NC3 INSIDER THREATS
RON SCHOUTEN
11/14/19

I. INTRODUCTION

In this essay, Ron Schouten examines fundamental concepts of insider threats and provides an overview of the extent and significance of insider threats in US and other NC3 systems.

A podcast with Ron Schouten, Peter Hayes, and Philip Reiner on NC3 insider threats is found here.

Acknowledgments: The workshop was funded by the John D. and Catherine T. MacArthur Foundation.

Banner image is by Lauren Hostetter of Heyhoss Design

TECH4GS SPECIAL REPORT BY RON SCHOUTEN
NC3 INSIDER THREATS
10/14/19

Summary

Threats arising from within NC3 systems can have particularly devastating consequences. Drawing on knowledge of insider threats from the nuclear enterprise and other fields, this paper examines fundamental concepts of insider threats and provides an overview of the extent and significance of insider threats. It outlines some current models of insider threat, including behavioral indicators, and current efforts at ensuring personnel reliability. Finally, it focuses on the vulnerabilities of the nuclear enterprise to insider threat in the current environment and discusses some challenges to addressing the insider threat problem on a global scale.

Introduction

Risk is commonly conceptualized as a function of the probability that a given event will occur and the nature and magnitude of the consequences of that event (R = P x C). Applied to the nuclear enterprise generally, and NC3 particularly, this formulation yields a level of risk rivalled by few, if any, other endeavors.

To date, we have drawn comfort from the belief, justifiable or not, that the probability of an adverse nuclear event is low. A guarded sense of safety and security has been derived from the concept of mutual deterrence and the belief that nuclear-empowered states hew to the "always-never" posture discussed in more detail by other authors in this collection: to have their nuclear arsenals always ready to respond to the order of a legal authority, but never available to unauthorized persons or subject to accidental release. As such, all nuclear players are assumed to be motivated to exercise restraint and guard against negligence in the handling of stockpiles and fissile materials, thus minimizing the likelihood of an event. Confidence in that low probability fluctuates, of course, in the face of political tensions between nuclear capable states, incidents of sabotage, the disappearance of fissile materials that have ended up in unknown hands with unknown intent, and periodic cases of U.S. citizens with security clearances, both civilian and military, who convey classified information to adversaries.

Accepting, for now, that the probability of an adverse nuclear event is low, the overall risk is nevertheless high due to the potentially devastating consequences of a nuclear incident, whether intentional or accidental. The probability is low, but the consequences could be cataclysmic. In light of that, it has been essential to contain the risk by doing everything possible to keep the probability of occurrence as close to zero as possible. With regard to insider threats, Personnel Reliability Programs (PRPs), developed to ensure the suitability and reliability of those engaged in the handling of and access to nuclear and other dangerous materials, have been present since the Cold War, with periodic revisions in the face of evolving concerns. They have proven to be imperfect solutions, however, as evidenced by multiple examples of military service members and civilians (both government employees and contractors), with varying levels of security clearances, betraying their country through theft, espionage, disclosure of classified materials, and mass shootings.

In recognition of this problem, and prompted by a series of insider incidents, President Obama issued Executive Order 13587, ordering all executive branch agencies (including the Department of Defense) to set up "an insider threat detection and prevention program consistent with guidance and standards developed by the Insider Threat Task Force."[1] That program is likely responsible for the intervention that prevented Coast Guard Lieutenant Christopher Hasson from carrying out a planned act of right wing-inspired mass violence.[2]

[1] Executive Order No. 13587, 3 C.F.R p. 276 (2011).

[2] Bui L, Lamothe D, Miller ME. Coast Guard lieutenant used work computers in alleged planning of widespread domestic terrorist attack, prosecutors say. Washington Post February 21, 2019. https://www.washingtonpost.com/local/public-safety/ex-coast-guard-lieutenant-ordered-held-for-14-days-while-government-weighs-terrorism-related-charges-in-his-planning-of-widespread-terrorist-attack/2019/02/21/57918f12-3573-11e9-854a-7a14d7fec96a_story.html?utm_term=.99543a1b37ec

There are multiple reasons to doubt that the probability of an adverse nuclear event is, and will remain, low. Increases in international tensions and belligerence, the rise of domestic and international extremism across the political spectrum, the theft of fissile materials, the increase in nuclear-capable states, and changes in organizational culture and societal attitudes, are just some of the factors pointing to an increased likelihood that an intentional or accidental adverse nuclear event will occur.

In terms of both probability and consequences, some of the greatest threats to any organization or institution arise from within. The Insider Threat Task Force defines an insider threat as follows:

> The insider threat is the risk an insider will use their authorized access, wittingly or unwittingly, to do harm to their organization. This can include theft of proprietary information and technology; damage to company facilities, systems or equipment; actual or threatened harm to employees; or other actions that would prevent the company from carrying out its normal business practices.[3]

Thus, insider threats are malicious or inadvertent acts that can imperil the safety and security of the organization as well as the surrounding community. Maliciously motivated individuals positioned inside a nuclear facility, armed with knowledge, skills, and ability (KSA), are uniquely positioned to engage in acts of fraud, theft, sabotage, or violence. Similarly, an insider who is unmotivated, uncommitted to the organization's mission or its policies and procedures, distracted by personal matters, or suffering from health problems is at risk of unintentional lapses in safety and security that can have dire results.

This paper examines the problem of insider threat as it relates to the nuclear enterprise. Section One lays out fundamental concepts of insider threat. Section Two provides an overview of the extent and significance of insider threat in nuclear facilities. Section Three describes conceptualizations of insider threat, including behavioral indicators of risk. Section Four focuses on the vulnerabilities of the nuclear enterprise to insider threat in the current environment and in light of recent events. Section Five explores possible responses to the insider threat problem, both nationally and internationally.

1. Terminology

The term "insider threat" refers to a category of risks of harm or actual harm, as well as to individuals who are the agents through whom those risks arise. As a category, insider threats are actual or potential harms to a specific entity or institution, or the larger society, that arise from an individual who has a current or former association with that entity and who, by virtue of that association, has information and materials that then provide the basis for intentional or unintentional harm. The term is also used to refer to the individuals who engage in the behavior that leads to potential or actual harm. The term will be used in both senses here. Where necessary for clarity, individual actors will be referred to as "insiders" or "inside attackers."

The United Nation's International Atomic Energy Agency (IAEA) addressed the issue of insider threat in 2008, stating:

---

[3] National Insider Threat Task Force. Protect Your Organization from the Inside Out: Government Best Practices (2016) *https://www.dni.gov/files/NCSC/.../Govt_Best_Practices_Guide_Insider_Threat.pdf*;
See also, https://www.dni.gov/files/NCSC/documents/nittf/NITTF-Insider-Threat-Guide-2017.pdf

Insider threats in particular present a unique problem for a physical protection system. Insiders could take advantage of their access rights, complemented by their authority and knowledge of a facility, to bypass dedicated physical protection elements or other provisions such as measures for safety, material control and accountancy, and operating measures and procedures. Further, as personnel with access in positions of trust, insiders are capable of carrying out 'defeat' methods not available to outsiders when confronted with protection elements and access controls. Insiders have more opportunities to select the most vulnerable target and the best time to execute the malicious act.[4]

The IAEA report focuses on malicious insiders and describes them along several dimensions:

- Motivation: "ideological, personal, financial and psychological factors and other forces such as coercion"
- Level of involvement
    - "Active": willing to provide information, perform actions; may be violent or non-violent
    - "Passive": non-violent and limit their participation to providing information that could help adversaries to perform or attempt to perform a malicious act
- Violence
    - Non-violent active insiders: "not willing to be identified or risk the chance of engaging response forces and may limit their activities to tampering with accounting and control and safety and security systems"
    - Violent active insiders: "may use force regardless of whether it enhances their chances of success; they may act rationally or irrationally"

Notably, the IAEA report did not describe any known insider attacks on nuclear facilities.

Mundie and colleagues[5] identified forty-two different definitions of insider and insider threat, noting the difficulty this can cause when reading the research literature. Four of those definitions include an ex-employee, thus creating a hybrid insider-outsider threat.

Capelli, et al define insider threat as follows:

[A] current or former employee, contractor, or business partner who has or had authorized access to an organization's network, system or data and intentionally exceeded or misused that access in a manner that negatively affected the confidentiality, integrity, or availability of the organization's information or information systems.[6]

This definition, which speaks only to intentional actors, relates to insider threats to information systems but is easily translated to other enterprises, including nuclear, chemical, radiological, and the life sciences.

---

[4] International Atomic Energy Agency. Preventive and Protective Measures Against Insider Threats. U.N.: Vienna (2008).
[5] Mundie DA, Perl S, Huth CL. Toward an Ontology for Insider Threat Research: Varieties of Insider Threat Definitions, in 2013 Third Workshop on Socio-Technical Aspects in Security and Trust, 2013, pp 26-26.
[6] Capelli DM, Moore AP, Trzeciak RF. (Cappelli, Moore, & Trzeciak, 2012) The CERT Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes, Addison-Wesley Professional 2012.

While intentional malicious insider threats are generally considered to pose the greatest risk of harm, and thus receive the majority of attention, it is important to keep in mind that considerable harm can arise from unintentional or negligent insiders. Unintentional insider threats are those posed by individuals who, whether due to impairment or indifference, violate workplace rules, policies, or procedures resulting in lapses in safety or security and subsequent harm. Arguably, when it comes to nuclear facilities, unintentional negligent insiders are likely to be more common and have the potential for as much harm as malicious insiders.

Greitzer and colleagues define the unintentional insider threat as follows:

> (1) [a] current or former employee, contractor, or business partner (2) who has or had authorized access to an organization's network, system, or data and who, (3) through action or inaction without malicious intent, (4) unwittingly causes harm, or substantially increases the probability of future serious harm to the confidentiality, integrity, or availability of the organization's resources or assets, including information, information systems, or financial systems.[7]

As with Capelli, et al.'s definition of malicious insider threat, this definition refers to information technology and cybersecurity, but it can easily be adapted to other enterprises.

2. The Significance and Extent of Insider Threat

Security for most organizations tends to be outward facing, as external threats are typically perceived as more serious and more common. Indeed, when it comes to workplace violence, for example, most workplace homicides are consistently committed by outsiders.[8] In contrast, insiders are disproportionately represented in crimes involving finance and technology.

Security in nuclear facilities has traditionally been focused on "guns, gates, and guards," ensuring that fissile materials and weapons themselves are not stolen, sabotaged, or used. The IAEA report cited above addressed the issue physical security relative to insider threat in 2008, stating:

> Insider threats in particular present a unique problem for a physical protection system. Insiders could take advantage of their access rights, complemented by their authority and knowledge of a facility, to bypass dedicated physical protection elements or other provisions such as measures for safety, material control and accountancy, and operating measures and procedures. Further, as personnel with access in positions of trust, insiders are capable of carrying out 'defeat' methods not available to outsiders when confronted with protection elements and access controls. Insiders have more opportunities to select the most vulnerable target and the best time to execute the malicious act.[9]

---

[7] Greitzer FL, Strozer J, Cohen S, Bergey J, Cowley J, Moore, Mundie D. Unintentional Insider Threat: Contributing Factors, Observables, and Mitigation Strategies. 2014. 47th Hawaii International Conference on System Sciences https://ieeexplore.ieee.org/document/6758854

[8] U.S. Department of Labor Bureau of Labor Statistics. Injuries, Illnesses, and Fatalities 2017. https://www.bls.gov/iif/oshwc/cfoi/workplace-homicides.htm

[9] International Atomic Energy Agency. Preventive and Protective Measures Against Insider Threats. U.N.: Vienna (2008).

In contrast to physical violence, to date insiders appear to have posed the greatest risk to nuclear and cyber security. Bunn and Sagan[10] note that all cases of theft of nuclear materials were carried out by insiders, either working alone or with outsiders. They further attribute many of the known cases of nuclear sabotage to disgruntled workers at nuclear facilities, presumably motivated by a desire to send messages to management, rather than to spread radioactivity.

Abrams's 1991 examination of human reliability and safety in the handling of nuclear weapons focused on the Bangor Submarine Base in Washington State, which at the time housed 1700 nuclear weapons and was staffed by 5000 service members. Just over 20% of those service members were certified by the Nuclear Weapons Personnel Reliability Program. Abrams's paper describes four case examples arising in a one-year period at Bangor that demonstrate PRP failure to detect dangerous individuals. In each of these, PRP-certified service members engaged in acts of violence: one suicide, one murder-suicide, and two murders. Abrams discusses the prevalence of substance use disorders and mental illness in the military generally and among those in nuclear facilities, particularly, and the risks arising from these conditions among those handling the U.S nuclear stockpile.[11]

The digital world has proven to be fertile ground for insiders, although the majority of threats to information systems come from outside the organization. A Department of Defense (DoD) Inspector General report, published in 1997, concluded that 87% of detected intrusions into DoD information systems were carried out by employees or others within the organization.[12] In the 2011 Cybersecurity Watch Survey, which included 607 respondents, 58% said most attacks were from outsiders, while 21% said malicious insiders were responsible for the majority of intrusions. However, 33% of the respondents said the insider attacks were more costly.[13]

3. Who does these things? Behavioral Characteristics of Insider Threats

Malicious insiders may join their organizations with the intent to carry out nefarious activities or their intent may develop over time in response to world or life events, including disgruntlement at work. It goes without saying that the proclivities of unintentional insiders to accident or error may go undetected at the time of hire, or they may develop over time in response to health or personal problems.

As written elsewhere regarding terrorism,[14] malicious insider threats can be divided into three, often overlapping, categories:

1. Individuals operating alone but on behalf of state or non-state groups

[10] Bunn M, Sagan SD. A Worst Practices Guide to Insider Threat: Lessons from Past Mistakes. Cambridge, MA: American Academy of Arts and Sciences, 2014.

[11] Abrams HL. Human reliability and safety in the handling of nuclear weapons. Science & Global Security, 1991, Volume 2, pp.325-349.

[12] DoD Office of the Inspector General, DoD Management of Information Assurance Efforts to Protect Automated Information Systems (Washington, D.C.: U.S. Department of Defense, 1997).

[13] Brenner B. Report: Insider threats expensive, but there's a silver lining. CSO February 3, 2011.https://www.csoonline.com/article/2126760/privacy/report--insider-attacks-expensive--but-there-is-a-silver-lining.html?source=rss_network_security

[14] Schouten R, Saathoff G. Insider Threats in Bioterrorism in Meloy JR and Hoffman J (eds) International Handbook of Threat Assessment. New York: Oxford (2014).

2. Individuals acting alone but in support of a radical ideology they wish to support
3. Individuals who are acting for idiosyncratic reasons that may relate to mental illness, substance abuse, or personality disturbance

Individuals in the third category can include:

a. Disgruntled employees seeking to cause harm for revenge against the organization or individuals within it
b. Disgruntled employees seeking to demonstrate the ability/capacity to do harm
c. Individuals attempting to demonstrate weakness in the system
d. Individuals seeking to demonstrate their expertise and skill to prove their worth
e. Those attempting to test the bounds of science and their ability through unauthorized experimentation

While our modern focus is often on malicious insiders who are ideologically motivated, evidence has tended to indicate financial gain is the primary inspiration for malicious insiders. Hoffman and associates prepared a report on insider attacks for the Department of Energy in 1990 and examined 62 cases of insider crime from other industries.[15] The report focused on characteristics of potential criminal actions against nuclear facilities by insiders. They divided the cases into three categories:

- Crimes committed by insiders conspiring with outsiders
- Crimes committed by insiders conspiring with other insiders
- Crimes committed by lone insiders

They concluded that events in the first category posed the greatest risk for an attack on a nuclear facility, in the form of a terrorist attack, but that the risks posed by the other two categories were quite real. Analyzing the motivations of the perpetrators in each of the categories, they found the following:

1. Insiders conspiring with outsiders: 85% were financially motivated
2. Insiders conspiring with other insiders: 92% were financially motivated
3. Lone insiders:
    1. 68% were financially motivated
    2. Remainder primarily fueled by emotional disturbance, including anger at the employer

In their chapter on terrorist threats to nuclear facilities, Heggehammer and Dæhli[16] suggest the following typology of insider operations, arguing that they take one of four ideal forms:

1. Insertion: an existing terrorist group member is placed in an organization as an operative.
2. Recruitment: a group reaches out to an existing employee.
3. Outreach: an employee reaches out to a group.

[15] Hoffman B, Meyer C, Schwarz B, Duncan J: Insider Crime: The Threat to Nuclear Facilities and Programs. Rand Corporation: Santa Monica, CA (1990).
[16] Heggehammer T, Dæhli AH. Insiders and Outsiders: A Survey of Terrorist Threats to Nuclear Facilities in Bunn M and Sagan SD Insider Threats. Ithaca: Cornell University Press (2016).

4. Autonomous action: an employee develops terrorist motivations on their own and acts independently.

Not surprisingly, it has been suggested that those who develop their motivation over time are more common than those who join with nefarious intent.[17] This has implications for efforts to prevent and mitigate insider threats, suggesting that while initial security screening is important, periodic screening and ongoing monitoring are even more so.

Malice and negligence among insiders are not mutually exclusive. Dr. Bruce Ivins, a civilian employee of the U.S. Army Medical Research Institute of Infectious Diseases (USAMRIID) and a leading anthrax researcher, is believed to have carried out the anthrax mailings of 2001 in the United States, killing five and sickening at least 17 others.[18] Dr. Ivins's specific motivations have never been determined, but may have been a mixture of restoring his status within USAMRIID, impressing current and former colleagues, drawing attention to the threat of biological attacks, and financial self- interest (e.g., he was part owner of a patent for a new vaccine.)[19] Any one of these could have formed the basis for him intentionally propagating the anthrax spores, preparing them for distribution, and mailing them. In addition, Dr. Ivins also committed a number of safety violations that eventually led to him losing access to the anthrax laboratory and were likely due to his deteriorating mental and physical health.[20]

Noting the relationship between nuclear safety and security threats, Healey[21] offered the following taxonomy of these threat as shown in table 1 on the following page.

[17] Noonan T, Archuleta E. The National Infrastructure Advisory Council's Final Report and Recommendations on The Insider Threat to Critical Infrastructure, in, The National Infrastructure Advisory Council https://www.dhs.gov/publication/niac-insider-threat-final-report, 2008, pp 1-55; CPNI, Insider Data Collection Study, Report of Main Findings *https://www.cpni.gov.uk/.../insider-data-collection-study-report-of-main-findings.pdf* 2013; Director of Central Intelligence/Intelligence Community Staff Memorandum, Project Slammer Interim Progress Report, *https://www.cia.gov/library/readingroom/docs/DOC_0000218679.pdf*

[18] U.S. Department of Justice. Amerithrax Investigative Summary: Released Pursuant to the Freedom of Information Act. Released February 19, 2010.

[19] Stern J, Schouten R**:** Chapter 3 Lessons from the Anthrax Letters. In Bunn M, Sagan SD, Eds. Insider Threats. London: Cornell University Press, 2016; Saathoff, G, DeFrancisco G, Benedek D, Everett A, Holstege C, Johnson S, Lamberti J.S., Schouten R, White, J. The Amerithrax Case: Report of the Expert Behavioral Analysis Panel. Charlottesville, VA: Research Strategies Network, 2011

[20] id

[21] Healey AN. The insider threat to nuclear safety and security. Security Journal (2016) 29, 23–38 (2016)

Table 1: A basic taxonomy of human threat to nuclear safety and security

Human error		*Misuse*		*Abuse*	
1. Unintended slip or lapse Skill-based error	2. Unintended mistake Rule-based or knowledge-based error	3. Unintended violation Unclear rule/s or rule/s not understood	4. Intended violation Situational requirements forces violation	5. Intended abuse Personal gain motivates abuse without intent to harm	6. Intended harm Planned, malicious attack; a criminal act
(1) Insider threat to security – *Definition A*					
(2) Insider threat to security – *Definition B*					
(3) Insider threat to security – *Definition C*					
(4) Internal threat to safety – assessed in a safety case					

A variety of behavioral indicators of insider threat have been offered by different authors. These include, among other things, changes in language that reflect increased self-focus and isolation from colleagues[22] and social media.[23]

A major challenge to identifying and mitigating insider threats has been the unwillingness of colleagues to report behaviors of concern on the part of coworkers. In a paper that has been accepted for publication, Bell and colleagues describe behavioral indicators of insider threat and the factors that may affect the decisions of bystanders to report concerns about colleagues. Using an online survey conducted at a large Critical National Infrastructure energy sector organization, they inquired what factors would influence coworkers to take action if they observed risk indicators including engaging in illicit activities, revealing intentions to cause harm ("leakage"), or other aberrant behaviors that reflect changing loyalties and attitudes about work and the organization.[24]

A model used to explain fraud committed by insiders in the financial services industry, the Fraud Diamond,[25] can be applied in other fields, including the nuclear enterprise. Originally formulated as the Fraud Triangle, the Fraud Diamond contains four elements: Motivation, Opportunity, Capability, and Rationalization.[26] The insider, motivated by one or more perceived needs or desires, takes advantage of environmental vulnerabilities and

[22] Taylor et al [Taylor PJ, Dando CJ, Ormerod TC, Ball LJ, Jenkins MC, Sandham A, Menacere T. Detecting insider threat through language change. Law & Human Behavior, 37 (2013)267-275.

[23] Park W, You Y, Lee K. Detecting potential insider threat: analyzing insiders' sentiments exposed in social media. Security and Communications Networks. Volume 2018, Article ID 7243296. https://doi.org/10.1155/2018/7243296

[24] Bell AJC, Rogers MB, Pearce JM. The Insider Threat: Behavioral indicators and factors influencing likelihood of intervention. International Journal of Critical Infrastructure Protection 24 (2018) 166-176. https://doi.org/10.1016/j.ijcip.2018.12.001

[25] Wolfe DT, Hermanson DR The Fraud Diamond: Considering the Four Elements of Fraud. The CPA Journal December 38-42 2004.

[26] Abdullahi R, Mansor N, Nuhu MS. Fraud Triangle Theory and Fraud Diamond Theory: Understanding the Convergent and Divergent for Future. European Journal of Business and Management. 7:28; 30-37 (2015).

victim characteristics to apply his or her technical knowledge and ability to manipulate others to carry out the malicious act. Rationalization of the malicious behavior explains, in part, how a seemingly normal and upstanding member of the organization can engage in malicious and self-serving behavior.

There are multiple motivations that can give rise to malicious insider behavior and more than one motivation may be at work in any given situation. Hoffman et al.'s finding in 1990 suggest that personal financial gain is at the heart of most cases. Notably, a study of espionage cases by the DoD Personnel Security Research Center found evolving motivations for spying.[27] The study found that between 1990 and 2007 financial gain was not the prime motivation for those who engaged in espionage. Of that sample, only 7% spied for money alone, in comparison to 47% in the first cohort (1947–79) and 74% in the second cohort (1980–1989). From 1990 to 2007, 57% spied because of divided loyalties and 22% because of disgruntlement. Ingratiation, coercion, thrills, and recognition or ego were the identified motivations in a small percentage of cases. While they fluctuated over the study period, vulnerabilities to getting involved in espionage included allegiance to another country, misuse of drugs and illegal drug use, alcohol abuse and gambling, foreign contacts (family or business), and financial problems. Life events, both positive and negative, within the previous 6–8 months served as triggers for spying in 33% of their sample.

4. Vulnerabilities of the Nuclear Enterprise to Insider Threat

In their chapter on terrorist threats to nuclear facilities, Heggehammer and Dæhli observe that terrorists seem to have been deterred by the difficulty of recruiting insiders in nuclear facilities.[28] Given the motivations for insider betrayal described above, current trends in the nuclear enterprise and in the larger world may make terrorist recruiting less difficult and increase the risk of other insider events, both intentional and unintentional.

The report of the Defense Science Board Task Force on Nuclear Deterrence Skills[29] describes a number of technical, manpower, and cultural changes in our nuclear weapons enterprise that can potentially lead to increases in insider risks. They include, among others:

1. A shrinking labor pool of qualified workers, due to attrition, with an average increasing age of the workforce and competition for skilled workers and competition for skilled workers.
2. Inadequate staff to manage complex procedures due to a decline in the number of science graduates, competition from the private sector for computer scientists and programmers, and the requirement that those handling nuclear materials be U.S. citizens.
3. Low PRP certification rates.
4. Lack of training and experience.

[27] Herbig KL. Changes in Espionage by Americans: 1947-2007. Technical Report 08-05 Monterey, CA: Defense Personnel Security Research Center (2008).

[28] Heggehammer T, Dæhli AH. Insiders and Outsiders: A Survey of Terrorist Threats to Nuclear Facilities in Bunn M and Sagan SD Insider Threats. Ithaca: Cornell University Press (2016).

[29] Defense Science Board Task Force. Final Report on Nuclear Deterrence Skills. Office of the Under Secretary of Defense For Acquisition, Technology, and Logistics. Washington, D.C. (2008).

5. Loss of a sense of mission, with declining morale. This, along with other problems, was discussed by the Director of the Los Alamos National Laboratory in 2000 in a published interview.[30]
6. Shortage of intelligence analysts focusing on nuclear threats and a shifting emphasis in the intelligence community to counterterrorism. In combination with the shrinking pool of talent across the nuclear enterprise, this may lead to lowering PRP standards and placing individuals who may not have previously deemed trustworthy, reliable, or suitable in positions where they have the potential to do harm. An example of such a disaster is the case of Major Nidal Hasan, the Army psychiatrist who killed 13 DoD employees and wounded 43 others at Ft. Hood, Texas. Hasan, whose poor performance as a psychiatrist and espousing of radical jihadist ideology were well known, was nevertheless promoted and "packaged for export" to Ft. Hood because of the shortage of Army psychiatrists.[31]

In addition to the loss of morale, diminished sense of mission, and general disgruntlement, world events have also conspired to increase the vulnerability of members of the nuclear workforce to recruitment or individual decisions to pursue malicious insider actions. Factors to consider include the following:

1. The rise of international and domestic political and religious extremism across the ideological spectrum has increased the risk that employees of nuclear facilities may already be radicalized at the time of hire or be radicalized or recruited to violence extremism during the course of their employment. Heggehammer and Dæhli studied terrorist aspirations for the use of nuclear weapons and other WMD.[32] They document a number of aspirational expressions from jihadi terrorists regarding the acquisition and use of nuclear and radiological materials. They opine, however, that right wing terrorists pose the greatest threat of nuclear terrorism, citing the fantasies of using CBRN weapons outlined in William Pierce's *The Turner Diaries* and the manifesto of Norwegian right wing terrorist Anders Breivik. More significantly, citing Peter Bergen, they point out that between 2001 and 2013, individuals with right wing connections were responsible for 13 chemical, biological, and radiological incidents, while jihadi terrorists were responsible for none.

The prospect of right wing extremism is of particular concern with regard to the military services, in which there has been an increase in attraction to right wing extremist ideology.[3334] Similarly, military veterans who

[30] Los Alamos Director Talks About Security Problems, Morale, and Recruiting Young Scientists at Lab. Physics Today. **53**, 2, 46 (2000).

[31] Zegart AB. The Fort Hood Terrorist Attack in Bunn M, Sagan SD Insider Threats. Ithaca, NY: Cornell University Press (2016).

[32] Heggehammer T, Dæhli AH. Insiders and Outsiders: A Survey of Terrorist Threats to Nuclear Facilities in Bunn M and Sagan SD Insider Threats. Ithaca: Cornell University Press (2016).

[33] Sterman D. The greater danger: military-trained right-wing extremists. The Atlantic. April 24, 2013. https://www.theatlantic.com/national/archive/2013/04/the-greater-danger-military-trained-right-wing-extremists/275277/

[34] Presley, SM. Rise of Domestic Terrorism and its Relation to United States Armed Forces. Research Paper submitted to the Faculty of the U.S. Marine Corps Command and Staff College. April 19, 1996.

experience a loss of identity upon involuntary separation from the service or who feel that their contributions were underappreciated may be drawn to far right extremism.[35]

2. Increased risk of recruitment by virtue of the growing availability of private personal data. This is particularly problematic for those who were victims of the 2015 hacking of the U.S. Office of Personnel Management (OPM) hack, in which the records of approximately 21.5 Americans were stolen. The records included security background check materials, Social Security numbers, and extensive other personal data for employees and others who had applied for security clearances. The availability of the information from OPM, stolen health care records, DNA sequencing data, and information from hacks of hotel chains and financial service firms sets the stage for adversaries to use that information to recruit or coerce individuals with security clearances, including those who work in nuclear facilities.

3. Socio-cultural changes, including growing disenchantment with the impact of technology on human lives and the world, societal inaction on climate change, income disparity, and other social justice issues can affect the attitudes and loyalties of workers in all aspects of the nuclear enterprise.[36] This can include radicalization of individuals who may then actively seek out positions in nuclear facilities in order to do harm, mirroring past tactics of animal rights activists, or acquisition of those radical beliefs later in their employment.[37]

5. What can be done?

Recommendations for decreasing the risk of insider threat, both the probability of such an event and its impact, have traditionally focused on security measures. These have typically involved guns, gates, and guards, as noted above, and background screening. By necessity, cybersecurity has played an increasingly important role.

Prevention measures based on human factors and behavior are just as important as physical and information security measures. Recommendations along these lines have typically involved enhanced personnel screening, such as is called for in the Nuclear Personnel Reliability Program.[38] If the majority of insider threats arise after individuals have joined an organization, screening alone, no matter how rigorous and necessary to keep out known bad actors, will be of limited long-term value. Initial and repeat security screenings are only effective if those conducting them have access to relevant records, including medical records, and know how to interpret the records and conduct thorough interviews.

Suggested tools for screening and monitoring have included linguistic analysis and behavioral analysis aimed at

[35] Simi P, Bubolz BF, Hardman A. Military experience, identity discrepancies, and far right extremism: an exploratory analysis. Studies in Conflict & Terrorism. 36(8):654-671 (2013).

[36] Noonan C. Spy the Lie: Detecting Malicious Insiders. Prepared for the U.S. Department of Energy under Contract DE-AC05-76RL01830 Pacific Northwest National Laboratory Richland, Washington.

[37] Richardson JH. Children of Ted. New York Magazine. December 11, 2018. http://nymag.com/intelligencer/2018/12/the-unabomber-ted-kaczynski-new-generation-of-acolytes.html

[38] Department of Defense Instruction 5210.42 DOD NUCLEAR WEAPONS PERSONNEL RELIABILITY ASSURANCE. April 27, 2016.

developing "profiles" of malicious insiders and those at risk of unintentional insider risks.[39] [40] The efficacy of these measures has yet to be proven. Comprehensive approaches to screening for malicious insiders, rather than a single screening tool, have the highest probability of success.[41]

Initial and periodic rescreening and reassessment of personnel reliability and security are arguably essential. It is noteworthy, however, that not all nuclear powers use the PRP model from the United States.[42] Regardless of the technical components of any system designed to identify and mitigate insider threat, the success of such systems depends on the attitudes of those expected to implement them and the cultures of their organizations. While, for example, monitoring of on-line behavior and keyboard strokes may help detect nefarious activity, those methods are doomed to failure in the absence of a culture of shared responsibility for security and safety in which managers and coworkers are trained to be aware of behavioral changes in each other that indicate health issues or possible nefarious intent. No matter how rigorous the nuclear surety standards imposed, they are only as effective as the people who must implement them.

Efforts to assess and monitor the military work climate are essential to identifying those workplaces at greatest risk of insider threats.[43] Such efforts should address the Bystander Effect described earlier: the problem of individuals failing to act even when faced with direct evidence of dangerous or illegal behavior is well documented. An example of the extent of this problem is found in the examination of 49 sabotage cases Keeney and colleagues. They documented that behaviors of concern were observed by management or coworkers in 97% of the cases.[44]

As noted above, Bell, et al., studying factors that contribute to the Bystander Effect, found that the likelihood of intervention was diminished by "the relative seniority and perceived motivations of the actor, confidence of confidentiality, and clarity of reporting processes." The primary barriers to intervention were related to the observers' perceived ability to correctly interpret behavioral what they observed and their awareness of how to respond.[45] Consistent with recommendations made elsewhere, organizations need to provide training regarding

---

[39] Schultz EE:A framework for understanding and predicting insider attacks. Computers & Security 21(6): 526-531 (2002;

[40] Taylor et al [Taylor PJ, Dando CJ, Ormerod TC, Ball LJ, Jenkins MC, Sandham A, Menacere T. Detecting insider threat through language change. Law & Human Behavior, 37 (2013)267-275; Park W, You Y, Lee K. Detecting potential insider threat: analyzing insiders' sentiments exposed in social media. Security and Communications Networks. Volume 2018, Article ID 7243296. https://doi.org/10.1155/2018/7243296.

[41] Buck KR, Rose AE, Wiskoff MF, Liverpool KM. Screening for Potential Terrorists in the Enlisted Military Accessions Process. Defense Personnel Security Research Center Technical Report 05-8 April 2005.

[42] Gower J. Personal communication. January 22, 2019.

[43] Bann CM, Williams-Piehota PA, Whittam KP. Development and validation of the Navy Climate Index. Military Psychology. 23:253-271 (2011).

[44] Keeney M, Kowlaski E, Cappelli D, Moore A, Shimeall T, Rogers S. Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors. U.S Secret Service and CERT Coordination Center/SEI (2005)

[45] Bell AJC, Rogers MB, Pearce JM. The Insider Threat: Behavioral indicators and factors influencing likelihood of intervention. International Journal of Critical Infrastructure Protection (2018) doi https://doi.org/10.1016/j.ijcip.2018.12.001.

behavioral indictors of insider threats, clear, confidential reporting processes, and a culture where respectful challenge is encouraged.[46]

The insider threat problem, while global in nature,[47] may not lend itself to similar solutions in all nations and cultures where the threat arises. Even in the West, there is incomplete adoption of efforts to reduce insider threat by fostering organizational cultures of mutual responsibility for safety and security, encouraging coworker willingness to intervene when colleagues appear to be in need of assistance, and an occupational health approach that encourages employees to seek help for mental health problems and other conditions. In other cultures, where the prevalence of mental illness is just has high, but acceptance of the idea of treatment is much lower, fulfilling such recommendations will be even more difficult. In countries with past or current authoritarian rule, coworkers will likely be reluctant to speak to a supervisor about a colleague who appears to be in distress.

Thus, while nuclear nations have a shared interest in the prevention of insider threats, the development of effective prevention and intervention measures must be part of a larger conversation aimed at developing culturally appropriate measures.

Conclusion

The risk of insider threats is real, global, and likely to increase along with world and domestic tensions and socio-cultural changes. Combatting that risk will require a comprehensive approach that recognizes cultural and societal differences, as well as awareness that policies, procedures, and technical solutions are dependent upon acceptance of the risk and the full engagement of the nuclear work-force.

III. ENDNOTES

IV. TECHNOLOGY FOR GLOBAL SECURITY INVITES YOUR RESPONSE

Technology for Global Security invites your responses to this report. Please send responses to: info@tech4gs.org. Responses will be considered for redistribution to the network only if they include the author's name, affiliation, and explicit consent

[46] Bunn M, Sagan SD. A Worst Practices Guide to Insider Threat: Lessons from Past Mistakes. Cambridge, MA: American Academy of Arts and Sciences, 2014; Stern J, Schouten R**:** Chapter 3 Lessons from the Anthrax Letters. In Bunn M, Sagan SD, Eds. Insider Threats. London: Cornell University Press, 2016; Saathoff, G, DeFrancisco G, Benedek D, Everett A, Holstege C, Johnson S, Lamberti J.S., Schouten R, White, J. The Amerithrax Case: Report of the Expert Behavioral Analysis Panel. Charlottesville, VA: Research Strategies Network, 2011.

[47] Grogan S. China, nuclear security and terrorism: implications for the United States. Orbis. 53(4): 685-704 (2009); Bunn M, Sagan SD. A Worst Practices Guide to Insider Threat: Lessons from Past Mistakes. Cambridge, MA: American Academy of Arts and Sciences, 2014; Bunn M. Scenarios of Insider Threat to Japan's Nuclear Facilities and Materials—Steps to Strengthen Protection. Nautilus Peace and Security NAPSNet Special Report. November 2, 2017.