobby profesionist, dar și de a exercita o influență normativă prin anticiparea normelor și standardelor internaționale și, eventual, participarea la dezvoltarea lor.

Astfel, conform lui Claude Revel (*Intelligence economique*), intelligence-ul economic permite o cunoaștere mai bună a concurenților, principiilor, normelor și standardelor ce pot influența activitatea și, prin urmare, asigură capacitate adecvată de acțiune pe pieţele de profil. Intelligence-ul economic se bazează pe mecanisme deontologice și este total diferit de spionaj, furt și trafic de influență.

Tot în Franța, Christophe Deschampes și Nicolas Moinet (2011) susțin că, în contextul globalizării și al exacerbării competiției mondiale, intelligence-ul economic – ca mod de obținere a informației strategice utile agenților economici – constituie tot mai evident o necesitate stringentă. Operatorii economici, regiunile sau statele nu pot să ignore și chiar trebuie să impună și să fructifice această funcție esențială pentru consolidarea piețelor, garantarea calității și, mai recent, pentru asigurarea dezvoltării durabile.

În România, Valeriu Ivan (2014) subliniază că intelligence-ul economic sau intelligence-ul competitiv la nivel de stat, domeniu relativ nou în preocupările internaționale de intelligence, își propune să augmenteze competitivitatea economică și să creeze sinergie între interesele private și cele ale statului, pentru un maximum de eficiență și eficacitate în competiția globală pentru resurse și piețe. Informația, ca neo-factor de producție, corect procesată și valorificată, are potențialul de a contribui semnificativ la creșterea și consolidarea economiei naționale.

Coordonate ale sistemului francez de intelligence economic

Momentele istorice principale. ***După lucrările câtorva pionieri (Jacques Villain, Philippe Baumard, Amiral Pierre Lacoste, Henri Dou, François Jakobiak, Vahe Zartarian[1]), intelligence-ul economic a fost introdus oficial în Franța în aprilie 1992, prin crearea filialei franceze a Society of Competitive Intelligence Professionals (SCIP – Franța), la inițiativa lui Robert Guillaumot, Yves-Michel Marti, Bruno Martinet și Jean-Pierre Bernat[2].***

În anul 1994, raportul Comisariatului General al Planului *Intelligence économique et stratégie des entreprises,* denumit și Raportul Martre (după numele autorului său, Henri Martre, fostul șef al structurii aerospațiale), conferă legitimitatea statului în acest nou domeniu de activitate. Ideea creării unui grup de studiu cu privire la problematică este inclusă în Plan de Philippe Baumard și Christian Harbulot. Grupul s-a constituit în mod informal și a inclus, în marea lui majoritate, apropiați ai lui Philippe Baumard și Christian Harbulot, ceea ce a constituit o premieră în materie.

În aprilie 1995, s-a înființat Comitetul pentru competitivitate și securitate economică, constituit pe lângă primul ministru francez și cuprinzând șapte membri aleși pentru câte doi ani (manageri de companii,

---

[1] Publicate în anii '80, conform http://www.portail-ie.fr/article/571/Historique-de-l-intelligence-economique (accesat în 01.06.2015).

[2] Strategic and Competitive Intelligence Profesionals (SCIP) este o asociație internațională ce reunește 400 de membri în Franța și 6.000 în cincizeci de țări.

oameni de ştiinţă şi sindicalişti). Acest for a devenit desuet începând cu anul 1997, în timpul guvernului lui Lionel Jospin, care nu a numit noi membri în Comitet. Misiunea acestui for era de a-l informa pe premier despre aspecte de competitivitate şi securitate economică, consiliindu-l cu privire la proiectarea şi implementarea politicii urmărite în acest sens de autorităţile publice.

Prin intermediul unui raport înaintat Preşedintelui Franţei, François Mitterand, publicat odată cu Decretul nr. 95-350 din 01 aprilie 1995 privind crearea unui comitet pentru competitivitate şi securitate economică, se evidenţiază rolul informaţiei ca materie primă strategică şi determinarea statului de a-şi mobiliza toate energiile în jurul marii provocări naţionale pe care o reprezintă intelligence-ul economic[3]. Acest demers a fost pus în practică prin stabilirea unor priorităţi clar delimitate. Prima dintre acestea se referă la orientarea către necesităţile întreprinderilor, în special ale celor mici şi mijlocii, pentru a avea acces la informaţii şi la cerinţele aferente pentru redirecţionarea culegerii publice de date şi a facilităţilor de prelucrare. A doua prioritate se referă la promovarea interacţiunii între autorităţile publice şi private în chestiuni de intelligence economic, în vederea creării şi coordonării unor reţele de schimb de informaţii. A treia prioritate se referă la dezvoltarea unui set de practici, prin diseminarea la scară largă a unei abordări pe linie de intelligence economic, context în care au fost elaborate cursuri în universităţi şi şcoli de afaceri. În plus, s-a evidenţiat o dinamică regională, prin înfiinţarea unor programe de training şi conştientizare destinate întreprinderilor mici şi mijlocii în domeniul intelligence-ului economic. Prima iniţiativă experimentală la scară naţională a fost lansată în regiunea pariziană în octombrie 1995, pentru o perioadă de un an, pe un eşantion incluzând 300 de companii.

În 2000, două fonduri de investiţii americane, suspectate că ar avea conexiuni cu CIA (*Intelligence economique*), Texas Pacific Group şi Spectrum Equity Investors, au încercat să preia controlul asupra companiei franceze Gemplus, liderul mondial de carduri electronice. Ministerul francez de Externe a fost avertizat a doua oară cu privire la dosarul EUTELSAT[4], vizat atunci de aceleaşi două fonduri de investiţii.

În iunie 2003, deputatul Bernard Carayon, a prezentat premierului francez Raportul *Intelligence économique, compétitivité et cohésion sociale*,

---

[3] Vezi detalii pe https://www.bo.sga.defense.gouv.fr/boreale_internet/popup.php?no_cache=2&mode= 1&txt_id=194446&format=pdf& (accesat în 01.06.2015).

[4] EUTELSAT Franţa este unul dintre cei mai mari operatori de satelit din lume, având o flotă de sateliţi ce deservesc utilizatori în întreaga Europă, Africa, Asia şi cele două Americi.

care abordează intelligence-ul economic drept o politică publică destinată garantării coeziunii sociale prin asigurarea dezvoltării economice. Într-una din anexele Raportului sunt incluse mai multe definiţii, unele contradictorii, tocmai pentru a demonstra dificultatea definirii intelligence-ului economic. Printre efectele induse de apariţia Raportului lui Bernard Carayon figurează numirea, în 2003, a unui înalt responsabil cu intelligence-ul economic, Haut Responsable à l'Intelligence Économique - HRIE, pe lângă primul ministru, dar şi crearea de poli de competitivitate, în timpul mandatului lui Dominique de Villepin, şi, respectiv, implementarea unei politici de intelligence teritorial, în mandatul lui Nicolas Sarkozy (*Intelligence economique*).

Mecanismele instituţionale. ***În data de 31 decembrie 2003, Alain Juillet a fost numit înalt responsabil cu intelligence-ul economic în cadrul Secretariatului General al Apărării Naţionale (Secrétariat général de la défense nationale – SGDN), dată fiind credibilitatea sa deosebită la nivel naţional conferită de posturile de decizie pe care le-a avut în domeniul afacerilor şi, respectiv, în cadrul serviciilor de informaţii franceze, ceea ce a surmontat lipsa de experienţă în domeniul intelligence-ului competitiv. În acelaşi timp,*** **a fost creată o Delegaţie Generală de Intelligence Economic, la Bercy, iar, în 12 octombrie 2004, director al acestui for a fost numit François Asselineau (*Intelligence economique*).**

În septembrie 2005, au fost definite sectoarele considerate „sensibile", odată cu anunţul public făcut de ministrul industriei în acest sens, cu privire la modificarea Codului monetar şi financiar (mass media au citat domeniul jocurilor de noroc/cazinourilor, industria specială, criptologia, biotehnologia, securitatea sistemelor informatice etc.). Tot în septembrie 2005, s-a asigurat coordonarea activităţilor între delegatul interministerial pentru dezvoltare durabilă şi înaltul responsabil cu intelligence-ul economic.

În august 2006, a fost numit coordonatorul ministerial al intelligence-ului economic în cadrul ministerelor/departamentelor de la Bercy (*Intelligence economique*). A fost pus în aplicare sistemul de intelligence economic în cadrul ministerelor economic şi financiar de la Paris şi de la nivelul regiunilor. Prin Circulara din 21 martie 2007 (publicată în Monitorul Oficial din Franţa, cu nr.108 din 10 mai 2007), au fost creaţi responsabilii regionali cu intelligence-ul economic.

În semestrul I/2009, au avut loc mai multe activităţi publice importante, astfel (*Intelligence economique*):

- desemnarea responsabililor cu intelligence-ul economic în diverse ministere. Spre exemplu la Ministerul Afacerilor Externe s-a prevăzut câte o

structură pe lângă fiecare ambasador, în timp ce la ministerele de interne, economie, finanţe şi industrie, a fost numit câte un responsabil, dar fără echipă şi fără instrumente de lucru.

- implementarea, de către prefecţi, a reţelelor regionale de intelligence economic;

- crearea unui sistem destinat profesioniştilor pentru formarea/ pregătirea în domeniul intelligence-ului economic;

- crearea unei federaţii a profesioniştilor în domeniul intelligence-ului economic.

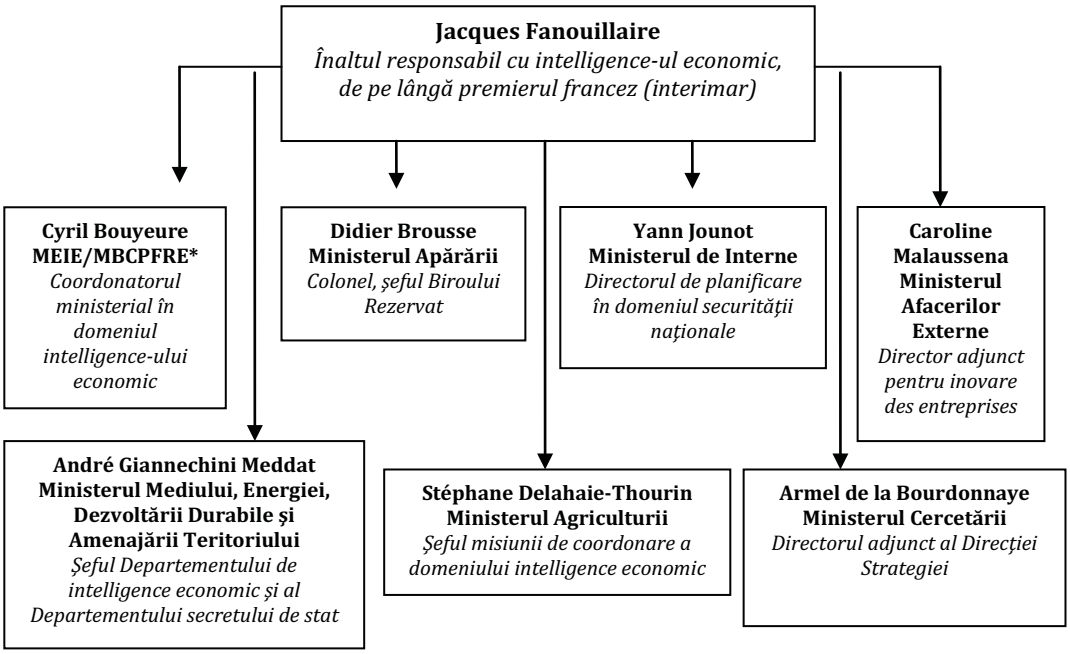
În 17 septembrie 2009, a fost numit delegatul interministerial pentru intelligence economic, iar în august 2010, a fost desemnat un nou coordonator ministerial pentru intelligence economic al ministerelor economic şi financiar.

Prin Circulara din 15 septembrie 2011, primul ministru a declarat publică Acţiunea statului în domeniul intelligence-ului economic la nivelul autorităţilor centrale şi serviciilor deconcentrate (*Politique-publique-d-intelligence-economique*).

În 29 mai 2013, Claude Revel a fost numită delegat interministerial în domeniul intelligence-ului economic, post creat pe lângă primul ministru francez (*Intelligence economique*).

În concluzie, sistemul francez de intelligence economic se bazează pe mecanisme centrale de implementare, dar şi pe o reţea teritorială, formată din centre regionale, responsabilă cu operaţionalizarea strategiilor de acest gen (CRIE), care depinde de Serviciul de Coordonare a Intelligence-ului Economic (SCIE) a ministerelor economiei, industriei şi locurilor de muncă. O reformă a acestui sistem a avut loc în ultimii ani, pentru a creşte gradul de performanţă (*Intelligence économique: historique*). Practic, s-a recurs la înlocuirea mecanismului înaltului responsabil cu intelligence-ul economic (HRIE) cu delegatul interministerial, dar şi la trecerea celor 22 centre regionale (CRIE) în subordinea direcţiilor regionale de afaceri, concurenţă, consum, muncă şi locuri de muncă (DIRECCTE), care, în 2010, au fuzionat în 7 structuri administrative deconcentrate (*Intelligence économique: historique*).

Sistemul francez de intelligence economic include un mecanism central, reprezentat grafic în figura 1, coordonat de înaltul responsabil şi format din exponenţi din cadrul a şapte structuri instituţionale majore.



* MEIE/MBCPFRE – Ministerul Economiei, Industriei și Locurilor de Muncă/ Ministerul Bugetului, Conturilor Publice și Reformei de Stat

Figura nr. 1 – Sistemul central de intelligence economic (2009)
Sursa: adaptare după *Intelligence économique: historique* în *Intelligence économique: deux nouvelles missions pour l'expert-comptable,* 64ème Congrès de l'Ordre des Expert-Comptables

La nivel teritorial, sistemul de intelligence economic din Franța se fundamentează pe patru structuri instituționale centrale, Ministerul Apărării, Ministerul de Interne, Ministerul Economiei și Finanțelor și Ministerul Afacerilor Externe, precum și pe: sistemul cameral francez, universități, Agenția de Difuzare a Informațiilor Tehnologice, Agenția Franceză de Investiții Internaționale, rețeaua publică de sprijin al exporturilor, Agenția Națională de Cercetare, entități asociative teritoriale etc. În linii mari, sistemul teritorial este coordonat de fiecare prefect și are două tipuri de intervenții (ofensive și defensive) – reflectate grafic în figura nr. 2.

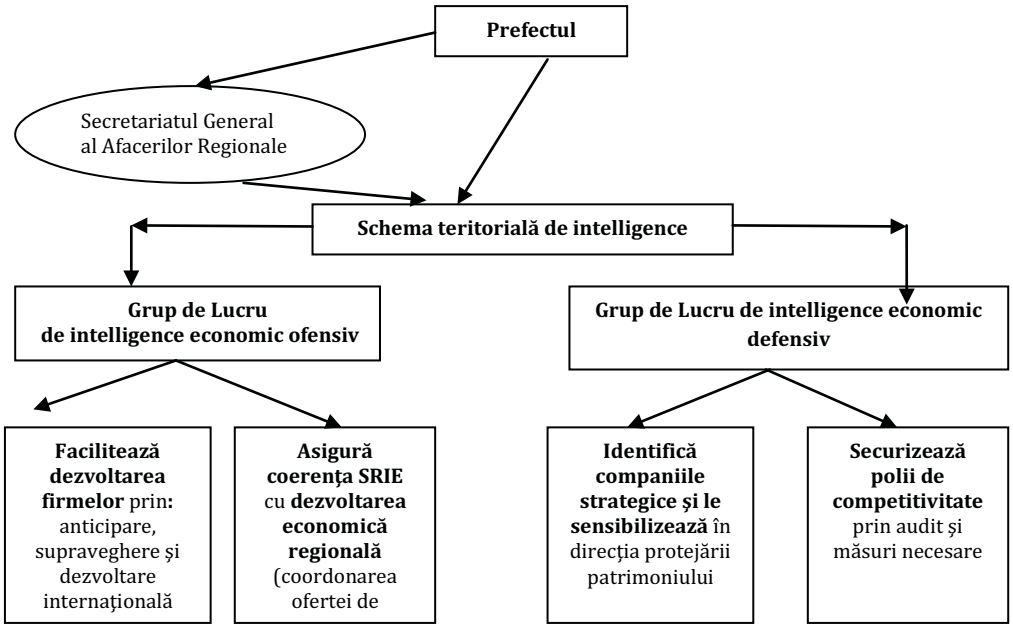


Figura nr. 2 – Sistemul teritorial de intelligence economic (august 2009).
Sursa: adaptare după *Intelligence économique: historique* în *Intelligence économique: deux nouvelles missions pour l'expert-comptable,*
64ème Congrès de l'Ordre des Expert-Comptables

Sistemul de pregătire şi perfecţionare în domeniul intelligence-ului economic

Sistemul de pregătire şi perfecţionare în domeniul intelligence-ului economic este format din următoarele structuri, conform SMBG[5]:

- Şcoala de Război Economic, de la Paris, plasată pe locul 1 în Franţa din 2002 şi până în 2013;

- Şcoala Europeană de Intelligence Economic (EEIE), de la Versailles, ocupanta locului 3 în 2013, pregăteşte licenţiaţi în domeniul consultanţei pentru intelligence economic;

[5] SMBG este primul cabinet de orientare, specializat în pregătirea candidaţilor pentru a accede în şcoli superioare şi universităţi. De asemenea, este un clasament al cursurilor de pregătire post-universitară în Franţa.

- Institutul de Administrare a Afacerilor din Poitiers (Pol de Informaţii-Comunicare), ce asigură cursuri de masterat în intelligence economic şi comunicare strategică;
- Universitatea din Paris-Est Marne-la-Vallée, ce oferă cursuri de masterat nivelul 2 în domeniul intelligence-ului economic şi al analizei de risc. Este prima formă de învăţământ universitar în intelligence economic, creată în Franţa în 1993 de cărtre amiralul Pierre Lacoste;
- *École d'Ingénieurs Génie Informatique Génie Mathématique* (EISTI), plasată pe locul 4 în 2013, pe locul 2 în 2014 şi 3 în 2015, ce asigură programe de masterat nivelul 2 în domeniul analizei strategice şi al intelligence-ului economic;
- Universitatea Bordeaux, ce oferă cursuri de masterat profesional nivelul 2 în economia inovării şi intelligence (Universitatea Montesquieu Bordeaux IV);
- Universitatea Paul Cézanne Aix-Marseille III, ce asigură programe de masterat nivelul 2 în domeniul intelligence-ului tehnologic şi al inovării;
- Institutul Internaţional pentru Comerţ şi Dezvoltare (ICD), ce oferă, în parteneriat cu IEP Aix-en-Provence, certificări în domeniul intelligence-ului economic;
- Universitatea din Angers, ce asigură programe de masterat în domeniul intelligence-ului economic şi strategiilor competitive;
- SKEMA Business School, plasată pe locul 2 în 2013 şi ce oferă cursuri de intelligence economic.

Concluzii

În spaţiul francez, intelligence-ul economic comportă o varietate de definiţii şi o multitudine de practici, fiind descris drept colectarea, procesarea, analiza prospectivă şi utilizarea informaţiei şi cunoştinţelor pentru a spori eficienţa actorilor economici (Baulant, 2004). Principalul său obiectiv este creşterea competitivităţii firmelor, regiunilor şi naţiunilor prin managementul strategic al informaţiei. Instrumentele folosite, adaptate la transformările economice actuale, globalizarea, respectiv economia cunoaşterii, sunt: supravegherea, influenţa şi analiza de reţea.

Franţa pare să fie prima ţară care a decis să ridice intelligence-ul economic la rang de prioritate naţională, în urma publicării studiilor realizate de un grup de experţi întrunit în Comisariatul General al Planului în perioada 1992-1994, având ca temă *Intelligence-ul Economic şi Strategia Corporatistă* (Commissariat Général du Plan, 1994). Fiind alcătuit din reprezentanţi ai mediului de afaceri, administraţiei, sindicatelor, universităţilor şi profesioniştilor pe linie de informaţii, grupul de lucru a identificat punctele

forte şi slabe ale sistemului francez, în baza unei analize detaliate a celor mai performante sisteme de intelligence economic. Beneficiind de o tradiţie bogată în domeniu, statul francez joacă întotdeauna un rol major, creând reţele de informaţii economice şi tehnice şi structuri de sprijin pentru progresul tehnic.

Francezii definesc intelligence-ul economic drept o serie de acţiuni coordonate vizând investigarea, procesarea şi diseminarea de informaţii utile pentru a fi exploatate de actorii economici. Definiţia are în vedere două aspecte: pe de o parte, investigarea surselor ştiinţifice accesibile pentru a descoperi noi domenii ştiinţifice care ar putea furniza avantaje economice suplimentare, iar, pe de altă parte, urmărirea activităţii laboratoarelor sau fabricilor din ţările sau industriile rivale, în vederea conştientizării breşelor şi îmbunătăţirii competitivităţii (Economic Intelligence in a Global World, 2014, p. 16).

La rândul lui, mediatizatul raport Carayon este un indiciu clar al importanţei pe care aceste tehnici şi servicii o au pentru forţele politice franceze, punctând intrarea Franţei în epoca societăţii informaţionale, cu toate consecinţele ce decurg asupra bunăstării naţionale, care constă, „dincolo de calitatea umană, în suma de informaţii juridice, financiare, comerciale, ştiinţifice, tehnice, economice sau industriale" (Carayon, 2003). Raportul avertizează că ameninţările la adresa structurii productive a ţării au evoluat, devenind mai subtile, iar exacerbarea competenţei internaţionale transformă informaţiile strategice deţinute de companii într-un adevărat **„război economic"**.

Sistemul francez este proiectat şi adaptat noilor circumstanţe şi necesităţi, astfel că, pe lângă agenţiile de stat, în acest proces sunt cooptate companii prestigioase specializate în intelligence strategic, precum şi o reţea de camere de comerţ care acţionează pentru a apăra interesele Franţei pe plan intern şi extern. Acestora li se adaugă mecanismele intelligence-ului economic teritorial, în principal, consiliile regionale, iar în unele cazuri consiliile generale şi comunităţile aglomerărilor departamentale, care participă progresiv şi din ce în ce mai activ la demersurile din domeniul intelligence-ului economic. Lista continuă cu alte structuri implicate în dezvoltarea regională precum Institutul Naţional al Proprietăţii Industriale, Agenţia de Difuzare a Informaţiei Tehnologice, Camerele de Meserii şi Artizanat, Agenţia franceză pentru dezvoltarea internaţională a întreprinderilor, dar şi cu organizaţiile şi grupările profesionale precum Cluburile Securităţii Informatice, Federaţia Profesioniştilor din domeniul Intelligence-ului Economic (FEPIE), Mişcarea Întreprinderilor din Franţa (MEDEF), Confederaţia Generală a Întreprinderilor Mici şi Mijlocii (CGPME) etc.

Referinţe bibliografice:

1. Baulant, Camille, (2004), *Les outils de l'intelligence économique face aux défis de la mondialisation*, Angers disponibil pe http://master-iesc-angers.com/(accesat în 08 iunie 2015).
2. Carayon, Bernard, (2003), *Intelligence économique, compétitivité et cohésion sociale*, disponibil pe http://www.bdc.aege.fr (accesat în 01 iunie 2015).
3. Deschampes, Christophe, Moinet, Nicolas, (2011) *La boîte à outils de l'Intelligence économique,* Dunod, Paris.
4. *Economic Intelligence in a Global World*, 2014.
5. *Intelligence économique: historique*, în *Intelligence économique: deux nouvelles missions pour l'expert-comptable*, 64ème Congrès de l'Ordre des Expert-Comptables.
6. Ivan, Valeriu, (2014), *Analiza informaţiilor: de la intelligence competitiv la componenta economică a securităţii naţionale*, Academia Română (Teza de doctorat), Bucureşti.
7. *Intelligence economique*, accesibil pe https://fr.wikipedia.org/wiki/Intelligence_%C3%A9conomique (accesat în 01.06.2015).
8. Martre, Henri, coord., (1994) Rapport du Commissariat au Plan consacré à *«l'intelligence économique et la compétitivité des entreprises»*, La documentation française.
9. Martre, Henri, Clerc, Philippe, Harbulot, Christian, (1994), *Intelligence économique et stratégie des enterprises*, France, Commisariat general du plan, disponibil la http://www.ladocumentationfrancaise.fr/rapports-publics/074000410/index.shtml (accesat în 21.03.2015).
10. Seal of de the President of the United States of America, A national security strategy of engagement and enlargement, 1995, disponibil la http://www.au.af.mil/au/awc/awcgate/nss/nss-95.pdf (accesat în 21.03.2015).
11. UK Government, Our competitive future – building the knowledge driven economy: The UK Government's Competitiveness White Paper, December 1998.
12. http://www.portail-ie.fr (accesat în 01.06.2015).
13. http://www.intelligence-economique.gouv.fr (accesat în 01.06.2015).
14. http://www.bdc.aege.fr (accesat în 01.06.2015).
15. http://www.watsoninstitute.org/gs/Security_Matrix/(accesat în 21.03.2015).
16. http://www.ladocumentationfrancaise.fr/rapports-publics/074000410/index.shtml (accesat în 21.03.2015).
17. http://www.au.af.mil/au/awc/awcgate/nss/nss-95.pdf (accesat în 21.03.2015).
18. http://stats.bis.gov.uk/competitiveness5/Past%20Indicators/UKPC1999.pdf (accesat în 21.03.2015).
19. http://master-iesc-angers.com/ (accesat în 08.06.2015).

20. *Politique-publique-d-intelligence-economique* accesibil pe http://www.economie.gouv.fr/politique-publique-d-intelligence-economique (accesat în 01.06.2015).
21. http://www.portail-ie.fr/article/571/Historique-de-l-intelligence-economique (accesat în 01.06.2015).
22. http://www.revista22.ro/22-plus-nr-304-ce-este-ordoliberalismul-9048.html (accesat în 01.06.2015)
23. Monitorul Oficial din Franţa, cu nr.108 din 10 mai 2007, pe http://www.legifrance.gouv.fr/affichJO.do?idJO=JORFCONT000000003492 (accesat in 11.12.2015).

ANALIZA DE INTELLIGENCE

TEORIE ŞI PRACTICĂ ÎN INTELLIGENCE: DRIVERI AI CUNOAŞTERII

Cristina POSAŞTIUC*

Abstract

Cooperation with academia is seen by intelligence theorists and practitioners alike as a way to support change management, improve analytic capabilities and better cope with emerging challenges. Intelligence scholars often focus on 'big phenomena' such as social change, the shifting nature of threats or ethics in intelligence, while practitioners are concerned (in public statements, at least) with more mundane issues such as human resource management, workflow streamlining and establishing good rapport with beneficiaries.

Not even apparently clear-cut terms such as 'strategic' bear the same meaning within the two groups: theorists seek to correlate social and organizational change, while practitioners are more interested in detecting risks and threats in their nascent stages so as to better prepare for 'worst case' scenarios.

Managing the knowledge production process is, unfortunately, a topic which doesn't rank high with the intelligence community.

Keywords: change management, cooperation, theory and practice, knowledge production.

Perspective particulare

Pentru a asigura producerea de cunoaştere şi inovarea într-un mediu competitiv, abilitatea unei organizaţii de a învăţa şi a se adapta trebuie să fie consolidată de înţelegerea dinamicii proceselor de cunoaştere (de la structuri şi surse la producere, validare şi aplicare) (Crompton, 2002, p. 10).

Impactul evoluţiilor tehnologice şi sociale, care au produs schimbări substanţiale atât în mediul de afaceri cât şi în cel de securitate, a determinat agenţiile de informaţii să îşi reevalueze structura organizaţională şi obiectivele, dat fiind că, potrivit Sandrei Brizga şi Patriciei Geraghty (2011, p. 7), orice schimbare instituţională sau personală prezintă modificări particulare şi oportunităţi pentru managementul cunoaşterii, însă şi riscuri semnificative ca părţi ale cunoaşterii şi informaţiei să se piardă în procesul de tranziţie.

*Serviciul Român de Informaţii.

În cadrul procesului de restructurare, serviciile de intelligence lasă să se înţeleagă că au luat în considerare atât posibilitatea externalizării activităţilor analitice şi dezvoltarea unei maniere moderne de realizare a acestor activităţi, cât şi implementarea politicilor de deschidere. Potrivit lui Lahneman (2003), colectarea şi analiza pot fi externalizate ca funcţii ce nu sunt de bază deoarece comunitatea de intelligence nu deţine toată expertiza de care este nevoie. Este mai bine ca analiştii să fie lăsaţi să îşi ocupe timpul cu probleme mai presante.

Influenţa *new media*, numărul mare de *think-tank*-uri şi companii private care pot oferi suport analitic, securitatea cibernetică, tipul de relaţii stabilite cu decidenţii politici sunt, în zilele noastre, unele dintre cele mai importante subiecte de dezbatere în rândul practicienilor şi teoreticienilor din intelligence.

Potrivit lui Magnus Hoppe[1], „perspectivele de cunoaştere nu au fost punctul central în cercetarea în intelligence. În schimb, acest domeniu este dominat de obiective de cercetare care se referă la oferirea de sfaturi practice celui care lucrează în intelligence" (Hoppe, 2013, p. 60).

Dintr-o perspectivă pesimistă, Joshua Rovner[2] subliniază că agenţiile de intelligence se confruntă cu noi provocări ce provin din faptul că „un număr tot mai mare de *think-tank*-uri şi companii din sectorul privat de analiză se prezintă adesea drept cvasi-organizaţii de intelligence, unele recrutând chiar analişti activi din agenţiile guvernamentale pentru a da credit acestei imagini" (Rovner, 2013).

Social media a determinat o explozie a noilor surse de informare, dar creşterea sectorului privat de intelligence a amplificat competiţia în direcţia atragerii atenţiei decidenţilor politici. Ambele aspecte ridică întrebări importante cu privire la modul în care agenţiile tradiţionale pot rămâne în continuare relevante pentru decidenţi. Cu toate acestea, rolul intelligence-ului, importanţa studiilor de intelligence, tranziţia de la societatea „1.0" la cea „3.0", nevoia aplicării de metode pentru colectarea şi utilizarea informaţiilor în susţinerea deciziilor şi pregătirea academică a personalului – toate acestea sunt aspecte de interes pentru profesioniştii din intelligence.

Nevoia de reformă pentru adaptarea la schimbările societăţii cunoaşterii a devenit o prioritate a majorităţii organizaţiilor de intelligence, iar modalităţile de atingere a unui astfel de obiectiv include, în cele mai multe

---

[1] Conferenţiar la Facultatea de Afaceri, Societate şi Inginerie din cadrul Universităţii Mälardalen, Västerås, Suedia.

[2] Profesor asociat în Strategii şi politici, la U.S. Naval War College.

dintre cazuri, consolidarea relaţiei cu mediul academic şi remodelarea celei stabilite cu factorul politic.

Există însă o diferenţă majoră între punctele de vedere exprimate de fiecare parte, diferenţă care se regăseşte în tipul de activitate şi priorităţile acestora, stresul practicienilor şi importanţa asigurării securităţii naţionale, în vreme ce teoreticienii se concentrează pe modelarea fondului pe care activitatea de intelligence ar trebui să se bazeze.

Provocări

Avansul tehnologic, instabilitatea regională şi riscul conflictului în diferite regiuni ale lumii, descurajarea cibernetică, posibila intensificare a prezenţei actorilor non-statali, schimbările climatice şi demografice, terorismul, sporirea cererii pentru alimente, apă sau energie sunt doar câtva dintre provocările pe care agenţiile de informaţii se focalizează, pentru a asigura securitatea naţională.

Focalizarea mai sus menţionată asupra acestor trenduri ar trebui sincronizată cu o viziune potrivită pentru o societate a cunoaşterii consolidată care combină interesele tuturor stakeholder-ilor. Această perspectivă cuprinde noi soluţii, o viziune modernă, o abordare transdisciplinară, resurse umane mai bine pregătite, precum şi o infrastructură tehnologică ultramodernă.

Din punct de vedere teoretic, această sarcină poate părea simplu de îndeplinit, chiar într-un termen scurt şi mediu. Însă necesitatea oferirii decidenţilor a unor produse analitice eficiente ori de detectare a riscului şi ameninţării în etape timpurii ale formării acestora poate prevala peste probleme precum rolul sau importanţa unei literaturi consolidate de intelligence – unul dintre principalele topic-uri de dezbatere la nivelul teoreticienilor –, nu pentru că subiectul nu este de interes, ci din cauza presiunii pe care aceste provocări le exercită în activitatea zilnică.

Unele dintre cele mai importante subiecte de dezbatere la nivelul experţilor sunt: natura intelligence-ului – metodologii, schimb de bune practici; problema teorie versus practică; politizarea intelligence-ului; volumul de informaţii cu care se confruntă atât analiştii, cât şi decidenţii; tensiunea dintre libertăţile civile/drepturile omului şi practicile operaţionale ale serviciilor de informaţii; etica; relaţia dintre securitatea naţională şi cea internaţională; responsabilitate versus eficienţă (Johnson şi Shelton, 2013).

În ceea ce priveşte literatura de intelligence, experţi precum Mark Lowenthal şi Walter Dorn (Johnson şi Shelton, 2013) sunt de acord că există decidenţi şi practicieni „departe" de studiile de intelligence, şi că nu este alocat

timp sau interes în citirea produselor „academice". În consecinţă, rareori oferă feedback asupra a ceea ce citesc.

Cunoaşterea – nucleu al misiunii de intelligence

Potrivit lui Ruben Arcos (2013) „în general, organizaţiile de afaceri, non-profit şi guvernamentale au devenit conştiente de necesitatea gestionării relaţiilor cu stakeholder-ii dacă doresc să îşi îndeplinească misiunile". Similar altor agenţii guvernamentale, organizaţiile de intelligence trebuie să îşi îndeplinească misiunile în mod oportun, competent şi eficient, pentru a furniza produse performante şi să satisfacă cerinţele decidenţilor. Există cazuri în care organizaţiile de *intelligence* nu pot obţine suport public pentru acţiunile lor, o realitate explicabilă prin natura secretă a marii proporţii a activităţii specifice serviciilor de informaţii. De aceea, o percepţie publică incorectă a misiunii şi practicii acestor organizaţii poate duce la scăderea susţinerii colectivităţii.

În ultimii ani, rolul sferei academice în domeniul *intelligence* a devenit strategic, iar această dimensiune este văzută, astăzi cel puţin, ca un input important în procesul de producere a cunoaşterii şi, implicit, în ceea ce priveşte suportul decizional. Astfel, conform acestei noi paradigme a *intelligence-ului*, serviciile de informaţii nu pot ignora relaţia cu mediul academic, domeniul ce gestionează, în mod tradiţional, cunoaşterea (Arcos, 2013).

Asemeni jurnaliştilor, reprezentanţii mediului academic sunt acei stakeholder-i care îşi cultivă constant capacitatea de a găsi şi a interpreta informaţii, inclusiv în ceea ce priveşte dezvoltările în sfera *intelligence,* atât în ţara de provenienţă cât şi în lume. Pe cale de consecinţă, devin actori-cheie în modelarea opiniei publice şi a decidenţilor, precum şi a tendinţelor din media.

În contextul politicilor de deschidere implementate de multe servicii de informaţii în ultimii ani, lumea academică poate deveni o resursă-suport în misiunea de a construi o percepţie publică precisă şi corectă a misiunii agenţiilor guvernamentale, a procesului şi rolului pe care acestea îl joacă în apărarea intereselor naţionale. Mai mult, universul academic a fost dintotdeauna şi va rămâne unul din principalii furnizori de formare pentru analiştii serviciilor de informaţii.

Resursele umane în societatea cunoaşterii

Societatea prezentului, unde totul este sau tinde a deveni deschis, este caracterizată de inovaţie şi o disoluţie accentuată a graniţelor. Astfel, managementul incertitudinii nu poate fi realizat cu succes fără resurse umane de calitate. Experţi în domeniu afirmă că „talentul individual devine din ce în ce mai important în secolul XXI. Ceea ce ştie un individ şi ceea ce poate face

cu acest corpus de cunoaştere în diferite formate şi contexte defineşte capitalul său profesional. Cu alte cuvinte, persoanele care pot inova şi genera plus-valoare cu ajutorul cunoştinţelor deţinute vor fi motoarele dezvoltării organizaţionale. Cei care nu au această capacitate vor fi înlocuiţi de maşini sau job-urile lor vor fi externalizate." (Moravec, 2013)

Colectarea şi analizarea unui volum de date şi surse în creştere exponenţială a devenit o sarcină dificilă pentru practicienii intelligence-ului. Cu toate că rolul tehnologiei ca facilitator al dezvoltării resurselor umane nu poate fi negat, răspunsul la această provocare cantitativă prin consolidarea infrastructurii *software* şi *hardware* nu reprezintă o soluţie completă. Rolul colectorului şi al analistului rămâne o variabilă importantă a ecuaţiei gestionării fluxurilor informaţionale.

Creşterea portofoliului de cunoştinţe, abilităţi şi aptitudini a corpului de experţi de care dispune un serviciu de informaţii trebuie asigurată prin diverse modalităţi: lărgirea câmpului de expertiză (de la istorie, la matematică, la lingvistică), implementarea învăţării continue şi a aplicării constante a gândirii ca bune practici în domeniu sunt doar câteva astfel de iniţiative *sine qua non*. Din fericire, pe măsură ce domeniul *intelligence* s-a cristalizat şi formalizat academic, literatura de specialitate şi programele de educaţie dedicate au început să apară cu o frecvenţă încurajatoare.

În acest context, tot mai multe universităţi (din ţări precum Statele Unite ale Americii, Marea Britanie, Franţa, Spania sau România) au abordat domeniul intelligence din perspectiva educaţiei, captând expertiza furnizorilor de cunoaştere atât din zona civilă cât şi din cea militară.

De regulă, cursurile de *intelligence* cuprind informaţii despre principalele repere ale activităţii (colectare şi analiză, etică, istoria activităţii, limitele de cunoaştere etc.) dar şi despre nişe mai specializate (operaţiuni militare, terorism şi contraterorism, contraspionaj, intelligence strategic, business intelligence, diplomaţie şi relaţii internaţionale, criminalitate organizată, economie, ştiinţe politice, managementul cunoaşterii ş.a.m.d.).

De asemenea, există cursuri specializate cu privire la tehnici şi metode avansate de analiză, creativitate, gândire critică sau *social media*. Un exemplu relevant în acest sens este cel al Office of the Director of National Intelligence (SUA), instituţie care a sponsorizat Centers of Academic Excellence Program ca răspuns la creşterea nevoii resimţite pentru formarea profesioniştilor din comunitatea naţională de informaţii. Zece universităţi au luat parte la acest program.

Într-un articol publicat în *International Journal of Intelligence and Counterintelligence*, Ruben Arcos (2013, p. 332) a subliniat faptul că „înfiinţarea programelor de parteneriat universitar şi a iniţiativelor de colaborare cu mediul

academic în ţări precum SUA şi Canada reprezintă cea mai evidentă expresie a emergenţei unei noi abordări în intelligence în ceea ce priveşte gestionarea riscurilor şi ameninţărilor specifice unui mediu de securitate tot mai dinamic". În acest context, expertul prezintă rezultatele obţinute prin *Intelligence Culture Initiative*, susţinută de Comunitatea Naţională de Informaţii (CNI) din Spania. În 2005, CNI a semnat o serie de acorduri cu universităţi spaniole, în încercarea de a compensa lipsa de cercetare şi programe academice în domeniul intelligence. Această iniţiativă a condus la multiplicarea echipelor de cercetare în domeniu şi apariţia unei reţele de universităţi şi experţi spanioli având preocupări ştiinţifice în acest sens.

Principalele obiective ale acestei iniţiative academic au fost: transformarea intelligence-ului în disciplină de studiu şi cercetare ştiinţifică, încurajarea includerii sale în curricula universitară şi derularea de proiecte de cercetare pe aspecte relevante pentru progresul în domeniu; transferul beneficiilor obţinute din cunoaşterea şi expertiza teoreticienilor către serviciile naţionale de informaţii, pe probleme relevante de interes pentru acestea (Arcos, 2013, p. 341). Ruben Arcos a consemnat, de asemenea, că „pentru a obţine expertiza teoreticienilor din multele discipline şi zone academice diferite este nevoie ca aceştia să înţeleagă misiunile organizaţiilor de intelligence, susţinere din partea autorităţilor şi un program de educare a acestui public-ţintă astfel încât să se obţină ceea ce serviciile de informaţii necesită, respectiv expertiză" (Arcos, 2013, p. 340).

Aspecte-cheie: politizare şi etică

Transparenţa este un principiu fundamental al democraţiilor şi, din această perspectivă, este esenţială identificarea unei modalităţi eficiente de comunicare către opinia publică despre natura intelligence-ului, misiunile şi priorităţile unei agenţii de informaţii, serviciile pe care le oferă şi modul în care îşi îndeplinesc funcţiile. Astfel, se asigură sprijinul tuturor stakeholder-ilor implicaţi în protejarea securităţii naţionale. În consecinţă, este foarte important procesul educării publicului cu privire la aspectele specifice intelligence-ului, la procesele pe care le presupune şi la funcţiile pe care le îndeplinesc.

Rolul pe care organizaţiile de intelligence îl îndeplinesc în relaţionarea cu factorul politic este un subiect intens dezbătut. Din punct de vedere teoretic, factorii de decizie politică şi serviciile de intelligence au nevoie unele de celelalte: fără un auditoriu receptiv, orice material produs de serviciile de intelligence nu va avea valoare, însă, din moment ce politica internaţională se caracterizează prin ambiguitate, informaţia secretă oferită de serviciile guvernamentale poate reduce incertitudinea.

Ar trebui menţionat că existe limite în ceea ce priveşte aserţiunea că „obiectivitatea analitică" este cu adevărat gradul în care aceste lucruri trebuie îndeplinite (acelaşi principiu de aplică aşa-numitei independenţe a procesului analitic). Stephen Marrin (2013) a subliniat vasta varietate a concepţiilor referitoare la gradul în care intelligence-ul influenţează sau ar trebui să influenţeze factorul politic. Drept urmare, rolul intelligence-ului este privit fie ca unul limitat – să informeze, să evalueze şi să prognozeze (focalizarea se face pe producţia de informaţie şi cunoaştere) – fie ca parte a unei interpretări mult mai complexe: sprijin pentru decizie şi modalitate de reducere a incertitudinii şi a incidenţei surprizei (Marrin, 2013, pp. 1-4).

O mai mare distanţă între intelligence şi factorul politic (perspectiva tradiţionalistă) poate conduce la crearea de produse mai corecte dar cu influenţă mai redusă, în timp ce o mai mare apropiere (perspectiva activistă) conduce la o influenţă mai mare, dar şi la o exactitate redusă. Într-ul alt articol, acelaşi autor a avansat un nou termen utilizat pentru descrierea tipurilor de politizare – „politizare analitică", menţionând că aceasta poate conduce la adoptarea de decizii slabe calitativ şi, drept consecinţă, la eşec, „dorinţele" şi presiunile politice putând devia analiza experţilor şi consilierea de la calea adevărului (Marrin, 2013a, p. 34).

Stephen Marrin l-a citat pe Gregory Treverton, potrivit căruia politizarea poate avea cel puţin cinci înţelesuri, care se aplică simultan: presiune directă din partea eşaloanelor politice superioare; linie directoare asupra unui anumit subiect ce conduce la suprimarea interpretărilor alternative; în unele cazuri, alegerea opiniei preferate dintr-o gamă mai largă prezentată de evaluări; lansarea de întrebări ajutătoare sau în mod repetat; o mentalitate comună, în care exponenţii intelligence-ului şi politicienii împărtăşesc prezumţii puternice (Marrin, 2013a, p. 34).

Ca parte a dezbaterii privind politizarea, cercetătorii se focalizează de asemenea pe aspecte critice precum încrederea, solicitând politicului să nu abuzeze ori să utilizeze în mod ilegal instituţiile de intelligence. Problema politizării ar trebui să fie cântărită pentru costuri şi beneficii prin prisma atingerii scopurilor politice, dar linia este subţire între contaminarea politică şi prezentarea evaluărilor de intelligence în modalităţi care atrag îngrijorarea decidenţilor. Aşa-numita contaminare politică poate fi evitată printr-un control democratic consolidat asupra activităţii de *intelligence* care, potrivit lui Amit Steinhart şi Kiril Avramov (2-13), depinde atât de istoria unei ţări şi de sistemul său constituţional şi legal, cât şi de gradul de democraţie şi de cultură politică.

Asigurarea unor valori publice şi a unei bune percepţii a publicului asupra activităţii serviciilor de informaţii şi problemelor de securitate naţională constituie o sarcină dificilă pentru orice agenţie guvernamentală,

în contextul în care opinia publică reprezintă un *stakeholder* important. Cetăţenii se aşteaptă la o protecţie eficientă împotriva vulnerabilităţilor şi ameninţărilor (corupţie, terorism, crimă organizată etc.), dar vor ca activitatea de informaţii să se desfăşoare potrivit legii şi în concordanţă cu protejarea drepturilor şi libertăţilor civile. Din această perspectivă, unul dintre cele mai importante elemente care pot modifica percepţia publică şi care pot asigura încrederea publicului în serviciile de informaţii este media.

Gestionarea secretului serveşte interesului public, însă au existat cazuri care au evidenţiat limitele politicilor de deschidere, dat fiind că interesul naţional constituie principalul obiectiv al oricărui serviciu de informaţii. În contextul în care terorismul şi atacurile cibernetice sunt două dintre cele mai importante ameninţări menţionate în strategiile de securitate adoptate în ţările dezvoltate, în ultimii ani, cel puţin, a fost aproape imposibil pentru practicienii în *intelligence* să evite dezbaterile referitoare la etică sau la protejarea dreptului la libera exprimare.

Sir David Omand şi Mark Phythian (2013) observă că, în urmă cu un deceniu, literatura referitoare la relaţia dintre etică şi *intelligence* era limitată. După atacurile din 11 septembrie 2001, s-au schimbat atât rolul agenţiilor de securitate – transformate în actori-cheie ai războiului împotriva terorismului –, cât şi modul în care opinia publică înţelege securitatea. Mark Phythian a punctat faptul că „multe dileme etice cu care se confruntă practicienii, agenţiile şi guvernele rezidă într-un fapt simplu: agenţiile naţionale de *intelligence* sunt tocmai aceasta – naţionale", ceea ce înseamnă că „responsabilităţile şi obligaţiile lor sunt definite prin raportare la statul pentru care funcţionează ca instrument de colectare de informaţii şi avertizare timpurie" (Omand şi Phythian, 2013).

Rezultatele sondajelor de opinie cu privire la modul în care agenţiile guvernamentale asigură securitatea naţională, derulate în ultimii ani, au relevat faptul că cetăţenii au încredere în guverne şi chiar aprobă metodele utilizate. Însă dincolo de această încredere, serviciile de informaţii tot trebuie să dovedească de fiecare dată că practicile lor sunt etice şi în conformitate cu legea.

Dezbaterile referitoare la programul secret de supraveghere electronică dezvoltat de Agenţia Naţională de Securitate/ NSA pot fi abordate din perspectiva a ceea ce Mark Phythian numea „acceptabilitate socială", ce înseamnă că „a putea demonstra sau susţine, cu un anumit grad de plauzibilitate, că ceva este legal are un anumit impact asupra modului în care este perceput de indivizi" (Omand şi Phythian, 2013).

Aşa cum au observat anumiţi experţi, primele reacţii la informaţiile referitoare la programul NSA au fost că „a eliminat încrederea în libertatea mediului online" şi „ameninţă intimitatea indivizilor în mediul virtual"

(Cheong, 2013). Acest tip de perspectivă readuce în prim-plan câteva dintre problemele menţionate anterior, respectiv transparenţă şi responsabilitate, însă ignoră principiul relevanţei, de asemenea, esenţial pentru o guvernare democratică, însă mai puţin important în acest context.

Este bine ştiut faptul că Internetul şi *social media* au devenit principalul mediu de comunicare pentru actorii non-statali. Iar autorităţile trebuie să dea asigurări opiniei publice cu privire la faptul că programele lor sunt utilizate în scopuri valide. Cu toate acestea, o justificare sau o explicaţie în general acceptată este aproape imposibil de furnizat, la fel ca şi asigurarea unui echilibru între intimitate/drepturile omului şi asigurarea securităţii naţionale.

Concluzii

O „sincronizare" a priorităţilor teoreticienilor şi practicienilor este posibilă, însă nu în viitorul apropiat. Primii încearcă, de obicei, să coreleze schimbarea socială şi organizaţională, iar probleme precum îmbunătăţirea metodelor de analiză şi natura şi rolul studiilor de *intelligence* sunt foarte importante. Cei din urmă, deşi preocupaţi la fel de mult de aceleaşi aspecte menţionate anterior, vor viza întotdeauna mai degrabă identificarea riscurilor şi ameninţărilor, în vederea asigurării securităţii naţionale.

Referinţe bibliografice:

1. Arcos, Ruben, (2013), *Academics as Strategic Stakeholders of Intelligence Organizations: A View from Spain*, in International Journal of Intelligence and CounterIntelligence, vol. 26.
2. Brizga, Sandra, Patricia Geraghty, (2011), *Strategic Framework for Integrated Natural Resource Knowledge Management*, Victorian Catchment Management Council, accessed on July 20, 2013 at www.vcmc.vic.gov.au/PDF/FrameworkKnowledgeManagement.pdf.
3. Cheong, Damien D., (June 24, 2013), *Intelligence-Gathering in the Digital Age: Building Trust in PRISM?*, in *RSIS Commentaries*, no. 115/2013, S. Rajaratnam School of International Studies, accessed on August 16, 2013 at www.rsis.edu.sg/publications/Perspective/RSIS1152013.pdf.
4. Crompton, Helen, (2002), *Knowledge Production and Management in the 21st Century*, Manchester Metropolitan University Business School Working Paper Series Online, accessed on August 20, 2013 at www.ribm.mmu.ac.uk/wps/papers/03-02.pdf.
5. Hoppe, Magnus, (2013), *The intelligence Worker as A Knowledge Activist – An Alternative View on Intelligence by the Use of Burke's Pentad*, in *Journal of Intelligence Studies in Business 1*, accessed on May 29, 2013 at https://ojs.hh.se/index.php/JISIB/article/download/57/63.

6. Johnson, Loch K., Shelton, Allison M., (2013), *Thoughts on the State of Intelligence Studies: A Survey Report*, in *Intelligence and National Security*, vol. 28, no. 1, 2013.
7. Lahneman, W. J., (2003), *Outsourcing the IC's stovepipes*, in *International Journal of Intelligence and CounterIntelligence*, nr. 16, 2003.
8. Marrin, Stephen, (2013), *Revisiting Intelligence and Policy: Problems with Politicization and Receptivity*, in *Intelligence and National Security*, vol. 28, no. 1, 2013.
9. Marrin, Stephen, (2013a), *Rethinking Analytic Politization*, in *Intelligence and National Security*, vol. 28, no. 1, 2013.
10. Moravec, John (ed.), (2013), *Knowmad Society*, in Minneapolis: Education Futures LLC, accessed on May 19, 2013 at http://www.knowmadsociety.com.
11. Sir Omand, David, Phythian, Mark, (2013), *Ethics and Intelligence: A Debate*, in *International Journal of Intelligence and Counterintelligence*, vol. 26, no. 1, 2013.
12. Rovner, Joshua, (2013), *Intelligence in the Twitter Age*, in *International Journal of Intelligence and CounterIntelligence*, vol. 26, 2013.
13. Steinhart Amit, Avramov, Kiril, (2013), I*s Everything Personal?: Political Leaders and Intelligence Organizations: A Typology*, in *International Journal of Intelligence and Counterintelligence*, vol. 26, March 2013.

DILEME ŞI SOLUŢII PENTRU MODELUL CICLULUI DE INTELLIGENCE

Mircea MOCANU*

„Dintre toate slăbiciunile paradigmei specifice Războiului Rece pentru domeniul intelligence, hegemonia modelului ciclului informativ este, probabil, cel mai important factor în producerea unui concept inadecvat al domeniului intelligence, din punct de vedere intelectual"
(Wilhelm Agrell, 2009)

Abstract

As result of the pressure put by globalisation and Information Age on all informational processses, various sugestions to adapt the intelligence cycle range from slightly amending the model to radical change. The author supports an adaptation of the cycle, and gets inspiration from the communication theory, where the receiver of the communication is, of course, part of this process. The decision taken by the beneficiary and the subsequent actions take place in the risk management system, abobe the intelligence system. So, intelligence operates as an open system, and Dissemination seems to be the weakest link of the cycle. Complexity theory issues and the Clausewitzian friction are also considered. The author proposes Utilisation as a main link of the cycle, instead of Dissemination and discusses the consequences, variations of the model, and the implications in intelligence management.

Key words: intelligence cycle, dissemination, communication process, intelligence management.

Modelul ciclului informaţional într-un mediu complex

Începând cu ultimele decenii ale secolului XX, transformările majore generate de Era informaţională au impact asupra oricărei activităţi umane care presupune folosirea datelor şi informaţiilor, de la jurnalism la lumea afacerilor, de la servicii publice sau educaţie la servicii secrete.

Presiunile funcţionale generate de globalizare şi progresul tehnologic asupra tuturor proceselor informaţionale scot în evidenţă necesitatea evaluării critice a ciclului informaţional ca model funcţional ce defineşte

* Articolul preia şi dezvoltă paragrafe din volumul de autor Mocanu, Mircea, *Intelligence de la reţele la decizie şi acţiune*, Editura Universităţii Naţionale de Apărare „Carol I", Bucureşti, 2014, ISBN 978-606-660-138-2.

esenţa pentru toate domeniile care operează cu informaţii. Din punctul de vedere al teoriei complexităţii, presiunile funcţionale amintite reflectă intensificarea şi accelerarea interacţiunilor între actorii din mediul informaţional, creşterea entropiei şi accentuarea caracterului neliniar al fenomenelor, descrisă prin „*efectul fluture*": o schimbare minoră ce are loc într-o parte îndepărtată a sistemului cauzează o schimbare semnificativă într-o locaţie situată în partea opusă a sistemului. Într-un *sistem complex*, efectele disproporţionate prezintă o cauzalitate neclară, pentru cunoaşterea şi controlul căreia este necesară o parcurgere mult mai rapidă a tuturor proceselor informaţionale.

Fenomenele contemporane generează implicaţii mai pronunţate în special pentru sistemul decizional şi întreg metabolismul organizaţiilor sau macro-sistemelor asociate noţiunii de putere în sensul cel mai larg, pentru că relaţiile de putere sunt cele mai afectate de impactul noilor tehnologii informaţionale (Marguin, 2001, p. 120). De aceea, examinarea subtilităţilor şi interdependenţelor ciclului informaţional prezintă un interes sporit pentru domeniile critice, cu impact social major, cum sunt mass-media, economia, educaţia, securitatea naţională şi ordinea publică.

Dar ce este procesul informaţional? Pe scurt, informaţiile de orice fel trebuie obţinute, prelucrate – mai mult sau mai puţin – iar rezultatul este folosit cumva. Considerând sistemul propriu o cutie neagră, informaţiile trebuie să intre din mediul înconjurător în cutie, în interior sistemul le prelucrează, într-un fel sau altul, apoi sistemul se manifestă ca urmare a absorbirii acelor informaţii, deci apare o reacţie a sistemului: se mişcă, sau se colorează, sau decide aderarea la un tratat internaţional. Folosirea informaţiilor, în principiu pentru luarea unor decizii şi întreprinderea unor acţiuni, generează necesitatea unor noi informaţii, care să continue şi să aprofundeze procesul cunoaşterii pentru progresul acţiunii în slujba unui interes urmărit. În interiorul cutiei negre, ca urmare a prelucrării informaţiei, cineva a produs o altă informaţie, pe care a transmis-o altcuiva, care a decis aderarea sistemului la tratatul internaţional.

În termeni ai teoriei complexităţii, ca urmare a acelei decizii, *sistemul info-decizional*, aflat într-o anumită *criticalitate*, a desfăşurat o acţiune/ *tranziţie* care i-a schimbat *starea* în cadrul mediului înconjurător. Aflat într-o nouă situaţie, sistemul are nevoie de alte informaţii, pentru a decide modul de interacţionare (ce să facă) în noua stare, cum să controleze noua *criticalitate*.

Considerând numai informaţia, deci numai (sub-)sistemul informaţional din cutia neagră, nu şi acţiunea, ciclul se încheie şi, totodată, porneşte din nou, dar pe un alt palier al cunoaşterii, de unde şi imaginea tridimensională de spirală a ciclului informaţional în perspectivă iterativă.

Aceste trei faze sunt esenţiale în cadrul procesului informaţional pentru că sunt cele care operează nemijlocit cu informaţia: obţinerea informaţiei, prelucrarea acesteia, apoi de transmiterea către un decident (care o foloseşte pentru a iniţia o acţiune).

Complexitatea activităţilor aferente sub-sistemului informaţional scoate în evidenţă şi alte operaţii de importanţă mai mare sau mai mică, ce pot fi adăugate trinomului esenţial al modelului (obţinerea, procesarea/ analizarea şi distribuirea informaţiilor). Cel mai important este cazul componentei ce include conducerea, direcţionarea, dezvoltarea şi planificarea întregii activităţi, orientarea şi prioritizarea activităţilor din celelalte etape ale ciclului informaţional luate separat, cât şi ale procesului informaţional ca întreg. Această componentă funcţională este inclusă în cele mai multe reprezentări ale proceselor informaţionale, de cele mai multe ori sub numele de *Direcţionare*.

În consecinţă, forma clasică a ciclului informaţional are patru faze: *Direcţionarea – Culegerea – Analiza – Diseminarea*, reprezentate în modelul din Figura nr. 1.

În business, efectele comunicaţiilor globale moderne au fost evidente, în primul rând, în domeniul bursier. Apoi, în domeniul securităţii, efectele Erei informaţionale asupra ciclului informaţional s-au făcut simţite în primul rând în cadrul operaţiilor militare, întrucât dinamica acţiunilor de luptă a grăbit necesitatea schimbărilor, mai ales în cazul conflictelor neconvenţionale[1]. Aceste conflice au constituit prima formă de manifestare a complexităţii la scară revoluţionară în domeniul militar, considerând *asimetria* ca expresia a *comportamentului neliniar*.

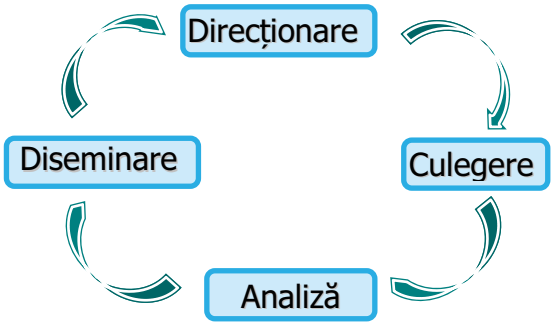


Figura nr. 1. Modelul clasic al ciclului informaţional

În afară de forma esenţializată din Figura nr. 1, există mai multe variante grafice ale modelului ciclului informaţional, care ilustrează considerentele expuse mai sus folosind diferiţi termeni pentru etapele procesului. Unele modele sunt mai elaborate, pentru a scoate în evidenţă şi transferuri

[1] Atributul de «neconvenţional» este folosit, în lucrarea de faţă, şi în variantele «asimetric» sau «transnaţional».

secundare care reflectă diferite funcţionalităţi specifice activităţilor de intelligence. De exemplu, în unele variante, *Analiza* apare separată de *Procesarea informaţiilor*, văzută ca etapă distinctă, ce precede analiza propriu-zisă, pentru că include activităţile[2] menite să aducă informaţiile colectate la o formă ce poate fi exploatată de analişti.

În cazul particular al informaţiilor de securitate (activitatea de intelligence), ciclul informaţional este denumit «ciclu informativ» pentru a sublinia componenta de informaţii secrete şi activităţile specifice domeniului securităţii. Similar, termenul de «sprijin informativ» defineşte partea specifică a sprijinului informaţional general (cu informaţii din toate domeniile) asigurat factorilor de decizie, pentru cazul particular al domeniului intelligence (în principal, *informaţii secrete*).

Critici şi amendamente aduse modelului clasic al ciclului informativ

Limitele modelului clasic al ciclului de intelligence au fost subliniate de mulţi teoreticieni ai domeniului, reproşându-se deficienţe mari de reflectare a multor activităţi importante din practica serviciilor de informaţii şi de exprimare a noilor realităţi din domeniul securităţii, care impun întrepătrunderea sau omiterea unor etape considerate esenţiale.

Kristan Wheaton (2011) realizează un adevărat rechizitoriu împotriva modelului clasic al ciclului de intelligence, pe care îl consideră o „relicvă a celui de-al Doilea Război Mondial", cauza unor risipe de resurse şi un obstacol în calea progresului în intelligence, pentru că reformele preconizate ar trimite serviciile de informaţii în direcţii eronate dacă ar fi fundamentate pe un model eronat (Wheaton, 2011, pp.1-2). K. Wheaton obiectează faptul că modelul susţine o reprezentare liniară, secvenţială, pentru un proces neliniar care se manifestă interactiv, simultan, colaborativ şi iterativ, mai ales în condiţiile ameninţărilor asimetrice globale. Autorul remarcă faptul că nici mintea omenească nu operează liniar şi indenti-fică două direcţii de efort pentru reflectarea procesului de intelligence actual, anume corectarea modelului pentru a răspunde realităţii, respectiv regândirea în întregime a reprezentării grafice a funcţionării serviciilor de informaţii (Wheaton, 2011, pp. 5-7).

Cele mai radicale viziuni prezentate de K. Wheaton sunt «lanţul generării de sens» (*sensemaking loop*) al cercetătorilor Peter Pirolli şi Stuart Card şi «abordarea centrată pe ţintă» (TCA – *Target Centric Approach*), propusă de Robert Clark.

---

[2] De exemplu, decriptarea, traducerea, interpretarea imaginilor, chiar transferul de informaţie către analist, dar şi indexarea şi organizarea informaţiilor pentru utilizarea lor judicioasă în întreaga structură de intelligence.

Pirolli şi Stuart (2006) au propus o înlănţuire de cinci bucle de acţiuni succesive care reproduc, în esenţă, elemente şi activităţi aparţinând etapelor de culegere, analiză şi diseminare ale ciclului clasic. Procesul începe cu «surse externe de date», iar reacţia apare în fiecare buclă, însă întregul proces este prezentat tot liniar, prin desfăşurarea ciclului clasic întrerupt după diseminare, limitată aici la pasul numit «prezentare». În efortul de reprezentare fidelă a mai multor activităţi concrete, modelul introduce concepte noi, se complică şi nu rezolvă limitările ciclului clasic. Mai grav, modelul nu face nicio referire la beneficiari şi cerinţe, iar reacţia generală este omisă, ciclicitatea activităţii de intelligence fiind ignorată.

Modelul TCA, mai recent (2009), a avut mai mult succes pentru că răspunde foarte bine activităţii de intelligence desfăşurată în campaniile militare, unde se poate concentra efortul unei anumite structuri (nu numai analitice) pe o anumită ţintă. Concret, R.Clark (2009) propune un model grafic în care două bucle sunt tangente în punctul reprezentat de obiectivul eforturilor structurii de intelligence („ţinta") şi materializează cerinţa imperioasă de integrare a activităţii analiştilor cu cea a culegătorilor. Meritul acestui model reprezintă, totodată, şi neajunsul său, pentru că secializarea contravine generalizării, adică faptul că nu se poate aplica *in extenso* la organizaţii mari care monitorizează evenimente, crize şi conflicte de pe întreg globul, inclusiv fenomene transnaţionale.

K. Wheaton propune şi o variantă proprie de reprezentare a procesului de intelligence sub forma unor unde paralele şi suprapuse parţial, dar prezentând şi vârfuri succesive ca măsură a ponderii în efortul structurii de intelligence. Aceste unde reprezintă *modelarea mentală*, *culegerea*, *analiza* şi *producţia*, lipsind orice referire la diseminare sau utilizator.

Modelele care propun doar revizuirea ciclului clasic vizează fie includerea utilizatorului în model (Lisa Krizan, 1999 şi Gregory Treverton, 2003), fie redenumirea culegerii prin termenul mai larg de „Acces" (David Omand, 2013), fie observă ciclul în reprezentare multistrat (Mark Lowenthal, 2005) sau detaliază foarte mult activităţile cunoscute (Rob Johnson, 2005).

Posibilă cale de depăşire a dilemei

Majoritatea profesioniştilor din intelligence admit faptul că modelul ciclului informativ este „imperfect", dar constituie încă cea mai bună descriere disponibilă pentru un proces complex şi dinamic, dovedindu-şi utilitatea pentru explicarea conceptelor generale ale activităţii de intelligence (Wheaton, 2011, p. 1). Oricum, „ciclul este o simplificare – posibil chiar o supra-simplificare – iar activitatea reală de intelligence trebuie să fie înţeleasă în termeni de o complexitate mult mai ridicată decât modelul *„ad-hoc*" (Agrell, 2009, p. 108) consacrat.

Între imperfecţiuni, K.Wheaton (2011, pp. 3 şi 5) consideră că simplitatea este atât seducă-toare, cât şi înşelătoare, dar admite că durabilitatea continuă a modelului clasic şi sugerează că inconsistenţele sunt contrabalansate, întrucâtva, de simplitate. De altfel, simplitatea şi firescul construcţiei modelului conceptual în discuţie conferă generalitate, flexibilitate şi soliditate paradigmei pe care sunt clădite toate arhitecturile informaţionale şi toate activităţile ce au ca obiect operarea cu informaţii. De aceea, susţin *adaptarea* ciclului de intelligence la realităţile actuale şi nu renunţarea la acest concept, care oferă două caracteristici esenţiale într-o formă concisă: prezintă etape logice de acţiune şi reflectă caracterul ciclic, iterativ, al procesului de intelligence.

Veriga slabă a modelului, zona care pare susceptibilă a fi examinată cu prioritate, pare a fi cea a Diseminării, a finalizării sprijinului de intelligence.

De ce? Problematica perenă a distanţei funcţionale dintre structura de intelligence şi factorii de decizie atrage atenţia asupra poziţionării întregului sistem informativ faţă de sistemul superior, care este sistemul decizional. Astfel, sprijinul informativ este plasat în interiorul unei alte funcţii, cea proprie activităţii de *management al riscului,* fie că este vorba despre securitatea naţională, impunerea legii sau business. Totodată, destinaţia practică a produselor de intelligence, anume integrarea informaţiilor «acţionabile» incluse în aceste produse în decizie şi acţiune concretă a subliniază importanţa relaţiei funcţionale dintre activităţile domeniului informativ şi realităţile din mediul economic, de securitate naţională sau al ordinii publice, după caz.

Interacţiunea dintre structura de intelligence şi domeniul decizional se realizează prin două puncte ale modelului ciclului informativ, anume transmiterea cerinţelor informative şi a reacţiei beneficiarilor, respectiv diseminarea, adică realizarea sprijinului informativ.

Aceste două momente ale activităţii de intelligence sunt considerate cele mai delicate, mai problematice. Afirmaţia este justificată tocmai prin faptul că aceste «porţi» reprezintă punctele de contact cu *sistemul decizional*, iar celelalte activităţi din ciclul informativ se desfăşoară în interiorul structurii de intelligence, mai stabil reglementată. Activităţile interne ale oricărui sistem birocratic beneficiază de coerenţa unui sistem rutinat, autocorector şi validat.

Cele două «porţi» ale ciclului informativ care marchează intrarea – ieşirea informaţiei din structura de intelligence materializează faptul că structura de intelligence este un *sistem deschis*. Astfel, modelul defineşte şi fluxul informa-ţional ce traversează atât structura de intelligence, cât şi compartimente externe, ale beneficiarului. Ciclul informativ este prezentat în Figura nr. 2 într-o formă care scoate în evidenţă caracterul de sistem deschis al structurilor de intelligence.

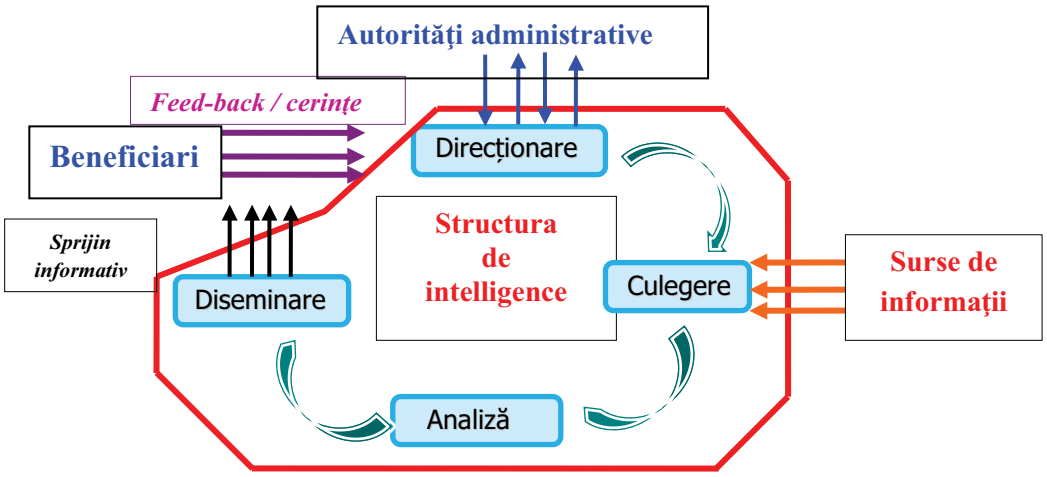


Figura nr. 2. Porţile de comunicare între structura de intelligence şi exterior

Modelul din Figura nr. 2 prezintă şi alte interacţiuni cu exteriorul: relaţiile cu autorităţile ierarhice (în capacitate administrativă, nu ca beneficiari) şi injecţia de informaţii din mediul de securitate în fluxul informativ al structurii de intelligence. Acestea sprijină ideea de sistem deschis şi interrelaţionarea complexă din domeniul informaţiilor de securitate, dar nu fac obiectul acestor pagini.

Studiile privind etapele clasice ale ciclului informativ nu elucidează destinul informaţiilor după diseminarea produselor de intelligence către beneficiar, deşi unele menţionează vag *utilizatorul* sau *integrarea/consumul informaţiilor* ca urmând *diseminării*, unele studii menţionând chiar cuvântul *Acţiune*. Există studii privind distanţa dintre analist şi beneficiar, despre importanţa reacţiei beneficiarului şi despre acţiuni rezultate în urma sprijinului informativ. Nu a fost însă aprofundat transferul către beneficiar «dincolo de poarta regimentului», conţinutul etapei denumite «*diseminare*» văzută *ca sprijin informativ*, nu ca livrare, şi nici procesele parcurse de informaţie după transferul ei către factorul de decizie, inclusiv «chimia» reacţiei acestuia.

Referitor la diseminare, studiul sprijinului informativ ca proces de comunicare oferă concluzii semnificative privind raportul dintre structura de intelligence şi beneficiarul muncii informative. Revederea acestui raport funcţional este relevantă în condiţiile de presiune impuse

de Era informaţională şi de abordarea operării în reţea (prin considerarea de reţele de capacităţi distribuite). De altfel, în ştiinţa militară contemporană, „conceptul de Război bazat pe reţea (RBR) este construit în jurul noţiunii de diseminare a informaţiilor şi mijloacelor" (Dumitru şi Roncea, 2005, p. 41). Rolul menţionat pentru diseminare şi formatul consacrat al ciclului informativ reflectă abordarea structurilor de intelligence ca sisteme închise, iar încheierea ciclului informativ cu etapa numită *Diseminare* denotă un blocaj de raţionament şi o viziune «regimentală» asupra domeniului intelligence. Aceste neajunsuri sunt cauzate de responsabilităţile instituţionale ale serviciilor de informaţii conform doctrinelor dezvoltate în Era industrială şi, mai ales, în cursul Războiului Rece. De altfel, „procesul de transportare a informaţiilor de la producători la consumatori este standardizat în mare măsură. Comunitatea de intelligence a stabilit o «linie de producţie» care acoperă tipurile de produse şi beneficiarii pe care trebuie să îi deservească" (Lowenthal, 2005, p. 48). Cu această «furnizare de produse», datoria serviciului de informaţii a fost considerată îndeplinită.

Consider însă că modul de integrare a produselor de intelligence în *decizia* luată de beneficiar şi în *acţiunea* desfăşurată pe baza acestei decizii oferă concluzii importante asupra înseşi structurii ciclului informativ, deschizând calea către optimizarea activităţii de intelligence ca domeniu de interes strategic pentru securitatea naţională, dar şi pentru celelalte domenii majore de aplicare, anume lumea afacerilor şi impunerea legii.

Pe măsura creşterii intensităţii (fricţiunii clausewitziene a) confruntării – de ordin militar, economic sau de ordine publică – sprijinul informativ în condiţiile operării cu capacităţi distribuite (în reţea) prezintă particularităţi care impun mutaţii semnificative nu numai asupra cerinţelor de management al domeniului intelligence, ci chiar, din nou, asupra etapelor esenţiale ale ciclului informativ.

Propunere de îmbunătăţire a modelului clasic al ciclului de intelligence

Constatând că factorii de decizie politică joacă un rol semnificativ în toate etapele procesului de intelligence, iese în evidenţă necesitatea depăşirii limitării ciclului informativ exclusiv la activităţi proprii structurilor de intelligence. Astfel, excluderea beneficiarilor din ciclul informativ apare ca o eroare conceptuală în condiţiile tehnologiei moderne şi ale ameninţărilor neconvenţionale. Totodată, considerând sprijinul de intelligence ca *proces de comunicare*, prezenţa destinatarului comunicării într-un model al procesului

este obligatorie, aşa cum au argumentat savanţii din Şcoala de la Palo Alto[3]. Aceştia au propus un *model psihosocial/interacţionist* al procesului de comunicare, prezentat în Figura nr. 3, model ce include *determinanţii psihologici* ai actorilor procesului de comunicare.

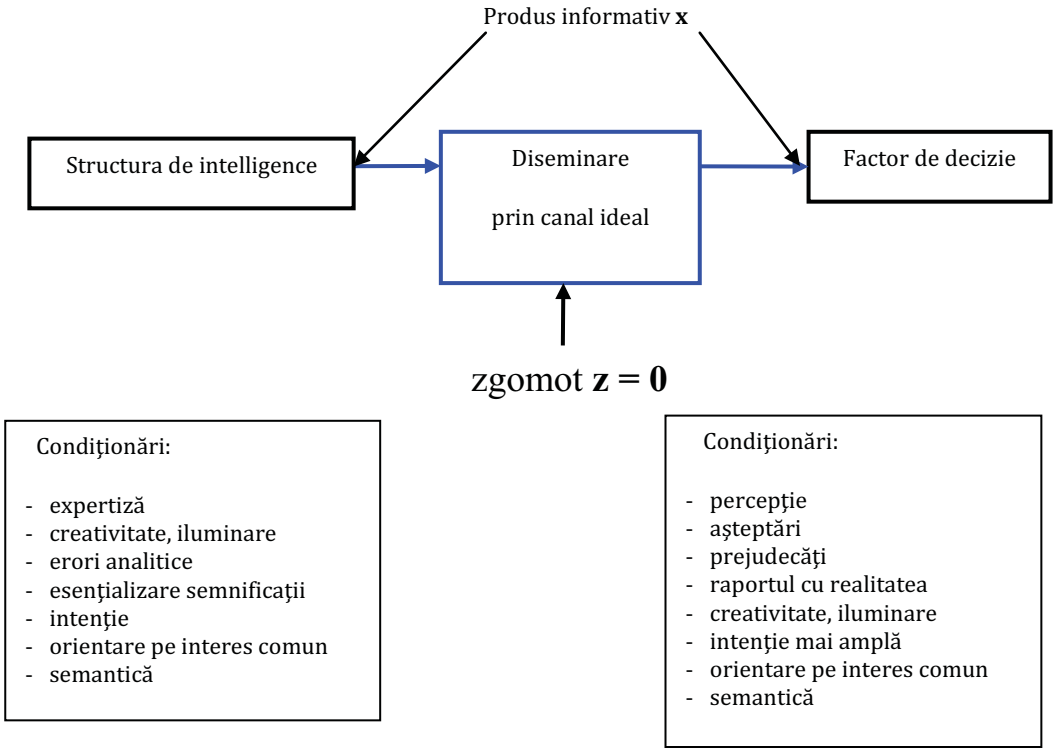


Figura nr. 3. Modelul procesului informaţional în concepţia interacţionistă (sursa Sălăvăstru, 2004, pp. 116-117)

Beneficiarul se distinge a fi declanşatorul deciziilor ce constituie înseşi *obiectivele* sprijinite de activitatea de intelligence şi este normal sa fie inclus ca actor esenţial participant în activităţile de intelligence, aşa cum propune Greg

[3] Grup de cercetători de diferite specialităţi (sociologi, lingvişti, psihiatri, antropologi) reuniţi în jurul lui Gregory Bateson. Din Şcoala de la Palo Alto (Stanford University) fac parte Donald Jackson, Paul Watzlawick, Janet Beavin, Edward Hall, Ray Birdwhistell, Erving Goffman, Margaret Mead, Virginia Satir, Jay Haley, John Weakland, Richard Fish ş.a.

Treverton. De asemenea, este firească o formă a ciclului informativ care să reflecte **rolurile actorilor esenţiali**: *director - culegător - analist - beneficiar*.

Activitatea proprie factorului de decizie în raport cu produsele de intelligence poate fi definită ca *Valorificare* sau *utilizare*, care a mai fost propusă ca etapă a ciclului, dar nu a fost aprofundată conceptual. Pe baza funcţiilor definite în procesele de comunicare, susţin că *valorificarea* materializează realizarea a trei categorii funcţionale ale sprijinului informativ: *construcţia superiorităţii informative*, *avertizarea*, *integrarea în acţiune* (Mocanu, 2014). Aceste noţiuni propuse reflectă niveluri diferite de manifestare a fricţiunii clausewitziene, diferenţierea impactului cantităţii de substanţă acţională transferată prin produsele de intelligence, precum şi paliere diferite de intensitate a criticalităţii, în abordarea teoriei complexităţii pentru mediul de securitate internaţional, a celui economic sau de ordine publică.

Argumentele expuse conduc la concluzia că *valorificarea produselor de intelligence* prin integrarea lor în decizie şi în acţiunea ce decurge din decizie *face parte, în mod firesc, din ciclul informativ*, după procedura de diseminare şi închide ciclul în mod logic, prin reacţia beneficiarului, către etapa de direcţionare. De asemenea, *Valorificarea* apare ca fiind sursa firească a activităţii de feed-back, ceea ce completează logica noii forme a ciclului de intelligence.

În noul model propus, prezentat în Figura nr. 4, *diseminarea apare ca o procedură care face legătura între două etape esenţiale şi nu o etapă propriu-zisă,* este conexiunea dintre Analiză şi Valorificare, nu o etapă esenţială a ciclului informativ.

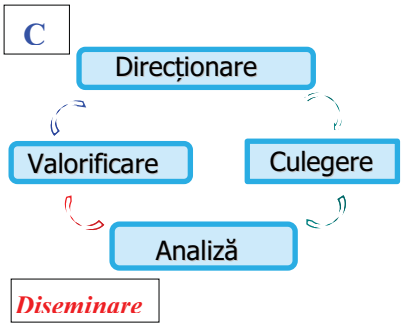


Figura nr. 4. Modelul propus pentru ciclul informativ

La fel, transmiterea cerinţelor, apoi, pe alt nivel al spiralei, reacţia beneficiarului, sunt activităţi plasate între etapele esenţiale de Valorificare şi Direcţionare.

Totodată, modelul propus permite şi dezvoltări în elucidarea nivelurilor de bucle de reacţie (analitică, de sistem şi de fenomen)(Mocanu, 2014) şi în studierea cerinţelor de informaţii în funcţie de tipul de valorificare a produselor informative. Reacţia beneficiarului fiind tot o activitate ce se realizează printr-o poartă de interacţiune cu exteriorul, ea completează în mod natural ciclicitatea modelului.

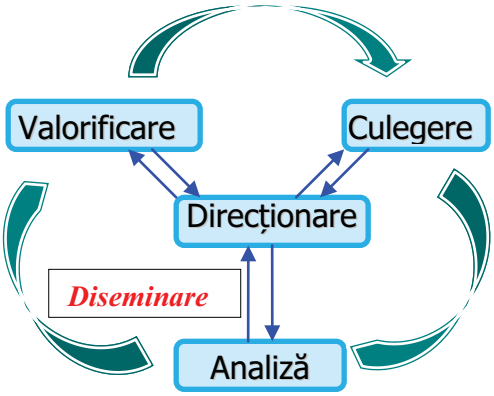


Figura nr. 5. Ciclu informativ cu direcţionare centrală

Dezvoltări conceptuale ale modelului propus

Completarea modelului propus prin detalierea activităţilor este simplă. Interesantă este însă direcţia de simplificare a modelului, pentru esenţializare şi generalizare. Pentru o simplificare şi mai avansată, nu etapa de *valorificare* a produselor este prima susceptibilă a fi exclusă din buclă, ci, probabil, etapa de *direcţionare*. Un argument este faptul că direcţionarea nu este traversată de informaţie decât pentru validare în vederea diseminării. Însă, pentru faptul că direcţionarea se aplică, prin activitatea de coordonare ierarhică, tuturor etapelor ciclului informativ, ea poate fi considerată ca element central al ciclului, conform modelului din Figura 5. Prin spiţele ciclului, către cele trei etape rămase, acest model scoate în evidenţă legătura directă a Direcţionării cu domeniile principale ale activităţii de intelligence, deci responsabilitatea de managementul separat al structurilor care realizează activităţile de culegere, analiză şi valorificare.

Includerea etapei de *valorificare* ca etapă esenţială a ciclului informativ oferă deschideri conceptuale pentru dezvoltări în managementul structurilor de intelligence în perspectiva optimizării sprijinului informativ. Prin considerarea *valorificării* ca etapă a ciclului informativ, structurile de intelligence pot modela sprijinul informativ în integralitatea sa, direcţionat pe cele trei categorii funcţionale identificate construcţia superiorităţii informative (informarea, îm general), avertizarea şi integrarea în acţiune. Astfel, modelul nou propus pentru ciclul de intelligence poate fi completat

pentru a include activităţile de management specializat identificate: managementul culegerii (CCIRM[4]), managementul producţiei şi *managementul valorificării produselor informative*. Ultima dintre acestea include, în mod firesc, tot ceea ce este legat de interacţiunea dintre sistemul de intelligence şi sistemul managementului de risc. Această nouă activitate preia responsabilităţile referitoare la simpla diseminare, cooperarea şi analiza reacţiilor de la beneficiari, dar aprofundează eficientizarea sprijinului informativ într-o *politică a valorificării produselor de intelligence*.

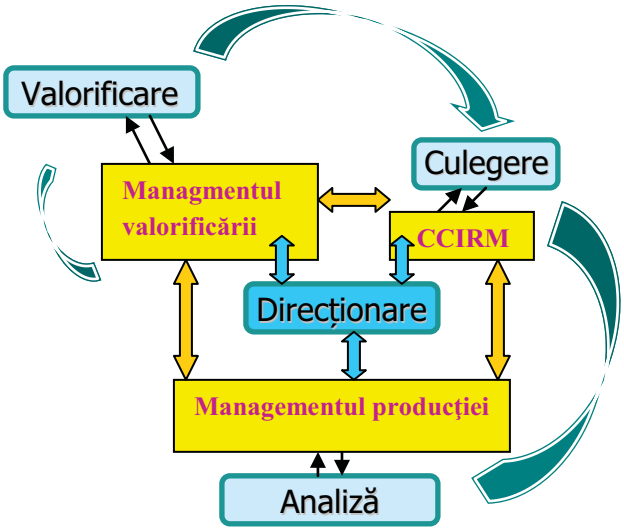


Figura nr. 6. Ciclul de intelligence cu management specializat

Activităţile de management corespunzătoare etapelor esenţiale ale ciclului informativ pot fi repre-zentate ca o coroană de cerc în jurul direcţionării. În afară de direcţiona-rea separată, modelul din Figura 6 sugerează proceduri de cooperare pe orizontală între compartimentele de management ale diferitelor domenii ale structurii de intelligence.

[4] CCIRM (Collection Coordination and Intelligence Requirements Management) – Coordonarea culegerii şi managementul cerinţelor informative.

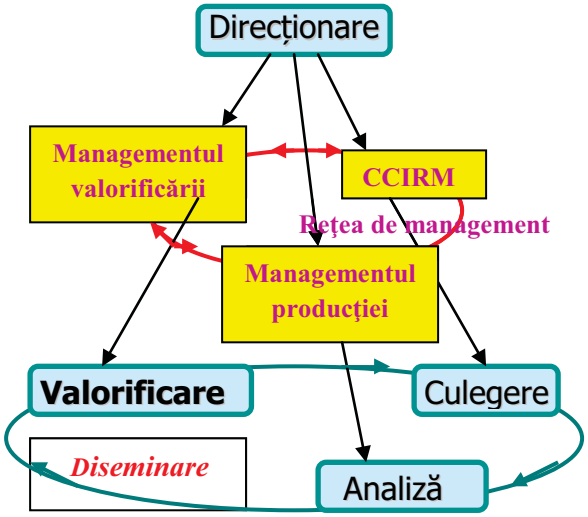


Figura nr. 7. Model conic al ciclului informativ

Modelul poate fi reprezentat şi tridimensional (Figura nr. 7), ca un con cu bucla etapelor esenţiale formând baza circulară, direcţionarea în vârful conu-lui, iar cele trei tipuri de management formând un cerc median. Această variantă sugerează mai bine dinamica în spirală a procesului de intelligence.

Concluzii

Studiul ciclului de intelligence şi eforturile de identificare de noi soluţii conceptuale, care servească mai bine adaptarea serviciilor de informaţii la realităţile curente, sunt în plină desfăşurare. În variantele propuse în aceste pagini, noul model al ciclului de intelligence, care include Valorificarea ca etapă esenţială în locul diseminării, deschide căi de optimizare a utilizării capacităţilor de intelligence şi îmbunătăţirea sprijinului informativ prin considerarea aspectelor de management al riscului în integritatea şi complexitatea lor.

Referinţe bibliografice:

1. Clark, Robert, (2009), *Intelligence Analysis: A Target Centric Approach*, Congressional Quarterly Press, Washington DC:.
2. Cristea, Dumitru, Ion Roceanu, (2005), *Războiul bazat pe reţea. Provocarea erei informaţionale în spaţiul de luptă*, Editura Universităţii Naţionale de Apărare „Carol I", Bucureşti.

3. Lowenthal, Mark, (2005), *Intelligence. From Secrets to Policy*, CQ Press, Washington DC.
4. Marguin, Jean, (2001), *Tehnologia informației va schimba lumea?*, în *Puteri și influențe*, Editura Corint, București.
5. Mocanu, Mircea, (2014), *Intelligence de la rețele la decizie și acțiune,* Editura Universității Naționale de Apărare „Carol I", București.
6. Pirolli, Peter, Card, Stuart, (2006), *The sensemaking process and leverage points for analyst technology as identified through cognitive task analysis*, PARC paper, accesibil la www.vadl.cc.gatech.edu/taxonomy/docInfo.
7. Sălăvăstru, Dorina, (2004), *Psihologia educației*, seria Collegium. Psihologie, Editura Polirom.
8. Treverton, Gregory, Agrell, Wilhelm (coord.), (2009), *National Intelligence Systems. Current Research and Future Prospects*, Cambridge University Press.
9. Wheaton, Kristan J., (2011), *Let's Kill The Intelligence Cycle*, accesibil la www.sourcesandmethods.blogspot.com/2012/03/part-13-whole-picture-lets-kill.html.

OSINT

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 tranziția de la era industrială la era informațională și mai apoi la societatea cunoașterii.

«Expansiunea lumii virtuale a condus la emergența unei noi dimensiuni a puterii statale, „puterea digitală", cu efecte pe termen lung asupra cunoașterii strategice și acțiunilor statului în plan național și internațional. De asemenea, individul a dobândit noi instrumente de acțiune, prin intermediul accesului la baze de date și rețelele informatice, instrumente prin care poate influența în mod direct exercitarea puterii în plan intern sau internațional. Recurența revoluțiilor „Facebook" sau „Twitter" din Europa până în Orientul Mijlociu demonstrează impactul acestor instrumente virtuale asupra regimurilor politice, impact de neimaginat acum mai puțin de un deceniu. Formele de evoluție a „puterii digitale" vor reprezenta, în egală măsură, oportunități de dezvoltare, dar și vulnerabilități și provocări la adresa securității, iar gestionarea acestora va fi determinată de capacitatea de accesare, decelare și utilizare a informației» (Maior, 2011, p.2).

În acest context, amenințările asimetrice s-au diversificat, atât ca număr, cât și ca intensitate. Evoluția tehnologiei și trecerea de la societatea industrială la societatea informațională au facilitat mijloacele de propagare a acestor amenințări, serviciile de informații fiind nevoite să se racordeze la noile cerințe ale mediului de securitate și să dezvolte noi mijloace și metode de contracarare a amenințărilor și riscurilor moderne.

Aparte, întrepătrunderea și coexistența unor elemente aparținând erei informaționale alături de componentele și stratul și substratul noii societăți a cunoașterii, creează contextul actual în care se regăsește lumea în secolul XXI.

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

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

După uciderea lui Mark Duggan de către poliția din Anglia, o serie de ipoteze privind moartea acestuia au început să se răspândească în cadrul comunității de culoare, acestea generând tensiuni și mai mari, ce au degenerat rapid. Dacă la început se vorbea despre un protest a unui grup de 200 de persoane care cerea explicații 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 speculații conform cărora acesta ar fi fost ucis intenționat de către polițistul care l-a arestat și că ar fi fost împușcat în piept după ce a fost încătușat. O altă speculație viza faptul că acesta ar fi transmis cu 15 minute înainte, de moartea acestuia prietenilor săi, că a fost încercuit de către poliție, dar că este în siguranță (Lewis, 7 august 2011). Ceea ce ar fi creat de fapt nemulțumire în rândul protestatarilor a fost, în esență, incertitudinea asupra morții lui Mark Duggan, aceștia acuzând Poliția Metropolitană că nu a existat un schimb de focuri, bărbatul neavând o armă în posesia sa și că omorârea acestuia contravine legii. Rapoartele poliției 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 și procesele pe care acesta din urmă le-a avut nu au putut demonstra și proba această acuzație, 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 și în baza nemulțumirii comunității de culoare din Anglia, încep protestele. Dacă la început s-a vorbit despre un protest pașnic, în noaptea de 7 august 2011, protestele degenerează și creează violență și tensiune. Astfel, au apărut o serie de întrebări în legătură cu viteza transformării unor proteste pașnice reduse ca localizare și număr de participanți în manifestări violente pe scară largă. Inițial cauzele degenerării protestelor au fost identificate în modalitatea de prezentare e evenimentelor în presa locală și posturile de televiziune cu acoperire națională. *Totul a fost pus pe seama presei locale pe de-o parte, iar pe de altă parte pe fondul televiziunii din Marea Britanie.* Totuși ceea ce a particularizat violențele din Londra a fost promovarea masivă a fenomenului în *social media*.

În acest sens, în cadrul rețelei 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 și cei uciși

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

de poliție, *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), comunități *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*). Deși apar mai multe astfel de grupuri, toate își îndreaptă atenția către același gen de conținut promovat, administratorii grupurilor cerând sprijinul susținătorilor de a ieși în stradă și de a cere dreptate în cazul lui Mark Duggan. Exemplele de postări în acest sens (utilizatorul Shannon Loch: *Screw Police Brutality* – Împotriva brutalității poliției sau utilizatorul Milad Gh.: *Hey guys come on… I waiting for YOU! Are YOU with me?* – Haideți cu toții… Vă aștept! Sunteți cu mine?) au folosit în general un limbaj mult mai tendențios, însoțit adesea de cuvinte obscene la adresa poliției sau la adresa celor întâmplate. Majoritatea postărilor din cadrul rețelei de socializare Facebook au avut ca scop principal, pe lângă blamarea celor întâmplate și mai ales a poliției londoneze, strângerea unui număr cât mai mare de susținători *care* sunt dornici să iasă în stradă și să participe la proteste, după cum se vede și în postarea utilizatorului Milad Gh.

La mai bine de 3 ani jumătate de la moartea lui Mark Duggan și de la revoltele sângeroase din Anglia, aceste pagini nu și-au încheiat activitatea, administratorii acestor continuând să posteze mesaje împotriva poliției și să solicite solidaritatea pentru cei uciși de către ofițerii de poliție *(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* – Poliția este cea mai mare mafie, doar că în acest caz poartă uniformă. Fapt dovedit!, urmând o înșiruire a unor pagini care îi susțin pe cei uciși de poliție). Totodată, aceștia își exprimă frecvent nemulțumirea față de evenimentele întâmplate, iar pe parcursul procesului lui Kevin Hutchinson-Foster a fost cerută din nou ieșirea în stradă și susținerea 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 judecății 2013! Haideți 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 demonstrație? Admin Tommy D, Planul B).

Așadar, în ceea ce privește Facebook, a putut fi observată ofensivitatea de care a dat dovadă comunitatea *on-line* în susținerea și apărarea lui Mark Duggan, având lideri virtuali informali, un limbaj codat specific, promovând chiar și conținut multimedia care să instige și să atragă cât mai mulți

protestatari care să ia parte la violențe, aceștia aflând foarte ușor din *social media* despre locul și ora violențelor.

Pe lângă utilizarea aplicației Facebook, protestatarii recurg și la exploatarea platformei de socializare Twitter, pentru a se face auziți în susținerea cauzei lui Mark Duggan. Prin intermediul *tweet*-urilor, utilizatorii rețelei au reușit să răspândească informațiile rapid, profitând de ideea de *SMS*-ul *Internetului* și de toate avantajele acesteia. Astfel, prin intermediul unor mesaje scurte, aceștia au comunicat rapid date, în special cu privire la ora și locul protestelor și 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* – Vorbiți cu ei. Sunt pe drum. O să fiu cu voi curând, făcând referire la reunirea tuturor protestatarilor.

Aparte de aceste mesaje de chemare a susținătorilor și a protestatarilor, în cazul Twitter și al revoltelor din Londra se poate vorbi și despre propaganda *social media*. În zilele cuprinse între 6 și 11 august, în cadrul postărilor din rețeaua Twitter, apar o serie de zvonuri cu privire la nemulțumirea socială a comunității și asupra formelor pe care le-au îmbrăcat protestele acestora. În acest sens, au apărut *tweet*-uri ale utilizatorilor care susțineau faptul că protestatarii au atacat grădina zoologică din Londra și au reușit să elibereze animalele. Astfel @Twiggy_Garcia, un utilizator al rețelei Twitter care avea 5.178 de susținători, este primul care răspândește în cadrul platformei zvonuri conform cărora protestatarii au intrat în grădina zoologică și eliberează toate animalele. Această informație apare și cu *hashtag*-ul Twitter #LondonRiots. La ora 2 dimineața, în data de 7 august, utilizatorul @Deadfreaks răspândește o serie de informații conform cărora revoltele au degenerat, iar protestatarii au reușit chiar să intre în lanțul de fast-food-uri McDonald's și își gătesc singuri mâncarea, zvon ce apare cu *hashtag*-ul #Tottenham. Tot în cadrul aceluiași *hashtag*, @DeclanJMN oferă câteva informații ce fac referire la faptul că o fetiță de 16 ani ar fi fost bătută de către poliția londoneză, lucru ce ar fi alimentat și mai tare tensiunile și nemulțumirea socială. Lucrurile merg însă mult mai departe, iar @zadio postează în cadrul *hashtag*-urilor #LondonRiots, #Londonriot și #Prayforlondon imagini cu Ochiul Londrei în flăcări, *tweet*-ul fiind preluat rapid și răspândit cu ușurință, înăsprindu-se starea de incertitudine și tensiune în rândul populației. Un alt exemplu în acest sens, îl constituie faptul că @jazz_kaur răspândește, folosindu-se de #Londonriots și #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 conștientizează nevoia culegerii de informații și din acest spațiu. Revoluția Twitter din Republica Moldova și Primăvara Arabă au fost puse sub semnul politicului, fiind ample mișcări de organizare a populației pentru a deturna regimurile aflate la putere, în special cele comuniste, ale căror instituții de informații nu au luat în calcul sau doar au condamnat și blamat implicarea rețelelor de socializare în evenimentele ce au avut loc în 2009 și 2010, fără a avea în vedere exploatarea tuturor informațiilor disponibile în cadrul *social media*.

Astfel, depășite de caracterul de noutate, precum și de rapiditatea cu care informațiile s-au răspândit prin intermediul rețelelor de socializare, departamentele de culegere a informațiilor din cadrul Poliției Metropolitane din Marea Britanie s-au văzut nevoite să preia în aria lor de competență și acest spațiu virtual, asumându-și misiunea de a preveni și contracara amenințările provenite din mediul *on-line*. Cu toate că mulți 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 emergenței erei informaționale și a societății cunoașterii.

Șeful Departamentului de Surse Deschise al poliției londoneze, Umut Ertogral, declara că pentru OSINT-ul pe care îl conduce „*social media* se comportă precum CCTV în spațiul 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 existența unei echipe care să monitorizeze rețelele de socializare și postările aferente ce fac referire la tensiunile politice. Echipa ar fi compusă din 17 ofițeri și ar purta numele de *SocMint*, având misiunea de a monitoriza Facebook-ul, Twitter-ul, YouTube-ul, precum și 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 ofițeri dezvoltă noi mijloace și metode pentru a-și îmbunătăți activitatea de intelligence. Ca unitate componentă a Poliției Metropolitane, echipa are jurisdicție de acțiune la nivelul tuturor districtelor Marii Britanii, precum și în Țara Galilor (Wright, 26 iunie 2013).

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

Așadar, 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 definește noua disciplină ca „existența unor capabilități prin care autoritățile accesează datele de comunicare și accesează sub mandat, atunci când acesta este necesar, conținutul comunicațiilor din Internet, în speță din *social media*" (Sir Omand, Bartlett și Miller, 2012, p. 802). Tot el susține că utilizarea capabilităților SOCMINT poate contribui într-un mod decisiv la asigurarea securității publice prin identificarea activităților criminale, asigurarea unei avertizări timpurii cu privire la existența unor stări de tensiune sau amenințări publice sau crearea unei avertizări operative, atunci când evenimentele evoluează într-un ritm alert (Sir Omand, Bartlett și Miller, 2012, p. 9). Astfel, Sir David Oman, împreună cu echipa sa, pune bazele a ceea ce înseamnă culegerea de informații din cadrul rețelelor de socializare, care în esență se poate rezuma la culegerea de informații disponibile din comunicarea realizată *on-line via social media*, totodată oferind și câteva exemple de domenii de asigurare a securității, fie ea naționale sau internaționale, precum și modalități 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 informații din surse deschise de către specialiști în tehnica de supraveghere *on-line* de pe site-urile de socializare, chat-uri, site-uri web și Internet" (*Use of Internet for Terrorist Purposes*, 2012, p. 68) sau particularizează ceea ce înseamnă SOCMINT, ca fiind un domeniu subsecvent culegerii de informații din surse deschise, pornind de la ideea că *social media intelligence* reprezintă o ramură a OSINT, dar care are un domeniu de acțiune specific, în speță, rețelele de socializare (SOCMINT, 31 octombrie 2012). Așadar, se poate considera faptul că se vorbește despre o nouă disciplină a intelligence-ului, aflată, însă, încă într-o faza incipientă de dezvoltare și introducere în activitatea serviciilor de informații. Cu toate acestea, se observă și materializează, chiar dacă pentru moment sub forma unor lecții învățate, oportunitățile pe care *social media intelligence* le-ar putea oferi, odată cu implementarea acesteia în cadrul agendei de lucru a activității de informații, oportunități ce nu sunt deloc de neglijat, datorită contribuțiilor pe care acestea le-ar putea aduce în vederea asigurării climatului de securitate.

Social Media Intelligence – oportunităţi pentru serviciile de informaţii

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

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

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

Vorbind de oportunitățile aduse de utilizarea *social media intelligence*, se vorbește de fapt despre plusurile pe care acestea le oferă pe de-o parte activității de informații, iar pe de altă parte serviciilor de informații, care uneori își pot ușura munca, culegând cu o mai mare ușurință date, locații sau ore de desfășurare a unor evenimente sau persoane ce iau parte la acestea. Pe lângă cele menționate, există o serie de concepte cheie ce fac obiectul studierii oportunităților pe care activitatea de *social media intelligence* le aduce.

În acest sens, vorbind despre oportunitățile aduse de fenomenul *social media intelligence*, se poate vorbi despre utilitatea conceptului de *crowd sourcing*. James Surowiecki, repurtat jurnalist al publicației *The New Yorker*, vorbește despre inteligența mulțimilor și, implicit, despre culegerea informațiilor din rândul unei mulțimi. El își asociază teoriile cu cele ale lui Gustave Le Bon în ceea ce privește ideea de mulțime. Totodată, el susține faptul că mai mulți oameni ce abordează o problematică, vor oferi o soluție mult mai bună spre rezolvarea ei, decât dacă aceasta ar fi rezolvată de una sau două persoane. În cartea sa, *Wisdom of Crowds*, el întregește ce înseamnă de fapt *crowd sourcing*-ul (culegerea de informații din cadrul unor mulțimi), insistând însă asuprea unui aspect esențial, și anume că atunci când se vorbește despre inteligența mulțimilor nu se vorbește despre mai multe minți puse la un loc, ci despre descentralizare, mai multe persoane abordând subiectul de interes în cadrul unei colectivități extinse, dar în mod individual, fiecare oferind propria soluție de rezolvare a problematicii. Astfel, susține el, va apărea o persoană cu cea mai bună ideea de a rezolva subiectul abordat (Surowiecki, 2005).

Același fenomen poate fi observat și în rândul platformelor de socializare. Încă din prezentarea principalelor rețele de socializare, a fost stabilit faptul că utilizatorii diseminează conținut și informație în cadrul unei

pagini *social media*. Spre exemplu, în cazul revoltelor din Londra, în anul 2011 și al zvonurilor apărute pe Twitter, fiecare utilizator al platformei a putut să posteze propriile informații cu privire la ce se întâmpla, de fapt, în realitatea tangibilă. În acest context, se poate vorbi despre *crowd sourcing* în cadrul rețelelor de socializare, Poliția 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 direcțiile de acțiune (analiză), iar în final să aleagă cea mai bună cale de acțiune în baza unei informații provenite din *social media*, pentru a preveni sau contracara violențele stradale (operaționalizare și valorificare). Astfel, poate fi demonstrată utilitatea activității de *crowd sourcing* chiar pe baza unui instrument cheie al activității de informații, în speță ciclul de intelligence.

O altă dimensiune a acestui fenomen, ca oportunitate SOCMINT pentru serviciile de intelligence, este dată de Sir David Omand, care susține faptul că atunci când se vorbește despre *crowd sourcing*, din punct de vedere instituțional, se poate vorbi despre asigurarea unui flux mai bun de informații între guvern și proprii cetățeni, mai ales atunci când se vizează situații de criză. El pornește de la teoria conform căreia persoanele ce asistă la producerea unui eveniment se pot transforma în *jurnaliști de ocazie*, având posibilitatea să posteze în *social media*, informații din teren, ce ar putea fi ulterior verificate și valorificate de către ofițerii de informații. Prin facilitățile oferite de rețelele de socializare, mai ales prin posibilitatea diseminării de conținut multimedia, acești *jurnaliști de ocazie* pot posta fotografii sau filmulețe de la fața locului, pe care mai apoi, instituțiile abilitate le pot folosi pentru a deschide noi operațiuni sau în cadrul celor deja existente. Conexând conceptul de *crowd sourcing* cu ideea de *wisdom of crowds* în ceea ce privește activitatea serviciilor de intelligence, a fost elaborată o platformă web, denumită Ushahidi, unde cei interesați puteau posta informații de orice natură, „de la cutremurul din Haiti, până la blocajele rutiere din Washington, DC" (Sir Omand, Bartlett și 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 emergenței *social media intelligence* poate consta în cercetarea și înțelegerea survenită din analiza rețelelor de socializare. Studierea platformelor *social media* poate ajuta serviciile de informații să înțeleagă anumite fenomene emergente în cadrul WEB 2.0. Acestea pot face referire la o serie de aspecte esențiale, precum indicatori ai violenței, căile promovate pentru auto-radicalizarea teroriștilor islamiști sau praguri și indicatori ai criminalității survenite din cadrul rețelelor de socializare. Astfel, acest lucru poate contribui la înțelegerea modalităților prin care se formează

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

Aparte de cele menționate, în cazul oportunităților oferite de SOCMINT, se vehiculează conceptul de cunoaștere operațională în timp real a activităților ce se desfășoară în spațiul virtual al rețelelor de socializare. Analiza statisticilor Twitter a relevat faptul că există postări, atât *pre*, cât și *post* apariției 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 ușor decât dacă ar fi folosite tehnici investigative tradiționale. Spre exemplu, dacă s-ar realiza o geo-localizare a evenimentelor promovate în *social media*, analiștii de intelligence ar putea obține hărți de evoluție ale posibilelor noi locații fizice de realizare ale unui protest, revolte sau de ce nu, chiar act criminal (Sir Omand, Bartlett și Miller, 2012, p. 805).

Conex cunoașterii activităților desfășurate și promovate în cadrul rețelelor de socializare, se poate vorbi despre cunoașterea persoanelor și a grupurilor care desfășoară astfel de activități. Adesea, grupări teroriste sau extremiste își creează pagini de Facebook sau Twitter pentru a-și promova ideologia, mesajul sau valorile proprii. Astfel, ofițerii de intelligence pot pătrunde în cadrul acestor grupuri, dobândind astfel o cunoaștere mult mai bună a mentalității și a modalităților de acțiune a acestora. Pentru aceasta se poate studia nivelul nemulțumirilor 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 intențiilor criminale, extremiste sau teroriste, prin realizarea unor operațiuni de amploare de monitorizare a rețelelor de socializare, de către ofițeri tehnici specializați, aceștia având posibilitatea să monitorizeze activitatea grupurilor și a persoanelor cunoscute a desfășura acțiuni ce pot aduce atingere securității naționale (Sir Omand, Bartlett și Miller, 2012, p. 806).

Totuși, nu doar grupările teroriste sau extremiste se organizează în *social media* pentru a-și recruta noi membrii. După emergența fenomenului rețelelor de socializare și serviciile de intelligence au început puternice campanii de recrutare din acesta spațiu. Aceste campanii capătă două direcții de dezvoltare. Pe de-o parte se poate vorbi despre promovarea instituțiilor de securitate și a transparenței acestora și de atragerea de personal către acestea, după modelul companiilor private care prin campanii de marketing își promovează imaginea și 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 esențial ce trebuie avut în vedere de către ofițerul de intelligence în stabilirea profilului persoanei în cauză. Astfel, persoana ce realizează *profiling*-ul, prin analiza relațiilor de prietenie ale utilizatorului și a altor legături stabilite în *social media*, își completează datele de cunoaștere cu privire la cercul relațional al persoanei aflată în atenția recrutării. Atenta observare a persoanelor adăugate ca prieteni în cadrul profilului utilizatorului, precum și analiza legăturilor strânse pe care acesta le păstrează cu anumite persoane poate conduce la determinare unui anumit mediu relațional și stabilirea unor caracteristici cu privire la acesta, identificându-se starea socială a persoanei, cercurile sociale în care își desfășoară activitatea, precum și cele în care se simte cel mai comod. Așadar, se pot obține date de cunoaștere importante cu privire la motivația recrutării sau cu privire la crearea unui context favorabil recrutării.

Opțiunea 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 și apelând la funcția de *check-in* marchează prezența sa în locul respectiv. Astfel, ofițerul poate ști cu exactitate locul în care se află persoana, beneficiind de coordonatele GPS oferite de Facebook, dar și de numele unor locații publice sau private ce se regăsesc în cadrul *check-in*-ului. Astfel, în cazul unei postări se poate observa zona, cu aproximație, din care s-a făcut postarea, ofițerul având posibilitatea să verifice prezența persoanei într-un anumit cartier, sector, într-o anumită localitate sau regiune.

Astfel, în acest sens, ofițeri ai serviciilor de intelligence pot apela la această metodă de *profiling* prin intermediul *social media*, obținând prin analiza unor elemente cheie ale rețelei Facebook, date de cunoaștere primară cu privire la viitori candidați la recrutare, care coroborate și verificate prin comparația cu alte informații obținute prin intermediul altor surse pot oferi o imagine de ansamblu asupra recrutării noilor surse de informații, a calităților acestora, precum și a trăsăturilor psihologice care cu condus la demararea procesului de recrutare.

Dacă pe palierul informativ operativ al activității de intelligence se poate vorbi despre realizarea unui profil cu date primare de cunoaștere a candidaților pentru recrutare culese prin intermediul rețelelor de socializare, în ceea ce privește partea tehnică a acestei activități, căci a fost susținut faptul că și în acest spațiu activitatea de informații se desfășoară după aceleași norme, mijloace, metode și principii, *social media* se bucură de un aport al oportunităților, adus prin intermediul programelor informatice de analiză

a rețelelor de socializare, de care pot beneficia cu ușurință analiștii serviciilor de intelligence.

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

Pornind de la ideea că în mod succint, o rețea socială reprezintă un set finit sau seturi finite de actori care realizează conexiuni unul cu celălalt, analiza rețelelor sociale implică detectarea și 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 îmbunătățit în mai multe rânduri. Acesta este unul dintre cele mai cunoscute programe de analiză a rețelelor sociale, fiind totodată și cel mai folosit, deoarece oferă o serie de instrumente de măsurare a datelor provenite din platformele de socializare, precum și alte instrumente de management al datelor. Toate acestea contribuie la măsurătorile estimative ale topografiei rețelei, oferind informații despre actorul central al rețelei, identificând subgrupurile și estimând valorile de măsurare ale echivalenței structurale a platformei vizate. Mai mult decât atât, UCINET oferă o serie de instrumente prin care se pot selecta subseturi de date din cadrul rețelei și prin care se pot importa și exporta date sub orice format, toate acestea făcând din UCINET un redutabil program folosit în realizarea analizei rețelelor de socializare (Everton, 2013, p. 50).

Concluzii

Așadar, 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 oportunități, care exploatate de către cadrele serviciilor de intelligence, acestea pot oferi o serie de date de cunoaștere 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 își desfășoară 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 își ghidau activitatea serviciile de informații. Totuși, trebuie avut în vedere un fapt simplu și anume că și cei ce folosesc *social media* în scopuri care nu deservesc valorilor și intereselor naționale pot cunoaște 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 riște pentru a putea cuceri spaţiul virtual? Vor fi gata serviciile de intelligence să ducă o nouă activitate de cercetare și cunoaștere pentru a înțelege 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.

ISTORIE ŞI MEMORIE ÎN INTELLIGENCE

MOTIVAŢII ALE TRĂDĂRII. CAZURI ISTORICE PRIN PERSPECTIVA MODELELOR DE ANALIZĂ CONTEMPORANE

Ioan Codruţ LUCINESCU*
Valentin STOIAN*

Abstract

The article aims at harnessing the analytical power of theoretical models employed in studying defection in favor of the enemy and use them to study Romanian historical sources originating during the First World War. These models have been developed in the United States during the 1950s and 60s and are used by this article to study a very different case. The article's main research question is „Can models explaining reasons for defection developed in the US during the Cold War be applied on behaviors detected in Romania at the beginning of the XX century?" The article answers this question in the affirmative, showing how reasons for defection are, many times, similar despite large differences in time and space.

The article's first section relies on an exhaustive review of several theoretical models, especially MICE. Further empirical studies have refined this simplification of motivations, uncovering new potential reasons for betrayal such as the existence of „divided loyalties" or of disgruntlement against one's own organization. These represent the analytical blueprint which is later applied on Romanian documents dating from World War I.

The second part of the article employs an analytical approach to uncover reasons for defection in Romania and its vicinity. It presents both cases of ethnic Romanians who were Austro-Hungarian citizens and defected in favor of Romania, as well as intelligence successes by the Austro-Hungarian enemy in Romania of that time. The article concludes that the first cases are mainly motivated by „divided loyalties" while the second was mostly caused by money and ideological reasons.

Keywords: defection, motivation, ideology, loyalty

Introducere

Literatura ficţională, dar şi filmele de acţiune, de multe ori simplificări ale unor realităţi complexe, creionează, în cadrul paletei relativ restrânse de personaje cu care operează, imaginea trădătorului ca fiind, de multe ori,

* Academia Naţională de Informaţii „Mihai Viteazul".

mult mai condamnabilă decât cea a principalului personaj-negativ. Trădătorul este prezentat ca o ființă slabă, tentată de avantaje pe care nu le merită, sau acționând din invidie nejustificată, împiedicând, niciodată decisiv, acțiunea protagonistului de a învinge personajele negative.

Motivațiile trădării, în lumea spionajului real, sunt, de multe ori, mult mai complexe. Mai ales în situații de război sau de confruntare ideologică accentuată, trădarea reprezintă un risc serios la adresa propriei persoane, iar motivele pentru care anumiți indivizi acceptă aceste riscuri sunt diverse. De asemenea, trebuie menționat și faptul că, în multe situații, cei care acceptă să lucreze împotriva propriului stat pentru o putere străină nu sunt prinși, iar resorturile intime care au generat o astfel de decizie nu sunt cunoscute niciodată. În multe alte situații, deși cei care comit astfel de acte sunt prinși, documentele care reliefează motivațiile lor (fie documente elaborate de serviciul de informații care i-a recrutat, fie cele ale interogatoriilor post-factum) rămân clasificate pentru o lungă perioadă de timp. Astfel, concluzii asupra acestor situații pot fi trase doar la o distanță apreciabilă de timp după ce evenimentul a avut loc.

Articolul de față introduce o abordare invadatoare în domeniul studiilor de intelligence, în sensul că aplică un model teoretic dezvoltat de către specialiști americani din timpul și imediat după Războiul Rece asupra surselor istorice românești referitoare la perioada Primului Război Mondial. Articolul urmărește să răspundă la următoarea întrebare de cercetare: „Pot fi translatate modelele de analiză dezvoltate în SUA Războiului Rece asupra comportamentelor detectate în spațiul românesc la începutul secolului XX?”. Argumentul central al articolului este că aceste modele sunt universalizabile, arătând că principala motivație a etnicilor români din imperiul Austro-Ungar care colaborau cu structurile informative românești era aceea a ideologiei sau a „loialităților împărțite”, iar cea a cetățenilor români care trădau în favoarea Puterilor Centrale era cea financiară. Bineînțeles, cele două posibile situații nu se exclud reciproc, ambele fiind întâlnite în toate cazurile. Se remarcă însă o anumită prevalență a pattern-urilor de acțiune de fiecare parte a baricadei, determinate în mare măsură de situația politică și militară a celor două state combatante. Austro-Ungaria stăpânea un vast teritoriu cu o majoritate românească, care fusese supusă unui proces de asimilare culturală violentă și care generase alienare și frustrare. Pe de altă parte, Imperiul Dualist putea mobiliza resurse financiare mult superioare, exercitând și o putere de atracție culturală considerabilă.

Prima secțiune a articolului va prezenta modelele teoretice ale motivațiilor colaborării cu un serviciu de informații străin, modele realizate prin cercetarea cazurilor concrete din Statele Unite ale Americii. Aceste

modele au apărut în contextul dezvoltării fără precedent a spionajului sovietic în SUA și a intervievării unui număr mare de cetățeni americani care au lucrat pentru sovietici. Principalul model discutat este MICE (Money-Ideology-Compromise-Ego), menționat de mai multe lucrări de studii de intelligence, atât teoretice, cât și empirice. Acest model a fost modificat în mai multe circumstanțe, fiind propuse chiar schimbări radicale ale sale.

Cea de-a doua secțiune aplică aceste modele asupra surselor istorice românești din perioada primului război mondial, analizând atât motivația trădării etnicilor români cetățeni ai Imperiului Austro-Ungar, cât și a românilor care au lucrat pentru Puterile Centrale. Secțiunea conclude că primul fenomen a fost mult mai de amploare, dar a vizat primordial persoane cu un statut social mediu, atrase de idea de a servi un stat cu care se identificau mai mult, pe când cel de-al doilea a fost motivat primordial financiar și ideologic, vizând mai mult elitele politico-militare.

Dincolo de aceste concluzii științifice, se poate desprinde ideea că motivațiile umane sunt perene, acțiuni similare fiind motivate identic în perioade și în contexte politico-militare radical diferite. Astfel, acest studiu permite tragerea de concluzii nu doar asupra validității unor modele teoretice, ci și asupra legităților universale ale motivației umane.

Literatura de specialitate

Literatura care documentează motivațiile persoanelor care au desfășurat activități de spionaj se bazează aproape exclusiv pe cazuri care au avut loc în SUA, în timpul și după Războiul Rece. Având în vedere numărul mare de cazuri de spionaj petrecute în SUA, dar și dorința guvernului de a elabora un profil al spionului, cele mai importante cercetări empirice bazate pe spioni condamnați au avut loc în această țară. Într-o oarecare măsură, motivațiile cetățenilor SUA condamnați pentru spionaj împotriva propriei țări și despre care s-au păstrat informații în literatura de specialitate sunt contextual dependente de situația politică din perioada în care au acționat. Pe de altă parte, anumite categorii de motivații pot fi extinse și unei alte perioade istorice și situații politice. Ceea ce rămâne însă constant în toate timpurile este faptul că o persoană care acceptă să lucreze ca sursă de informații pentru un serviciu inamic pe teritoriul statului al cărui cetățean este se expune unor riscuri extreme, pedepsele cu moartea sau cu închisoare pe viață fiind frecvente în astfel de situații, mai ales pe timp de război. Astfel că, deși situația politică poate fi diferită, anumite specificități neputând fi surprinse de literatura și rapoartele scrise despre cetățenii americani care au spionat împotriva SUA după începerea Războiului Rece, consultarea acestei literaturi

poate oferi categorii de bază asupra motivației umane de a efectua acte de spionaj.

Literatura studiilor de intelligence utilizează, primordial, modelul MICE (Money-Ideology-Compromise/Coercion-Ego) pentru a descrie posibilele motivații ale unei persoane care acceptă să devină sursă de informații pentru un serviciu secret advers. Conform anumitor autori, acest model general a fost prezentat publicului pentru prima dată de către Stanislav Levchenko, maior al KGB care a defectat în Vest în Octombrie 1979 (Lowenthal, 2011, p. 150; Charney și Irvin, 2014). Conform acestui model există patru motivații care determină o persoană să devină spion împotriva propriei țări sau organizații.

Primul motiv propus de acest model sunt banii, una dintre motivațiile cele mai simple și ușor de înțeles. O mare parte din spionii prinși în SUA, dar și din cei pe care CIA-ul i-a folosit pentru a spiona Uniunea Sovietică au fost recompensați financiar. Unul dintre cele mai cunoscute cazuri este al lui Aldrich Ames, care a fost dat de gol de cheltuielile sale extravagante. O formă specifică a acestei motivații este descrisă se Sebastian Michalak, cercetător polonez care citează un studiu intern al Serviciului de Securitate al Ministerului de Interne Polonez din 1980, în care se menționează că circa jumătate din cetățenii Poloniei comuniste care au spionat pentru țările occidentale între 1957-1970 au făcut-o pentru bani, în mod direct, pe când un sfert au dorit să fie sprijiniți pentru a emigra în Vest (Michalak, 2011, pp. 1-4).

Ideologia se referă la o serie de credințe despre ceea ce este corect în lume, fie în general, fie în ceea ce privește politica țării asupra într-un anumit domeniu. În general, conform literaturii de specialitate, spionajul cu motivații ideologice a fost o caracteristică a primei perioade a războiului rece, fiind în considerabilă scădere în a doua parte a conflictului, dar revenind, într-o oarecare măsură, în perioada post-război rece. Scăderea suferită în a doua perioadă a Războiului Rece a fost determinată de revelațiile asupra politicilor Uniunii Sovietice, care au redus atractivitatea ideologiei comuniste. Cele mai cunoscute cazuri de spionaj ideologic sunt grupul „Cambridge Five", cel mai bine cunoscut fiind Kim Philby sau Ana Belen Montez, care au spionat împotriva Marii Britanii și a SUA fiind convinși de orientarea ideologică greșită a acestor două guverne (Burkett, 2013). Philby a spionat în favoarea URSS, iar Montez în favoarea Cubei. De asemenea, o dată cu prăbușirea Uniunii Sovietice și creșterea amenințării islamului radical, au existat o serie de cetățeni americani ce au încercat să spioneze în favboare al-Qaida, convinși de necesitatea jihadului global (Burkett, 2013).

Compromise/Coercion – Compromitere sau obligare se referă la șantajarea unor persoane sau obligarea lor prin alte mijloace (ex. amenințări

la adresa familiei) pentru a îi determina să comită acțiuni de spionaj. Literatura ficțională se referă la cazuri de bărbați seduși de agente ale serviciilor secrete adverse și apoi șantajați sau bărbați homosexuali împotriva cărora s-a folosit această orientare (Charney și Irvin, 2014).

Ego se referă la dorința trădătorului de a se simți superior celor din jur prin activitatea sa sau de a trăi „senzații tari" cu scopul de a evada din rutina zilnică. Cei care trădează din aceste motive își imaginează că trăiesc o viață aventuroasă datorită activității lor, crezând că astfel sunt mai buni decât ceilalți (Burkett, 2013, pp. 7-9).

Alte abordări teoretice vin să completeze sau să modifice modelul MICE, propunând noi factori care să contureze posibile motivații ale persoanelor implicate în activități de spionaj. Stan Taylor și Daniel Snow (1997) propun înlocuirea ultimilor doi factori (Compromise/Ego) cu termenii de „Ingratiation" (încercare de a intra în grațiile cuiva) și Disgruntlement (nemulțumire). Primul se referă la o situație în care o persoană spionează pentru a-i face pe plac unui prieten/iubit cu scopul ca celălalt să aibă o imagine bună despre persoana în cauză. Cel de-al doilea factor descrie o situație în care potențialul trădător este nemulțumit de modul în care percepe că organizația din care face parte îl tratează și, din acest motiv, decide să se răzbune pe organizație. Cel mai bun exemplu al unei astfel de situații este un angajat care consideră că ar fi meritat să fie promovat, dar nu a fost sau că a fost pedepsit pe nedrept (Taylor și Snow, 1997, pp. 101-125).

Un alt factor posibil care determină spionajul în favoarea altei țări este, conform celui de-al treilea raport al proiectului PERSEREC (vezi mai jos), existența „loialităților împărțite", adică o situație în care o persoană, fie datorită unor legături culturale, fie datorită unora de familie, se simte apropiată de o altă țară spre deosebire de cea a cărui cetățean este (Herbig, 2008).

O modificare radicală a framework-ului MICE sau a diferitelor sale variante a fost propusă de Randy Burkett, reprezentant al CIA la școala post-universitară a Marinei SUA. Acesta propune înlocuirea acronimului MICE cu cel de RASCLS (Reciprocation-Authority-Scarcity-Commitment and Consistency-Liking-Social Proof), bazat pe principiile universale ale acțiunii umane propuse de psihologul italian Cialdini. Acestea sunt, conform teoriei lui Cialdini Reciprocitatea, Autoritatea, Limitarea Resurselor, Consistența, Relațiile plăcute, Dovada importanței sociale a unui comportament. În viziunea lui Burkett, reciprocitatea se referă la disponibilitatea ofițerului recrutor de a ajuta o potențială sursă cu o favoare sau de a-i îndeplini o nevoie înainte de a pretinde orice. Conform teoriilor psihologice, indivizii se simt obligați să răsplătească o favoare care li s-a făcut. Autoritatea presupune

abordarea unui aer care să sugereze că ofițerul recrutor face parte dintr-o organizație importantă ce poate influența considerabil cursul unor evenimente. Al treilea termen, tradus ca resurse limitate, presupune ca ofițerul recrutor să îi spună sursei de informații că ceea ce are nevoie de la el este urgent și important în situația dată, generând o situație de acțiune imediată. În viziunea lui Burkett, este necesar ca ofițerul unui serviciu de informații să demonstreze că este deplin implicat în relație și nu își schimbă comportamentul, cerând același lucru și sursei sale (commitment and consistency). Penultimul factor presupune ca sursa de informații să fie măgulită pentru a avea o relație interumană plăcută (Liking) cu ofițerul serviciului de informații iar ultimul (social proof – dovada importanței sociale) se referă la inducerea ideii că agentul nu este singur, că există și alți agenți și că acest comportament este unul dezirabil și pentru alte persoane (Burkett, 2013, pp. 7-9).

Din punct de vedere al studiilor empirice, se remarcă trei surse primordiale (articole academice, raportul proiectului Slammer, rapoartele proiectului PERSEREC) care au cercetat motivațiile indivizilor implicați în activități de spionaj împotriva propriei țări. Din păcate, toate aceste studii au fost realizate în SUA și se referă exclusiv la cetățeni care au spionat în această țară. Motivațiile spionilor din alte contexte pot fi reținute doar prin analiza secundară a articolelor de specialitate care discută cazuri de spionaj, fără a avea motivația ca unul dintre factorii de studiu.

În articolul menționat mai sus, Stan A. Taylor și Daniel Snow analizează cazurile a 139 de americani acuzați oficial de trădare în SUA conform schemei Bani-Ideologie-Încercarea de a intra în grațiile cuiva - Nemulțumire. Analiza celor doi autori are în vedere doar anii 1940-1990 (perioada Războiului Rece), motivațiile fiecărui caz de spionaj fiind deduse pe baza studiului unor surse deschise. Atribuirea motivațiilor pentru spionaj fiecărui caz este făcută de autori direct, fără însă a avea acces la inteviuri detaliate cu cei acuzați de spionaj. Articolul concluzionează că motivația ideologică este prezentă aproximativ la același nivel ca motivația financiară pe parcursul anilor 1940-1970 (în special în primele două decade ale Războiului Rece), iar în anii 1970-1990 importanța motivației financiare crește semnificativ, ceilalți trei factori fiind mai puțin pronunțați. Conform autorilor, plata foarte proastă a militarilor din funcțiile inferioare (militari voluntari, subofițeri) a generat tentații serioase, favorizând spionajul. Doar 23,7% din totalul spionilor au făcut acest lucru datorită motivațiilor ideologice, procent mult mai scăzut în anii ’70-’90, mai ales după revelațiile crimelor din Uniunea Sovietică și înăbușirea revoltelor din Ungaria (1956) și Cehoslovacia (1968) (Taylor și Snow, 1997, pp. 101-125).

Studii empirice la nivel academic asupra motivațiilor celor care au spionat împotriva SUA au fost făcute de psihologul Leroy Stone. Acesta a construit o bază de date de 186 de indivizi acuzați de spionaj, utilizând 59 de variabile care îi caracterizează pe fiecare. Codarea variabilelor a fost făcută pe baza consultării surselor deschise despre fiecare caz. Ca și în studiul lui Taylor și Snow, Stone a atribuit el însuși motivația spionilor, incluzând și informații despre suma de bani primită de fiecare și despre atașamentul său ideologic. Utilizând metoda analizei componentelor principale (o metodă statistică ce presupune restrângerea variabilelor primare în noi variabile generate automat pe baza corelației dintre variabilele deja existente), Stone a concluzionat că există o diferență vizibilă între trădătorii motivați financiar și cei motivați ideologic. Astfel, cei care trădează pentru bani nu au motivații ideologice și invers, cei care au primit bani pentru activitatea lor neputând fi considerați ca atașați de orice fel de ideologie. De asemenea, autorul nu a putut observa o relație între alte motivații precum obligarea de a spiona sau nemulțumirea cu starea carierei, fiecare dintre aceste motivații fiind de sine stătătoare (Stone, 1992).

Una dintre cele mai importante surse de studiu a spionilor condamnați pentru spionaj împotriva SUA este proiectul PERSEREC (Defense Personnel and Security Research Center), un centru de cercetare înființat în cadrul Departamentului Apărării din SUA, în urma scandalului de trădarea lui John Anthony Walker (subofițer în Marina SUA, care a vândut documente clasificate sovieticilor, fiind arestat în 1985). Centrul de cercetare a fost înființat pentru a îndeplini recomandările Comisiei Stillwell, care a evaluat slăbiciunile sistemului de acordare a accesului la informații clasificate în SUA. Proiectul PERSEREC deține cea mai mare bază de date de persoane condamnate pentru spionaj împotriva SUA, generând până acum trei rapoarte asupra motivațiilor acestora. Cel mai important pentru acest articol este ultimul, cuprinzând activitatea de spionaj începând cu 1947 și terminând cu 2007. Din nou, trebuie menționat că motivațiile pentru spionaj au fost stabilite de către cercetători pe baza consultării surselor deschise, fără a intra direct în contact cu cei condamnați pentru spionaj. Rapoartele PERSEREC utilizează o schemă de posibile motivații bazate pe: bani - loialități împărțite - nemulțumire - intrarea în grațiile cuiva - obligare - „senzații tari" (thrills) - recunoaștere sau ego. Spre deosebire de alte studii, acest raport include și posibilitatea ca un spion să fie motivat de mai multe lucruri, prezentând și date despre prevalența motivelor primordiale atunci când există mai multe motive pentru spionaj (Herbig, 2008).

Precum studiul lui Stan și Taylor, al treilea raport PERSEREC observă creșterea importanței motivației financiare în a doua perioadă a Războiului Rece, urmată de scăderea acestei motivații în perioada post-Război Rece. Dacă

în prima parte a Războiului Rece (1947-1979) spionii care au avut banii ca singură motivaţie erau în procent de 47%, acest procent creşte la 74% în perioada 1980-1989, pentru a scădea la doar 7% între 1989 şi 2007. De asemenea, procentul spionilor motivaţi primordial, dar nu exclusiv de bani variază de la 43% la 60%, pentru a scădea la 39% după 1989. Alternativ, existenţa loialităţilor împărţite ca singură motivaţie trece de la 16% (în perioada 1947-1979) la 11% între 1980-1989 sărind la 57% după 1990. O evoluţie similară o are prevalenţa loialităţilor împărţite ca factor primordial între alte motive. Nemulţumirea ajunge la valoarea de 22% pentru perioada 1989 şi 2007, după ce fusese mult mai puţin importantă în perioada anterioară. Celelalte posibile motivaţii au un număr mult mai mic de cazuri, fiind mai puţin relevante. Una dintre concluziile raportului este că spionajul împotriva SUA după 1989 este influenţat de procesul de globalizare, mult mai mulţi spioni fiind cetăţeni americani naturalizaţi, (de origine străină), care păstrează legături culturale cu o ţara de origine, a lor sau a părinţilor (Herbig, 2008).

O altă sursă de informaţii despre motivaţia celor condamnaţi pentru spionaj împotriva SUA este raportul editat de proiectul Slammer (intitulat astfel deoarece activitatea de cercetarea a avut loc în închisorile de maximă securitate unde erau închişi cei condamnaţi, slammer = „puşcărie"). Acesta s-a desfăşuat sub auspiciile CIA la sfârşitul anilor 1980 şi începutul anilor '90, raportul fiind finalizat în aprilie 1990, dar declasificat parţial doar circa 16 ani mai târziu (Stein, 2010). Spre deosebire de studiile anterioare, raportul proiectului Slammer s-a bazat pe intervievarea detaliată a 30 de condamnaţi pentru trădare în prezenţa unui psiholog specializat în comportamentul uman şi a unui ofiţer de contrainformaţii. De asemenea, au fost intervievaţi şi membri ai familiei sau apropiaţi ai trădătorilor, pentru a putea fi studiată motivaţia acestora. Astfel, proiectul a putut identifica motivaţiile spionilor condamnaţi în mod direct, discutând cu aceştia. Informaţiile sintetice prezentate public conturează un profil al trădătorului ca fiind motivat în principal de nemulţumire faţă de modul în care organizaţia din care face parte îl tratează, considerând că ar fi meritat mai mult, spre exemplu o promovare sau o situaţie materială mai bună (Project Slammer interim report, 1996). În plus, trădătorul consideră că este mai bun decât ceilalţi colegi şi că organizaţia sa nu recunoaşte acest lucru. Mai mult, cei condamnaţi pentru spionaj se consideră superiori procedurilor de securitate stabilite la nivelul organizaţiei, lucru întărit de succesul acestora de a lucra nedetectaţi o perioadă de timp şi de a păcăli sistemul intern de securitate. Un mod de a se detaşa de rezultatele propriului lor comportament este percepţia trădătorilor condamnaţi că acţiunea lor nu produce victime, o potenţială schimbare a unui iluzoriu „echilibru de forţe" la nivel global fiind percepută ca extrem de

abstractă (Project Slammer interim report, 1996). Comentând raportul, psihologul William Pollack, a emis ipoteza că banii pe care cei care spionează îi primesc au și rolul de a valida propriul ego, pe care organizația pentru care lucrează l-a rănit (Pertman, 2001).

Spre deosebire de modelele statice prezentate mai sus, Terrence Thompson, fost psiholog al CIA (șeful structurii de testări cu poligraful), care a intervievat o parte dintre cei condamnați pentru trădare, a elaborat un model dinamic de evoluție a motivației celui care comite fapte de spionaj. Conform lui Thompson, decizia de a începe activitatea de spionaj este dată de intersecția dintre „o oportunitate, o criză de viață, o trăsătură negativă de caracter, peste care se suprapune un eveniment declanșator". Thompson consideră faptul accesul la informații clasificate reprezintă ca o oportunitate de a comite spionaj. În cele mai multe cazuri, criza de viață este generată de absența veniturilor suficiente, de o mutare intempestivă ordonată de superiori sau de reevaluarea vieții cauzată de atingerea vârstei mijlocii (în cazul lui Robert Hanssen, acesta nu își putea permite să își ducă copiii la școala catolică, așa cum percepea că religia sa o cere). Trăsăturile de caracter slabe sunt, în viziunea lui Thompson, predispoziția spre infracționalitate, spre jocurile de noroc sau spre o viață de lux, prezentă, de exemplu, la Aldrich Ames. Pentru a atenua caracterul negativ al propriilor acțiuni, anumiți spioni consideră că faptele lor nu sunt rele, ci că fac un lucru bun, de exemplu Earl Pitts afirmând că dorește să se răzbune pe FBI, dar nu își trădează cu adevărat țara. În final, evenimentul declanșator este reprezentat de situații precum probleme financiare sau maritale (Thompson, 2014).

Alte cazuri relevate de literatura de specialitate nu s-au concentrat exclusiv pe motivație, fiind analizate în contextul studiilor despre activități de informații în anumite state și în anumite perioade de timp. Într-un articol despre operațiunile MI5 împotriva Provisional Irish Republican Army, este prezentat cazul agentului cu nume de cod „Observatorul B", care a furnizat serviciilor de informații britanice elemente din activitățile grupării teroriste, dar și ale grupărilor militante rivale (aparținând protestanților loialiști din Irlanda de Nord). Conform ofițerului de caz, „Observatorul B" putea fi încadrabil în categoria celor motivați ideologic, principalul său resort fiind dorința de a „combate extremismul și violența, indiferent de sursa acestora". Astfel, într-un raport confidențial studiat de autorul articolului, „Observatorul B" era descris ca „având o dorință de pace" și „puternic anti-Republican, intens loial Regatului Unit, dar profund opus utilizării forței de către comunitatea protestantă pentru a își impune voința asupra Guvernului din Ulster și a minorității Romano-Catolice" (Charters, 2013).

Un studiu asupra operaţiunilor desfăşurate de KGB în Israel în perioada Războiului Rece relevă că principala motivaţie a celor care au ales să lucreze pentru serviciul de informaţii sovietic au fost banii. Unul dintre spioni, Israel Bar, a intrat în atenţia organelor de contrainformaţii israeliene datorită stilului luxos de viaţă pe care îl ducea, în contrast cu relativa lipsă de mijloace materiale preponderentă în Israelul anilor '50. Un alt exemplu este cel al lui Levi Levi, care a lucrat pentru serviciile de informaţii poloneze în interiorul serviciului de contrainformaţii Israelian (Shabak sau Shin Bet), devenind suspect şi datorită unui ceas de aur pe care îl purta. Singurul caz de motivaţie ideologică prezentat în articol este cel al lui Zeev Avni, care a lucrat pentru KGB datorită convingerilor sale comuniste. De altfel, articolul concluzionează că serviciul sovietic oferea sume mari de bani agenţilor săi din Israel, aceasta fiind principala motivaţie în activitatea de spionaj (Shpiro, 2011).

O lucrare memorialistică scrisă de Henry Crumpton, fost ofiţer CIA prezintă motivaţiile pentru spionaj ale diverselor surse pe care le-a recrutat în cariera sa. Astfel, în lipsa unor studii documentate, din literatura memorialistică se pot observa motivaţii ale celor care au lucrat ca spioni în favoarea (şi nu în detrimentul) SUA. Acesta aplică schema MICE pentru a descrie motivele surselor sale. În descrierile sale, sunt prezentate cazurile unei surse motivate financiar datorită salariului său foarte scăzut, care şi-a negociat salariul pe care CIA urma să îl plătească, situaţia unui lider tribal african dornic să ajute SUA pentru că considera că organizarea tribală este depăşită şi conduce la războaie şi violenţe (ideologie), spionajul făcut de un ofiţer de transmisiuni dintr-o ambasadă a unui stat din Blocul Estic, iniţiat după ce acesta pierduse o sumă din banii ambasadei şi ar fi urmat să fie pedepsit (compromise), sau de un funcţionar mărunt care considera că nu este băgat în seamă de nimeni în propria organizaţie (ego) (Crumpton, 2013). Datorită modelului aplicat de autor, ultimul caz este clasificat în categoria ego, dar ar putea fi inclus şi în categoria „nemulţumire".

Spionaj şi trădare în spaţiul românesc, la începutul secolului XX

Deşi modelele prezentate au fost elaborate în cea mai mare parte bazându-se pe experienţa Războiului Rece, translatarea în spaţiul românesc al începutului de secol XX vine să confirme faptul că motivaţia trădării este universal valabilă şi se confundă cu istoria omenirii.

Din momentul în care era evident faptul că România se va alătura Antantei (1915) şi, astfel, armata va declanşa ofensiva în Transilvania, structurile de intelligence naţionale au avut ca sarcină principală asigurarea

unui flux informativ continuu, diversificat şi cât mai exact despre capabilităţile militare și nu numai, ale Austro-Ungariei.

Pe lângă asigurarea informativă a unităţilor armatei române în vederea contracarării acţiunilor spionajului Puterilor Centrale, acestea au organizat, pe parcursul celor doi ani de neutralitate (1914-1916), acţiuni complexe de culegere a informaţiilor în Transilvania.

În acest sens, s-a urmărit recrutarea, în special, a persoanelor cu largi posibilităţi de informare prin natura meseriei lor şi, foarte important în timp de război (când circulaţia oamenilor şi a bunurilor este restricţionată în toate statele beligerante), cu capacitate de deplasare în regiunile respective fără a trezi suspiciuni deosebite din partea autorităţilor austriece sau maghiare.

Principala motivație a „trădării" a fost existența „loialităţilor împărţite", românii din Transilvania simţindu-se mai apropiaţi de România, pe care o percepeau ca „ţara lor", simţind, de multe ori, dorinţa românilor de a se uni cu ceea ce considerau că este patria-mamă; de asemenea, nu putem nega faptul că unii dintre aceştia au fost şi remuneraţi, dar, indiscutabil, nu beneficiile materiale i-au determinat să ia o asemenea decizie periculoasă (în caz de descoperire, sentinţa era, de cele mai multe ori, moartea prin împuşcare sau spânzurare). De altfel, agenţii structurilor de intelligence naţionale, atât cele ale Ministerului de Interne cât şi ale Armatei urmăreau să recruteze, cu predilecţie, persoane de origine română care s-au manifestat, sub diverse forme, în acest sens. Majoritatea au fost recrutaţi din rândul intelectualilor – doctori, farmacişti, avocaţi, profesori, ingineri, învăţători sau preoţi şi al salariaţilor de stat – pădurari, factori poştali, lucrători ai căilor ferate şi al comercianţilor (Brestoiu şi Bobocescu, 1979, p. 105).

În diverse documente elaborate de agenţii Siguranţei Statului (structura de intelligence a Ministerului de Interne) se reliefează acest aspect, al conştiinţei unei apartenenţe la România pe care o au cei ce îşi oferă serviciile ţării noastre. Într-o Notă redactată la 23 decembrie 1914 şi adresată conducerii Siguranţei, un agent al acesteia informează despre marele ajutor pe care l-ar putea oferi, în momentul începerii ofensivei armatei române în Transilvania preotul greco-catolic din Iablanița (Banat) George Tătucu. Despre acesta din urmă se specifică:„Numitul este un bărbat vrednic, cinstit, nepătat, poate cel mai vrednic preot român din Dioceza Caransebeşului…Demn de toată încrederea statului român..." (ANIC, DPSG, 592/1914, f. 2).

Acelaşi agent atrage atenţia şi asupra preotului ortodox Iulius Musta din comuna Glimboca (Banat), aflat, în decembrie 1914 la Bucureşti cu afaceri, care poate oferii servicii importante şi prin cunoaşterea unor trasee peste Carpaţi vitale pentru trupele române care urmau să treacă munţii. Se cere permisiunea conducerii Siguranţei ca preotul Musta să fie recrutat imediat,

pentru ca să poată începe furnizarea de informații din momentul în care s-ar întoarce în Banat. De asemenea, semnalează faptul că, datorită situației materiale bune a celor doi preoți, aceștia nu vor cere nici un fel de remunerație de la statul român, pentru activitatea secretă desfășurată (ANIC, DPSG, 592/1914, p. 3).

Pe lângă civilii, numeroși și bine motivați în activitatea secretă întâlnim și militari în armata imperială care au lucrat pentru România, „trădând" din patriotism armata imperială, față de care datorau, la acel moment, loialitate. Informaţii strategice au fost obţinute, conform celor relatate de mareşalul Alexandru Averescu, de la un husar de naţionalitate română; acesta, în vara anului 1916 a dezertat din armată, trecând munții. La București, a arătat Marelui Stat Major faptul că planul de campanie al Puterilor Centrale contra Românie prevedea, ca prim obiectiv, încă din momentul declanșării ostilităților, ocuparea Olteniei.

„Am dat crezământ acestei informaţii – arăta mareşalul Averescu în însemnările sale – căci corespundea unui plan judicios şi de aceea când s-au produs eforturile cele mari contra grupului Nămăeşti, prin concentrarea a 3 ½ divizii inamice, am presupus că se urmărea izolarea Olteniei prin ocuparea Piteştiului'' (Averescu, p. 365).

Studierea documentelor de arhivă reliefează complexitatea activității de culegere a informațiilor din Imperiul Austro-Ungar, în cei doi ani de neutralitate (1914-1916). Se estimează că aproximativ 1.000 de persoane (Ştefănescu, 2009, p. 41) – români, dar şi alte naţionalităţi care trăiau în Ardeal, au fost, sub o formă sau alta, agenţi ai Armatei, Siguranţei Generale sau Jandarmeriei statului român. Evident că, din perspectiva autorităților imperiale, cetățenii coroanei care desfășurau acțiuni secrete erau considerați „trădători", fiind tratați cu maximă asprime în momentul în care erau descoperiți.

Eugen Cristescu, şeful Serviciului Special de Informaţii (1940-1944) scria, referitor la această problematică: „...Prin acţiuni informative ofensive, Siguranţa generală şi Marele stat major au reuşit să se orienteze din punct de vedere militar asupra situaţiei din Ardeal, servindu-se în special de românii ardeleni, folosiţi ca informatori şi care după război au fost încadraţi ca funcţionari superiori în serviciul de siguranţă al statului întregit" (*Din Memoriile lui Eugen Cristescu*, 1968, pp. 14-15).

Din *Memoriile* generalului Maximilian Ronge, şeful serviciului de informaţii al comandamentului imperial austro-ungar în perioada 1914-1918 aflăm că a existat un număr semnificativ de cazuri descoperite de contraspionajul imperial în perioada neutralității României; peste 100 de cazuri de „trădare'' ale unor civili şi militari cetăţeni ai monarhiei habsburgice în favoarea intereselor ţării noastre (ANIC – MR. MSM, 119, pp. 181-182).

Pe de altă parte, și serviciile secrete ale Puterilor Centrale înregistrează succese notabile în racolarea unor înalte oficialități militare dar și politice ale Vechiului Regat în perioada neutralității țării, principala motivație a trădării fiind banii. Amintim numai cazul elocvent al generalului de divizie Vasile Zottu, şeful Marelui Stat Major al armatei române în perioada 1914-1916. Destinul generalului este unul tragic, sinuciderea sa, la 12 noiembrie 1916, survenind pe fondul sustragerii de către agenţii Siguranţei (16 august 1916), din automobilul cu care ambasadorul Germaniei, baronul von dem Busche se pregătea să părăsească Bucureştiul, a servietei care conţinea un dosar „exploziv" şi anume lista de 200 de pagini pe care „erau trecute numele partidelor, ofiţerilor, oamenilor politici, gazetarilor şi samsarilor ce s-au lăsat corupţi şi plătiţi" (Neagu, Marinescu și Georgescu, 1977, pp. 86-87).

Pentru a arăta amploarea fenomenului de „cumpărare", amintim faptul că s-a descoperit și o scrisoare prin care centrul de spionaj german având sediul la Sofia, comunica Legaţiei Reichului la Bucureşti că i-a fost expediată suma de 25 mii mărci-aur pentru a susține activitățile rețelei de spionaj în România (Brestoiu și Bobocescu, 1979, p. 132).

Întrucât pe listele reţelei de informaţii a serviciului de spionaj german în România se găseau persoane cu funcţii importante în stat (apărea chiar şi numele marelui om politic conservator Alexandru Marghiloman), directorul general al DPSG, Iancu Panaitescu, înaintează regelui Ferdinand şi primului-ministru Ion. I. C. Brătianu dosarul sustras de la diplomat.

Cu toate că descoperirile făcute impuneau luarea unor urgente măsuri organizatorice, deoarece pe 15/28 august 1916 a început ofensiva în Transilvania, nu mai era posibilă înlocuirea imediată a militarilor superiori din conducerea armatei care fuseseră deconspiraţi.

Pentru evitarea „demoralizării armatei" s-a hotărât ca numele generalilor şi ofiţerilor trădători să nu fie adus la cunoştinţa opiniei publice; totuşi, li s-a interzis accesul la documentele operative, fiind puşi sub supraveghere până în momentul în care puteau fi scoşi din funcţii şi aduşi în faţa Curţii Marţiale. Despre generalul Zottu se spunea că a favorizat transmiterea către Puterile Centrale a Planului de campanie al armatei române, în cazul intrării în război de partea Antantei. Aflând că numele lor se găseau pe lista sustrasă de la von dem Busche, atât generalul Zottu cât şi maiorul Ionescu, şef de Stat Major la Corpul II Armată s-au sinucis, pentru a nu mai îndura interogatoriile fireşti în asemenea cazuri şi oprobiul public, urmate de sentinţa capitală (Ştefănescu, 2007, p. 45).

Însă atragerea unor militari aflați în funcțiune sau în retragere la acțiuni subversive prin intermediul banilor nu este o metodă infailibilă; avem în vedere un exemplu concludent de la începutul primei conflagrații mondiale.

În contextul prelungirii conflictului declanşat în vara lui 1914 (în acel moment nici una dintre marile puteri implicate nu bănuia că războiul va deveni unul mondial şi va duce la remodelarea lumii), atât Puterile Centrale cât şi Antanta încearcă, sub toate formele posibile, sabotarea efortului de război al coaliţiei adverse. Un caz interesant este semnalat de agenţii Siguranţei Generale a Statului (componenta cu rol informativ a Ministerului de Interne), al cărei protagonist este ambasadorul Imperiului German în România, von dem Busche.

Acesta încearcă cumpărarea unui căpitan de marină în rezervă, Gheorghe Coandă pentru acţiuni de perturbare a traficului fluvial de aprovizionare cu materiale militare a Serbiei, aflată în prima linie contra trupelor austro-germane (ANIC – DPSG, 177/1914, p. 1). Se dorea scufundarea şlepurilor cu arme şi diverse materiale încărcate în portul rusesc Reni şi descărcate pe teritoriul sârb; urma ca minele marine necesare să îi fie procurate căpitanului român de oficialul german şi plantate în apele Dunării între Cernavodă şi Galaţi.

Coandă a pretins să i se dea o garanţie pentru plată şi, în acelaşi timp, un aconto de 6.000 lei. Însă, după primirea banilor, comandorul a divulgat aranjamentul ataşatului militar al Rusiei în România, colonelul Semenoff, căruia i-a propus aranjarea unor serii de „atentate" împotriva navelor de transport ruseşti. Diversiunile au rămas la stadiul de proiect (ANIC – DPSG, 177/1914, p. 8), Germania plătind sume mari de bani fără a obţine vreun beneficiu, iar acţiunile de blocare a Dunării eşuând în totalitate.

Universalitatea trădării pentru beneficii financiare este dată şi de un exemplu prezentat de structurile de intelligence naţionale, referitoare la noile autorităţi bolşevice care ajung la putere în Rusia, după Revoluţia din 25 octombrie 1917. Astfel, prin reţeaua informativă creată de Siguranţa Generală în interiorul mişcării comuniste ruse din Basarabia şi Ucraina, conducerea de la Bucureşti era permanent informată despre intenţiile şi planurile liderilor acesteia. S-a reuşit penetrarea grupului bolşevic de elită din jurul temutului lider Cristian Racovski, care îşi stabilise cartierul general în regiunea Odessa, cu scopul de a „aprinde" revoluţia comunistă inclusiv în România.

Dintr-o Notă catalogată de maximă urgenţă, sfârşitul lunii octombrie 1917, aflăm că „Agentul de Siguranţă din Odessa" (nu se oferă alte detalii referitoare la identitatea sa), raporta: „Sunt informat din anturajul lui Rakovsky, că acesta ar fi trimis un memoriu la Petrograd, prin care cere a fi ajutat la o acţiune decisivă contra Regelui şi României. Ştiu că el prepară o lovitură serioasă contra României. Rakovsky şi evreii din Rusia conduc complotul…

Doi agenţi ce-i am în solda mea, la Rakovsky, ar putea, dacă le-aş oferi o frumoasă sumă de bani, să facă sforţări ca să poată afla intenţiunile Comitetului evreu şi a conducătorului acestuia. Unul din ei mi-a declarat că este gata de a suprima din lume pe Rakovsky, în schimbul unei importante sume de bani.

Daţi-mi instrucţiuni urgente relatif la suma de bani ce aş putea oferi la aceşti oameni pentru a-i stimula să-mi furnizeze cât mai urgent complotul condus de Rakovsky & Com., contra Regelui şi Guvernului. O oră de întârziere acestei afaceri am putea risca să o pierdem" (ANIC – DGP, 3/1913, f. 48). Din păcate, documentele aflate la Arhiva Naţională a României nu ne-au permis să identificăm deznodământul afacerii, dar este clar că nu s-a reuşit asasinarea revoluţionarului Racovski.

De asemenea, întâlnim şi exemple de trădare a unor militari de carieră din considerente ,,morale", datorită convingerilor lor politico-ideologice. Pe lângă şocul produs de înfrângerile de pe front (suferite într-un timp extrem de scurt) şi necesitatea refugierii autorităţilor în Moldova pentru a nu cădea în mâinile Puterilor Centrale, o vie emoţie a produs în rândurile armatei trădarea colonelului Alexandru Sturdza, fiul marelui om politic liberal Dimitrie A. Sturdza, comandant al Brigăzii a 7-a Mixtă (Otu şi Georgescu, 2011). Acesta a dezertat la germani fiind convins că numai o alianţă cu Reich-ul lui Wilhelm al II-lea putea salva România de a fi ocupată de Imperiul ţarist. Însă acţiunea sa nu a fost spontană, ci urmare a unui plan gândit, aşa cum relevă rapoarte ale agenţilor Siguranţei Statului.

Din deciziile luate în calitate de comandant al unei unităţi care se afla în prima linie, este evidentă dorinţa colonelului de a sabota intenţiile funcţionarilor Siguranţei cu privire la trimiterea unor agenţi în spatele frontului germano-austro-ungar: ,,Gheorghe Gherman locuitor din comuna Tulnici, munţii Vrancei este trimis de noi a trece munţii cu însărcinări determinate date de noi, dându-i în acest scop o recomandaţie către autorităţile militare române de la punctul de trecere. Dl. Colonel Sturdza, comandatul Brigăzii 7 Mixte ne înştiinţează prin adresa nr. 1062 din 20 noiembrie 1916, că prezentându-se în ziua de 18 noiembrie 1916 Gheorghe Gherman recomandat de noi spre a fi lăsat să treacă frontiera, i se refuză categoric trecerea peste frontieră pe motivul că e simplist, naiv şi nu inspiri încredere. Dispărând, l-a pus în urmărire. Dl. Colonel Sturdza, comandatul Brigăzii 7 Mixte prin adresa nr. 1088 din 21 noiembrie 1916 ne înştiinţează că Gheorghe Gherman trecând totuşi graniţa în mod clandestin, a făcut spionaj în favoarea inamicului, trădând austro-germanilor mişcările armatelor ruse. Dă ordin ca orice individ ce-i vom mai trimite în acest scop să fie arestat din lipsă de încredere... Şeful Biroului de Informaţiuni de la Armata de Nord prin adresa nr. 62 din 2 decembrie 1916, având în vedere cazul adus la lumină de dl. col. Sturdza, interzice Centrului de Informaţiuni de a mai

trimite informatori peste graniţă. Centrul de informaţiuni, în baza unor documente oficiale aflătoare în original la dosar, a căror autenticitate nu a fost până acum de nimeni contestată, raportează că toate informaţiunile d-lui colonel Sturdza nu corespund adevărului" (ANIC – DGP, 16/1926, ff. 54-55v).

Acţiunile sale de sabotare a efortului militar naţional se vor concretiza prin trecerea în tabăra inamicului în zorii zilei de 6 februarie 1917, act care va produce consternare atât în rândurile armatei, cât şi ale opiniei publice româneşti. Entuziasmul său s-a spulberat rapid, deoarece propaganda pe care a desfăşurat-o în lagărele germane cu prizonieri români în vederea creării unei „armate" care să lupte alături de Puterile Centrale nu a avut ecou, în ciuda promisiunilor făcute militarilor aflați în situații deosebit de grele (lipsa hranei și munca epuizantă a produs mii de victime printre românii prizonieri).

Concluzii

Principalul scop al acestui articol a fost de a translata modelele de analiză dezvoltate pentru studiul motivației trădării în favoarea inamicului de la timpul și contextul geopolitic în care acestea au fost create la un context complet diferit și de a verifica validitatea acestora. Prin studiul surselor istorice românești din perioada Primului Război Mondial sunt validate modele de studiu create cu 30-50 de ani mai târziu în situația specifică Războiului Rece. Utilizarea acestor modele permite o analiză inovatoare a unor surse istorice utilizate până acum în moduri primordial descriptive. Astfel, se oferă o nouă perspectivă asupra unui fenomen, pe de-o parte universal, pe de altă parte, susceptibil de manifestări diferite în funcție de situația și contextul specific.

Articolul se referă primordial la modelul MICE (Money-Ideology-Compromise-Ego), atingând însă și modificările sale parțiale. În accepțiunea clasică, o persoană care acceptă să lucreze pentru un serviciu de informații străin poate fi motivată fie de bani, de credințe ideologice, de șantaj sau de aroganță. Acest model a fost aplicat asupra spionilor prinși în Statele Unite, studiul empiric determinând uneori înlocuirea ultimilor doi termeni cu motivații precum „loialități împărțite", „nemulțumire" sau „încercarea de a intra în grațiile cuiva". De asemenea, o propunere radicală a fost înlocuirea modelului cu cel denumit RASCLS, reprezentând o îndepărtare mult mai considerabilă față de original.

Analiza istorică a surselor relevante pentru perioada primului război mondial în spațiul românesc a relevat motivații ce se pot înscrie în grila MICE dar, totodată radical diferite, pentru cei implicați în conflict pentru colaborarea cu servicii de informații inamice. În primul rând au fost analizate activitățile serviciilor de informații românești în Transilvania, aflată la acel moment încă în Imperiul Austro-Ungar, demonstrându-se influența puternică

pe care acestea o aveau în rândul populației de etnie română, care, în ciuda unor riscuri ridicate la adresa propriei securități era dispusă să ofere informații cruciale. Principala motivație a acestor acțiuni a fost, conform surselor consultate, loialitatea pe care aceștia o simțeau față de România, un stat de care se simțeau mai apropiați decât cel al cărui cetățeni erau. Politicile asimilaționiste maghiare din perioada dualismului au contribuit probabil, într-o mare măsură, la un astfel de rezultat.

Pe de altă parte, nu trebuie negată nici activitatea serviciilor de informații austro-ungare pe teritoriul României, și acestea reușind să obțină succese notabile. Printre importantele surse de informații ale acestor servicii s-au aflat ofițeri de rang superior ai Armatei Române, seduși fie de banii oferiți de Puterile Centrale, dar și de apelul unei culturi ce putea părea superioare, mai ales în competiție cu Rusia țaristă, aliatul formal al României. De asemenea, mișcarea comunistă a reprezentat o sursă permanentă de îngrijorare pentru autoritățile românești, cercul liderului revoluționar Rakovsky fiind penetrat de agenți ai Siguranței, cu ajutorul unor importante sume de bani.

Concluzia finală a acestui articol, dincolo de cea a aplicabilității unui sau altui model de analiză, este că fenomenul trădării este universal, depășind granițele timpului și spațiului. Înțelegerea motivațiilor perene care îl determină poate ajuta un serviciu de informații să se protejeze de intruziunile inamice, dar și să obțină succese pe linia activității informative împotriva unui competitor.

Referinţe bibliografice:

1. Arhivele Naționale ale României, Fonduri – *Direcția Generală a Poliției*, *Direcția Poliției și Siguranței Generale*, *Ministerul de Război* (Parte structurală Marele Stat Major).
2. Brestoiu, Horia, Vasile Bobocescu, (1979), *Momente din activitatea organelor de ordine, informații și contrainformații românești în perioada 1878-1918*, Serviciul Editorial și Cinematografic, București.
3. Burkett, Randy, An Alternative Framework for Agent Recruitment: From MICE to RASCLS", *Studies in Intelligence Vol. 57, Nr. 1,* accesibil pe https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol.-57-no.-1-a/vol.-57-no.-1-a-pdfs/Burkett-MICE%20to%20RASCALS.pdf, (accesat la 27.08.2015).
4. Charney, David L. și John A. Irvin *A Guide to the Psychology of Espionage,* accesibil pe http://www.afio.com/publications/CHARNEY_The_Psychology_of_Espionage_DRAFT_2014Aug28.pdf, (accesat la 22.08.2015).
5. Charters, David A. *'Have A Go': British Army/MI5 Agent-running Operations in Northern Ireland 1970–1972*, in *Intelligence and National Security*, 28 (2013):2.

6. *Din Memoriile lui Eugen Cristescu*, (1968), Consiliul Securităţii Statului, Direcţia Învăţământ, Bucureşti.
7. Crumpton, Henry A. (2013), *The Art of Intelligence: Lessons from a Life in the CIA's Clandestine Service*, New York: Penguin Books.
8. Herbig, Katherine L (2008) *Changes in Espionage by Americans: 1947-2007,* accesibil pe https://www.fas.org/sgp/library/changes.pdf, (accesat La 29.08.2015).
9. Lowenthal, Mark M. (2011), *Intelligence: From Secrets to Policy*, CQ Press: Los Angeles.
10. Mareşal Averescu Alexandru, *Notiţe zilnice din război 1915-1918*, ediţia a III-a, Editura Cultura Naţională, Bucureşti.
11. Michalak, Sebastian, (2011), *Motives of espionage against one's own country in the light of idiographic studies*, in *Polish Psychological Bulletin, vol. 42(1), 1-4,* accesibil pe *http://www.degruyter.com/view/j/ppb.2011.42.issue-1/v10059-011-0001-2/v10059-011-0001-2.xml,* (accesat la 22.08.2015).
12. Neagu, C., D. Marinescu, R. Georgescu, (1977), *Fapte din umbră*, vol. II, Editura Politică, Bucureşti.
13. Otu, Petre, Maria Georgescu, (2011), *Radiografia unei trădări. Cazul colonelului Alexandru D. Sturdza*, Editura Militară, Bucureşti.
14. Pertman, Adam (2001), *Why They Spy Be It Ideology, Ego or Disaffection, Almost Always a Thread Connects Motive and Money*, 25.02.2001, accesibil pe http://fas.org/sgp/news/2001/02/bg022501.html, (accesat la 1.09.2015).
15. Project Slammer interim report, 1996 http://www.foia.cia.gov/sites/default/files/document_conversions/89801/DOC_0000218679.pdf, (accesat la 1.09.2015).
16. Shapiro, Shlomo (2011), "KGB Human Intelligence Operations in Israel 1948–73", *Intelligence and National Security*, 26:6.
17. Stein, Jeff Wikileaks: CIA studied why people steal secrets, 06.07.2010, accesibil pe http://voices.washingtonpost.com/spy-talk/2010/06/wikileaks_cia_studied_why_peop.html, (accesat la 20.08.2015).
18. Stone, Leroy (1992), A principal component analysis of 59 variables of uncovered spies" în *34th Annual Conference of the Military Testing Association, Proceedings,* Volume II, Octombrie 1992, http://www.dtic.mil/dtic/tr/fulltext/u2/a268816.pdf, (accesat la 1.09.2015).
19. Ştefănescu, Paul (2007), *Istoria serviciilor secrete române*, Editura ANTET, Prahova.
20. Taylor, Stan A. și Daniel Snow (1997), *Cold war spies: Why they spied and how they got caught*, in *Intelligence and National Security*, 12 (1997):2, 101-125.
21. Thompson, Terence J., (2014), Towards an Updated Understanding of Espionage Motivation", *International Journal of Intelligence and CounterIntelligence*, 27:1, 58-72.

RECENZII ŞI NOTE DE LECTURĂ

Publicaţii româneşti de business intelligence

Recenzie de Oana Puie (ANIMV)

Evoluţiile dinamice ale mediului de securitate global şi naţional au determinat adaptarea şi reconfigurarea intelligence-ului guvernamental. Pornind de la acelaşi model, fluctuaţiile imprevizibile ale mediului de afaceri au dus la dezvoltarea şi utilizarea frecventă a practicilor ce ţin de business intelligence. Această raliere la nevoile curente de informare s-a făcut vizibilă deopotrivă în practicile curente ale companiilor şi în domeniul publicistic. Astfel, pe fondul unei necesităţi crescânde de informaţii, s-*a amplificat importanţa şi impactul revistelor de specialitate*, care abordează teme vizând sfera business intelligence-ului şi subiecte conexate acesteia.

Scopul acestei recenzii este acela de a propune scurte prezentări a două astfel de publicaţii periodice apărute în ultimii ani în spaţiul publicistic românesc: *Business & competitive intelligence. Revista de informaţii pentru afaceri* şi *Network Intelligence Studies*.

Astfel de publicaţii sporesc gradul de cunoaştere şi conştientizare a noilor provocări apărute în mediile de afaceri şi totodată permit accesul la dezbateri şi cercetări pe teme de actualitate. Pe de-o parte editorii şi autorii colaboratori au posibilitatea de a exprima ipoteze şi de a le argumenta cât mai pertinent, contribuind astfel la îmbogăţirea fondului de cunoaştere şi înţelegere a evoluţiilor din domeniul business intelligence. Pe de altă parte, cititorii sunt familiarizaţi cu perspective şi viziuni care, trecute prin filtrul personal şi adaptate unor contexte specifice, se pot transforma în oportunităţi de dezvoltare şi promovare.

Business & competitive intelligence. Revista de informaţii pentru afaceri este publicaţia oficială a Asociaţiei Specialiştilor în Informaţii pentru Afaceri (ASIA), fiind disponibilă pe web-site-ul http://asia.org.ro/html/revista.html. Deşi cu o apariţie de numai 6 numere, în perioada 2012-2013, se remarcă în rândul publicaţiilor din domeniul business intelligence fiind printre primele publicaţii de specialitate. Cu o apariţie bilingvă, revista şi-a propus să contribuie la realizarea obiectivelor Asociaţiei: „dezvoltarea domeniul „Informaţii pentru Afaceri" (Business & Competitive Intelligence), contribuind astfel la creşterea competitivităţii companiilor din ţara noastră" (http://asia.org.ro/Macheta_BI-CI_-_Nr.1.pdf). Potrivit mesajului de deschidere, echipa din jurul Asociaţiei şi, implicit al revistei sale oficiale, „reuneşte experţi şi practicieni din mediul de afaceri şi cel academic, care şi-au propus definirea şi garantarea unor repere profesionale, la care să se raporteze toţi cei care doresc să cunoască şi să folosească sistematic informaţiile pentru afaceri în scopul creşterii performanţei."(http://asia.org.ro/Macheta_BI-CI_-_Nr.1.pdf)

Network Intelligence Studies, disponibilă la http://nis.bxb.ro/, este specializată în studiul reţelelor colaborative intra şi interorganizaţionale. Sub egida Fundaţiei Române pentru Inteligenţa Afacerii (Romanian Foundation for Business Intelligence, vezi detalii pe la http://bxb.ro/) şi coordonarea Departamentului Business X Business (bxb) revista are o apariţie bianuală, primul număr fiind publicat în anul 2013.

Din punct de vedere tehnic, este concepută ca un întreg, întrucât în fiecare an apare un volum alcătuit din două numere. Programul editorial al NIS vine în întâmpinarea şi sprijinirea nevoii de colaborare între indivizi, companii, universităţi, organizaţii non guvernamentale şi comunităţi, cu scopul de a genera obţinerea unor rezultate utile, care ulterior să poată fundamenta decizii benefice. Conform viziunii clar statuate, misiunea revistei este de a crea un mediu de cercetare şi învăţare, care să se bucure de participarea şi interesul deopotrivă a comunităţii academice şi economice. Astfel, prin contributorii şi cititorii interesaţi, se stimulează discuţii pe teme ce ţin de sfera business intelligence, accentul fiind pus pe importanţa şi impactul colaborării în acest domeniu.

Articolele sunt semnate atât de autori români, cât şi de autori străini, rezultatul generând un mix de perspective şi abordări care susţin ideea de interculturalitate, promovată de editorii revistei. Se remarcă inclusiv articole elaborate în urma unei colaborări între oameni aparţinând mediului academic, economic sau administrativ autohton şi specialişti ai unor sfere diverse, din ţări precum India, Italia, Statele Unite ale Americii sau Ungaria.

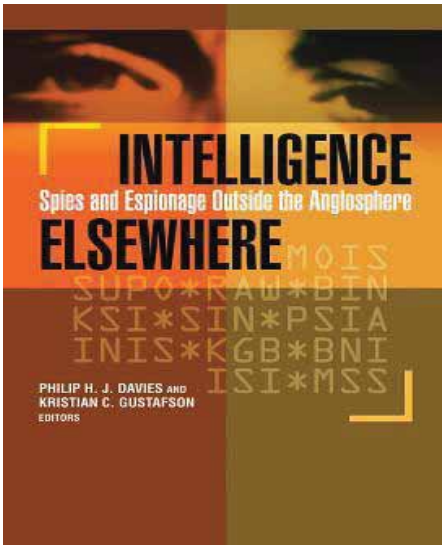
Cititorilor li se oferă o gamă largă de subiecte, care transced sfera teoretică a business intelligence-ului şi abordează problematici ce ţin de

inovarea interculturală şi interorganizaţională, elemente de teoria managementului, antreprenoriat şi afaceri internaţionale, antropologie, performanţă interculturală, metodologia trainingului intercultural, măsurarea şi creşterea performanţei economice, impactul economic, social, politic şi de securitate al diferitelor schimbări la nivel global.

În concluzie, cele două publicaţii oferă posibilitatea de a accesa mai mult decât nişte informaţii de business intelligence, întrucât poate fi privită ca o platformă deschisă, care mediază colaborarea, pe multiple nivele între educaţie, cercetare, economie şi mediul de afaceri privat. Indiferent de temele abordate, avantajul major al celor două publicaţii este acela că au o aplicabilitate generoasă şi pot reprezenta oricând un punct de plecare fie în domeniul studiului şi cercetării academice pe palierul business intelligence, fie în domeniul dezvoltării şi îmbunătăţirii afacerilor. Publicarea articolelor în limba engleză vine în completarea ideii de interculturalitate şi facilitează accesul unui public larg, care depăşeşte graniţele naţionale şi lingvistice.

Philip Davies şi Kristian Gustafson editori, (2013),
Intelligence elsewhere: spies and espionage outside the anglosphere,
***Georgetown University Press,* Washington D.C.**

Recenzie de Cosmina-Elena Epure (ANIMV)



Volumul intitulat *Intelligence Elsewhere: Spies and Espionage Outside the Anglosphere* se structurează sub forma unei colecţii complexe ce gravitează în jurul unui singur pol: intelligence. Coordonatorii săi, Philip Davies şi Kristian Gustafson, cunoscute personalităţi cu preocupări în domeniu, tezaurizează o serie de lucrări şi referinţe ale mai multor specialişti cu scopul construirii unei viziuni largi asupra ceea ce înseamnă intelligence.

Aportul ştiinţific este cu atât mai mare cu cât asistăm la o abordare academică orientată pe două paliere: dimensiunea istorică – pilon în construirea şi dezvoltarea unor concepte şi idei şi dimensiunea prezentă, focusându-se pe contextele politice şi culturale.

Perspectiva istorică. Cunoaşterea porneşte de la origine, prin urmare perspectiva istorică asupra intelligence-ului devine fundamentală pentru determinarea prezentului şi a viitorului. În acest sens, autorii recurg la analiza rolului comparativ al culturii în intelligence, oprindu-se asupra câtorva exemple: India, China, Lumea Arabă, dar şi Rusia. Astfel, este atrasă atenţia asupra importanţei şi actualităţii operei lui Sun Tzu, prin prisma faptului că la baza oricărei intervenţii armate chinezeşti se află subversiunea şi spionajul. În ceea ce priveşte Rusia, este realizată o comparaţie între Imperiul Bizantin – care punea accentul pe previzionări – şi perioada sovietică. Concluzia asupra acestui exemplu marchează importanţa perioadei bizantine în democratizarea practicilor ruseşti în intelligence.

Capitolul referitor la lumea arabă, plasează culegerea clandestină de informații și spionajul în istoria islamică și arabă, mai exact în lupta profetului Mohammed de a-și menține si dezvolta religia nou apărută.

Perspectiva actuală. Cea de-a doua parte a cărții este dedicată unei analize particulare a fiecărui stat referitoare la practicile actuale în intelligence precum și nevoile și cerințele de schimbare și de adaptare la cerințele factorilor de decizie dar și la mediul de securitate.

În cazul Pakistanului, serviciile interne de informații exercită o influență puternică asupra statului. Activitatea de intelligence a Iranului este rezultatul unei interacțiuni între trei factori – șiismul, birocrația, dar și facțiunile clerice. Consensul politic privilegiat asupra informării factorilor de decizie este cel care gravitează în jurul a ceea se reprezintă orientarea Japoniei în intelligence. Acest fapt contribuie în mod profund la afectarea bunei desfășurări a procesului de intelligence.

În continuare, atenția se mută asupra reformei din sectorul de securitate și sunt invocate drept exemple Ghana, Argentina și Indonezia. De precizat în acest caz este faptul că adoptarea practicilor și a măsurilor în intelligence este strâns legată de experiența est europeană.

Ca un element de noutate, autorii se opresc asupra unor subiecte care nu au fost exploatate în lucrările ce au ca domeniu de referință intelligence-ul. Astfel, este vorba despre statele nordice care abordează strategii diferite de cele europene. În sprijinul acestei afirmații vine Suedia, caracterizată de o tradiție birocratică și tendințe socialiste. În ceea ce o privește, activitatea de intelligence s-a desfășurat în mod independent.

Atât Suedia cât și Finlanda își evaluează orientarea și prioritățile în lumea post Război Rece, cu precizarea că tind către direcții diferite datorită factorilor istorici, economici și intereselor de securitate, dar și extrem de important și datorită culturii strategice.

Concluzii. Punctul de pornire al activității de intelligence este tocmai incertitudinea. Plecând de la o bază atât de instabilă și într-o continuă schimbare, autorii admit un dezavantaj al acestui tip de activitate: nu poate fi luată în considerare ca fiind totdeauna veridică. Însă, meritul activității de intelligence stă tocmai în încercarea de a limita sau micșora incertitudinea. Prin urmare, prin intermediul culegerii, prelucrării și analizei informațiilor se pot construi niște perspective solide care să contribuie la procesul decizional dintr-un stat precum și la menținerea securității și prezervarea intereselor naționale.

Cunoscând scopul unui serviciu de informații, se poate trece la elemente particulare fiecărui stat – primul și cel mai important este cultura, care stă sub umbrela tradiției și moștenirii (ca exemplu Pakistan și Indonezia unde se evidențiază *tradiția sanscrită*).

Atingerea obiectivelor unui serviciu de informații stă în aplicarea tehnicilor și metodelor ce caracterizează intelligence-ul. În această secțiune, autorii lansează diada acțiuni acoperite – diplomație. Astfel, istoria plasează în aceeași sferă spionajul, sabotajul și asasinatele, în vreme ce realitatea propune o dimensiune lipsită de violență de gestionare a politicii externe – diplomația. Trecerea timpului este cea care a contribuit la evoluția conceptului de intelligence și a modului în care acesta poate fi aplicat.

În cadrul demersului academic, lucrarea lui Philip Davies și a lui Kristian Gustafson vine ca o piatră de temelie procesul de cunoaștere și aprofundare a zonei de intelligence. În acest sens, rolul fundamental este atribuit istoriei și tradiției care acționează ca o amprentă asupra prezentului și a practicilor actuale. Totodată, volumul se înscrie în încercarea definirii studiilor de intelligence drept o disciplină academică.

Meritul acestui volum constă în abandonarea pentru un moment a lumii spionajului alcătuită strict din Statele Unite ale Americii, Marea Britanie și Europa. Prin urmare, cei doi autori demonstrează că în procesul de cercetare academică a intelligence-ului, cunoașterea nu se poate realiza la nivel nișat.

Această colecție de lucrări științifice poate fi tratată ca o posibilitate de a găsi un model universal a ceea ce înseamnă intelligence alături de metode și tehnici specifice de punere în practică a sa.

Dimensiunea care nu apare tratată la nivelul cărții este cea de implementare la nivel național a activității de intelligence, precum și aspecte legate de relația cu beneficiarul. Maniera de abordare a conceptelor se raliază unui palier teoretic. În acest fel, se propune aprofundarea subiectului în vederea construirii unei viziuni cuprinzătoare (care să permită ulterior, studiile comparative).

Continua schimbare a arhitecturii de securitate precum și transformările care survin la nivelul distribuției puterii în plan internațional, *„Intelligence Elsewhere: Spies and Espionage Outside the Anglosphere"* asigură cunoașterea de bază pentru o mai bună înțelegere a fenomenelor actuale și viitoare.

Pornind de la un cunoscut citat al lui Nicolae Bălcescu *„Istoria este cea dintâi carte a unei naţii. Într-însa ea îşi vede trecutul, prezentul şi viitorul"* se poate conchide faptul că orice demers, indiferent de natura sa, presupune o întoarcere către istorie, către origini. În cazul de față, zona de intelligence se află într-o permanentă dezvoltare și pentru o fundamentare a studiilor și ideilor este nevoie de o privire în trecut. Scopul este de a se asigura o prognoză cât mai apropiată de realitate care să devină punct de referință în elaborarea politicilor și deciziilor strategice.

FOCUS ACADEMIC

EDIŢIA A XII-A A CONFERINŢEI INTERNAŢIONALE ANUALE A ASOCIAŢIEI INTERNAŢIONALE PENTRU EDUCAŢIE ÎN INTELLIGENCE (IAFIE), BREDA, OLANDA, 22-24 IUNIE 2016

Organizaţie internaţională de referinţă pentru Educaţia în Intelligence, IAFIE a fost creată în iunie 2004, ca urmare a iniţiativei a peste 60 de profesori şi instructori în domeniu. Cu o pregătire în diverse domenii conexe Intelligence-ului, precum securitatea naţională, aplicarea legii sau Intelligence-ul competitiv, aceştia au recunoscut nevoia unei asociaţii profesioniste care să reunească domenii variante, acţionând ca un catalizator şi furnizor de resurse cu scopul de a dezvolta Studiile de Intelligence.

Misiunea Asociaţiei este cea de a promova cercetarea, cunoaşterea şi dezvoltarea profesională în direcţia consolidării educaţiei în Intelligence prin:

- Crearea unui mediu de schimb al ideilor şi informaţiei.
- Încurajarea relaţiilor şi cultivarea cooperării printre profesioniştii comunităţii de Intelligence, mediul academic şi de afaceri şi instituţiile statelor.
- Dezvoltarea, transmiterea şi promovarea teoriei, programei, metodologiilor, tehnicilor şi bunelor practice pentru un Intelligence original şi aplicat.
- Facilitarea, în calitate de factor de legătură, al interacţiunii între organizaţii profesioniste şi centre de excelenţă de profil.

Deja o tradiţie la nivel internaţional, conferinţa anuală IAFIE se va concentra anul acesta pe conectarea comunităţilor de educaţie în Intelligence din Europa, America de Nord, dar şi restul, lumii relevant fiind tematica propusă *Connecting Intelligence Education Communities: Europe, North America, and Beyond.*

Evenimentul va avea loc în Breda, Olanda, între 22 şi 24 iunie 2016, şi va reuni reprezentanţi ai mediului academic şi profesionişti din cadrul

mai multor comunităţi de Intelligence, pe parcursul a două zile şi peste 20 de workshop-uri.

Prin diversitatea participanţilor de calitate şi diferitele paneluri organizate, conferinţa IAFIE îşi propune să exploreze întrebări de actualitate pentru domeniul Intelligence şi să iniţieze dezbateri privind posibile răspunsuri la acestea, contribuind astfel atât la o mai bună înţelegere a Intelligence-ului, cât şi la îmbunătăţirea calităţii teoriei şi practicii în domeniu. Mai multe informaţii despre calitatea de membru IAFIE, proiectele asociaţiei şi detalii ale conferinţei se găsesc pe site-ul www.iafie.org.

EDIȚIA A III-A A PROGRAMULUI „SECURITY IN THE BLACK SEA REGION. SHARED CHALLENGES, SUSTAINABLE FUTURE" (SBSR), BUCUREȘTI-SIBIU, 30 MAI– 4 IUNIE 2016

Serviciul Român de Informaţii organizează în perioada 30 mai - 4 iunie 2016, prin intermediul Academiei Naţionale de Informaţii, cea de-a treia ediţie a Programului Internaţional „Security in the Black Sea Region. Shared challenges, sustainable future" (SBSR). Cea de-a treia ediţie de anul acesta va avea ca temă „Convergente forms of power in the Blacjk Sea Region. Think hard, act smart".

Programul se desfăşoară în parteneriat cu Universitatea Harvard, cu participarea National Intelligence University (Statele Unite) şi sub patronajul Preşedinţiei României. Acesta continuă filosofia, misiunea şi obiectivele Programului Regional Black Sea Security (BSSP), iniţiat de Universitatea Harvard acum 20 ani. Actualul program şi-a asumat, de asemenea, misiunea de a promova şi sprijini responsabilitatea şi iniţiativa actorilor regionali cu privire la provocările de securitate din regiunea Mării Negre.

În ultimii ani, regiunea Mării Negre a fost martora unor schimbări ale balanţei de putere. În timp ce evoluţiile democratice şi de suveranitate ale ţărilor din regiune s-au aflat sub presiunea unei geopolitici a confruntării, a războiului hibrid, a terorismului global sau, de multe ori, a corupţiei interne şi a dezechilibrelor politice, răspunsurile directe au devenit un factor critic în organizarea securităţii regionale. Astfel, noua ecologie a puterii, care este semnificativ diferită de situaţia existentă acum un deceniu, se caracterizează prin nevoia de a identifica şi reîncadra interesul naţional, de a reface alianţele regionale şi de a îmbunătăţi interdependenţele complexe. Astfel, în acest

context, ediţia 2016 a programului „Security in the Black Sea Region. Shared Challenges, Sustainable Future" (SBSR) îşi propune să dezbată formele convergente de putere în Regiunea Mării Negre şi impactul pe care îl au în crearea instrumentelor potrivite în rezolvarea conflictelor şi dezvoltarea sustenabilă de-a lungul regiunii.

Ediţia de anul acesta va reuni participanţi din Armenia, Azerbaijan, Bulgaria, Canada, Germania, Georgia, Grecia, Olanda, Statele Unite, Rusia, Moldova, România, Turcia şi Ucraina, printre invitaţi aflându-se, de asemenea, oficiali de rang înalt şi experţi din cadrul Uniunii Europene şi NATO. Pentru mai multe detalii, vă rugăm să vizitaţi www.sbsr.ro.

EDIŢIA A XXII-A A CONFERINŢEI INTERNAŢIONALE INTELLIGENCE IN THE KNOWLEDGE SOCIETY, BUCUREŞTI, 13-14 OCTOMBRIE 2016

Studiile de securitate şi intelligence şi utilizarea acestora de către practicieni au rămas o preocupare şi o provocare constantă, solicitând perspective interdisciplinare. Astfel, adresăm invitaţia reprezentanţilor mediului academic, experţilor şi practicienilor din domeniul studiilor de securitate şi intelligence, precum şi a celor din alte arii precum IT şi comunicare, drept, matematică, ştiinţe sociale şi umaniste, de a contribui cu puncte de vedere specifice zonei de expertiză a fiecăruia.

Cea de-a XXII-a ediţie a Conferinţei Internaţionale *Intelligence in the Knowledge Society (IKS)* are ca scop explorarea unor perspective mulţi- şi interdisciplinare asupra interacţiunii, intersecţiei şi interdependenţei dintre creşterea exponenţială a noilor tehnologii, securitate şi intelligence.

Secţiunea dedicată studiilor de securitate, *The Future World(s) of Security*, are plăcerea de a invita specialişti din diverse domenii de studiu care să contribuie cu reflecţii asupra unor teme de interes precum: revoluţii la nivelul comunităţii de teoreticieni şi ale structurilor de putere – implicaţii pentru securitatea naţională; noi forme de bună guvernare, cetăţenie activă şi securitate colectivă; tehnologia informaţiei şi a comunicării; conectare, bunăstare şi supraveghere; ingineria viitorului securităţii; apartenenţă, conflict şi folosirea identităţii drept armă; identitate, supunere şi implicaţii de securitate în cadrul loialităţilor multiple; înţelegerea istoriei, înţelegerea trecutului pentru un mediu de securitate.

Tema secţiunii de intelligence, *Intelligence at a Crossroads*, invită specialiştii din diverse domenii să contribuie la o dezbatere complexă în jurul unor teme precum: intelligence-ul ca proces, activitate, produs; educaţia de intelligence între nevoia de păstrare a secretului şi avantajele competitive ale deschiderii; transformările culturii organizaţionale la nivelul agenţiilor de intelligence; complexul Cenuşăresei şi analiştii de intelligence; evoluţia

tehnologică – amplificarea cunoaşterii sau vulnerabilitatea în practica de intelligence; modele de evoluţie accelerată vs. sistematizarea practicii de intelligence.

Conferinţa va explora, de asemenea, moduri în care metodele şi practica de securitate şi intelligence trebuie să fie regândite pentru a adresa provocările agresorilor asimetrici, inteligenţi, mai buni şi mai rapizi. Teme controversate, soluţii inovative, bune practici şi provocări ce trebuie depăşite vor fi adresate de-o manieră interactivă de către invitaţi de prestigiu şi participanţi din diverse domenii. Pentru mai multe detalii, vă rugăm să vizitaţi site-ul conferinţei www.intelligencestudies.ro.

CITYCOP
CITIZEN INTERACTION TECHNOLOGIES YIELD COMMUNITY POLICING
IUNIE 2015 – MAI 2018

Academia Națională de Informații „Mihai Viteazul" este partener în proiectul CITYCoP, care reunește 22 de instituții din 13 țări și beneficiază de o finanțare Orizont 2010 din partea Uniunii Europene. Partenerii din CITYCoP au construit, de-a lungul mai multor ani, cu ocazia cooperării de succes în cadrul Uniunii Europene, proiecte cu conținut generat de beneficiar sau referitor la supraveghere și intimitate (CONSENT, SMART, RESPECT), urmărind integrarea soluțiilor proiectelor în ecosistemul orașelor. Proiectul CITYCoP va urmări dezvoltarea unor aplicații în mai multe limbi pentru smartphone, precum și portaluri și pachete de jocuri de pregătire în București (România), Lisabona (Portugalia), Florența (Italia) și Sheffield (Marea Britanie).

Proiectul CITYCoP va beneficia de o abordare multidisciplinară care include sociologia poliției comunitare, precum și perspective specifice științei cognitive privind interacțiunea cetățeanului cu ansamblul comunității și aplicarea legii prin intermediul tehnologiei.

Teoriile care stau la baza activității poliției comunitare au primit un nou impuls odată cu apariția recentă a smartphone-ului și a canalelor de socializare online, dar mai ales a conținutului generat de către utilizator ce permite cetățenilor să se angajeze într-o interacțiune mai apropiată atât cu comunitatea locală, cât și cu agențiile de aplicare a legii.

Perioada cuprinsă între 2010-2014 a înregistrat o creștere rapidă a numărului aplicațiilor disponibile pe smartphone menite să îmbunătățească semnalarea infracțiunilor sau a altor forme de informări de interes pentru poliția comunitară. Cu toate acestea, aceste aplicații sunt caracterizate printr-o

abordare predominant anglo-saxon, cel mai mare număr dintre acestea provenind din SUA și câteva din Canada, Australia și din Marea Britanie (aparent singurul stat european care a folosit tehnologia modernă în această direcție).

CITYCoP își propune să afle motivul pentru care UE pare a fi rămas în urmă, deși poliția comunitară este o structură implementată în mai multe state din Uniunea Europeană. Se urmărește astfel dezvoltarea unei soluții care să includă o nouă aplicație pentru smartphone și un portal online care pot fi implementate în orice oraș european, păstrându-și în același timp „specificul local" și diversitatea. Aceste soluții informatice vor fi proiectate de la zero pentru a fi pe deplin conforme cu legislația în vigoare privind viața privată și protecția datelor. Un program de formare, care să cuprindă inclusiv utilizarea de jocuri serioase, va fi dezvoltat pentru a ajuta în pregătirea ofițerilor și a cetățenilor în utilizarea aplicației și a portalului.

CARISMAND
CULTURE AND RISKMANAGEMENT IN MAN-MADE AND NATURAL DISASTERS
OCTOMBRIE 2015 -SEPTEMBRIE 2018

Academia de Informații „Mihai Viteazul", ca partener în cadrul consorțiului care implementează proiectul CARISMAND, va coordona un pachet de lucru responsabil cu partea din proiect privind percepțiile de risc în contextul factorilor culturali, a dezastrelor naturale și a celor cauzate de activitatea umană.

Riscurile nu sunt o manifestare „obiectivă", acestea fiind construite social și cultural, ceea ce face ca managementul riscului sa fie conștient, să respecte și să folosească aspectele culturale; astfel, acesta nu este doar efectiv, ci contribuie, de asemenea, la capacitatea comunității de a face față dezastrelor.

Proiectul CARISMAND își propune să identifice acești factori, să exploreze diferențe și oportunități pentru îmbunătățirea politicilor și a procedurilor destinate gestionării dezastrului, dezvoltând în același timp un instrumentar cuprinzător care va permite persoanelor responsabile în acest sens să adopte practici zilnice care corespund culturii caracteristice. Acest obiectiv va fi atins prin abordarea legăturilor și a diferențelor existente între gestionarea dezastrelor, cultură și percepția riscului dintr-o perspectivă cât mai amplă din punct de vedere multidisciplinar și, în același timp, să stabilească un ciclu de feedback între părțile interesate la nivel de management și cetățeni, în scopul de a stabili, testa și rafina soluții pentru cele mai bune practici bazate pe o cunoaștere a culturii în materie de management al dezastrului.

În timp ce experți din diverse domenii (în special, IT, drept, științe cognitive, antropologie, psihologie, sociologie) vor efectua o compilație cuprinzătoare de cunoștințe și structuri existente, o serie de summit-uri ale cetățenilor și întâlniri ale părților interesate vor fi organizate în acest cadru.

În mod sistematic, proiectul CARISMAND va folosi o abordare ce examinează dezastrele naturale, tehnice și determinate de acțiunea umană,

punând în centrul atenţiei aspecte specifice ce afectează percepţii ale riscului determinate de factorul cultural, cum ar fi, de exemplu, dacă dezastrele sunt cauzate intenţionat sau nu, diferita „vizibilitate" a hazardelor şi variaţia în timp a dezastrelor cum ar fi efectele de lungă sau de scurtă durată.

Proiectul CARISMAND implică 19 instituţii din 14 de ţări, beneficiind de obţinerea unei finanţări Orizont 2020 din partea Uniunii Europene. Prin organizarea a şase Summit-uri ale cetăţenilor, (câte două per categorie de dezastru în fiecare an şi într-o locaţie diferită), acolo unde riscul apariţiei dezastrelor este prevalent, şi trei Întâlniri a părţilor interesate (una pe an), cu ocazia cărora rezultatele sunt discutate prin intermediul unui transfer de cunoaştere între managerii de dezastru din diferite locaţii şi cu expertiză culturală diversă.

SAFFRON
SEMANTIC ANALYSIS AGAINST FOREIGN FIGHTERS RECRUITMENT ONLINE NETWORKS 2015-2018

Academia Naţională de Informaţii „Mihai Viteazul" este parte a proiectului SAFFRON – Semantic Analysis Against Foreign Fighters Recruitment Online Networks –, finanţat de către Comisia Europeană prin Programul de Prevenire a Radicalizării sub forma Activităţilor Teroriste şi a Extremismului Violent.

Războiul din Siria poate fi considerat primul conflict în care un număr mare de luptători din Occident s-au documentat cu privire la implicarea directă în timp real, şi unde, în schimb, canalele de socializare online reprezintă principala sursă de informare şi inspiraţie pentru aceştia. Analizând tendinţele recente privind recrutarea luptătorilor străini de către grupuri teroriste şi comparând strategiile de comunicare online, proiectul SAFFRON are ca punct de plecare identificarea unei strategii de utilizare a canalelor de socializare online, care facilitează trecerea individului de la forme de manifestare non-violentă la cele violente.

Dat fiind rolul tot mai important pe care socializarea online îl reprezintă în procesul de recrutare şi radicalizare a luptătorilor străini, proiectul urmăreşte să dezvolte un instrument-test capabil să identifice din timp ansamblul activităţilor folosite în radicalizarea prin reţele de socializare şi să semnaleze elementele care conduc la radicalizarea individuală.

REACT
PN-II-RU-TE-2014-4-1669
PERCEPŢIE SOCIALĂ ŞI STRATEGII COMUNICAŢIONALE PRIVIND RISCURILE DE SECURITATE NAŢIONALĂ
OCTOMBRIE 2015 - SEPTEMBRIE 2017

Proiectul *Percepţie socială şi strategii comunicaţionale privind riscurile de securitate naţională* (REACT) beneficiază de finanţarea primită din partea Unităţii Executive pentru Finanţarea Învăţământului Superior, a Cercetării Dezvoltării şi Inovării – UEFISCDI şi va fi implementat de către Academia Naţională de Informaţii „Mihai Viteazul" prin Institutul Naţional de Studii de Intelligence.

Managementul şi comunicarea privind riscurile au devenit o problemă majoră de politică publică şi dezbatere intelectuală în lumea modernă. Analiza percepţiei riscului se concentrează pe judecăţi subiective pe care oamenii le fac cu privire la caracteristicile şi severitatea unui anumit risc. Acest proiect de cercetare propune folosirea metodelor cercetării calitative pentru a măsura şi a defini cunoaşterea românilor, atitudinile şi practicile în ceea ce priveşte riscurile de securitate naţională.

Pentru a îmbunătăţi capacitatea de prevenire, pregătire şi răspuns la riscurile majore la adresa securităţii naţionale, dorim să răspundem la următoarele întrebări: Care este nivelul de cunoaştere asupra riscurilor de securitate naţională în societatea românească? Care sunt principalele preocupări de risc ale românilor? De ce fel de informaţie are nevoie societatea în privinţa riscurilor de securitate naţională?

În această privinţă, principalele obiective ale cercetării sunt:

1) Analiza şi înţelegerea limitelor managementului actual al riscului şi strategiile de comunicare a riscului, printr-o analiză de conţinut a documentelor strategice elaborate de către instituţiile de securitate naţională.

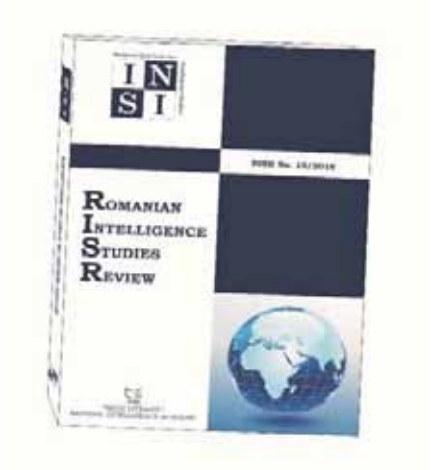
2) Îmbunătăţirea înţelegerii noastre privind modul în care oamenii percep şi acţionează cu privire la risc. Având o mai mare cunoaştere în domeniul percepţiei riscului social, pot fi îmbunătăţite calitatea şi impactul deciziilor în cadrul societăţii, precum şi calitatea strategiilor de comunicare a riscului.

3) Furnizarea unei noi perspective asupra percepţiei de risc social în România, propunând o metodă alternativă de măsurare a acesteia (metoda sortării de tip Q).

Prin urmare, obiectivul principal al cercetării noastre constă în elaborarea unor soluţii de optimizare a managementului riscurilor de securitate şi a strategiilor de comunicare pentru instituţiile naţionale de securitate, prin analiza şi evaluarea percepţiei sociale asupra riscurilor de securitate naţionale. Proiectul REACT are ca obiectiv şi îmbunătăţirea abilităţilor de cercetare privind analiza de risc a membrilor echipei de cercetare prin implicarea acestora în efectuarea de cercetări sociologice într-un domeniu relativ nou la nivel naţional: analiza percepţiei de risc social.

Dincolo de contribuţia academică la studiul riscurilor la adresa securităţii naţionale, intenţionăm să furnizăm o evaluare a percepţiei acestor riscuri de către societatea românească, conducând o cercetare sociologică bazată pe un eşantion de indivizi din medii variate, precum cel academic, privat, societate civilă şi instituţional (instituţii de securitate naţională). Proiectul are un impact politic, economic, cultural şi social, contribuind la reducerea diferenţelor de cunoaştere în zona analizei de risc existente între România şi, poate, la diminuarea vulnerabilităţii românilor şi la o mai mare reziliență a acestora faţă de riscurile existente la adresa securităţii naţionale.

INVITAŢIE LA CONTRIBUŢII
RRSI nr. 15/2016



Academia Naţională de Informaţii „Mihai Viteazul" publică, prin Institutul Naţional de Studii de Intelligence (INSI), Revista Română de Studii de Intelligence, publicaţie de calitate, indexată în bazele de date internaţionale, editată în limbile română şi engleză, a cărei apariţie este bianuală.

Scopul jurnalului este de a crea un cadru adecvat pentru dezbaterea academică şi o platformă accesibilă cercetătorilor, academicienilor, practicienilor şi doctoranzilor deopotrivă. Se doreşte, astfel, împărtăşirea cunoaşterii sub forma articolelor ştiinţifice de înaltă calitate, care au la bază demersuri de cercetare empirică sau teoretică, sub forma studiilor de caz, a metodelor şi simulărilor analitice, precum şi a recenziilor din literatura de specialitate, cu relevanţă pentru domeniul studiilor de securitate şi intelligence, cât şi pentru alte domenii ştiinţifice conexe.

Temele de interes includ, fără a se limita la acestea:

- Paradigme de securitate în secolul al XXI-lea
- Mediul internaţional şi regional de securitate
- Strategii şi politici de securitate
- Cultura de securitate şi diplomaţia publică
- Intelligence în secolul al XXI-lea
- Analiza de intelligence
- Intelligence din surse deschise (OSINT)
- Istorie şi memorie în intelligence

Acceptarea şi publicarea manuscriselor este condiţionată de o recenzare prealabilă. Articolele vor fi selectate pentru publicare în funcţie de relevanţa pentru tematica revistei, originalitate şi corectitudine ştiinţifică, ţinând cont în acelaşi timp de respectarea normelor de publicare. Materialele care au fost publicate anterior sau acceptate spre publicare în alte reviste nu vor fi incluse în portofoliul RRSI. Recenzarea manuscriselor este realizată

de către cel puţin doi recenzori independenţi, care deţin expertiză în problematica abordată.

Autorii sunt rugaţi să urmeze stilul APA de citare. Pentru mai multe detalii, vă rugăm să vizitaţi www.apastyle.org, precum şi site-ul www.animv.ro pentru mai multe informaţii privind condiţiile şi oportunităţile de publicare.

Termenele limită de trimitere a manuscriselor sunt 1 februarie şi 1 iulie. Autorii interesaţi în publicarea unui articol în RRSI sunt invitaţi să trimită propunerile electronic în format .doc/.docx pe adresa de email rrsi@sri.ro, cu titlul *RRSI propunere articol*.

COLEGIUL REFERENȚILOR ȘTIINȚIFICI

Dragoş ARDELEANU
– lect. univ. dr. Academia Naţională de Informaţii „Mihai Viteazul”
Cristian BARNA
– prof. univ. dr. Academia Naţională de Informaţii „Mihai Viteazul”
Sorin CHIŢU
– expert Serviciul Român de Informaţii
Cristian CIOBANU
– dr. Academia Naţională de Informaţii „Mihai Viteazul”
Ella CIUPERCĂ
– conf. univ. dr. Academia Naţională de Informaţii „Mihai Viteazul”
Irena CHIRU
– prof. univ. dr. Academia Naţională de Informaţii „Mihai Viteazul”
Constantin DEGERATU
– prof. univ. dr. Universitatea Creştină „Dimitrie Cantemir”
Valentin FILIP
– dr. Academia Naţională de Informaţii „Mihai Viteazul”
Niculae IANCU
– conf. univ. dr. Academia Naţională de Informaţii „Mihai Viteazul”
Ligia LEAUA
– conf. univ. dr. Academia Naţională de Informaţii „Mihai Viteazul”
Sergiu MEDAR
– prof. univ. dr. Universitatea „Lucian Blaga” din Sibiu
Karin MEGHEŞAN
– conf. univ. dr. Academia Naţională de Informaţii „Mihai Viteazul”
Veronica MIHALACHE
– conf. univ. dr. Academia Naţională de Informaţii „Mihai Viteazul”
Gabriel NEDELA
– lect. univ. dr. Academia Naţională de Informaţii „Mihai Viteazul”
Alina PĂUN
– expert Serviciul Român de Informaţii
Bogdan PRISECARU
– expert Serviciul Român de Informaţii
Gabriel SEBE
– lect. univ. dr. Universitatea din Bucureşti
Marian SEBE
– prof. univ. dr. Academia Naţională de Informaţii „Mihai Viteazul”