ANALIZĂ DE RISC CONTRAINFORMATIV: INFRASTRUCTURI CRITICE, STRUCTURI MILITARE ŞI 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

Ameninţările rezultate în urma unor acţiuni de infiltrare şi/sau trădare reprezintă o provocare majoră pentru structurile de contrainformaţii. Acest tip de ameninţare este ubicuă şi periculoasă, în special în Serviciile Armate, în care sunt localizate infrastructurile critice, în organizaţiile de intelligence şi în mediul industrial, în care proprietatea intelectuală impune o serie de măsuri de securitizare.

* Cercetător dr. în cadrul Centrului Canadian de Studii de Intelligence şi Securitate, Universitatea Carleton Ottawa şi cercetător asociat al Centrului Internaţional 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 şi 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 şi 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, şi 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 şi pentru Comisia Politicii de Apărare. A fost consilier atât al lui Henry Kissinger, cât şi 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 şi 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 şi raţional"(*Globe and Mail*, 8 februarie 2013). Delisle a mărturisit că şi-a trădat ţara şi 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 şi 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 şi trebuie racordate la fiecare situaţie în parte. Delisle este un exemplu de individ evaluat ca fiind de încredere şi loial la un anumit moment dat, dar care în timp şi-a modificat comportamentul. Circumstanţele care determină un anumit tip de comportament şi 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 behavioralã 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" comunişti germani. În ciuda acestei poveşti şi 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 exploraţi cu privire la relevanţa pentru Nidal Hasan şi informaţiile pe care ar fi putut să le furnizeze pentru a ajuta la identificarea unei potenţiale ameninţări din interior. Pentru a fi considerat un nivel de risc semnificativ (moderat sau mare) pentru extremismul violent, nu toţi indicatorii reuniţi în acest instrument de evaluare trebuie să fie identificaţi ca fiind prezenţi şi cu un grad mare de manifestare. Toţi aceşti indicatori sunt luaţi în calcul şi evaluaţi dacă informaţia este valabilă, iar dacă informaţia lipseşte, informaţia este identificată în încercarea de a realiza evaluarea. Evaluarea finală a riscului nu este determinată de o metodă adiţională. Este determinată printr-o evaluare profesională , asistată de folosirea unei metodologii sistematice şi structurate care foloseşte întregul set de indicatori de risc în cazul extremismul violent. Fiecare indicator de risc este evaluat pe baza unor criterii pre-stabilite şi cuantificabile, un nivel de risc pentru fiecare indicator fiind obţinut în mod individual. Prin urmărirea acestui indicator complet printr-o analiză specifică, informaţia strânsă şi structurată cu punctajele realizate este revizuită şi analizată. O decizie asupra riscului obiectivă şi de încredere este determinată ca urmare a acestei analize şi reevaluări. Prezenţa unui număr limitat de indicatori de risc semnificativi evaluaţi ca fiind moderaţi 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 potenţialului 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 prezenţi şi 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 Securităţii Interne şi Afacerilor Guvernamentale, publicat în februarie 2011 (*O bombă cu ceas*, februarie 2011).

Indicatorul de risc nr. 1: Victimă a nedreptăţii şi nemulţumirilor. Nemulţumirile lui Hasan erau mereu exprimate public colegilor şi supraveghetorilor săi. Acestea aveau legătură cu poziţia SUA, trimiterea de trupe militare americane pe pământ musulman (Afganistan şi Irak) şi considera poziţia Statelor Unite ca una de război împotriva Islamului. El şi-a exprimat de asemenea nemulţumirea faţă de superiorii săi din Armata SUA care nu au reacţionat la nemulţumirile exprimate privind acţiunile oamenilor pe care îi trata şi care se întorseseră din Afganistan. Considera că acţiunile realizate de cei cu care discută cu ocazia şedinţelor clinice ar fi trebuit considerate crime de război.

Indicatorul de risc nr. 2: Indentificarea persoanei, locului sau grupului responsabil pentru nedreptate şi 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 şi 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 şcoala 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 şi că Hasan ar fi trebuit confruntat cu privire la atitudinile sale anti-americane (Passatino şi 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. Deşi Hasan nu era cunoscut ca practicând prozelitismul despre credinţa musulmană printre pacienţii săi şi colegi în cel e-al treilea an la USUHS, un indicator de risc major în mod particular semnificativ era natura atitudinilor şi convingerilor sale. Nu era capabil să facă diferenţa între opiniile sale politice şi 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 şi colegii care participau la aceste prezentări se aşteptau 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 şi a Armatei SUA. În mod specific, o prezentare intitulată „Vederea lumii coranice din prisma musulmanilor din Armata SUA" a evidenţiat elemente prezente în atitudinea şi ideologia sa. Aceasta a fost, de asemenea, un semnal de alarmă omis. Slide-ul 49/50 din prezentare afirmă că „Dumnezeu aşteaptă deplină loialitate", că „Dumnezeu nu acceptă compromisuri" şi că „lupta pentru stabilirea unui Stat Islamic pentru a-l bucura pe Dumnezeu, chiar şi prin folosirea forţei, este tolerată de către Islam". Mai mult, Hasan a afirmat că soldaţii musulmani nu ar trebui să îşi îndeplinească atribuţiile în deplină capacitate, altfel riscă să îi rănească sau să îi ucidă pe credincioşii din rândul Islamului.

Lucrarea ar fi putut fi interpretată cu uşurinţă 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 şi pe terenul de luptă. Această ideologie susţinută de către dovada comportamentală, îl pune pe Hasan în conflict direct şi în opoziţie cu politica SUA. El se află de asemenea în conflict cu activitatea militară stabilită prin lege pe care SUA o desfăşoară.

Din punct de vedere minim, aceşti indicatori solicită o explorare serioasă printr-un protocol al evaluării riscului amănunţit. Hasan, în calitate de cetăţean, avea dreptul şi 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 îşi aminteşte că Hasan le spunea colegilor şi profesorilor săi: „Sunt un musulman înainte de toate şi respect Sharia, Legea islamică, înaintea Constituţiei americane." (Passatino şi Winter, 10 noiembrie 2009).

Indicatorul de risc nr. 4: Contact personal cu extremişti violenţi. Între decembrie 2008 şi iunie 2009, s-a ştiut 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 cunoştea 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 şi carismatic al atacurilor „jihadiste" din Statele Unite, responsabil în acelaşi timp cu recrutarea în cadrul Al-Qaeda. Hasan a fost investigat de către FBI după ce analiştii au interceptat schimbul de email-uri cu Anwar al-Awlaki. Al-Awlaki a apreciat atacul de la Ford Hood şi 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 ştia că investigatorii americani erau conştienţi că Hasan urma să contacteze Al-Qaeda şi că avea alte „legături greu de explicat cu oameni care erau urmăriţi de către FBI" în afară de Anwar al-Awlaki (Raddatz, Ross, Abraham şi El-Buri, 10 noiembrie 2009). Aceştia reprezintă indicatori de risc serioşi.

Evaluarea realizată de D.C. Joint Task Force a arătat că email-urile şi 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 şi 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 uciși într-un atac sinucigaş. Un email specific a fost cunoscut ca fiind problematic în mod particular în ceea ce privește 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 şi a caracteristicilor obişnuite ale agentului. Agenţii în domeniul securităţii şi 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 şi alte organizaţii pot conduce la dezastre semnificative şi cu potenţial catastrofal de natură fizică, umană şi de securitate naţională. Ameninţarea iniţială pe care un individ o reprezintă este dinamică. Este accidental în cazul unuia sau o combinaţie de atitudini şi circumstanţe economice, sociale şi personale. Deoarece ameninţarea internă poate fi identificată şi construită într-un instrument, în timp ce indicatorii pot fi evaluaţi printr-o metodă standardizată şi măsurată cu ajutorul unei metodologii de evaluare structurată profesional.

Aceasta oferă informaţii despre indicatorii de risc individuali, asistând în acelaşi 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 şi 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 şi 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.