RISK ASSESSMENT FOR INSIDER THREAT: CRITICAL INFRASTRUCTURE, MILITARY AND INTELLIGENCE APPLICATIONS

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.

Introduction

Insider threats are a major counterintelligence challenge. Such threats are ubiquitous. They are especially dangerous in the Armed Services, where critical infrastructure is located, in intelligence organizations and in industrial settings where intellectual property requires safeguarding.

Insider threats include acts of espionage, sabotage, terrorism, thefts, embezzlement, unauthorized disclosure of classified information, and other

* Senior Fellow, Canadian Centre for Intelligence and Security Studies, NPSIA, Carleton University, Ottawa and Associate Fellow, International Centre for Counter-Terrorism-The Hague, Netherlands.

malicious and criminal acts untaken by "trusted" personnel (Bronswill and Brewster, 2013)[1]. Insider threats are of special concern because the perpetrators of these acts have been granted access to sensitive equipment, protected files, and security installations. Insiders require vetting. This scrutiny has been undertaken in most cases. Such analyses are flawed or not sufficiently sensitive, if they are not capable of identifying in advance those individuals who present a threat to the organization. Risk assessments should be regularly undertaken on employees with access to secure facilities to determine the status they pose at a given time to the agency.

Individual risk assessment for insider threat refers to the analysis and evaluation of the danger posed by "trusted employees" or "trusted contractors". The risk assessment protocol includes a set of necessary and sufficient conditions pertinent to the specific type of risk which are structured into indicators that can be measured. This provides an evaluation of each of the indicators separately, as well as an overall judgment of risk and threat based on the outcome of the individual indicator evaluation and a weighting of the information available. Information that is not available is highlighted by the presence of empty cells. This missing evidence is taken into consideration in terms of its critical importance to any risk decision and provides useful direction for follow-up information retrieval.

It is this insider risk potential that an agency seeks to mitigate or eliminate. Risk assessment has been developed to evaluate and manage "dangerousness". This danger, when applied to a person rather than a physical, biological or other hazard, is referred to as individual risk assessment. Although the methodology was originally developed in the forensic setting by psychologists interested in predicting recidivism, it has been applied to violent extremism estimations of risk and is appropriate to the individual assessment of insider threat.

Insider threats occur when access is granted to "trusted persons" who abuse the trust and betray the organization that has granted the trusted status. This "trust" has usually followed from some form of an evaluation of the individual's potential risk. The assessment was intended to ascertain the reliability, trustworthiness and loyalty of the insider. In the Military and other government installations, the expert analysis that is undertaken on individuals is often supported by information provided by intelligence agencies, as well as other relevant institutions. The level of trustworthiness, reliability and loyalty

[1]This definition is consistent with that used by the Canadian Security and Intelligence agency (CSIS). See also "The Threat Environment to 2025" – a CSIS Document obtained by the CBC.

awarded to an individual will differ based on the information provided, the positions of the individual and the final evaluation.

The methodology currently applied by analysts and the risk indicators used for individual security scrutiny may not be fully transparent, objective, rigorous and systematic. They may be based on evidence available which is insufficient and on the consideration of this information and the analyst's experience. It has been argued by threat and risk assessment experts that security assessments should employ a structured and comprehensive approach that is reliable, consistent and quantifiable rather than subjective, inconsistent and analyst dependent. Results should be reliable and generate the same outcome when different analysts perform the assessment risk assessments, when a rigorous methodology is used, will include and apply the same comprehensive set of relevant risk indicators in a systematic manner. This will correct for difference in the assessor's level of experience and any bias present. Finally, the methodology will be sufficiently rigorous so as to permit the establishment of quantifiable baselines and repeat measures of risk that can be compared (Pressman, 2009).

In cases of insiders who betray, the "risk" review was either flawed, not sufficiently time sensitive, or there was insufficient ongoing monitoring of the individuals by supervisors. Flawed assessments are often the result of superficial observation due to earlier evaluations indicating "trusted status" or due to the perceptual blindness of supervisors and colleagues. Early identification of these risk indicators can result in timely action related to the mitigation of the individual's risk (Johnston).

Background: Insider Threat in the Armed Forces, Intelligence Agencies: The Role of Law Enforcement. Insider threats are a priority of armed forces and intelligence services in any country (MOSID:00161 and MOSID:00214). Most countries have gone through restructuring of their armed forces and their security and intelligence functions in the past decades often subsequent to government established commissions who have reviewed and recommended changes to their organization and function. Despite multiple re-organizations and policy changes in the past decades, the three fundamental roles of policing, (the peace officer, the intelligence officer and the enforcement officer) remain central to the prevention, mitigation and detection of insider threats. It is the police, in the end, who enforce the law when insider incidents occur. They are users of risk assessment tools and approaches (MOSID:00161 and MOSID:00214).

In a 2013 de-classified Canadian Security and Intelligence Service (CSIS) report, insider threats were identified as a significant and current concern of their intelligence agency (Bronswill and Brewster, 2013). The espionage case of Canadian naval officer Jeffrey Delisle was identified as typifying the danger of the 'insider threat' in the armed forces. In this case of Delisle, the "insider threat" extended well beyond Canada. It involved Canada's allies, and to the intelligence information to which Delisle had access. Delisle was sentenced in 2013 to 20 year imprisonment for his acknowledged multiple acts of insider espionage that had caused damage to Canada, the United States, Australia, The United Kingdom and New Zealand. His actions were described as "severe, irreparable and exceptionally grave" (Bronswill and Brewster, 2013). What is clear is that such insider threats are both serious and credible.

Experts at the FBI have defined insider threats as "authorized users who do unauthorized things for malicious purposes" (Chickowski, March 1, 2013). The insider is a trusted person who may have been loyal and honest for some time and then is recruited by another country or agency to betray his country. Such betrayals are usually due to one or more of three reasons:

(1) There is a change in the individual's values or goals;

(2) There is a perceived breach of trust between the insider and the agency or country involved which causes alienation and justifies the disloyalty in the mind of the subject;

(3) the insider may have been deceptive in his or her intentions from the onset and this was not detected.[2]

The detection of a betrayal by an individual requires an individual-based analysis. The risk assessment requires relevant risk indicators and approaches that can ascertain the values, attitudes, belief systems, ideologies, grievances, friendships, associations, vulnerabilities, intentions and capacities of the individual in question. As the FBI has noted, it is a person-centric problem. It is also important to understand the risk indicators that are present. A comprehensive risk assessment approach should contain both risk promoting and potential risk mitigating elements, in order to be able to take action and try to mitigate this risk. The risk decision is then determined after considering both types of information and all the independent risk variables.

The perpetrators of insider criminal offences are often highly educated and skilled. They frequently hold responsible positions. They usually have normal cognitive function and volitional control of their actions. Such

[2] Personal communication: FBI supervisory special agent on March 3, 2014.

individuals are capable of making rational decisions and changing the nature of their actions over time based on what they consider to be new compelling reasons. As a result, the risk indicators for insider threat have a dynamic component. This differs from tools that use static risk indicators such as sex, age, education, criminal history, childhood abuse and uncontrolled urges and impulsive actions. The presence of mental illnesses should be considered in a risk assessment, but this should be mostly for purposes of screening out of mentally ill employees. For purposes of the risk assessment protocols considered in this document for "insider threat", "insiders" are considered to be inherently "normal "functioning individuals who have chosen to act disloyally or violently, not out of mental illness or compulsions, but as a volitional and rational decision based on identifiable motivations.

Insiders are known to have engaged in espionage, sabotage or other treacherous and treasonous acts out of the lure of money, sex, blackmail, emotional trauma and ideological reasons. Expert reviews of the literature related to multiple cases of insider deception and betrayals have revealed that in almost all cases, the compromised individual exhibited identifiable signs. These signs went unreported for years due to what has been called the unwillingness of colleagues to accept the possibility of treasonous action by their friends or colleagues (*The Insider Threat*). Described in military terms, the adversary who makes a frontal attack is easier to anticipate or turn back with countervailing force than an adversary who attacks from within because this individual is "not so readily anticipated nor defeated by force alone" (Catrantzos, September 2009). Because the adversary is so difficult to anticipate, risk assessments of such individuals are no easy or certain task.

Required Elements for Risk Assessment of Insider Threat

The above suggests that an individual risk assessment for high security clearance should include the following characteristics:

(1) an exploration of relevant attitudes in a robust manner to identify potential deception;

(2) maintenance of an ongoing and regular sequence of dynamic reviews of those engaged in sensitive positions to permit the early identification of dynamic changes in situation or values that could affect loyalty, and

(3) monitoring of status of the individual relative to the organization including disgruntlement, lack of anticipated progress within the organization or other disillusionment with the agency that could be interpreted as breach of trust by the insider.

Individual risk assessments require vigor and comprehensiveness. Criminal background checks, credit reviews, financial status and educational background verification, while useful for selected elements of reliability do not address loyalty issues nor the values and ideologies held by an individual. They also do not account for the dynamic changes that may occur over time in terms of risk elements. Insider risk assessment, by its nature, is multi-dimensional and involves many factors. It is a complex problem and it requires a correspondingly complex analysis of the drivers motivating an individual, an exploration of the moral emotions, attitudes, values, personality characteristics other psycho-social elements and an examination of the associations of the individual. As all crime can be related to motivations that are personal, social, political or economic, so can insider threat be so attributed.

Proactive steps are necessary to detect and mitigate risks that exist before asthey mature into dangerous actions. These proactive steps require the development and implementation of countering insider threat strategies (CIT- strategies). The most fundamental of these is a comprehensive and perceptive risk assessment. The assessment can be followed by a sensitive and targeted intervention to mitigate this risk. This intervention is individualized and objectives can be identified from a distinctive features analysis of the generated risk assessment.[3] The military is particularly vulnerable to catastrophic consequences of insider attacks. This potential for devastating damage is due to the advanced weaponry training of insiders, their ability to strategically plan attacks and their capacity use military assets effectively. Other insiders are in a position to disclose national security secrets. A literature that examines individuals who have perpetrated unlawful and serious insider offences can provide valuable insight into the risk indicators to be included in a sensitive and appropriate risk assessment protocol. Due to purposes of space, only three such examples are presented below.

Insider Case Studies and Lessons Learned

The Insider who Represents a Risk. "Trusted persons" who have access to facilities or assets may not engage in acts of sabotage, espionage nor be perpetrators of violent attacks, but they may permit access to others who do have malicious intent. The individual providing the access may not have

[3] This is a basic clinical assessment model, specifically identification of problems through structured analysis and then targeted intervention to address the identified issues.

malicious intent. Similarly, an unlawful act of disclosing classified information may be unintentional rather than intentional and malicious.

Whether intentional or unintentional, malicious or non-malicious, the act itself is unlawful and the actor is subject to penalty. This was recently demonstrated. On February 7, 2014, Stephen Jin Woo Kim, age 46, was prosecuted for leaking information to the media. He entered a guilty plea and was sentenced to 13 months in prison (Ingram, 7 februarie 2014). Kim is one of only 11 cases in United States history where an individual was prosecuted for an unintended act of leaking information. Kim claimed he had no malicious intent. He did admit to "letting his guard down" which caused a lapse in his conduct.

Kim was a highly respected State Department contractor when he was arrested. He was a deeply embedded "insider" having worked for the Centre for Naval Analysis and the Defense Policy Board. He had been an advisor to both Henry Kissinger and Dick Cheney on issues related to his expertise. He had worked for the Under Secretary of Defense (*Wall Street Journal*, February 7, 2014).

Canada, like the United States and other nations, is not immune to insider threats. One year earlier than the Kim case, Jeffrey Delisle, as identified earlier, was convicted and sentenced to 20 years in prison in February 2013, for selling secrets to the Russians. Patrick Curran, the Chief Judge of the Nova Scotia Provincial Court, commented that Delislehad acted "coldly and rationally" beginning in 2007 (*Globe and Mail*, February 8, 2013). Delisle confessed to betraying his country by providing information from top secret-level computer networks to Russian agents for five years. He had been "risk assessed". In these assessments, he was judged by the officials responsible for this evaluation to be loyal and trustworthy. He had top level security clearance and his position included access to highly sensitive information as an intelligence analyst.

Such risk assessment sare time and situation dependent. Delisle is an example of an individual assessed at one point as reliable and trustworthy and who may have been so at this time but who was clearly not equally reliable and trustworthy at a later time point. Circumstances and behaviors of individuals change as had occurred with Delisle. He made a rational and volitional decision to betray his country.

Individual risk assessments for high level clearance personnel should be undertaken on a frequent and regular basis. The assessment should be standardized to enable a comparison of results at different time intervals. Although such repeated measures are time and human resource intensive,

ongoing monitoring at regular intervals is essential if risk assessments are to be reliable. Although individual assessments of risk may not always deviate over time, any generalization as to the consistency of loyalty and trustworthiness is reckless and imprudent, as well as potentially dangerous. The first risk assessment undertaken will generate baseline data from which other assessments can be compared. The use of quantifiable reliable measures will highlight observed changes. The application of a structured and objective professional judgment of risk will provide continuity.

It is vital that risk assessment protocols use pertinent risk indicators. These indicators include personality, psycho-social factors, values and ideology, political issues of concern, grievances both political and social and economic circumstances. Information on these points of interest are often provided as information lists to assessors rather than as a structured coherent tool that can be administered.

There are important lessons to be learned from a literature review of Canadian and international cases of insiders who have inflicted damage to the security and intelligence capabilities of their nations. These lessons can be summarized as follows:

(1) a requirement exists for a robust individual risk assessment protocol for insider threat;

(2) the protocol should be systematic, criterion based referenced and use an accepted behavioral methodology;

(3) a set of pertinent and comprehensive risk indicators are required;

(4) the risk assessment should be undertaken at regular time intervals and the results that are produced through the reliable methodology for an insider should be compared over the time line used;

(5) in addition to the formal protocol, it is important to obtain as much information as possible on the "insiders", including accessing informal observations, reports, intelligence information, information on personal motivations, values and other accessible information for use during the formal risk assessment protocol.

These recommendations are consistent with FBI insider threat experts who have identified behavioral approaches to risk assessment of insiders as the most promising of all options to identify and mitigate insider threats and who support a person focused multi-dimensional risk assessment for "insiders" (Chickowski, March 1, 2013). Many insiders who have betrayed their countries were active for years before they were identified and arrested. With the current status of computerization and network access to secrets, huge amounts of sensitive information can be obtained from agencies in a

shorter time than ever before. This information can be extracted from the computer networks and removed on portable memory drives with relative ease. The Office of the U.S Counterintelligence Executive noted that the amount of information lost through relatively recent insider threat constitutes more than the sum total of what was previously "given to our enemies throughout U.S. history" (*Insider Threat*).

Recent and serious insider betrayals have supported the urgency for improved security protocols and the use of new and more objective tools to permit detection of insider threats. The major objective of risk assessment is to identify potential risks in order to initiate preventative action to mitigate risk. Most government installations are improving physical security procedures, increasing cyber security and making technical improvements. The added application of new and improved behavioral analysis and individual risk assessment tools will further enhance comprehensive insider threat security provisions.

Case Examples: Espionage, Sabotage, Violence, Unauthorized Disclosure

Case Example 1: Jeffrey Paul Delisle: Navy Insider Espionage. Jeffrey Paul Delisle, a former Sub-Lieutenant in the Royal Canadian Navy, wasin a post at the Trinity Naval Intelligence Fusion- Centre in Halifax, Nova Scotia when he was arrested on charges of espionage which had been ongoing for five years. He had access to the "Stone Ghost" intelligence sharing network database of the Five Eyes used having received "Top Secret Five-Eyes Only" clearance. He passed sensitive information from this network to the GRU, the intelligence branch of the Russian Armed Services. Delisle had walked into the Russian Embassy in Ottawa in July 2007 to volunteer his services. Much of the information passed to the GRU was U.K., U.S. and Australian intelligence information. For Canadian Military Intelligence, he used "SPARTAN", a Department of National Defence network and he was thought to have provided Canadian civilian intelligence reports from CSIS, the RCMP, the PCO, Transport Canada and the Canadian Border Service Agency (CBSA).

Delisle, who was a naval intelligence officer and threat assessment analyst is quoted as saying after his arrest that "we spy on everybody, everybody spies". This was the explanation provided by him for giving the Russians sensitive materials. ``I tried to just give them [the Russians] stuff that shows them that `Hey, we're just paying attention.' (*RCMP full interview with Jeffrey Delisle*)''. He said that much of the information he passed on was from SIGINT (signals intelligence) and not from human sources.

Under interrogation, Delisle admitted passing Russia the information on material originating from Canada, Britain, the United States and Australia. He sent over conversations obtained from electronic surveillance, as well as "contact lists" of intelligence officials. He denied ever giving up undercover spies. At a court in October 2012, Delisle pleaded guilty to breach of trust and two counts of passing secret information to a foreign entity contrary to the Canadian Security of Information Act. On February 8, 2013 he was sentenced to 20 years in penitentiary, minus time already served.

There are lessons to be learned from Delisle's case. First, there should be ongoing assessments and monitoring of the attitudes of those having top secret clearance on an ongoing basis. This should be undertaken from an established baseline at time of onset of the clearance. Delisle's views on SIGINT information became problematic later in time and he is thought to also have become discontented with his position. Second, it is essential to monitor the personal context of those with high clearance to determine the changing vulnerabilities caused by marital, financial, other problems. This was a factor with Delisle. Third, it is necessary to observe and assess the personal characteristics of top clearance personnel to determine personality and behavioral characteristics such as narcissism, lack of compliance with rules, gaming and other addictions. Delisle reported to interrogators that he acted due to the emotional stress caused by the breakdown of his marriage and his wife's affair. Other elements such as his personal views are considered to have contributed to his betrayal decision.

Case Example 2: Robert Philip Hanssen-Insider (FBI) Espionage. Robert Philip Hanssen is a recent and serious case of insider espionage in the United States. Like Jeffrey Delisle, who was discussed previously, Hanssen, who was a FBI Special Agent, was providing significant amounts of sensitive information to the Russians. At the time of his arrest at a park in Vienna, Virginia in 2001, Hanssen was clandestinely placing a package containing highly classified information at a pre-arranged, or "dead drop" site for pick-up by his Russian handlers. Money was the apparent motive and Hanssen had previously received substantial sums of money from the Russians (FBI Press Release on Robert Philip Hanssen case, February 20, 2001).

FBI Director Louis J. Freeh described Hanssen's action as representing "the most serious violations of law and threat to national security" and that insiders in the military and civilian police are guilty of especially egregious"-betrayals of trust" because they are agents sworn to enforce the law and to protect our nation's security. Hanssen minimized his action stating on his arrest that "I could have been a devastating spy, I think, but I didn't want to be

a devastating spy. I wanted to get a little money and to get out of it" (FBI Press Release on Robert Philip Hanssen case, February 20, 2001).

Hanssen was charged and entered a guilty plea to espionage and conspiracy to commit espionage. In 2001 he was sentenced to life in prison without the possibility of parole. The criminal affidavit against Hanssen provided an account of how he first volunteered to furnish highly sensitive documents to KGB intelligence officers assigned to the Soviet embassy in Washington, D.C. He also chronicled the systematic transfer of highly classified national security and counterintelligence information in exchange for diamonds and cash worth more than $600,000 (estimated by other sources to be in the range of $1.4 million).

Hanssen clandestinely left packages for the KGB, and its successor agency, the SVR, at dead drop sites in the Washington area on at least 20 occasions, and caused significant damage by providing the KGB/SVR with over two dozen computer diskettes containing disclosures of over 6,000 pages of important material. He compromised numerous human sources of the U.S. intelligence community and provided Russia with dozens of classified U.S. Government documents, including "Top Secret" and "codeword" documents. He also provided information on what has been described as technical operations of extraordinary importance and value

Hanssen, similar to insiders like Delisle, had direct and legitimate access to voluminous information about sensitive programs and operations. He used his training, expertise and experience as a counterintelligence agent to avoid detection. He kept his identity and place of employment from his Russian handlers and avoided the customary "tradecraft" and travel usually associated with espionage. He was not detected by inside risk assessment, but as a result of other outside information that had been obtained by the government.

Case Example 3: David Sheldon Boon: Army Insider Espionage. David Sheldon Boon joined the U.S. Army when he was 18 years of age and remained in the military for over 20 years until he retired in 1991. He worked as a Signals Intelligence (SIGINT) Analyst of foreign communications. He also produced combat, strategic, and tactical intelligence reports. He had studied Russian at the Army's Defense Language Institute in Monterey, California and in 1985 was assigned as a senior cryptologic traffic analyst to the NSA at Fort Meade. In this position, which he held for three years, he had access to sensitive information about the capabilities and movements of Soviet forces and Soviet tactical nuclear weapons and he produced reports on Soviet Fire Support Operations. He was assigned to a US field station in Germany, Europe,

but before his transfer, he made the decision to become a spy for the Soviet Union and walked into the Soviet Embassy in Washington, D.C. and volunteered to sell classified military documents for cash[4].

Boone made the decision to betray his country in 1988 before he was sent to Germany. His marriage was broken down, he was financially struggling with support payments to his wife and children, he was angry over the "fair' rating received on his NSA performance evaluation and he was irritated at the U.S. legal system and the outcome in his divorce case, which put financial pressure on him. Boone admitted that "I needed money. Plus, well, I was extremely angry".

For between 3 and 7 years until Boone lost his security clearance, he was engaged in espionage activities with a Soviet handler who met with him several times a year. He received payments totaling estimated at more than $60,000. His periodic re-investigation for his security clearance revealed Boone's financial problems and debts and in 1990, his access to classified information was suspended when he lost his top secret clearance due to lack of personal and professional responsibility. He was reassigned to serve at a military hospital where he remained until his retirement in 1991, which put an end to his espionage career and relationship with the KGB. In 1998, Boone was contacted by an undercover FBI officer posing as an agent of the SVR (Russian successor to the KGB) who wanted to re-activate him due to some event that triggered an investigation of him.

Boone traveled to London for two meetings with his "handler" while he was being recorded. He recounted in the meetings in detail how he had volunteered his services to the KGB, and how he had passed highly classified and extremely sensitive national defense information to the Russians over a period of three years. Boone then agreed to resume spying and work with the SVR and accepted a payment of $9,000. Next, he was lured to the U.S. for another meeting with his handler where, on October 10, 1998, he was arrested at the Washington Dulles International Marriott Hotel in Reston, Virginia.

---

[4] Hardcopy from US Attorney's Office, Eastern District of Virginia; regarding David Sheldon Boone dated October 15, 1998 See related court docket: http://jya.com/dsb101498.htm*The Affidavit in Support of Criminal Complaint,Arrest, Warrant, and Search Warrantsfor David Sheldon Boon* provides comprehensive information from the FBI on this case. Available at http://cryptome.org/jya/dsb100998.htm Retrieved March 27, 2014. Information is also available from Department of Energy, Hartford on Boon at the following site http://www.hanford.gov/c.cfm/oci/ci_spy.cfm?dossier=170RetrievedMarch 24, 2014.

Boone was charged with espionage, entered a guilty plea to conspiracy as part of a plea bargain, forfeited $52,000 including his retirement fund and submitted a hand-held scanner he used to copy documents. On February 26, 1999, he was sentenced to over 24 years in prison (Davis, 1999).

Case Example 4: Theresa Squillacote-Pentagon Insider Espionage. Theresa Marie Squillacote, age 42, a Pentagon lawyer, was arrested and charged with spying for East Germany and Russia on October 4, 1997. She was arrested with her husband Kurt Stand, age 45, who was a left-wing labor activist and James Michael Clark, who was a private investigator. Clark entered a plea of guilty and was a prosecution witness against Squillacote and Kurt Strand. All three had been active in the Communist Party's Youth Movement at the University of Wisconsin in the 1970's. Squillacote and her husband were convicted in October 1998 of conspiracy to commit espionage, attempted espionage and related charges having relation to classified documents. Squillacote was sentenced in January 1999 to 21 years and 10 months and Kurt Stand was sentenced to 17 years and 6 months (*CBS news*).

Squillacote had graduated from Catholic Law School in Washington, D.C. and obtained a job at the National Labor relations Board, followed by the House Armed Services Committee as a staff attorney and finally a position at the Pentagon. It is believed that Squillacote's husband began his espionage activities in approximately 1972 and he recruited her approximately in 1980 when they were married. The espionage activities of Squillacote and the others were documented in STASI files obtained by the CIA after East Germany's collapse and after five years of inter-agency fighting, finally were released to the FBI. After the collapse of the Soviet Bloc, in June 1996, Squillacote sent a letter to a South African Official and Communist Party leader indicating that she had no admiration for bourgeois parliamentary democracy and suggested a working relationship. The letter was forwarded to the FBI. Squillacote was subsequently caught in an FBI sting operation in which she passed sensitive Defense Department documents to an undercover FBI agent. Her former associate Clarke testified against her that he had passed documents to an East German spy, Lothar Ziemer with whom Squillacote and Stand were alleged to have worked. The case and especially Squillacote did not receive much attention, but it has generated some controversy because of the nature of the evidence and the sting operation.

The case does underscore the need for relevant risk assessments which differentiate the "freedom" one has under the laws of a State to hold a political viewpoint that departs from the norm, from an assessment of the risk

which holding these views might represent in some circumstances and positions. A security clearance at a high level should assess this risk despite the freedoms and protections that exist to hold them. It also identifies the potential role of psycho-social factors in risk assessment[5].

Squillacote was a senior procurement analyst in the Office of the Deputy Under-Secretary of Defence for Acquisition Reform and had high-level clearances until she was arrested. She had never concealed her political views or her associations. She married the son of an open and active Communist. She traveled regularly through the Soviet Bloc. She named her children after German Communist "martyrs". Despite this history and her views she was able to secure a post as a staff attorney in the House Armed Services Committee during the Cold War and went on to work in the Pentagon after receiving a higher security clearance level. Squillacote is reported to have told an undercover FBI agent that she "turned to spying to support the progressive anti-imperialist movement". Squillacote's action was "Defence Department Insider Espionage". This case reflects an ideological motive with the potential involvement of psychological vulnerability.

Case Example 5: Nidal Hasan: Army Insider Violent Acts (Terrorism/Violent Extremism). On November 5, 2009 at 1:34 p.m., Nidal Malik Hasan, an American citizen and United States Army Medical Corps Officer, walked into the Soldier Readiness Center of Fort Hood in Killeen Texas, and fatally shot 13 people and injured 32 others. He used a semi-automatic Five-Seven pistol. Hasan was born in Arlington, Virginia September 8 1970, was 39 years old and was a United States Army psychiatrist. He readily admitted to the killings. There was controversy as to whether Hasan's act which was ideologically motivated was an act of "terrorism", or "workplace violence". He was tried on 13 counts of pre-meditated murder and 32 counts of attempted murder and convicted by a panel of 13 military officers on all counts (*A Ticking Time Bomb*, February 2011).

Investigators in the FBI and U.S. Army have determined that Hasan acted alone. His trial was delayed for a variety of procedural and representational issues. On June 3, 2013, a military judge allowed Hasan to represent himself at his murder trial. During the first day of the trial on August 6, 2013, Hasan admitted that he was the gunman during the Fort

[5]See a discussion in the American Psychological Association Monitor of the monitoring of conversations between Squillacote and her psychotherapist and the role of psychological profiling. Retrieved March 28, 2014. http://www.apa.org/monitor/julaug02/jn.aspx.

Hood shootings. He also told the panel hearing that he had "switched sides" and regarded himself as a Mujahedeen waging "jihad" against the United States. He justified his actions by claiming that the US military was at war with Islam. Hasan had communicated to medical health experts assessing him in 2010 that he "would still be a martyr" if convicted and executed by the US government. Hasan did not call any witnesses in his trial consistent with his admission and strong ideological position that his action was justified. He was sentenced to the death penalty on 28 August, 2013. The sentence is under appeal.

Hasan was the child of Palestinians who immigrated to the US from the West Bank. He joined the United States Army after high school graduation in 1988 and served eight years as an enlisted soldier while attending college. He graduated from Virginia Tech in 1997 with a Bachelor's degree in biochemistry and then studied medicine at the Uniformed Services University of the Health Sciences (USUHS), graduating in 2003. He followed this training with an internship and then a residency in psychiatry at the Walter Reed Army Medical Centre and obtained his psychiatry accreditation in 2007. This was followed by a further Master's Degree in Public Health at USUHS with a two-year fellowship in Disaster and Preventive Psychiatry at the Center for Traumatic Stress at USUHS. He completed this training in 2009. He was promoted the same year from captain to major.

There have been several government investigations into the Fort Hood Insider shooting. These have identified missed red flags in Hasan's case. The most salient question in relation to insider threat assessment highlighted by this case was the evident failure to identify the risk that Nidal Hasan represented. Either incorrect risk indicators were used in the risk assessment for Hasan for violent extremism, or no formalized and comprehensive risk assessment was undertaken. Many risk indicators relevant to the risk of violent extremism were present.

The risk indicators in the VERA 2 (Violent Extremism Risk Assessment-Revised Version) can be explored in terms of their relevance to Nidal Hasan and the information that they would have been able to provide to assist the identification of potential insider threat. To be considered a significant risk (moderate to high) level for violent extremism, all of the risk indicators in the tool do not need to be documented as present and evaluated at a high level. All of the indicators are considered and rated if information is available, and if information is missing, this identifies information to attempt to obtain for assessment. The final risk judgment is not determined by an additive method. It is determined by professional judgment that assisted by

the use of a structured and systematic methodology applying the comprehensive set of risk indicators for violent extremism (in this case). Each risk indicator is evaluated on the basis of pre-established and quantifiable criteria and a risk level for each of the indicators individually is obtained. Following this comprehensive indicator by indicator analysis, the information collected and structured with the ratings produced are reviewed and analyzed. An objective and reliable risk decision is determined following this analysis and review. The presence of a limited number of significant risk indicators assessed at a moderate to high level on the VERA 2 (Risk Assessment of Violent Extremism) is sufficient to arrive at a risk assessment that identifies serious concern as to the danger or potential hazard posed by the individual. In the case of Nidal Hasan, the red flags were present.

The VERA 2 indicators that would have clearly documented insider danger are listed and described below. The evidence for the analysis below is available in the report on the Fort Hood Shooting undertaken by the U.S. Senate Committee on Homeland Security and Governmental Affairs and released in February 2011 (*A Ticking Time Bomb*).

Risk Indicator 1: Victim of injustice and grievances. Hasan's grievances were often stated publically by him to colleagues and supervisors. They related to the U.S. position, the U.S. military deployment in Muslim lands (Afghanistan and Iraq) and he saw the U.S. position as a war against Islam. He also had expressed his grievance against his supervisors in the U.S. Military who did not react to his complaints concerning the actions of men he was treating and who had returned from Afghanistan. He thought their actions that they had discussed with him in clinical sessions should have been considered war crimes.

Risk Indicator 2: Identification of the person, place, or group responsible for the injustice or grievance. Hasan had openly identified the source of his grievances which was the U.S. Military. He made critical remarks to colleagues as evidence of this viewpoint and was known to have made anti-American remarks in his lectures prior to the shooting. Some of these remarks were reported to supervisors. Val Finnell, a former medical school classmate is reported to have complained to superiors about Hasan's "anti-American rants". He commented that the "system" was not doing what it was supposed to do and that Hasan should have been confronted about his anti-American views (Passatino and Winter, November 10, 2009).

Risk indicator 3: Commitment to an ideology justifying violence based on a higher authority rather than the jurisprudence of the nation. Although Hasan was disciplined for proselytizing about his Muslim faith with

patients and colleagues in his third year at the Uniformed Services University of the Health Sciences (USUHS), particularly significant as a risk indicator of a high level was the nature of his attitudes and beliefs. He was unable to differentiate his professional and political views and his ideological position was observed to be the primary driver of his worldview much before the attack on November 5, 2009. Hasan was required to give medical lectures as part of his responsibilities. Students and colleagues attending these presentations expected them to be related to medical issues, but they were often a denunciation of infidels.

It had been documented in a slide presentation to U.S. Army Physicians at the Walter Reed Army Medical Centre during his senior year of Psychiatric residency that his views were in opposition to those of the U.S. government and the U.S. military. Specifically, one presentation entitled "*The Quranic World View As It Relates to Muslims in the U.S. Military"* specified elements of his attitudes and ideology. This was a missed red flag. Slide 49/50 of this presentation asserted that "*God expects full loyalty*", that "*God is not compromising"* and that "fighting to establish an Islamic State to please God, even by force, is condoned by Islam". Further Hasan asserted that Muslim soldiers should not serve in any capacity that renders them at risk to hurting or killing believers in Islam.

This presentation could reasonably have been interpreted to suggest that:

(1) Hasan's primary loyalty was to God rather than to the U.S. military or the United States;

(2) that Hasan believed that the Taliban were correct and morally justified in fighting for an Islamic State in Afghanistan;

(3) that the use of force by "America's enemy" in Afghanistan is religiously sanctioned by God;

(4) that American Muslims cannot fight in any Muslim land due to the risk of hurting or killing other Muslims, even on the battle field. This ideology, supported by behavioral evidence, puts Hasan in direct conflict and opposition to U.S. policy. It also puts him in conflict with legally sanctioned military action taken by the United States.

At a minimum, these indicators required serious exploration in a comprehensive risk assessment protocol. Hasan, as a citizen, had the rights and freedoms to hold his religious beliefs, but as Dr. Finnell has pointed out, when you are in the military you have sworn to defend your country from its identified enemies. Finnell recalled Hasan telling classmates and professors that "I'm a Muslim first and I hold the Shariah, the Islamic Law, before the United States Constitution"(Passatino and Winter, November 10, 2009).

Risk Indicator 4: Personal Contact with Violent Extremists: BetweenDecember 2008 and June 2009, Hasan was known to be in personal contact with Anwar al-Awlaki, who was a violent extremist. As a single risk indicator noted, this would be considered extremely significant in terms of weighing potential risk. Hasan was known by the U.S. government to be in email contact with al-Awlaki, a virulent anti-American ideologue on 18-20 occasions. Al-Awlaki (now deceased as a result of an American attack) was an influential and charismatic promoter of "jihad" attacks in the United States, and a known and prominent Al-Qaeda recruiter. Hasan was investigated by the FBI after U.S. intelligence analysts intercepted the e-mails between him and Anwar al-Awlaki. Al-Awlaki praised the Fort Hood attack and is quoted as reporting that rather than convincing Hasan to engage in violence, Hasan was providing justification to him. It has been reported that U.S. investigators were aware that Hasan had also attempted to contact Al Qaeda and that he had other "unexplained connections to people being tracked by the FBI" in addition to Anwar al-Awlaki (Raddatz, Ross, Abraham and El-Buri, November 10, 2009). These are serious risk indicators.

The assessment by the D.C. Joint Task Force was that the emails and other material did not call for a larger investigation. Defense Department officials said they were not notified of these investigations before the shootings (Raddatz, Ross, Abraham and El-Buri, November 10, 2009). It is difficult to comprehend how a decision for no follow-up was reached considering the importance of this risk indicator alone for potential acts of violent extremism. The dynamic nature of the radicalization process could have justified ongoing monitoring. As former CIA officer Bruce Riedel has stated "emailing a known al-Qaeda sympathizer should have set off alarm bells" and "even if he was exchanging recipes, the bureau should have put out an alert"(Examiner, 2002).

Risk Indicator 5: Seeker, Consumer of Violent Extremist Materials It is known that Hasan was visiting radical Islamist websites. Although the full extent of this cyber behaviour was determined after Hasan's computer was examined which occurred after the shootings, any investigation based on the previous risk indicators would have uncovered these internet searches and Hasan's cyber behavior before the attack.

Risk Indicator 6: Feelings of Persecution, Alienation, and Isolation Hasan had been described by colleagues as withdrawn, socially isolated and stressed by his work. This stress was augmented by his work with returning soldiers. There is some suggestion that Hasan may have felt some religious harassment in the military and that he became alienated. He was considered

to be unassuming, brooding and socially awkward (*A Ticking Time Bomb*, February 2011). He was never known to have had a girlfriend. After the fatal shooting of two recruiters at the Army recruiting centre in Little Rock, Arkansas by Abdulhakim Mujahid Muhammad, who later claimed to be an Al Qaeda terrorist, Hasan was described as upset that the perpetrator was being charged with murder.

Risk Indicator 7: Early Exposure to Pro-Violence Militant Ideology. It is known that Hasan came from a Palestinian family that had left the West Bank area when they immigrated to the United States. Although the family's immigration was prior to Nidal Hasan's birth and he appeared to have led a normal American life, the views of his family members, associates and others with whom he may have been in contact during his childhood and youth should have been explored in a risk assessment. This exploration would have included those suggesting the legitimacy of militant action against the U.S. and other states that supported perceived anti-Muslim policies or the State of Israel. A risk assessment of Hasan should also have highlighted his prior exposure to al-Awlaki at the Dar al Hijrah Mosque in Northern Virginia where al-Awlaki was the Iman from January 2001 to April 2002. Hasan may have been influenced at a vulnerable time by al-Awlaki after his Mother's death or by "incipient radicalization" in his youth which progressed as he matured.

Risk Indicator 8: Willingness to die for Cause or Martyrdom. The willingness to consider the act of martyrdom or dying for one cause is an important risk indicator for violent extremism. This indicator also explores "suicide bombing" in terms of the subject's views of engaging in such an act. Elements pertaining to one's potential willingness to engage in or justify acts of martyrdom are also explored in this indicator. In theemails intercepted by U.S. officials from Hasan to Al-Awlaki, Hasan apparently wrote that "I can't wait to join you in the afterlife" and he asked al-Awlaki when *jihad* is appropriate, and whether it is permissible if innocents are killed in a suicide attack. One specific email was known to be particularly problematic in terms of the justification of suicide bombing and martyrdom. In the months before the shooting, Hasan is known to have increased his contacts with al-Awlaki which itself would raise red flags about Hasan and would support the behavioral evidence of a dangerous change in risk level. Hasan,during his trial in his trial, was open about his view that he will be be a martyr even if executed by the U.S. government.

Risk Indicator 9: Glorification of Violent Action. Hasan had come to the attention of federal authorities at least six months before the attacks

because of internet postings he appeared to have made discussing suicide bombings and other threats (CBS News, November 5, 2009). Authorities had not definitively tied these postings to him although they were made in the name of 'NidalHasan". The postings likened a suicide bomber to a soldier who throws himself on a grenade to save his colleagues, and sacrifices his life for a "more noble cause" and "is an act not despised by Islam but is rather to be considered a strategic victory". No investigation was opened. This indicator relates to the risk element that the subject may be or is motivated by the "glorification of violent action. This ties an action to a perceived noble cause which can be justified or that support a higher authority such as a directive of God.

Risk Indicator 10: Planning and preparing Unlawful Violent Action. Hasan, due to his military training had the capacity to use weapons and to plan and prepare an attack. He also had sufficient resources and organizational skills to plan an attack. This indicator would apply to most "trusted insiders" in the military. As a result, intention is a critical element in the risk analysis of military personnel.

These 10 indicators represent a moderately high to high risk rating for Hasan. They correspond to approximately 50 percent of the included risk indicators in the VERA 2 in addition to indicators exploring the motivational typology and the protective factors. The information available on these identified indicators would have generated enough red flags to identify Hasan as anrelatively high risk as an insider threat to the military prior to the attack. This rating would have ensured closer monitoring of Hasan and may have provided an opportunity for action related to the mitigation of his risk or preventive action. Although there is uncertainty in any risk assessment involving violent extremism, there is valuable systematic baseline information that can be obtained from an objective and transparent protocol. This can not only identify potential risks, but also initiate actions that are aimed at mitigating these risks.

Lessons Learned from Insider Cases

Risk Indicators for estimating "insider threat" can be extracted from an examination of these illustrative cases. The risk elements relate to economic, political, social and personal factors. Economic risk indicators are known to be a powerful motivating driver for many insider betrayals so any risk assessment approach for insider threat must include elements that evaluate the financial situation of subjects. In addition, psycho-social aspects of the financial circumstance should be examined. These are the elements of interaction between the personal, social and economic factors. This can relate

to the unmet expectations and wants of an individual in addition to the actual debts and financial status of the individual. In addition, economic factors may be affected by other personal stresses such as divorce, financial demands of children or wives, and vulnerable behaviors (addictions to gambling, alcohol, drugs). Personal risk factors relate to personality factors and include self-importance, narcissism and emotional instability, aggression and alienation. Social factors may relate to grievances related to the social environment such as perceived discrimination due to race, religion, social values or anticipated benefits or social classifications. Political factors relate to the political ideology and attitudes of the subject, the political positions that have been taken by the government, and the legal structures that affect political will.

Risk assessment tools, in order to provide applicable and useful results, must employ indicators that are specifically relevant to the type of risk assessed (Pressman and Flockton, 2012). As a result, it is recommended that a specific tool for risk assessment be developed pertinent to insider threat. This tool will include a comprehensive set of risk indicators identified from the lessons learned from the analysis of known cases. These risk indicators also address criminality in general. The risk indicators will be organized into a structured professional judgment protocol in a like manner to the VERA 2 risk assessment protocol (Pressman and Flockton, 2012), discussed earlier in this paper. However, unlike the VERA 2, the risk indicators will be broader than those related to violent extremism alone.

Risk Assessment Tool Development for of Insider Threat

Conceptual Overview. The lessons learned from the analysis of the various types of insider cases can be applied to the characteristics required for the development of a relevant risk assessment tool. Such a tool would have to apply to all the cases presented above and be sensitive to estimating the risk of individual insiders. The VERA-2, a risk assessment tool for violent extremists will apply to some ideologically motivated insiders who present a threat to agencies. However, none of the indicators in the VERA-2 tool are related to the economic motivations seen in many espionage cases, such as those identified and discussed in the previous section of this report. There are also no indicators in the VERA-2 that are relevant to troublesome and potentially indicative personality indicators such as narcissism, lack of compliance with rules; non-acceptance of the military culture, rejection of military values, job satisfaction; disgruntlement with job advancement and personal vulnerabilities. There are no indicators pertinent to addictions such as drug, gambling or alcohol or other personal problems that require

consideration in insider threat. It is advisable, therefore, that a risk assessment tool be developed specifically pertinent to the unlawful insider betrayals. The VERA-2 should be used in cases where ideological motivation is present and there are potential risks for violent extremism. In other cases of insider threat, the risk assessment of individuals should be undertaken with the tool developed for this purpose. Such a tool was developed for this purpose and is presented here. Details of the tool's user guidelines are available from the author. This tool, referred to as the RAIT (Risk Assessment for Insider Threat) will include the elements identified from the literature and case study reviews. The specific indicators are identified below. Specific rating guidelines are available under separate cover.

The Risk Assessment Tool for Insider Threat (RAIT). The RAIT tool is a structured professional judgment tool that uses the same systematic and reliable methodology as used in the VERA-2 risk assessment protocol. Reports from users of the VERA-2 have reported that this consistent and systematic methodology has been beneficial for security and intelligence applications. Reports from professionals on four continents over the past five years (including police, intelligence analysts, psychologists, psychiatrists and lawyers have supported the efficacy and relevance of this tool.) The RAIT uses the same behavioral method, but include specifically pertinent risk indicators for insider threat.

The RAIT uses 25 discrete risk indicators, each of which will be rated on a 3 point scale (extendable to a 5 point scale). The risk indicators are divided into four categories that are appropriate to unlawful insider action drivers. These are (1) political, (2) social, (3) economic and (4) personal motivations. In some cases, the actor may be motivated by more than one of these elements. According to FBI expert opinion, these four motivations account for the motivations of all criminal acts.[6]

The risk indicators extracted from the literature on insider threat and from the analysis undertaken on known cases were organized into a structured professional judgment (SPJ) protocol in a manner consistent with other SPJ tools. Criterion-based ratings for each of the risk indicators are consulted to establish a risk levels for each of the indicators. The risk factors are intended to be comprehensive. They apply to insiders engaged in

[6] This model of criminal motivation is based on personal discussion and collaboration with an FBI expert in insider threat at the FBI Critical Incidents Response Group and the FBI Academy at Quantico, VA.

espionage, sabotage, unauthorized disclosure, violent extremism, theft and other insider offences. The indicators incorporate risk and risk mitigating elements. A preliminary RAIT manual with user instructions is available from the author.

RAIT Consultative Risk Assessment Indicators (N=25)

A. POLITICAL FACTORS –ATTITUDES AND VALUES

A1. Political/ideological/religious causes have priority over national laws and military
A2. Perceives political injustice at home and/or abroad, other perceived grievances
A3. Rejects selective societal values
A4. Identity conflict related to political views and military values
A5. Anger at political decisions and actions of country/military
A6. Family living abroad in non-democratic/conflict zone areas

S. SOCIAL FACTORS

S1. Perceives self, group as victim of social injustice
S2. Believes specific race, religion, culture superior to all others
S3. Personal contact with extremists, unlawful violent actors (gang members, criminals)
S4. Prior criminal history/violence
S5. Prior paramilitary training, experience with weapons
S6. Lack of compliance with social/cultural code, military rules

P. PERSONAL FACTORS AND BEHAVIOR

P.1 Exhibits personal aggression, hostility, moral anger
P.2 Exhibits narcissism, self-importance
P.3 Under personal stress (divorce, conflicts, children)
P.4 Unhappy in job assignment
P.5 Exhibits mental instability, personality problems, behavioral disorders
P.6 Frustrations in personal life (relationships, friendships)

E. ECONOMIC FACTORS AND FINANCIAL GAIN

E1. Financial expectations unsatisfied in career
E2. Disgruntled with career advancement
E3. Financial problems
E4.Specific Addictions: gambling, alcohol, drugs, sex

M. MITIGATING-PROTECTIVE ITEMS

M.1 Compliance, participation counseling for personal stress, financial issues
M.2 Courses taken to support career advancement
M.3 Modification of views and grievances, more flexibility in attitudes

Each of these indicators is rated by a criterion-referenced definitional guide and an overall risk judgment is made. This judgment may recommend additional monitoring, interviews, follow-up or intervention.

Conclusions

Insider threat is ubiquitous. Identifying this risk is difficult and replete with challenges. This is in part due to the intentional deception of the perpetrator and the normal characteristics of the agent. Trusted agents in security and intelligence sensitive positions can and do change over time in the potential risk they represent. Insiders who are fiercely loyal at one time may choose to betray in another time period. Such betrayers of government, military or other organizations can cause significant and potentially catastrophic physical, human, economic or national security damage. The insider threat that an individual can pose is dynamic. It is contingent on one or a combination of political, economic, social and personal elements, attitudes and circumstances. For insider threat can be identified and constructed into a tool whereby each of the indicators can be assessed in a standardized method and measured in a structured professional judgment methodology. This provides information on the individual indicators or risk, as well as assisting the judgment of the assessor in an overall risk judgment. A tool for this purpose, referred to as the Risk Assessment for Insider Threat (RAIT) has been developed.

References:

1. Bronswill, Jim, Brewster, Murray, (September 19, 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, (March 1, 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 (September 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 declarație 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, (October 23, 1998), accesibil pe http://www.cbsnews.com/news/couple-found-guilty-of-spying/.
7. *CBS News*, (November 5, 2009), accesibil pe http://www.cbsnews.com/news/sources-hasan-web-posts-drew-fbi-interest/.
8. Davis, Patricia, (February 27, 1999), *Ex-NSA worker get 24 years for spying*, în The *Washington Post*, accesibil pe http://www.jonathaqnpollard.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* (February 8, 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, (February 7, 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 Poliției Militare Canadiene accesibile pe http://www.forces.gc.ca/en/about-policies-standards-medical-occupations/mosid161-military-police.page.
14. *O bombă cu ceas*, (February 2011), Raport al Comisiei pentru Securitate Internă și Afaceri Guvernamentale din cadrul SenatuluiStatelor Unite, accesibil pe http://www.hsgac.senate.gov//imo/media/doc/Fort_Hood/FortHoodReport.pdf?attempt=2.
15. Passatino, Jonathan, Winter, Jana, (November 10, 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. (November 10, 2009), *Raport pe ABC News*, accesibil pe http://abcnews.go.com/Blotter/official-nidal-hasan-unexplained-connections/story?id=9048590.

19. *RCMP full interview with Jeffrey Delisle,* accesibil pe https://archive.org/stream/564122-jeffrey-paul-delisle-rcmp-interview/564122-jeffrey-paul-delisle-rcmp-interview_djvu.txt.
20. U.S. Counterintelligence Executive, "Insider Threat" http://www.ncix.gov/issues/ithreat/Retrieved March 24, 2014.
21. *Wall Street Journal*, (February 7, 2014), *Devlin Barrett, Former State Department Contractor Pleads guilty in leak Case*, accesibil pe http://online.wsj.com/news/articles/SB10001424052702304450904579369153970706392.