This paper describes objective technical results and analysis. Any subjective views or opinions that might be expressed in the paper do not necessarily represent the views of the U.S. Department of Energy or the United States Government.

SAND2019-7140C

Preliminary Results from a Comparative Analysis of Counterintelligence and Insider Threat Mitigation in Nuclear Facilities

Noelle J. Camp & Adam D. Williams
Sandia National Laboratories, Albuquerque, NM, USA, [ncamp; adwilli]@sandia.gov*

Abstract

The threat of an insider with knowledge, access and authority remains one of the most pressing challenges to security within nuclear facilities. Insiders, witting or unwitting, working together or alone, possess the opportunity to enact grave damage to nuclear facilities through sabotage or unauthorized removal of nuclear material. However, the relative lack of insider case studies in the public domain makes identifying causal patterns and proposing effective protection/mitigation efforts difficult. To address this challenge, some scholars and practitioners interested in insider threat have leveraged lessons from other disciplines. Prominent contributions to insider threat literature have included case studies from high value jewelry heists and analyses of security measures within the casino and pharmaceutical industries.

Despite the conceptual and practice similarities, the existing literature has thus far failed to assess the potential applications of counterintelligence theory for insider threat within nuclear facilities. Counterintelligence, defined by United States Executive Order 12333 as "information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations," provides a useful corollary to insider threat. Both programs seek to protect high-value targets from human vulnerabilities. Further, the high security atmosphere of the Intelligence Community more closely approximates the uniquely protected environment of a nuclear facility.

This paper outlines how counterintelligence and nuclear insider threat will be compared, including the analytical rubric for evaluating program goals, perpetrator characteristics, and protection/mitigation efforts. This paper also introduces the fundamentals of contemporary U.S. counterintelligence practice, including background investigations, mandatory reporting requirements, and the use of counterintelligence indicators for investigative purposes. Using counterintelligence case studies from the past several decades in the United States, the paper explains how motivations and characteristics of prominent spies potentially applicable to insider threat analysis. Lastly, this paper will provide early insights from this comparative analysis, including discussing impacts for potentially improving insider threat programs at nuclear facilities across the globe.

Introduction

The threat of an insider remains one of the most pressing challenges to security within nuclear facilities.[1] Insiders, witting or unwitting, working together or alone, possess the opportunity to enact grave damage to nuclear facilities through sabotage or unauthorized removal of nuclear material. Yet effectively mitigating insider threat is extremely challenging. Insiders possess access, authority, and knowledge which can be leveraged to thwart physical protection systems designed to stop external adversaries. Insiders' access to a facility and/or sensitive material offers more opportunity to select a target and test protective measures at a facility, as well as more time to carry out potential theft or

[1] While *insider threat* "refers to one or more individuals with authorized access to critical facilities, materials, or information who could attempt unauthorized removal or sabotage or who could aid in an external adversary to do so" [Williams, A.D., S.N. Abbott, and A.C. Littlefield (2019) "Insider threat," In: Shapiro L., Maras MH. (eds) *Encyclopedia of Security and Emergency Management*. Springer, Cham.] for any facility, in this paper we focus on insider threats to nuclear facilities.

* SAND2010-XXXX. Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC., a wholly owned subsidiary of Honeywell International, Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

sabotage missions. Additionally, as trusted members of the workforce, insiders tend to fall under less suspicion of committing a malicious act.[2]

The primary objective of insider threat mitigation for nuclear facilities is to protect sensitive nuclear material. As such, the logic of insider threat mitigation suggests that if a facility is concerned about someone with authorized access maliciously acting against it, then all efforts should be taken to reduce the opportunity for malicious activity to occur. Current approaches to insider threat mitigation primarily focus on characteristics of individuals and seek to (1) reduce the number of individuals with authorized access and (2) make it as difficult as possible for an individual to act on malicious intentions.

According to the International Atomic Energy Agency's (IAEA) guidance, nuclear facilities should implement both "protective" and "preventive" measures to address the insider threat. Preventive measures include "measures to preclude or remove possible insider threats," such as assessments of employee trustworthiness and escort and surveillance of infrequent workers and visitors. Protective measures encompass "measures to detect, delay, and respond to malicious acts … and to mitigate or minimize their consequences." Ultimately, the IAEA encourages a "comprehensive approach" that incorporates both administrative and technical barriers—both *preventively* and *protectively*—for insiders to overcome in order to carry out a malicious act.[3]

Improving insider threat analysis and mitigation is particularly difficult in the nuclear industry due to the lack of publicly available information about and lessons learned from past cases. There are few cases of nuclear theft and sabotage in the public domain for industry professionals to draw from. In some cases, such as the 2014 sabotage of Doel 4 Nuclear Power Plant in Belgium, investigators were unable to identify a perpetrator, significantly limiting potential insights.[4] Other cases, like the 1979 theft of uranium oxide at a GE Nuclear Power Plant, feature unclear motives or missing details.[5]

Additionally, while many forums exist for information sharing within the nuclear safety industry, there is no comparable mechanism for practitioners of nuclear security to discuss incidents and lessons learned.[6] Nuclear facilities may be hesitant to disclose security incidents due to the potential for embarrassment or loss of reputation and public confidence. Further, a historical focus on external rather than internal actors has limited the attention paid to insider threat within the nuclear security community. These challenges prevent nuclear security professionals from effectively leveraging lessons learned from historical insider cases and present a high risk of repeating past mistakes.

Insider Lessons from Other Industries

The lack of publicly available case studies of insider threat incidents within nuclear facilities has led members of the nuclear security community to seek insights from other industries. In a 2013 study[7], researchers from Harvard University's *Project on Managing the Atom* proposed recommendations for nuclear facilities based on insider threat best practices within the high-security casino and pharmaceutical industries. This study also identified a six-part framework for evaluating insider threat mitigation programs.

---

[2] International Atomic Energy Agency, *Preventive and Protective Measures against Insider Threat: Implementing Guide*, Security Series No. 8 (Vienna: IAEA, 2008), 6-7.

[3] Ibid., 10

[4] Noah Pope and Christopher Hobbs, *Insider Threat Case Studies at Radiological and Nuclear Facilities*, Los Alamos National Laboratory, 2015, LA-UR-15-22642, 65.

[5] Ibid., 16

[6] Matthew Bunn and Scott D. Sagan, *A Worst Practices Guide to Insider Threats, Lessons from Past Mistakes* (Cambridge, Mass.: American Academy of Arts and Sciences, 2014), 2.

[7] Matthew Bunn and Kathryn Glynn, "Preventing Insider Theft: Lessons from the Casino and Pharmaceutical Industries," *Journal of Nuclear Materials Management* 41, 3 (2013): 4-16.

Drawing from structured interviews based on this framework with security managers at casino and pharmaceutical facilities and a review of relevant literature, this study offered nine potential recommendations for the nuclear industry ranging from employing constant video surveillance to strengthening employee buy-in.[8] While the authors recognized that key similarities exist, they clearly acknowledge that the for-profit-based attitude in casinos and pharmaceutical companies that preventing small thefts may not be cost effective is *not* a realistic assumption in nuclear facilities. Despite this difference, this study concluded that "the use of some or all of these practices from the casino and pharmaceutical industries may help the nuclear industry reduce the risks of insider theft."[9]

Similarly, a 2015 study from Sandia National Laboratories[10] examined lessons for protecting critical assets from 23 attempted and successful high-value heists. The authors conducted analysis of the heists in seven categories: 1) defeated security measures and devices, 2) deception methods, 3) timing and target selection, 4) weapons employed, 5) resources and risk acceptance, 6) insiders, and 7) failures and mistakes. This study offered several lessons directly applicable to insider threat, noting that insiders "almost always" played a role in the identification and exploitation of facility vulnerabilities and that multiple insiders, unwillingly or willingly colluding, were "not uncommon" within the heist dataset.[11] In the 23 heists studied, unwilling participants in the form of coerced, active, nonviolent insiders represented the most common inside help available to heist orchestrators.[12] The authors proposed future work on the insider question, including a more extensive categorization of insiders clearly defining at what point an "outsider" becomes an "insider."[13]

Related to these types of studies is the 2014 "Worst Practices Guide to Insider Threat" sponsored by the American Academy of Arts & Sciences.[14] This work provided a summarized list of ten lessons for nuclear insider threat practitioners drawing on diverse case studies including bank robberies, terrorist attacks, and information technology sabotage. The ten lessons outlined in the study are:

- Don't assume that serious insider problems are *not in my organization* (NIMO)
- Don't assume that background checks will solve the insider problem
- Don't assume that red flags will be read properly
- Don't assume that insider conspiracies are impossible
- Don't rely on single protection measures
- Don't assume that organizational culture and employee disgruntlement don't matter
- Don't forget that insiders may know about security measures and how to work around them
- Don't assume that security rules are followed
- Don't assume that only consciously malicious insider actions matter
- Don't focus only on prevention and miss opportunities for mitigation

Many of the case studies referenced in this work appear in more depth in the 2017 book *Insider Threats*.

Insights from Counterintelligence Theory

Despite similarities in concept and practice, the existing literature has thus far failed to assess the potential applications of counterintelligence theory for insider threat within nuclear facilities. The

[8] Ibid., 4
[9] Ibid., 15
[10] Jarret M. Lafleur et. al., *The Perfect Heist: Recipes from Around the World*, Sandia National Laboratories, 2015, SAND2014-1790.
[11] Ibid., 9
[12] Ibid., 74
[13] Ibid., 75
[14] Bunn and Sagan, *Worst Practices Guide*.

discipline of counterintelligence has been practiced in the United States from before the nation's founding. During the Revolutionary War, General George Washington penned a letter to Colonel Josiah Quincy on the threat posed by British spies, writing "there is one evil I dread, and that is their spies … I think it a matter of some importance to prevent them from obtaining intelligence of our situation."[15] Protecting sensitive and/or national security information from foreign entities is no less important in modern-day America. For example, 1985, the "year of the spy," brought public attention to U.S. counterintelligence programs with the arrest of five major spies—including Larry Wu-tai Chin and Jonathan Pollard—who had compromised more than one million classified documents to U.S. adversaries including Cuba, China, and the Soviet Union.[16] Recent high-profile espionage cases, such as the case of Edward Snowden, have continued to highlight the importance of measures employed by the U.S. government counterintelligence to appropriately protect sensitive and classified information.

Executive Order 12333, signed into law by President Reagan in 1981, provides the basis for modern U.S. federal government approaches to counterintelligence. The Order defines counterintelligence as, "information gathered, and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations or persons, or international terrorist activities."[17] Therefore, by definition, counterintelligence requires a connection to "foreign powers"—a geopolitical nexus indicating the severity of possible consequences. Practitioners of counterintelligence are engaged in an ongoing struggle against foreign intelligence entities, tasked with both preventing the loss of information that may prove harmful to U.S. national security and investigating incidents where loss of information has already occurred. An organization with robust workplace counterintelligence will employ multiple and diverse elements, from education to personnel security to offensive "double agent" operations.[18]

The primary objective of counterintelligence is the protection of sensitive and/or national security information, with an added emphasis on identification, attribution, and prosecution. Thus, the logic of counterintelligence suggests that if a facility is faced with the threat of a malicious actor with access to sensitive or classified information acting on behalf of a foreign entity, then all efforts should be taken to protect that information. If unable to do so, all efforts should be made to identify such individuals and their foreign entanglements. Current approaches include (1) screening/vetting individuals with access to sensitive information; (2) increasing the difficulty of successfully manipulating sensitive information by a motivated individual; and, (3) maximizing efforts to investigate any loss of sensitive information for appropriate responses.

Defining Counterintelligence Insights for Insider Threat

On a conceptual level, both counterintelligence and insider threat mitigation seek to address a threat to national security with serious consequences if mitigation efforts fail. Examples of such consequences for nuclear facilities range from nuclear power plant shut downs (e.g., the Belgian Doel-4 case) to radiological release (e.g., an "intentional" Fukushima). Espionage consequences may include economic losses, compromise of sources leading to imprisonment or death, and/or loss of information providing an adversary with a strategic or tactical advantage. More specifically, both programs seek to protect high-value targets (critical information in the case of counterintelligence and nuclear material in the case of insider threat) from human vulnerabilities. While the threat in counterintelligence is necessarily linked to a foreign entity, both disciplines involve an individual exploiting direct or indirect access to high-value information or materials to carry out a malicious act.

---

[15] George Washington to Josiah Quincy, March 24, 1776, in *The Papers of George Washington: Revolutionary War Series, vol. 3, 1 January 1776–31 March 1776*, ed. Philander D. Chase (Charlottesville: University Press of Virginia), 528-529.

[16] "Year of the Spy: 1985," *Famous Cases and Criminals*. Federal Bureau of Investigation. (accessed June 14, 2019).

[17] Exec. Order No. 12333, 3 C.F.R. (1981).

[18] James M. Olson, *To Catch a Spy: The Art of Counterintelligence,* (Washington, D.C.: Georgetown University Press, 2019).

In practice, both counterintelligence and insider threat mitigation involve preventive and protective mitigation efforts. Counterintelligence also includes a robust investigative function, an area that is not often emphasized in the insider threat community. Both disciplines are executed in a high security atmosphere. In the case of counterintelligence, this may include facilities related to intelligence collection, military activities, or diplomatic efforts, while insider threat mitigation activities take place in nuclear or radiological facilities. Finally, the potential for collaboration is present in both counterintelligence and insider threat mitigation. Espionage networks, such as the John Walker spy ring[19], present a unique challenge as spies working together may access a wider range of sensitive information and may combine knowledge and expertise to more effectively evade counterintelligence measures. Within insider threat, threat assessments often include the possibility of an insider colluding with an external actor. These conceptual and practical similarities are summarized in Table 1 below.

Table 1:

Counterintelligence	**Aspects & Characteristics**	**Insider Threat Mitigation**
Intelligence activities in support of foreign entities	**Threat Definition**	Malicious use of authorized access
Loss of critical or national security information	**Consequence of Failure**	Nuclear (or radiological) theft or release (via sabotage)
Prevent and respond to the loss of critical or national security information	**Mitigation Goal(s)**	Reduce/minimize the likelihood of a successful malicious use of authorized access
• Preventive • Protective • Investigative	**High Level Functions**	• Preventive • Protective
High *information* consequence locations (e.g., intelligence, national security, diplomacy)	**Operational Environment**	High *material* consequence facilities/activities (e.g., nuclear, radiological)
As part of *networks*	**Potential for collaboration**	In *collusion* with external actors

Based on these similarities, counterintelligence provides a useful corollary to insider threat mitigation. In particular, there are a wealth of counterintelligence case studies that may be leveraged by nuclear security practitioners to provide insight into insider threat mitigation best practices. Unlike the relatively few cases of nuclear insider threat in the public domain, there are more than 150 cases of espionage since 1947 in the United States alone.[20] Many of these cases have been analyzed extensively to better understand perpetrator motivations, successes and failures of preventive and protective measures, and best practices for conducting investigations. Counterintelligence case studies provide a rich data set from which to elicit insights to address insider threat mitigation within nuclear facilities. To provide insight into insider threat mitigation, the seven criteria in Table 2 were devised as a rubric for analyzing insights from counterintelligence case studies useful for insider threat mitigation.

[19] John Walker, a former U.S. Navy communications specialist, assisted the Soviet Union in decrypting more than one million naval messages over a nearly twenty-year period. He successfully recruited several others to aid in his espionage including a coworker, his brother, and his son. For more information see Pete Early, *Family of Spies: Inside the John Walker Spy Ring* (Random House Publishing Group, 1989).

[20] Katherine L. Herbig and Martin F. Wiskoff, *Espionage Against the United States by U.S. Citizens 1947-2001*, Defense Personnel Research Center, Technical Report 02-5, (Monterey, CA, 2002).

Table 2

Element Elicited from the CI Case Studies	Implications for Insider Threat Mitigation
Position/title of individual	Provides insight into the role of organizational position, access, authority, and status on insider threat potential
Motivation(s)	Provides insight into motivations attributed to insiders in international best practice documents
Recruitment/transition into intelligence collection	Provides insight into potential indicators of *individual* susceptibility for engaging in malicious acts
Mechanisms for accessing sensitive information	Provides insight into role of level of access on insider threat potential
Maturity of the "reporting culture"	Provides insight into role of *operational environment* susceptibility to manipulation for malicious acts
Impact of "preventive" & "protective" measures	Provides insight into insider threat potential by mapping to traditional, high level insider threat mitigation functions
Impact of investigative measures	Provides insight into potential insider response mechanisms

Data Collection

In consultation with professionals within the field of counterintelligence, ten case studies were chosen which exhibit a range of counterintelligence lessons learned.[21] The case studies span a 60-year period between 1941 and 2001, representing cases of both wartime and peacetime espionage. The spies comprise a range of nationalities, including German, Turkish, Swedish, and American. Additionally, the outcomes of the cases vary widely. While some spies were successfully investigated and prosecuted, others defected to another country or successfully evaded suspicion. The ten selected case studies and their primary consequences are summarized in Table 3.

Evaluating Counterintelligence Insights for Insider Threat

After selecting the ten case studies, the seven-criteria rubric was applied to each case to elicit insights for insider threat mitigation, according to Table 2. A summary of the insights from each case study based on the rubric is provided in Table 4. Analysis of the ten case studies reveals several notable patterns that may provide useful lessons for insider threat mitigation techniques.

Position/title of individual

Of the nine individuals employed by the government, the type of position and level of authority varied widely. CIA clerk Sharon Scranage served in a support role.[22] Ana Montes, on the other hand, was DIA's most senior Cuba analyst whose intelligence products were distributed at the highest levels of the U.S. government.[23] While most individuals were employed by the government in sensitive military, diplomatic, or intelligence roles, Boris Morros was a Hollywood producer with no access to classified information.[24] Additionally, level of authority did not directly correlate with severity of consequences. Despite a relatively low-paid and inconsequential position as valet for the British Ambassador, Elyesa Bazna compromised thousands of classified British documents on high-level conferences to Nazi intelligence at the height of World War II.[25]

[21] SAND2019-in press (SAND report detailing CI case studies)

[22] Robert Fritts, *A First-Class Spy Flap: CIA Agents Compromised in Ghana*, Association for Diplomatic Studies and Training, 2018.

[23] Scott W. Carmichael, *True Believer: Inside the Investigation and Capture of Ana Montes, Cuba's Master Spy*, (Annapolis: Naval Institute Press, 2007), viii.

[24] Borris Morros, *My Ten Years as a Counterspy*, (New York: Dell Publishing Co., Inc., 1959).

[25] Elyesa Bazna, *I was Cicero,* (New York: Dell Publishing Company, 1962).

The counterintelligence case studies demonstrate the complexity of creating an accurate profile of a potential insider. Insiders may span every rung of the organizational hierarchy, and even relatively junior employees may present a threat. Thus, while it is tempting to focus mitigation efforts on individuals with the highest levels of access and authority, it is important to recognize that even limited access can offer the potential for substantial damage.

Table 3[26]

Case No.	Spy Name	Years Active	Primary Consequence(s)
1	Aldrich Ames	1985-1994	Compromised every U.S. agent operating in the Soviet Union, directly leading to their deaths.
2	Elyesa Bazna	1943-1944	Passed thousands of classified British documents on high-level conferences to German intelligence during World War II.
3	Clyde Lee Conrad	1974-1988	Passed classified NATO war plans to Hungarian intelligence, including U.S. "tactical nuclear capabilities…[and] location of missile sites."[27]
4	Fritz Kolbe	1941-1944	Presented ~2600 classified documents including "vital information about where the Germans expected the allies to land in Normandy."[28]
5	Ana Montes	1984-2001	Provided Cuban intelligence with information on U.S. operations and intentions in Latin America.
6	Boris Morros	Soviet spy: 1934-1947; FBI double agent: 1947-1953	Offered spotting and assessing services and a front company to the Soviet Union; later served as a double agent for the FBI.
7	Jim Nicholson	1994-1996	Provided Russian intelligence with biographical data of hundreds of CIA case officers undergoing training, where he was an instructor.
8	Sharon Scranage	1983-1985	Espionage resulted in the execution of Ghanaian dissidents and a diplomatic incident which threatened fragile U.S.-Ghana relations.
9	Glenn Michael Souther	1980-1985	Compromised the U.S.' most sensitive satellite programs to the Soviet Union.
10	Stig Wennerström	Nazi spy: early 1940s; Soviet spy: 1950s-1963	Compromised "practically all of the Swedish air defense," including radar detection systems and capabilities to down enemy bombers.[29]

Motivations

Seven of the ten cases were also motivated—at least partially—by the prospect for financial gain. This result reflects past research on espionage motivations. Financial difficulties due to low pay or high cost of living can lead to negative feelings towards an employer. In other cases, a personal event such as a divorce can result in serious financial problems coupled with emotional turmoil that may "trigger" an employee to commit a malicious act.[30] Documented financial difficulties or sudden unexplained affluence may provide an indicator of a potential insider. Review of financial records was a useful investigative technique in multiple cases, helping to identify Aldrich Ames and Jim Nicholson.

This finding is consistent with previous analyses of both counterintelligence and insider threat mitigation. For example, the Defense Personnel and Security Research Center's study of 150 cases of U.S. spies from 1940 to the early 2000's concluded that money was the most common motivation for espionage, motivating spies in 69% of the cases and representing the sole motive in over 50 percent.[31]

---

[26] All information in Tables 3 and 4 is from SAND2019-in press unless otherwise noted.

[27] Michael J. Sulick, *American Spies: Espionage Against the United States from the Cold War to the Present*, (Georgetown University Press, 2013), 141.

[28] Tony Paterson, "Germany finally honours the 'traitor' spy who gave Nazi secrets to America." *The Independent,* 2004.

[29] Peter Wulff, "The Impact of a High-Tech Spy," *Intelligence & National Security*, 28, 2 (2013): 166.

[30] Herbig and Wiskoff, *Espionage Against the United States*, 55.

[31] Ibid., 40.

Similarly, lesson six from the *Worst Practices Guide to Insider Threat* encourages security professionals not to ignore employee disgruntlement and organizational culture.[32]

Recruited/transition into intelligence collection

Volunteering directly to a foreign intelligence entity was the most common (6/10 cases) method employed in the case studies analyzed. This phenomenon suggests that while spies received outside direction and assistance over the course of their espionage, the initial decision to spy was made on an individual level. This aspect requires further study to determine potential applicability to insider threat. This emphasizes the importance of understanding—and, ideally proactively identifying—potential "trigger" events that result in an individual engaging in malicious actions.

Mechanisms for assessing sensitive information

In eight of the ten case studies compromised information was accessed over the course of their normal duties. Sharon Scranage, for example, provided information to Ghanaian intelligence on CIA agents and informants obtained through her work at the CIA station.[33] This insight has important implications for insider threat mitigation, as many security programs focus on identifying insiders through tracking anomalous behavior. This approach is likely insufficient to identify insiders whose malicious acts are camouflaged by their ordinary responsibilities.

In a few cases, such as Ana Montes and Jim Nicholson, spies sought to expand their access to provide information of interest to their foreign intelligence handlers. Expanding access beyond their established "need-to-know," however, was risky. Nicholson's inquiries to colleagues about Chechnyan separatists, a subject unrelated to his daily duties, aroused the suspicion of the FBI in their search for a Russian mole.[34] Montes' aggressive efforts to gain access to sensitive information through special projects and meetings outside her area of expertise alarmed a coworker, who reported her to DIA counterintelligence staff.[35] Thus, attempts to expand access and deviations from normal duties remain a useful (if insufficient) indicator of potential insider threat.

Maturity of the "reporting culture"

Reporting culture in most of the cases was underdeveloped, allowing spies to continue their espionage undetected for longer. In a particularly egregious example, four of Clyde Lee Conrad's Army coworkers failed to report when Conrad approached them about an illegal moneymaking scheme.[36] Fritz Kolbe's colleagues in the Nazi Party overlooked multiple indicators of espionage including vocal anti-Nazi sentiment and suspicious foreign contacts.

Conversely, a robust reporting culture generally resulted in favorable outcomes for the investigation (3/10 cases). In the Ames case, for example, a 1989 report from a colleague noting Ames' undue affluence led investigators to consult his financial records. The benefits of reporting, however, were only realized if security professionals appropriately followed up. Glenn Michael Souther's wife reported his espionage to Navy officials in 1982 but was not taken seriously by investigators.[37] As a result, Souther continued to spy for an additional three years before his defection to the Soviet Union.

---

[32] Bunn and Sagan, *Worst Practices Guide*, 10.
[33] Fritts, *A First Class Spy Flap*.
[34] Bryan Denson, *The Spy's Son: The True Story of the Highest-Ranking CIA Officer Ever Convicted of Espionage and the Son He Trained to Spy for Russia*, (Scribe Publications, 2015), 76.
[35] Carmichael, *True Believer*, 4.
[36] Stuart A. Herrington, *Traitors Among Us: Inside the Spy Catcher's World,* (Presidio Press, 1999), 117.
[37] Ronald Kessler, *The Spy in the Russian Club: How Glenn Souther Stole America's Nuclear War Plans & Escaped to Moscow,* (Pocket Books, 1992), 50.

Table 4

Case No.	Position of individual	Motivation(s)	Recruitment into intelligence	Mechanisms for accessing information	Maturity of the "reporting culture"	Impact of "preventive" & "protective" measures	Impact of investigative measures[38]
1	Counter-intelligence Officer, CIA	Financial	Volunteered to Soviet contacts	Gained access based on his counterintelligence responsibilities	A CIA colleague reported Ames' undue affluence in 1989	*Preventive* (**failure** of hiring practices; **failed** background investigation)	Successful arrest and prosecution (with surveillance)
2	Valet for British Ambassador to Turkey	Financial	Volunteered through German embassy	Stole documents from safe in Ambassador's home	Despite awareness of unusual behavior, was never reported by colleagues	*Preventive* (**failed** background investigation) *Protective* (**failure** to secure classified information)	Investigation suffered from inter-service rivalries
3	U.S. Army Sergeant First Class	Financial, Ego	Recruited by Hungarian-born supervisor	Stole documents available to him as the custodian for classified documents	Despite several red flags (wealth, attempted recruitment of others), no reporting	*Preventive* (**failure** of reinvestigations) *Protective* (**failure** to secure classified information; **failure** to address networks)	Despite inter-agency challenges, successful arrest of individual and other members of the spy ring
4	Diplomat, German Foreign Ministry	Ideology	Volunteered as a "walk-in" to the embassy	Copied information from classified cables accessed during normal duties	Colleagues overlooked indicators, including anti-German views and suspicious contacts	*Preventive* (**failure** to address indicators) *Protective* (**failure** to secure classified information)	German intelligence unaware of loss and failed to launch an investigation
5	Senior Analyst, Defense Intelligence Agency	Ideology	Recruited by Cuban intelligence	Memorized classified information accessed during normal duties; sought to expand access to information	After receiving an educational CI brief, a colleague reported suspicions to a CI professional	*Preventive* (**failure** of background investigation) *Protective* (**failure** of compartmenting; **success** of education)	Successful interagency cooperation (with physical and electronic surveillance) resulted in arrest
6	Hollywood film/music producer	Blackmail, financial	Recruited by Soviets with financial aid to family	Spotted/assessed other contacts in Hollywood for recruitment	There is no indication activities were reported to U.S. authorities	N/A: A unique case with no access to classified information	Served as a FBI double agent
7	CIA Officer, instructor at "The Farm"	Financial, Ego, Disgruntlement	Volunteered to Soviet contacts	Accessed names and bio data as instructor at "The Farm"	Failure to report undue affluence and suspicious behavior	*Protective* (**success** of polygraph; **successful** reports; **failure** to address networks)	Successful investigation
8	Operations Support, CIA in Accra, Ghana	Love/ Seduction, Blackmail	Recruited by her Ghanaian lover	Information obtained from CIA files at the embassy and cable traffic	No timely report of inappropriate relationship with foreign national	*Preventive* (**failure** of training; success of reinvestigation) *Protective* (**failure** of reporting)	Success via routine polygraph, lured handler to U.S. for arrest
9	U.S. Navy Reservist	Financial, ego, ideological, disgruntlement	Volunteered while stationed abroad in Italy	Removed classified information from U.S. Navy reserve facility where he worked	Coworkers failed to report indicators (e.g., undue affluence, suspicious travel)	*Preventive* (**failed** background investigation) *Protective* (**failure** to secure classified information)	Failed investigation, individual escaped to the Soviet Union
10	Swedish Air Force Col. & diplomat	Financial, ego, disgruntlement	Volunteered to Nazi Germany/ Soviet Union	Photographed classified documents accessed as an attaché	No report by colleagues, reported by maid	*Preventive* (**failure** of biases)	Successful investigation & arrest (with surveillance)

[38] A "successful" investigation in this context entails only that the individual was identified, arrested, and prosecuted. It is important to note that many of the investigations identified as successful may also have experienced setbacks and delays or suffered from mismanagement.

Good reporting is essential to developing a strong security culture. However, encouraging the workforce to report is only the first step. Insider threat mitigation programs must also ensure there are proper procedures in place to act on reports.

Impact of "preventive" & "protective" measures

Failures of hiring practices, particularly background investigations (4/10 cases), showed up frequently in the dataset. Background investigations failed to uncover drug use, past criminal history, misrepresented educational credentials, extremist ideological views, undue affluence, and other potential indicators of espionage. Lesson two from the *Worst Practice's Guide to Insider Threat*, "Don't assume that background checks will solve the insider problem," gets to the heart of this issue. While background investigations are useful and necessary in limiting the individuals with access to sensitive material or information, they are insufficient to mitigate the insider threat and must be combined with other preventive and protective measures.

Additionally, security failures were common (4/10 cases) in the case studies analyzed. In the Elyesa Bazna case, highly classified information on British war plans was stored in an unsecured safe in the Ambassador's residence.[39] Employees at the supposedly high security Navy FICEURLANT building were not required to sign in and out of the facility, allowing Glenn Michael Souther to enter at odd hours to spy without detection.[40] Clyde Lee Conrad and his associates successfully removed boxes upon boxes of classified documents from the G3 War Plans Section. The quantity became so high that Conrad rented out an apartment for storage.[41]

The counterintelligence case studies demonstrate that failures in both areas can lead to successful orchestration of a malicious act, suggesting more research is needed to determine the right balance of preventive and protective measures in insider threat.

Impact of investigative measures

Counterintelligence investigations are highly complex. In the case studies examined, each investigation proceeded uniquely, leveraging diverse methods including double-agent operations, clandestine intelligence, face-to-face interviews and polygraph examinations. In some cases, such as Fritz Kolbe, an investigation was never launched. The diversity of approaches and outcomes made it difficult to discern useful patterns during preliminary analysis. One potential insight for insider threat mitigation may be the utility of electronic and/or physical surveillance measures, which were employed successfully in multiple investigations including Aldrich Ames, Clyde Conrad, Ana Montes, Jim Nicholson, and Stig Wennerström. *How* and *when* to implement such monitoring and surveillance measures for insider threat mitigation requires additional investigation for appropriateness and practicality.

Conclusions

While insider threat presents a persistent and grave threat to nuclear facilities, counterintelligence offers a potentially useful corollary to insider threat mitigation. Through presenting early results from a comparison of counterintelligence and insider threat mitigation, this paper represents the potential utility of leveraging espionage case studies to address the insider threat within nuclear facilities. Going forward, the authors intend to build on this research by expanding the number and scope of counterintelligence case studies included and completing a more detailed analysis to further explore outcomes.

---

[39] Bazna, *I was Cicero*, 44.

[40] Kessler, *The Spy in the Russian Club*, 185.

[41] Joe Navarro, *Three Minutes to Doomsday: An Agent, a Traitor, and the Worst Espionage Breach in U.S. History*, (Scribner, 2017), 237.