International Journal of Nuclear Security

Volume 9
Number 3 *International Journal of Nuclear Security–Nuclear Security Women 2024 Special Issue*

Article 9

1-2025

Enhancing Nuclear and Radiological Security in Polarized Times: Safeguarding Against Extremist Insider Threats

Jessica Baweja
Pacific Northwest National Laboratory

Madelyn Dunning
Pacific Northwest National Laboratory

Keithan Rogers
Pacific Northwest National Laboratory

Enhancing Nuclear and Radiological Security in Polarized Times: Safeguarding Against Extremist Insider Threats

Cover Page Footnote

The authors express appreciation to the US Department of Energy, National Nuclear Security Administration, Office of Radiological Security for their support of this work. Pacific Northwest National Laboratory (PNNL) is operated by Battelle Memorial Institute for the US Department of Energy under contract DE-AC05-76RL01830.

International Journal of Nuclear Security–Nuclear Security Women Special Issue, Vol. 9, No. 3, 2024

Enhancing Nuclear and Radiological Security in Polarized Times: Safeguarding Against Extremist Insider Threats

Jessica Baweja, Madelyn Dunning, and Keithan Rogers
Pacific Northwest National Laboratory

Abstract

Domestic violent extremism has been on the rise in recent years, fueled by growing political polarization, the COVID-19 pandemic, and the spread of misinformation online. This concerning trend raises an important question: has this increase in extremist violence manifested in more incidents involving radioactive or nuclear (RN) materials and a corresponding security concern? To explore this question, we analyzed existing data on events involving chemical, biological, radiological, or nuclear materials over time. Specifically, we examined the rate of RN-related incidents, the targets of these events, and the ideologies motivating the perpetrators by using the Violent Non-State Actor Chemical, Biological, Radiological, and Nuclear Event Database from the National Consortium for the Study of Terrorism and Responses to Terrorism. Our analysis aimed to determine whether the broader rise of violent extremism has translated to an elevated risk of attacks involving RN materials. Results of the analysis revealed that there was no clear increase in events involving RN material in the dataset. However, given the rarity of these events, this conclusion does not indicate that such a trend might not appear in coming years if violent extremism continues to rise. To address the potential risk presented by violent extremism, in addition to quantifying the frequency of RN events, we also reviewed traits that could make organizations more susceptible to insider threats from radicalized employees. Focusing on the literature around counterproductive workplace behavior, we identified organizational characteristics that might increase the risk of malicious acts committed by radicalized insiders. These risk factors include abusive leadership, situational constraints, and organizational injustice. Finally, using these organizational risk characteristics, we discuss interventions that organizations with RN material can take to reduce their risk of attacks stemming from violent extremism while still protecting individual rights to privacy and civil liberties. Overall, this

DOI: 10.7290/ijns09317753

International Journal of Nuclear Security–Nuclear Security Women Special Issue, Vol. 9, No. 3, 2024

article provides an overview of the intersections between rising domestic extremism, insider threats, and risks posed by RN materials. We present current data on trends and patterns in this space as well as practical guidance for organizational resilience.

Keywords: extremism, insider threat, organizational resilience

1. Introduction

In 2017, Brandon Russell emerged on the radar of law enforcement authorities during a homicide inquiry, wherein one of his three cohabitants had fatally assaulted another [1]. The ensuing investigation sought to unravel the circumstances of the murder but also inadvertently exposed the clandestine activities of the residents. Russell and his associates, identified as neo-Nazis, had been clandestinely amassing explosive substances and other components essential for the creation of destructive devices within their shared residence in Tampa, Florida. Notably, the discovery included two radioactive elements: thorium and americium. These materials were intended for use in violent attacks fueled by their extremist ideologies. Russell's involvement in these dangerous plots led to a 5-year prison sentence. Upon his release in 2021, he swiftly reverted to his previous extremist lifestyle. Currently, Russell is facing impending legal proceedings for his alleged involvement in orchestrating attacks on critical infrastructure [2]. This case of Brandon Russell serves as a stark illustration of how extremist ideologies can potentially culminate in attempts to execute acts of mass violence.

As the case of Brandon Russell illustrates, major national security concerns exist regarding the rise in domestic violent extremism (DVE) in the US. Domestic political polarization, the COVID-19 pandemic, and the growth in the spread of false information through online and other means have contributed to a rise in civil unrest domestically and internationally. This rise in civil unrest has manifested in an increase in violent extremist incidents, particularly from the far right [1, 3, 4]. In the US, this increase in extremist violence manifested most notably in the attack on the US Capitol on January 6, 2021. It has also resulted in concerns about the threat that such violent extremists might pose to the security of radioactive or nuclear material (RN). For example, Fleer [1] presents three case studies of radiological weapons from the far right, demonstrating that violent extremists can and do seek RN material to commit acts of violence. Nair and colleagues [5] also recently highlighted the threat that radicalized insiders might pose to facilities with nuclear materials.

As the threat has evolved, it is important to assess whether concerns about DVE have manifested in an increase in incidents involving RN material. Given that many of the incidents involving RN material have been perpetrated by insiders, it is also critical that we explore the characteristics that might make organizations more vulnerable to these insider threats [6]. This study therefore explored the potential changes in violent extremist incidents involving RN materials as well as the organizational traits that might make an organization vulnerable to insider threats seeking RN material.

DOI: 10.7290/ijns09317753

a. Violent Extremist Threat to RN Material

Little doubt exists that the threat landscape has changed drastically in recent years. The current highly polarized political environment has led to an increased risk of extremist attacks, particularly within the US. On May 24, 2023, the US Department of Homeland Security (DHS) released the most recent National Terrorism Advisory bulletin warning that the US remains in a heightened threat environment and there is an increased risk of attacks by lone offenders and small groups motivated by ideological beliefs [7]. The same week, Oath Keepers founder Steward Rhodes was sentenced to 18 years in prison for seditious conspiracy for his part in orchestrating the attack on the US Capitol Building on January 6, 2021 [8]. The Biden Administration has recognized the need to address this growing extremist threat within the US, releasing the first "National Strategy for Countering Domestic Terrorism" in June 2021 [9], followed by the first US "National Strategy to Counter Antisemitism" in May 2023 [10].

According to the Global Terrorism Index report [11], ideological terrorism has overtaken religious terrorism in the West (including North America), and there has been a steady increase in ideologically motivated attacks over the last decade. There were 14 deaths in 2022 from ideologically motivated terrorism; the deadliest attack occurred in the US, when a lone shooter killed 10 people in a racially motivated shooting in a Buffalo, New York, grocery store [12]. All those deaths were attributed to perpetrators with far-right views [11]. Existing reports suggest that the threat of extremism may have increased, particularly in the West and North America.

This changing threat, particularly from lone actors, may warrant a change in our understanding of the threats to RN material. One goal of the current study, therefore, was to explore recent attacks, especially those involving RN material, to understand whether a significant change has occurred in the rate or targets of these attacks over time.

b. Organizational Traits

In addition to exploring whether there have been changes in the capabilities and attributes of potential insider adversaries, this study also examined characteristics that might make organizations more or less vulnerable to insider threats seeking RN material. A surprisingly small amount of research exists on the characteristics of organizations that might make them vulnerable to insider threats. Some work that exists has looked at security culture or awareness and demographic characteristics that predict it [13]. Other work has explored an overall risk index for radiological material that accounts for the probability and magnitude of an event involving an radiological exposure device or radiological dispersal device for a specific facility [14].

Despite the lack of focus on organizational traits, it is clear that organizations contribute to the likelihood of insider attacks, particularly if they respond to a concerning situation in a maladaptive way [15]. Additionally, organizational policies and procedures, such as access control policies, can either increase or decrease the likelihood of success for an insider attack [16]. One important aspect of mitigating insider risk is understanding the ways that propensities toward insider threats might interact with specific organizational

DOI: 10.7290/ijns09317753

International Journal of Nuclear Security–Nuclear Security Women Special Issue, Vol. 9, No. 3, 2024

traits—for example, are there especially concerning combinations of risk and vulnerability that might occur at RN facilities? To address these questions, in addition to exploring the potential changes that may have occurred to insider risks, this study also explored organizational traits to identify those areas that might place an organization at greater risk for insider threats.

c. Current Study

The current study explored two primary research questions:

- Has the violent extremist threat to RN material changed substantially in recent years in the rate of incidents, the targets, or the ideologies of their primary actors?
- What characteristics might make organizations more vulnerable to insider threats, and how can those vulnerabilities be addressed?

As it relates to the risk of insider threats, this study explored trends in domestic violent extremism, RN incidents, and their ideologies and targets. Although the focus of this study is the US, to maximize understanding of RN incidents, we include data from both domestic and international incidents. Additionally, we examined the traits that might make RN organizations more vulnerable to insider threats as well as interventions to address them.

2. Method

To address these research questions, this study used a combination of secondary data analysis and literature review.

a. Secondary Data Analysis

To understand changes in the rate of RN events over time, data were analyzed from the University of Maryland's National Consortium for the Study of Terrorism and Responses to Terrorism (START) [17]. These data included records of chemical, biological, radiological, and nuclear (CBRN) events plotted or completed by violent non-state actors (VNSA). These data were analyzed to identify any trends in RN events domestically or internationally, particularly as they relate to radioactive material or events involving insiders. Note that data from all events (not just the US) were included to maximize sample size, although many of the issues and interventions discussed here are primarily US-focused.

b. Literature Review

The literature review was conducted to gather relevant information on insider threats and organizational characteristics from existing scholarly articles, books, conference papers, and other academic sources. A systematic search strategy was developed to identify relevant literature. Search engines and databases such as Google Scholar were used. The search terms included combinations of keywords such as "insider threats," "organizational characteristics," "organizational traits," "organizational risks and insider threat," "organizational risk and radicalization," and "domestic violent extremism and

DOI: 10.7290/ijns09317753

organizational risk." Articles were selected based on their relevance to RN extremism and insider threats as well as publication date (to ensure current social relevance).

3. Results

a. Event Rate, Targets, and Ideology Over Time

The VNSA CBRN event database catalogs all international events with CBRN material that involve intentional acts of violence or attempted violence perpetrated by non-state actors that are not purely criminal in nature (e.g., financially motivated). The events range in completion from protoplots to successful attacks. Like many other datasets, these events are compiled from media reports and other sources. There are 565 events in the database. Table 1 shows a breakdown of the events by type (i.e., RN and non-RN) and whether those events involved insiders. As the table shows, most of the events were non-RN and did not involve insiders. However, there were 69 RN events, and of those, 5 involved an insider.

Table 1. Type of events in VNSA CBRN event data.

	Insider	No Insider	Total
Non-RN	19 (3.4%)	477 (84.4%)	496 (87.8%)
RN	5 (0.9%)	64 (11.3%)	69 (12.2%)
Total	24 (4.2%)	541 (95.8%)	565 (100%)

The primary question of interest for these data is whether the rate of events involving RN material has changed over time. To answer this question, Figure 1 shows the rates of RN events over time. As the figure shows, few RN events have occurred in general, with the highest number of events occurring in 1996, 2001, and 2003 (all $n = 7$). If anything, recent years appear to show a declining trend, although given the low number of events overall, such a change is difficult to interpret.

To explore whether the targets or ideologies have changed in recent years, we also examined changes in ideology and target over time for RN events. Due to the small number of events annually, years were divided into 5-year spans. Figure 2 shows the ideologies associated with events each year (proportionally). Note that because the database exists at the *event* rather than the *actor* level, these analyses focus on the target or the ideology of the primary actor in each event. These ideologies are shown proportionally (i.e., by percentage of events associated with each ideology over time). Similarly, Figure 3 shows the targets of RN events annually (by proportion of events). Table 2 and Table 3 show the number of events within each timeframe by ideology and target, respectively, to help provide some context to the associated figures. For simplicity, some categories of targets were combined. The original dataset contained 28 different target types; these were combined into the eight categories shown in the chart. Overall, these figures suggest that there has perhaps been some change in ideology, with an increase in unknown ideologies associated with RN events. When examining the targets of the planned events, the results show that there appears to an increase in events targeting government, military, or police facilities or personnel.

DOI: 10.7290/ijns09317753

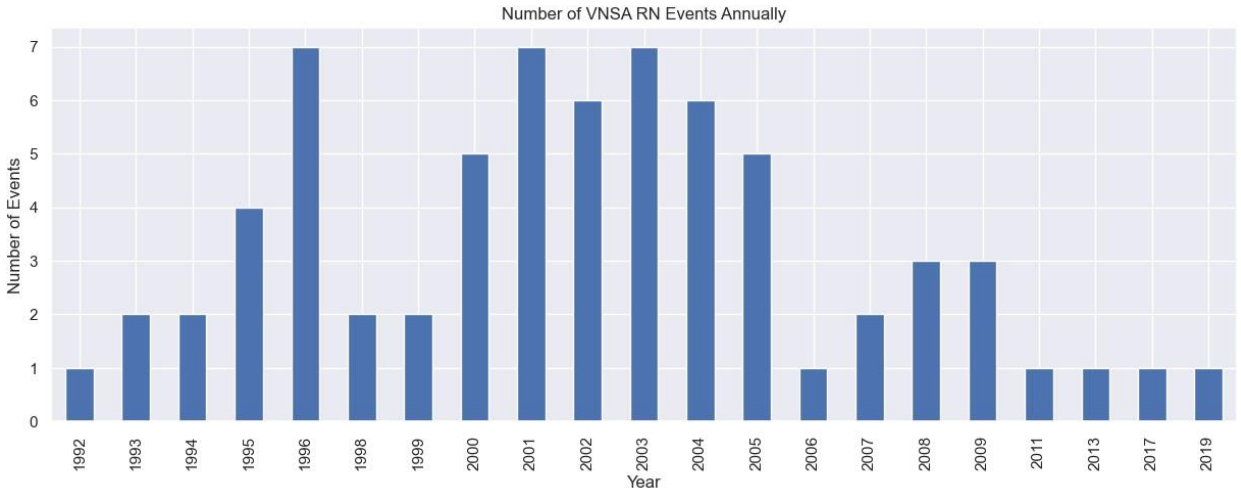

Figure 1. Number of VNSA RN events annually.

Table 2. Ideology and number of RN events in over time.

Years	Criminal	Ethno-nationalist	Religious (New)	Religious (Traditional)	Right-wing	Unknown	Total
1990–1994	0	2	2	1	0	0	5
1995–1999	1	11	0	1	1	1	15
2000–2004	2	7	1	18	0	3	31
2005–2009	3	1	0	5	0	5	14
2010–2014	0	1	0	1	0	0	2
2015–2019	0	0	0	1	1	0	2

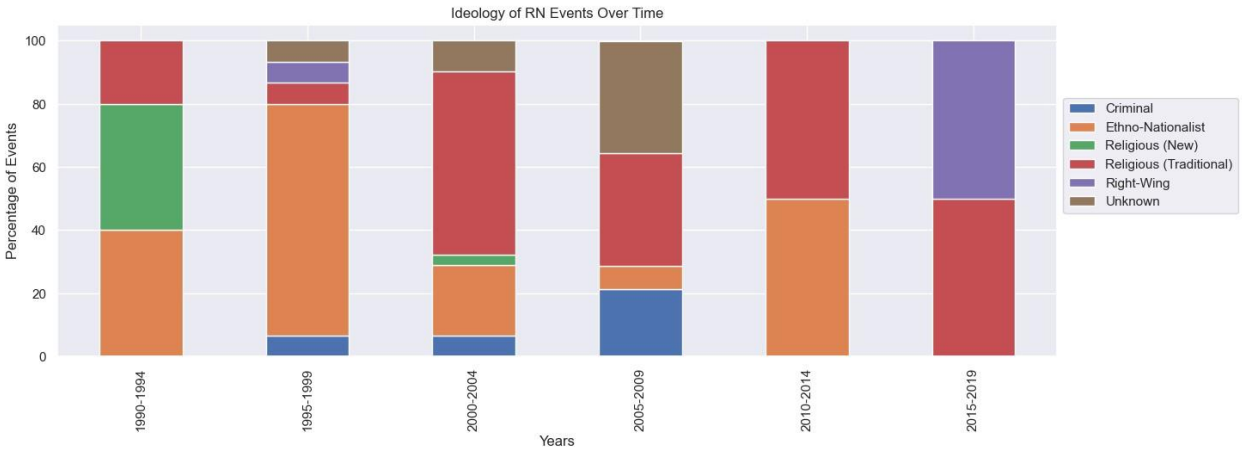

Figure 2. Proportion of RN events by ideology in over time.

DOI: 10.7290/ijns09317753

Table 3. Number of RN events by target over time.

Years	Business	Government, Military, or Police	None	Private	Public Institution	Religious or Historical	Unknown	Total
1990–1994	0	0	1	0	0	0	4	5
1995–1999	0	5	1	2	0	0	7	15
2000–2004	4	3	1	0	6	0	17	31
2005–2009	1	3	3	0	2	1	4	14
2010–2014	0	1	0	0	1	0	0	2
2015–2019	0	1	1	0	0	0	0	2

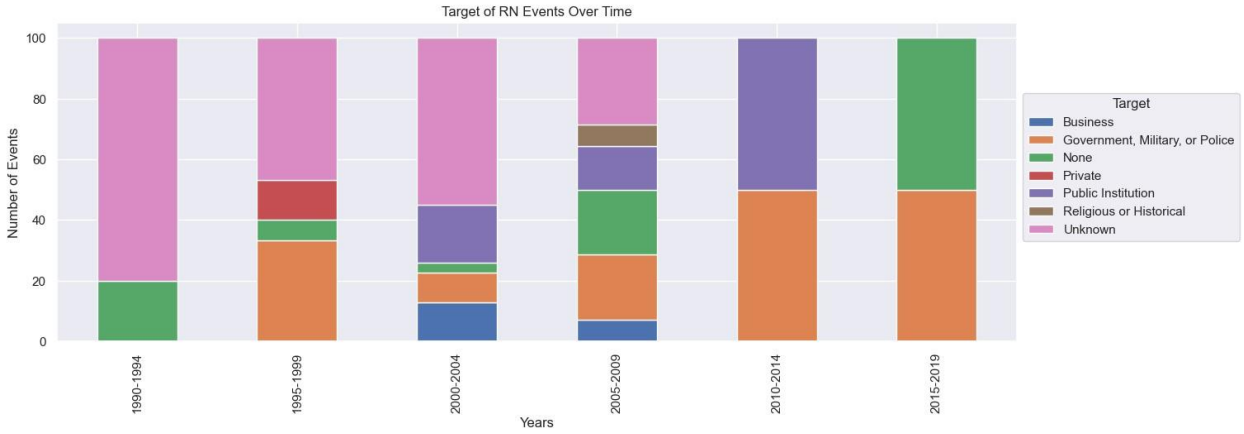

Figure 3. Proportion of RN events by target over time.

Finally, to understand whether the tactics for acquiring RN material have changed, Figure 4 shows the acquisition method for RN materials over time proportionally. Table 4 shows the corresponding numbers of events. The results generally suggest that in many cases, the method of acquisition remains unknown, although in a reasonable proportion of cases, the method of acquisition was production of the material.

Table 4. Number of events by acquisition method over time.

Years	Facility	Production	Purchase	Serendipity	Theft	Training	Unknown	Total
1990–1994	0	2	1	1	0	0	1	5
1995–1999	0	0	2	0	3	0	10	15
2000–2004	5	4	4	0	5	0	13	31
2005–2009	1	1	2	0	1	1	8	14
2010–2014	1	1	0	0	0	0	0	2
2015–2019	0	2	0	0	0	0	0	2

DOI: 10.7290/ijns09317753

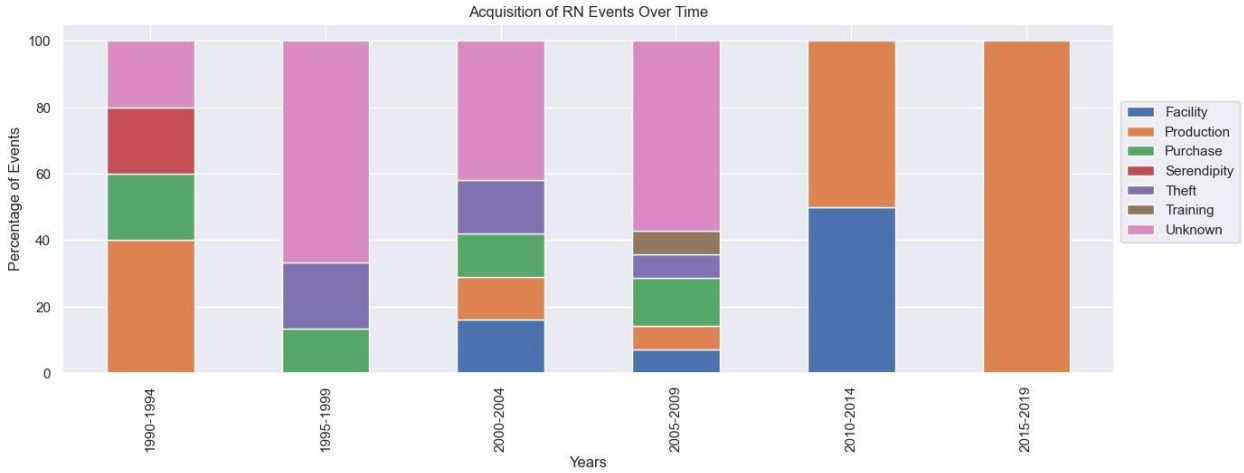

Figure 4. Proportion of events by acquisition method over time.

b. Organizational Traits and Vulnerabilities

Knowledge pertaining to insider threat and the risk it poses to organizations has been steadily increasing over the past two decades, and organizations increasingly recognize the threat posed by insiders to sensitive information, hazardous material, or critical infrastructure. Particularly for facilities with RN material, insiders are a known and recognized threat; every successful theft for which the circumstances are known involved an insider [6]. In this section, we review some of the organizational factors that may make that organization more vulnerable to insider threats. For the purposes of this review, both unintentional and intentional insider threats are discussed.

A literature review was conducted to identify the traits of an organization that might be associated with greater risk of insider threat. However, the results of that review revealed that the organization as a component of the insider threat is generally overlooked, especially in the context of an intentional insider [18]. When discussing unintentional insiders, organizational characteristics such as inadequate procedures, poor communication, insufficient resources, poor management, inadequate security, pressure, time, difficulty, change in routine, poor planning, and lack of knowledge, skills, and ability have all been discussed [19]. There is a substantial relationship between the operation of the organization and the generally accepted causes of unintentional insider threat activities—that is, the organizational traits that contribute to human error [19].

In general, though, intentional insider threat research is heavily focused on the individual as the cause of insider threats, with the goal of enabling organizations to mitigate the threat the individual poses. In this study, we focus on the organizational traits that may make an organization more susceptible to an insider or, in some instances, may even foster the radicalization or action of an insider. The existing research most relevant to organizational factors and intentional insider threat has generally centered around counterproductive workplace behaviors (CWBs). CWBs are defined as behaviors that are intended to have a detrimental effect on organizations and their members; they are acts of intentional harm within the workplace [20]. They can include abuse, bullying, absenteeism, theft, tardiness, sabotage, or any other behaviors

DOI: 10.7290/ijns09317753

that are intended to cause harm to the organization or its members in some way. They have previously been used as a precursor to insider threat or a behavior on the insider threat spectrum that may not rise to the level of making the person an adversary of the organization [21]. In other words, CWBs include a wide spread of behaviors, some of which reflect threat indicators (e.g., absenteeism, workplace conflict) and some of which represent actual adversary behaviors (e.g., theft, sabotage). Because the literature does not distinguish between indicators of possible threats and adversarial behavior, the review in this article is combined. Thus, in this section, we review the organizational factors that have been found to be associated with a greater risk of CWBs to understand which organizational factors might convey a greater risk of insider threat. To do so, we relied on a large existing body of research on CWBs and their opposite organizational citizenship behaviors (OCB). CWBs can include both active and passive acts, such as aggression, theft, sabotage, arriving to work late, taking excessive breaks, or purposefully ignoring policy or procedure. In this article, we divide the characteristics that were identified as contributing to the insider threat into operational and intangible traits. Of course, this is not an exhaustive list—as research continues within the nexus of organizational characteristics and insider threat, more traits will likely be identified. Based on the literature review, the traits identified as most relevant to risk of insider threat were leadership, situational constraints, security culture, organizational justice, organizational pride, and person–environment (PE) fit. Each of these characteristics is discussed in the following subsections.

Leadership

A clear relationship exists between leadership and CWBs [22–24]. Researchers have explored a few different theories to explain this association, including social learning theory (i.e., suggesting that employees learn by example), social exchange theory (i.e., CWBs may result when leaders violate a social contract), and social identity theory (i.e., pride and personal investment may relate to the likelihood of CWBs). A recent meta-analysis [24] suggested that social learning theory may be the best explanation for the association between leadership and CWB; however, regardless of the specific mechanism, leadership has shown to be highly important to the rate of CWBs and therefore is relevant to the risk of insider threat.

A few different leadership styles have been explored when examining precursors to employee CWB. On the positive end of the spectrum, ethical leadership is defined as the demonstration of normatively appropriate conduct through personal actions, interpersonal relationships, and the promotion of such conduct to follow two-way communication, reinforcement, and decision-making [25]. A direct correlation exists between promotion-focused ethical leadership and perceived or felt trust by employees toward their organization. Bush et al. [25] found that leadership styles that promote and reward good behaviors increase employees' sense of feeling trusted and lower CWBs. Leadership styles that focus on preventing bad behavior have the opposite effect. On the negative end of the spectrum, abusive supervision has been linked to higher rates of CWB in employees [26, 27]. In general, experiences of emotional abuse in the workplace have been found to lower organizational commitment, OCB, cohesiveness,

DOI: 10.7290/ijns09317753

productivity, and job satisfaction and also increase turnover, absenteeism, CWB, and withdrawal [28].

Like much of the literature relating to insider threats, the literature on CWBs focuses on explaining the behavior from an individual psychological perspective rather than an organizational one. Carpenter et al. [29] noted that this focus is surprising because most CWB driving factors are organizational—for example, human resources systems, leadership, norms, or policies. To explore this idea, they examined the concept of "unit-level" CWB, in which CWBs exist at a level higher than the individual. They found that abusive supervision increased unit-level CWB and transformational leadership (inspiration-based) decreased CWB [29]. By exploring the phenomenon of CWB at a greater-than-individual level, this study allowed for the exploration of larger organizational factors on the behavior among employees as a whole and demonstrated that characteristics such as leadership can affect employees as a group. This conclusion is in contrast to examining how individual characteristics might predict or explain CWBs (or insider threat).

Overall, many studies have found that leadership has a direct effect on CWB [22–24]. There is an increasing body of evidence that suggests that leadership behavior, when positive, can promote good behavior but when abusive or problematic can increase the likelihood of CWBs and potentially of insider threat activities. When addressing the vulnerabilities of an organization to insider threat, leadership behavior is therefore an important consideration.

Situational Constraints

Situational constraints are anything that prevent or stop an organization or an individual from attaining a personal or organizational goal [30]. Situational constraints can include a lack of office supplies, lack of support from management, lack of training, and more. Multiple studies have investigated the link between CWBs and situational or job constraints [30, 31]. CWBs are often considered to be a result of the frustration arising from situational constraints. In this perspective, situational constraints create frustration by preventing people from reaching their goals, and when frustration increases, it can lead to acts of aggression in the form of CWBs. Other studies have supported the link between organizational or situational constraints and CWBs—for instance, Fox et al. [32] found that organizations in which employes perceive greater work constraints, more negative emotions, more conflict, and lower autonomy have higher levels of CWBs among employees.

In addition to frustration resulting from situational or job constraints, there is also evidence that the opposite may be true—that is, a sense of ownership and control may be important to job satisfaction and reduced CWBs. Tsai [33] recently explored the concept of job crafting and its relationship to CWBs. Job crafting refers to the ability of an employee to shape their own work environment to fit their needs and interests. They found that job crafting predicted a sense of psychological ownership, or a sense that the job or the organization is theirs. Psychological ownership, in turn, positively predicted work engagement and negatively predicted the likelihood of CWBs. This prediction

DOI: 10.7290/ijns09317753

suggests that allowing employees to have control (i.e., a lack of constraints) can help to increase their engagement and decrease the likelihood that they will engage in misbehaviors. As a whole, these studies suggest that situational constraints can increase frustration, and an organization whose employees experience high levels of constraint might therefore have a greater risk of insider threat. In contrast, organizations in which employees feel a sense of control over their role are more engaged and less likely to engage in CWBs.

Security Culture

Security culture is a concept with a variety of definitions depending on the context, such as information or material. In the nuclear material domain, the International Atomic Energy Agency (IAEA) defines nuclear security culture as "the assembly of characteristics, attitudes, and behavior of individuals, organizations, and institutions that serves as a means to support and enhance nuclear security" [34]. In the academic literature, the related concept of information security culture is probably the most widely studied type of security culture and is defined as the collection of perceptions, attitudes, values, assumptions, and knowledge that guides how things are done in an organization to be consistent with information security requirements, with the aim of protecting the information assets and influencing employees' security behavior in a way that preserves the information security such that it becomes second nature [35]. Underlying both definitions is the idea that security culture involves integrating security within the daily lives of employees and the general recognition that security is a critical part of every employee's job and responsibilities. As a result of this belief and investment, it is reasonable to suggest that organizations with a mature security culture are less likely to suffer an insider threat.

One way that researchers have explored the effect of security culture is through studies of organizational climate. Organizations with a strong compliance climate—in which employees feel a high level of respect for organizational standards, procedures, and policies—were found to have a lower rate of CWBs [36]. In contrast, organizations that focus on a relational climate in which employees have strong social relationships had a greater rate of counterproductive work behaviors. However, the concept of security culture is one that is understudied, and so there is a lack of strong evidence linking security culture to CWBs or insider threats. Initial results do suggest that security culture is an important organizational trait for conferring risk of insider threats, and the enhancement of security culture might help to mitigate that risk.

Organizational Justice

Organizational justice consists of three components: distributive justice, or a fairness of outcomes; procedural justice, or the perceived fairness of the processes that end in outcomes; and interactional justice, or the fairness of interpersonal treatment and communication by management to employees [37]. A 2001 meta-analysis [37] explored the associations between these different components of organizational justice and CWBs and OCBs. Across 190 different studies, they found that a sense of organizational justice predicts the likelihood of engaging in OCBs and CWBs as well as employees' organizational commitment and turnover intentions (i.e., the likelihood that

DOI: 10.7290/ijns09317753

International Journal of Nuclear Security–Nuclear Security Women Special Issue, Vol. 9, No. 3, 2024

they plan to leave the organization). The study found that work performance was most closely related to procedural justice and that OCBs increased when distributive and procedural justice were high. They also found that job satisfaction was most closely tied to distributive justice—specifically, salary. Commitment to the organization was enhanced when the perception of justice was high. Finally, they found that CWBs were closely related to all three forms of justice. Studies have also explored the relationships between leadership, justice, and CWBs—Holtz and Harold [22] found that leadership behaviors affect employee perceptions of justice, although perceptions of justice did not mediate the relationship between leadership behaviors and CWBs. Leadership, then, may affect perceptions of justice, although both perceptions of justice and leadership directly relate to CWBs.

In another study demonstrating the interrelationships between these concepts, Jones [38] explored the associations between perceived injustice and desires for revenge against one's supervisor. Results of the study demonstrated that employees tended to direct their CWB toward the source of their mistreatment or perceived injustice, suggesting that a desire for revenge against leadership may explain at least some of the association between perceived injustice and CWBs. Overall, perceptions of injustice within an organization clearly relate to the likelihood of employee misbehavior, suggesting that addressing concerns about organizational justice is a promising avenue for reducing the risk of insider threats.

Organizational Pride

Organizational pride is a collective form of pride that describes the pleasure taken in being associated with one's employer [39]. To some extent, it is related to the employee's evaluation of the organization's external reputation—if employees believe that the organization is perceived well, they may be prouder to be associated with it. Good evidence exists that a sense of organizational pride relates to employee outcomes. A sense of concern for the organization, including a sense of pride for it, has been found to relate to a greater rate of organizational citizenship behavior [40]. Organizational pride and job satisfaction also mediated the relationship between employees' perception of the organization's external reputation and their turnover intentions [39]. A more recent study demonstrated that employees' level of pride in their organization affects their task performance as well as their OCBs. Similar to research exploring the effect of leadership, researchers have argued that the social identity (i.e., a sense of belonging or oneness with the group) can help to explain the relationships between organizational pride and CWB or OCB.

Overall, the literature suggests that an association exists between an employee's sense of pride in an organization and the likelihood of good or bad behavior at work. Employees who feel that the organization is one to be proud of are less likely to engage in problematic behavior and more likely to engage in positive behaviors, suggesting that organizations for which employees feel a greater sense of pride are at lower risk of insider threat.

DOI: 10.7290/ijns09317753

Person–Environment Fit

PE fit refers to the compatibility between an individual and a work environment, or when their "characteristics are well-matched" [41]. This broad concept can apply to the match between the employee and their interests, values, culture, preferences, or knowledge and a variety of environmental factors, such as the organization overall, their job, or their work group. It is probably not surprising that there is good evidence that this sense of fit is predictive of employee behavior—desired behaviors occur more often when the fit is good. For instance, high PE fit is associated with job satisfaction, organizational commitment, and a low intent to quit. There is also evidence that misfit causes stress and strain, especially what has been termed "needs–supplies" fit—the match between an employee's needs and what the organization is able to provide [42]. For example, if an employee has a high need for autonomy that is not met at their job, this may lead to needs–supplies misfit and stress or strain. Vocational interest, one aspect of PE fit (i.e., person–vocation fit), has been found to be related to job performance, CWB, and OCB [43]. Another study also found an association between vocational interest and job performance, suggesting that vocational interests may be important to a satisfying employment experience [44]. Overall, the match between the person and the job appears to relate to job satisfaction, turnover, and employee behavior, which suggest that efforts to maximize the fit through personnel selection procedures may be one way of reducing the risk of insider threat. Unlike other organizational traits examined here, PE fit is a combination of personal and organizational characteristics; however, organizational procedures that attempt to maximize employee fit could nonetheless be used as one method to reduce the likelihood of CWB, increase OCB, and potentially have more satisfied employees. Thus, increased PE fit for individuals in an organization might reduce the likelihood of insider threats.

c. Interventions

Based on the CWB and OCB literature, three categories of interventions are highlighted: interventions targeting security culture and employee reporting; leadership interventions, especially focused on fairness and justice; and organizational self-assessment.

Enhancing Security Culture, Reducing Situational Constraints, and Increasing Employee Reporting

Enhancing security culture is one method of helping RN facilities become more resilient to the threats posed by radicalized insiders. This sentiment is echoed in the broader literature on radicalization, in which experts discussed the need to foster resilience to help individuals avoid being drawn into extremist groups [45]. Recent guidance from the World Institute for Nuclear Security (WINS) also discussed nuclear security culture as one factor in helping organizations prevent the threat of DVE [46]. The IAEA provides specific interventions for enhancing nuclear security culture in organizations, including security awareness, management training, and codes of conduct [47]. Notably, however, a need exists for additional research on initiatives for strengthening security culture [48].

DOI: 10.7290/ijns09317753

International Journal of Nuclear Security–Nuclear Security Women Special Issue, Vol. 9, No. 3, 2024

As one way of fostering a stronger security culture while also reducing situational constraints, organizations should develop an employee reporting program to share concerns about the organization and ways the organization might improve. Such a program would help to reduce the feelings of frustration and constraints by giving employees a sense of control. In addition to associations with CWBs, the importance of this need for control is also highlighted in the literature on radicalization, in which studies have repeatedly identified grievances as playing a key role in radicalization [49–51]. Reducing situational constraints, increasing a sense of control, and providing a means for raising grievances to leadership is one way that organizations can intervene to reduce the likelihood that employees might turn to violence or other extremist acts.

Ethical Leadership Training, Justice, and Fairness

Leadership interventions can play a significant role in increasing ethical leadership, reducing abusive supervision, and mitigating the risk of insider threats. Training supervisors to understand the value of supportive supervision can be a practical first step toward reducing abusive supervision [52]. A recent study described training designed to provide supervisors with strategies to handle difficult situations and offer positive feedback as they observe the favorable reactions to supportive supervision. This training can help to educate supervisors about the negative consequences of abuse and promote constructive problem-solving approaches to minimize destructive employee responses to abuse [52]. The program was found to be successful in enhancing the perceived support provided by supervisors to their subordinates.

Jeon et al. [53] also recently described the results of an ethical leadership program designed to improve the ethical leadership skills of managers, which was especially effective in improving people's orientation and concern for sustainability. The program also had a positive effect on the OCBs and job outcomes of the unit managers. Furthermore, the program was found to positively influence the perceptions of staff nurses about their unit managers' ethical leadership, OCB, job outcomes, and ethical work environments. This result suggests that training on ethical leadership can play a crucial role in producing positive organizational outcomes and reducing insider threats.

These studies provide valuable insight into the role of leadership in fostering a sense of fairness and justice within organizations. Gonzalez et al. [52] proposed a training program for supervisors that emphasizes sincerity, mindfulness, and fairness, which have been found to enhance the perceived support provided by supervisors to their subordinates. This support, in turn, can foster a sense of fairness and justice and reduce the risk of insider threats. Jeon et al. [53] discussed an ethical leadership program designed to help these managers understand ethical leadership and facilitate their participation in creating ethical environments and cultures in their hospitals. Both interventions highlight the roles that leaders can play in improving culture and fairness as well as reducing the risk of insider threats within organizations.

Organizational Self-Assessment

The review of the literature demonstrated that organizational factors can be powerful determinants of employee behavior—both good (i.e., OCB) and bad (i.e., CWB). This

DOI: 10.7290/ijns09317753

result suggests that when examining the vulnerabilities of an organization to insider threats, in addition to examining those employees who may individually present a risk (e.g., through surveillance, vetting, monitoring, or observation), organizations should also conduct assessments of their own characteristics. In doing so, they may identify areas for organizational improvement that could reduce the likelihood of insider threats overall. Although no single trait can be targeted to eliminate the potential for insider threats, we believe that a holistic approach to evaluating an organization based on the identified traits can augment an insider threat mitigation program and would have significant downstream benefits to an organization that would include higher efficiency, retention, and organizational pride for its employees. To evaluate or assess organizational traits, Table 5 presents the organizational trait, the key question associated with that trait, and the potential data sources that might be relevant to evaluating that trait. Additional information about how to collect and analyze relevant information can be found in IAEA guidance on nuclear security self-assessment [54], which provides extensive examples of surveys specific to those topics. In general, the results of this report help to provide some information of the kinds of traits that are most relevant organizationally to the risk of insider threats; developing these into a self-assessment method would be a useful future addition.

Table 5. Data sources for organizational assessment.

Trait	Key Question	Data Sources
Material Consequence	What is the material used, what are the consequences if stolen or misused, and how easy is that potential misuse?	Document review (e.g., material accounting and control records)
Campus Accessibility	To what degree is access to the facility open or restricted?	Document review (e.g., access control procedures)
Leadership	What are the characteristics of leaders within the organization, and how are the leaders perceived?	Employee and leadership interviews, surveys, observations, document review (e.g., training procedures, leadership policies)
Situational Constraints	Do employees have access to the resources they need, and do they have the freedom and autonomy to do their jobs successfully?	Employee and leadership interviews, surveys
Security Culture	To what degree is security integrated in employees' daily activities?	Employee and leadership interviews, surveys, observations document review (e.g., security policies, employee training)
Organizational Justice	Do employees feel that they are treated fairly by the organization?	Employee and leadership interviews, surveys, observations document review (e.g., leadership policies, compensation procedures)
Organizational Pride	Do employees feel a sense of pride working for the organization?	Employee and leadership interviews, surveys
PE Fit	Do employees feel that their job and organization match their needs and interests?	Employee interviews, surveys

4. Discussion

This study examined the changes in risk to RN material specifically presented by the changes in risk of violent extremism or terrorism. We also conducted a preliminary

DOI: 10.7290/ijns09317753

exploration of the organizational traits that might be most relevant to the risk of insider threats. Implications of the findings for changes in threats to RN material and organizational traits relevant to insider risk are discussed in the following subsections.

a. Threats to RN Material

This study explored whether the threat of insiders to facilities with RN material has increased in recent years. To answer this question, we examined a secondary data source including information on theft or other events involving RN material to determine if the risk of these events has increased. Data from the University of Maryland did not show a consistent increase in ideologically motivated violence involving RN material. This conclusion, of course, does not exclude the possibility that RN events will increase based on the overall risk of violent extremism in the world. Rather, that increase may yet occur. Indeed, recent commentaries have suggested that, at least in the US, the response to the tempestuous political environment will likely determine how or whether political violence will increase [55].

The ideologies of RN actors were also explored. Notably, ideologies are useful from a practical standpoint only if they inform the targets or tactics used. Jones et al. [56] generated a comprehensive summary of the tactics and targets used by extremists of different ideological viewpoints; although there were some different trends among the three groups they generated, there seemed to be a general shift toward military, law enforcement, and government targets. This conclusion was mirrored in the results from the VNSA CBRN data examined here, which showed a shift toward the targeting of government, law enforcement, and military personnel as well as toward unknown ideology.

Connecting these findings to the overall risk to RN material, the somewhat optimistic result is that these incidents remain fortunately rare and do not seem to be increasing when reviewing the data used here. However, the more general data around DVE and the targeting of government, military, and law enforcement personnel suggest that the overall risk of these types of attacks has likely increased in recent years [4]. The threat posed to RN material is likely higher in the than in years past largely because of the fragile and fraught political environment increasing the risk of ideologically motivated actors.

b. Organizational Vulnerabilities

There is a general lack of research around the characteristics that might make an organization more vulnerable to a malicious insider attack [18]. However, a large body of work explores the factors that might increase the risk of CWBs in an employee population. To the extent that CWBs represent a form of insider threat, these characteristics might be helpful for consideration when assessing an organization’s vulnerability to insider threat.

Overall, the literature highlights several factors as being especially important to the occurrence of CWBs. Probably most mentioned are concepts around organizational justice, including procedural, distributional, and interactional justice [37]. Results also

DOI: 10.7290/ijns09317753

highlighted the roles of leadership, situational constraints, and security culture. Finally, a sense of organizational pride and a sense of fit with the organization, job, or vocation are also relevant to the risk of CWB or the likelihood of OCB. Overall, there is clear evidence that the ways that employees are treated (or the way that they perceive they are treated) by an organization is a critical component of job satisfaction and subsequent employee behavior. In this paper, we presented some of the key characteristics that seem to be most impactful from an organizational perspective for employee behavior. Information about these characteristics will need to be obtained by organizations using surveys, interviews, observations, and document reviews, which are the self-assessment methods described in IAEA guidance [54]. Future work should consider exploring the links between organizational traits and insider threats in past cases to understand how they may be linked. Additionally, conducting a pilot self-assessment of these characteristics would be a useful next step to explore the utility of these traits in identifying issues of security concern for facilities with radiological material.

c. Limitations

The primary limitation in this study is its reliance on a single dataset with a limited sample size. The extremely low frequency of RN events makes it difficult to establish definitive trends over time. The VNSA CBRN database may also have inherent biases based on the sources of information used to compile it, such as media reports, which may not provide a complete or unbiased representation of all RN events. Additionally, the findings here cannot demonstrate that the organizational interventions proposed will reduce the risk of insider threats because these factors were not studied experimentally. Furthermore, the findings—particularly those regarding organizational traits—may not be generalizable to all types of organizations or to those outside the US.

5. Conclusions and Future Research

This study presented a secondary analysis of violent events including RN materials as well as the organizational traits that may mitigate or amplify the risk of insider threats. Although the data do not indicate a significant increase in the frequency of RN events, there is a very slight shift toward unknown extremist ideologies and a potential change in targeted facilities moving toward government and military entities. The findings of the literature review highlight the possible role of organizational traits in influencing the likelihood of insider threats. Leadership quality, situational constraints, security culture, organizational justice, pride, and PE fit have all emerged as factors that may shape employee behavior and, by extension, organizational vulnerability to insider threats. Interventions aimed at enhancing these traits may therefore serve as protective measures against the potential radicalization and malicious actions of insiders.

The most notable finding here is that there is a lack of consistent data tracking for acts of domestic violent extremism in the US. The Federal Bureau of Investigation (FBI) and DHS have jointly been charged with tracking these events in the very recent past (i.e., beginning in 2020), but these two agencies use slightly different definitions of domestic terrorism. Due to the lack of a charging statute for domestic terrorism, specifically, these

DOI: 10.7290/ijns09317753

data are likely incomplete. Future work should explore ways to address this gap, including collaborations with federal agencies.

This study underscores the critical need for ongoing research and proactive measures in the realm of DVE and the protection of RN materials. The insights gained from examining the interplay between extremist ideologies, the frequency and nature of RN events, and organizational vulnerabilities provide a foundation for developing more effective countermeasures. As we refine our understanding of the factors that contribute to organizational resilience, it is important to implement evidence-based strategies that enhance detection, prevention, and response capabilities. The pursuit of enhanced security culture, leadership training, and organizational justice is a practical imperative to help mitigate the risks associated with violent extremism.

6. Acknowledgments

The authors express appreciation to the US Department of Energy's National Nuclear Security Administration Office of Radiological Security for their support of this work. Pacific Northwest National Laboratory is operated by Battelle Memorial Institute for the US Department of Energy under contract DE-AC05-76RL01830.

7. References

1. Fleer, B. K. Radiological-Weapons Threats: Case Studies from the Extreme Right. *The Nonproliferation Review* **2020,** *27* (1-3), 225–242. DOI: 10.1080/10736700.2020.1775987.
2. Kosnar, M.; Li, D. K. Neo-Nazi Leader Among 2 Arrested in Plot to Attack Baltimore's Power Grid, Feds Say. *NBC News*, February 6, 2023. https://www.nbcnews.com/news/us-news/fbi-arrests-2-suspects-accused-planning-attack-baltimore-power-grid-rcna69324.
3. Earnhardt, R. L.; Hyatt, B.; Roth, N. A Threat to Confront: Far-Right Extremists and Nuclear Terrorism. *Bulletin of the Atomic Scientists*, January 14, 2021. https://thebulletin.org/2021/01/a-threat-to-confront-far-right-extremists-and-nuclear-terrorism/.
4. Federal Bureau of Investigation; US Department of Homeland Security. *Strategic Intelligence Assessment and Data on Domestic Terrorism*; Federal Bureau of Investigation: Washington, DC, 2022. https://www.fbi.gov/file-repository/fbi-dhs-domestic-terrorism-strategic-report-2022.pdf/view.
5. Nair, S.; Pluff, A.; McAllister, C. The Threat from Within: An Overview of the Domestic Violent Extremist Threat Facing US Nuclear Security Practitioners; *Stimson Center*, November 2, 2023. https://www.stimson.org/2023/the-threat-from-within-an-overview-of-the-domestic-violent-extremist-threat-facing-us-nuclear-security-practitioners/.
6. Bunn, M.; Sagan, S. D. A Worst Practices Guide to Insider Threats: Lessons from Past Mistakes; American Academy of Arts and Sciences: Cambridge, Massachusetts, 2014. https://www.amacad.org/sites/default/files/publication/downloads/insiderThreats.pdf.

7. US Department of Homeland Security. *Summary of Terrorism-Related Threat to the United States' Security*; US Department of Homeland Security: Washington, DC, 2023.
8. Kunzelman, M.; Richer, A. D.; Whitehurst, L. Oath Keepers Founder Stewart Rhodes Sentenced to 18 Years for Seditious Conspiracy in Jan. 6 Attack. *Associated Press News*, May 25, 2023. https://apnews.com/article/stewart-rhodes-oath-keepers-seditious-conspiracy-sentencing-b3ed4556a3dec577539c4181639f666c.
9. White House. *National Strategy for Countering Domestic Terrorism*; US Government: Washington, DC, 2021.
10. White House. *The US National Strategy to Counter Antisemitism*; US Government: Washington, DC, 2023.
11. Institute for Economics and Peace. *Global Terrorism Index 2023*; Institute for Economics and Peace: Sydney, Australia, 2023. https://www.economicsandpeace.org/wp-content/uploads/2023/12/GTI-2023-web.pdf.
12. Joly, A.; Slater, J.; Barrett, D.; Hernandez, A. R. 10 Killed in Racially Motivated Shooting at Buffalo Grocery Store. *The Washington Post*, May 15, 2022. https://www.washingtonpost.com/nation/2022/05/14/buffalo-shooting-grocery-store-tops/.
13. Robinson, M. P.; German, N.; White, D. B.; Rane, S. V.; Harris, J. T. Nuclear Security Awareness Survey at a University. *International Journal of Nuclear Security* **2022**, *7* (2). DOI: 10.7290/ijns07j919.
14. Rane, S.; Harris, J. Development of a Potential Facility Risk Index for Radiological Security. *Risk Analysis* **2021**, *41* (8), 1257–1273. DOI: 10.1111/risa.13625.
15. Lenzenweger, M. F.; Shaw, E. D. The Critical Pathway to Insider Risk Model: Brief Overview and Future Directions. *Counter-Insider Threat Research and Practice* **2022**, *1* (1). https://citrap.scholasticahq.com/article/36186-the-critical-pathway-to-insider-risk-model-brief-overview-and-future-directions.
16. Sinclair, S.; Smith, S. W. Preventative Directions for Insider Threat Mitigation via Access Control. In *Insider Attack and Cyber Security: Beyond the Hacker*; Advances in Information Security; Springer: 2008; 165–194.
17. Sin, S. S.; Binder, M. K. Violent Non-State Actor Chemical, Biological, Radiological, and Nuclear (VNSA CBRN) Event Database, Version 1.0; Unconventional Weapons and Technology Division National Consortium for the Study of Terrorism and Responses to Terrorism (START); Asymmetric Threats Analysis Center (ATAC), University of Maryland: College Park, Maryland, 2022.
18. Greitzer, F.; Purl, J.; Leong, Y. M.; Becker, D. S. Sofit: Sociotechnical and Organizational Factors for Insider Threat. In *2018 IEEE Security and Privacy Workshops (SPW)*, San Francisco, California, May 24, 2018; IEEE: 2018, 197–206. DOI: 10.1109/SPW.2018.00035.
19. Greitzer, F. L.; Strozer, J.; Cohen, S.; Bergey, J.; Cowley, J.; Moore, A.; Mundie, D. Unintentional Insider Threat: Contributing Factors, Observables, and Mitigation Strategies. In *2014 47th Hawaii International Conference on System*

Sciences, Waikoloa, Hawaii, January 6–9, 2014; IEEE: 2014, 2025–2034. DOI: 10.1109/HICSS.2014.256.
20. Neumann, P. R. Options and Strategies for Countering Online Radicalization in the United States. *Studies in Conflict and Terrorism* **2013**, *36* (6), 431–459. DOI: 10.1080/1057610x.2013.784568.
21. Baweja, J. A.; McGrath, S.; Burchett, D.; Jaros, S. *An Evaluation of the Utility of Expanding Psychological Screening to Prevent Insider Attacks*; OPA Report No. 2019-067, PERSEREC-TR-19-05; US Department of Defense: Washington, DC, 2019. https://www.cdse.edu/Portals/124/Documents/jobaids/insider/perserc-study.pdf.
22. Holtz, B. C.; Harold, C. M. Effects of Leadership Consideration and Structure on Employee Perceptions of Justice and Counterproductive Work Behavior. *Journal of Organizational Behavior* **2013**, *34* (4), 492–519. DOI: 10.1002/job.1825.
23. Kessler, S. R.; Bruursema, K.; Rodopman, B.; Spector, P. E. Leadership, Interpersonal Conflict, and Counterproductive Work Behavior: An Examination of the Stressor–Strain Process. *Negotiation and Conflict Management Research* **2013**, *6* (3), 180–190. DOI: 10.1111/ncmr.12009.
24. Peng, A. C.; Kim, D. A Meta-Analytic Test of the Differential Pathways Linking Ethical Leadership to Normative Conduct. *Journal of Organizational Behavior* **2020**, *41* (4), 348–368. DOI: 10.1002/job.2427.
25. Bush, J. T.; Welsh, D. T.; Baer, M. D.; Waldman, D. Discouraging Unethicality Versus Encouraging Ethicality: Unraveling the Differential Effects of Prevention- and Promotion-Focused Ethical Leadership. *Personnel Psychology* **2021**, *74* (1), 29-54. DOI: 10.1111/peps.12386.
26. Sulea, C.; Fine, S.; Fischmann, G.; Sava, F. A.; Dumitru, C. Abusive Supervision and Counterproductive Work Behaviors. *Journal of Personnel Psychology* **2013**, 12 (4), 196–200. DOI: 10.1027/1866-5888/a000097.
27. Tepper, B. J.; Simon, L.; Park, H. M. Abusive Supervision. *Annual Review of Organizational Psychology and Organizational Behavior* **2017**, *4*, 123–152. DOI: 10.1146/annurev-orgpsych-041015-062539.
28. Keashly, L.; Harvey, S. Emotional Abuse in the Workplace. In *Counterproductive Work Behavior: Investigations of Actors and Targets*; S. Fox, P. E. Spector, Eds.; American Psychological Association: 2005. DOI: 10.1037/10893-009.
29. Carpenter, N. C.; Whitman, D. S.; Amrhein, R. Unit-Level Counterproductive Work Behavior (CWB): A Conceptual Review and Quantitative Summary. *Journal of Management* **2021**, *47* (6), 1498–1527. DOI: 10.1177/0149206320978812.
30. Fox, S.; Spector, P. E. A Model of Work Frustration–Aggression. *Journal of Organizational Behavior* **1999**, *20* (6), 915–931. DOI: 10.1002/(SICI)1099-1379(199911)20:6<915::AID-JOB918>3.0.CO;2-6.
31. Penney, L. M.; Spector, P. E. Narcissism and Counterproductive Work Behavior: Do Bigger Egos Mean Bigger Problems? *International Journal of Selection and Assessment* **2002**, *10* (1-2), 126–134. DOI: 10.1111/1468-2389.00199.
32. Fox, S.; Spector, P. E.; Miles, D. Counterproductive Work Behavior (CWB) in Response to Job Stressors and Organizational Justice: Some Mediator and Moderator Tests for Autonomy and Emotions. *Journal of Vocational Behavior* **2001**, *59* (3), 291–309. DOI: 10.1006/jvbe.2001.1803.

33. Tsai, H.-Y. Role of Psychological Ownership in Job Crafting, Work Engagement, and Counterproductive Behavior. *Journal of Theoretical Social Psychology* **2021**, *5* (4), 366–376. DOI: 10.1002/jts5.104.
34. International Atomic Energy Agency. *Nuclear Security Culture*; Nuclear Security Series 7; International Atomic Energy Agency: Vienna, Austria, 2008.
35. AlHogail, A.; Mirza, A. Information Security Culture: A Definition and a Literature Review. In *2014 World Congress on Computer Applications and Information Systems (WCCAIS)*, 2014; IEEE: 2014; 1–7. DOI: 10.1109/WCCAIS.2014.6916579.
36. Bollmann, G.; Krings, F. Workgroup Climates and Employees' Counterproductive Work Behaviours: A Social-Cognitive Perspective. *Journal of Management Studies* **2016**, *53* (2), 184–209. DOI: 10.1111/joms.12167.
37. Cohen-Charash, Y.; Spector, P. E. The Role of Justice in Organizations: A Meta-Analysis. *Organizational Behavior and Human Decision Processes* **2001**, *86* (2), 278–321. DOI: 10.1006/obhd.2001.2958.
38. Jones, D. A. Getting Even with One's Supervisor and One's Organization: Relationships Among Types of Injustice, Desires for Revenge, and Counterproductive Work Behaviors. *Journal of Organizational Behavior* **2009**, *30* (4), 525–542. DOI: 10.1002/job.563.
39. Helm, S. A Matter of Reputation and Pride: Associations Between Perceived External Reputation, Pride in Membership, Job Satisfaction and Turnover Intentions. *British Journal of Management* **2013**, *24* (4), 542–556. DOI: 10.1111/j.1467-8551.2012.00827.x.
40. Rioux, S. M.; Penner, L. A. The Causes of Organizational Citizenship Behavior: A Motivational Analysis. *Journal of applied Psychology* **2001**, *86* (6), 1306. DOI: 10.1037/0021-9010.86.6.1306.
41. Kristof-Brown, A.; Guay, R. P. Person–Environment Fit. In *APA Handbook of Industrial and Organizational Psychology, Volume 3: Maintaining, Expanding, and Contracting the Organization*; S. Zedeck, Ed.; American Psychological Association: 2011. DOI: 10.1037/12171-001.
42. Vianen, A. E. M. v. Person–Environment Fit: A Review of Its Basic Tenets. *Annual Review of Organizational Psychology and Organizational Behavior* **2018**, *5* (1), 75–101. DOI: 10.1146/annurev-orgpsych-032117-104702.
43. Nye, C. D.; Su, R.; Rounds, J.; Drasgow, F. Interest Congruence and Performance: Revisiting Recent Meta-Analytic Findings. *Journal of Vocational Behavior* **2017**, *98*, 138–151. DOI: 10.1016/j.jvb.2016.11.002.
44. Van Iddekinge, C. H.; Roth, P. L.; Putka, D. J.; Lanivich, S. E. Are You Interested? A Meta-Analysis of Relations Between Vocational Interests and Employee Performance and Turnover. *Journal of Applied Psychology* **2011**, *96* (6), 1167–1194. DOI: 10.1037/a0024343.
45. Stephens, W.; Sieckelinck, S.; Boutellier, H. Preventing Violent Extremism: A Review of the Literature. *Studies in Conflict and Terrorism* **2021**, *44* (4), 346–361. DOI: 10.1080/1057610X.2018.1543144.
46. World Institute for Nuclear Security. *3.8 Countering Violent Extremism and Insider Threats in the Nuclear Sector*; World Institute for Nuclear Security: Vienna, Austria, 2020.

47. International Atomic Energy Agency. *Enhancing Nuclear Security Culture in Organizations Associated with Nuclear and Other Radioactive Material*; Nuclear Security Series 38-T; International Atomic Energy Agency: Vienna, Austria, 2021.
48. Hobbs, C.; Moran, M. Exploring the Human Dimension of Nuclear Security: The History, Theory, and Practice of Security Culture. *The Nonproliferation Review* **2021**, *28* (4-6), 275–295. DOI: 10.1080/10736700.2020.1811532.
49. Hafez, M.; Mullins, C. The Radicalization Puzzle: A Theoretical Synthesis of Empirical Approaches to Homegrown Extremism. *Studies in Conflict and Terrorism* **2015**, *38* (11), 958–975. DOI: 10.1080/1057610x.2015.1051375.
50. Moghaddam, F. M. The Staircase to Terrorism: A Psychological Exploration. *American Psychologist* **2005**, *60* (2), 161–169. DOI: 10.1037/0003-066X.60.2.161.
51. Kruglanski, A.; Jasko, K.; Webber, D.; Chernikova, M.; Molinario, E. The Making of Violent Extremists. *Review of General Psychology* **2018**, *22* (1), 107–120. DOI: 10.1037/gpr0000144.
52. Gonzalez-Morales, M. G.; Kernan, M. C.; Becker, T. E.; Eisenberger, R. Defeating Abusive Supervision: Training Supervisors to Support Subordinates. *Journal of Occupational Health Psychology* **2018**, *23* (2), 151–162. DOI: 10.1037/ocp0000061.
53. Jeon, S. H.; Park, M.; Choi, K.; Kim, M. K. An Ethical Leadership Program for Nursing Unit Managers. *Nurse Education Today* **2018**, *62*, 30–35. DOI: 10.1016/j.nedt.2017.12.017.
54. International Atomic Energy Agency. *Self-Assessment of Nuclear Security Culture in Facilities and Activities*; Nuclear Security Series 28-T; International Atomic Energy Agency: Vienna, Austria, 2017.
55. Jenkins, B. M. Feature Commentary: Elements of a Pragmatic Strategy to Counter Domestic Political Violence. *Combating Terrorism Center Sentinel* **2022**, *15* (10). https://ctc.westpoint.edu/feature-commentary-elements-of-a-pragmatic-strategy-to-counter-domestic-political-violence/.
56. Jones, S. G.; Doxsee, C.; Harrington, N. *Tactics and Targets of Domestic Terrorists*; CSIS Brief; Center for Strategic and International Studies: Washington, DC, 2020.

DOI: 10.7290/ijns09317753