Pacific Northwest
NATIONAL LABORATORY

PNNL-32072

Domestic Extremism

Countering the Threat Posed to Critical Assets

September 2021

Jessica A Baweja
Madelyn P Dunning
Caitlyn M Ackerman
Christine F Noonan

U.S. DEPARTMENT OF ENERGY

Prepared for the U.S. Department of Energy
under Contract DE-AC05-76RL01830

DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor Battelle Memorial Institute, nor any of their employees, **makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights**. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof, or Battelle Memorial Institute. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

PACIFIC NORTHWEST NATIONAL LABORATORY
operated by
BATTELLE
for the
UNITED STATES DEPARTMENT OF ENERGY
under Contract DE-AC05-76RL01830

Printed in the United States of America

Available to DOE and DOE contractors from
the Office of Scientific and Technical
Information,
P.O. Box 62, Oak Ridge, TN 37831-0062
www.osti.gov
ph: (865) 576-8401
fox: (865) 576-5728
email: reports@osti.gov

Available to the public from the National Technical Information Service
5301 Shawnee Rd., Alexandria, VA 22312
ph: (800) 553-NTIS (6847)
or (703) 605-6000
email: info@ntis.gov
Online ordering: http://www.ntis.gov

PNNL-32072

Domestic Extremism

Countering the Threat Posed to Critical Assets

September 2021

Jessica A Baweja
Madelyn P Dunning
Caitlyn M Ackerman
Christine F Noonan

Prepared for
the U.S. Department of Energy
under Contract DE-AC05-76RL01830

Pacific Northwest National Laboratory
Richland, Washington 99354

Summary

Domestic extremism (DE) has been a growing concern in the United States in recent months, as illustrated in multiple bulletins from the Department of Homeland Security (DHS) warning law enforcement partners of the heightened threat. As concerns about these actors grows, it is important that facilities in the U.S. and internationally that protect critical assets, such as sensitive information, hazardous materials, or critical infrastructure, have effective methods in place to secure those assets. DE has challenged security systems through the threat of insider attack and violence, creating a new threat to be countered in the Office of Radiological Security's (ORS's) radiological source security mission. In this effort, therefore, we used a literature review and focus group discussions with experts in critical asset security and extremism to understand the nature of the domestic extremist threat, to identify best practices in securing assets, recognize potential gaps in security measures to be corrected, and recommend actions for ORS to address DE with its partners.

Twenty-two subject matter experts (SMEs) participated in a series of five focus group sessions. Questions focused on definitions of DE, potential changes in the threat, best practices in securing facilities, assets, and personnel, and any perceived gaps. Upon completion of the focus groups, notes were analyzed thematically to identify any recurring patterns in the results. In addition, a review of academic, industry, and government literature was conducted to understand the threat of DE, describe the process of radicalization to extremism, and to identify empirically informed practices in prevention and response.

Results of this project demonstrated that further work is needed to define DE in law, regulation, and policy, to help the U.S. develop a consistent response to the threat within organizations. This is especially important for DE, as SMEs emphasized the need for early intervention in prevention efforts, noting that organizations need clear guidance on when and how to intervene. In addition, the need for social media monitoring was discussed, although challenges remain to do so with appropriate respect for privacy and civil liberties concerns.

Best practices that were highlighted in this project emphasized the importance of organizational culture in preventing domestic extremist threats. The literature and SMEs all noted that organizations need to foster a culture of support, early intervention, and appropriate reaction (not overreaction) when responding to potential threats. Doing so will help organizations to retain valuable human capital, and it will also encourage employees to report when they or others might need support through employee assistance programs or other resources.

Overall, a strong organizational culture and a thorough insider threat mitigation program can help to ensure critical assets remain secure. Based on the results of the focus groups and literature review, specific recommendations for ORS are provided that can augment the program's existing protect and sustainability strategies.

Key Findings

- Seven key themes emerged from focus group research: “definitions”, “culture”, “privacy”, “sociopolitical environment”, “dynamic threat”, “human security”, and “collaboration.”
- Definitions and terminology for DE may need further refinement and clarification, especially considering the ever-shifting nature of the threat.

- Focus group responses tied into best practices found in the literature for mitigating domestic extremist threats included strengthening organizational culture and diversity, equity, and inclusion programs, implementing an employee code of conduct, using behavioral observation programs, using multidisciplinary teams, having an effective employee assistance program, and appropriately tailoring responses to potential threats.
- Both SMEs and statements from U.S. government agencies concur that the dynamic threat of DE is on the rise, exacerbated by the misinformation-poisoned information environment, increasing political politicization, distrust in authority, and the COVID-19 pandemic and its associated mental health effects.
- Literature and focus group participants agree that DE is a human problem requiring human solutions; for example, employee wellness, support, and training should be prioritized.
- Gaps of potential concern in DE and insider threat prevention include inadequate resource allocation and failure to effectively monitor social media. Other remaining challenges include a potential need for legislation and difficulty collecting data on domestic extremist events.
- Meanwhile, when implementing DE prevention and response measures, privacy and other civil rights concerns must be taken into consideration.

Acknowledgments

The authors express appreciation to the National Nuclear Security Administration’s Office of Global Materials Security and Office of Radiological Security, for their generous support of radiological risk reduction strategies both domestically and internationally. Pacific Northwest National Laboratory is operated by Battelle for the U.S. Department of Energy under contract DE-AC05-76RL01830.

Acronyms and Abbreviations

ADL	Anti-Defamation League
CBRN	chemical, biological, radiological, and nuclear
CBRNE	chemical, biological, radiological, nuclear, or explosive
CVE	countering violent extremism
DE	domestic extremism
DHS	Department of Homeland Security
DNI	Director of National Intelligence
DoD	Department of Defense
DVE	domestic violent extremism
HR	human resources
IAEA	International Atomic Energy Agency
ISIS	Islamic State of Iraq and Syria
ORS	Office of Radiological Security
RMVE	racially or ethnically motivated violent extremism
SME	subject matter experts
TTP	tactics, techniques, and procedures
USC	United States Code
WINS	World Institute on Nuclear Security

Contents

Figures

Tables

1.0 Introduction

Domestic extremism (DE[1]) is an area of increasing concern for the United States and its allies when securing their critical assets. Recent issuances from the Director of National Intelligence and Department of Homeland Security (DHS 2021a; DHS 2021b; Director of National Intelligence [DNI] 2021) warn law enforcement and agency partners to be vigilant against the increased likelihood of violent, terrorist acts from domestic extremist groups and lone actors in 2021 and beyond. Around the world, there is widespread evidence that the threat of extremism is rising and needs to be addressed.

The growing threat of DE is especially relevant to facilities that protect assets critical for national security, including sensitive information, hazardous materials (e.g., nuclear or other radioactive material), or critical infrastructure, as these sites contain materials that might make them attractive targets for extremist actors. It is essential that security programs at these facilities have measures in place to address the potential threat posed by DE. However, DE has introduced new and growing challenges to security that organizations must address. This report describes the results of an effort to define the threat of DE, find best practices for security measures to prevent or mitigate the threat, identify any potential gaps in security, and finally, provide recommendations to security programs to better prepare them to counter or prevent domestic extremist attacks. This information will help support the Office of Radiological Security (ORS) as it engages with partners to counter the potential threat of DE through training in insider threat mitigation and other security measures.

1.1 The Threat of DE

Although security measures to protect critical assets are often robust, the threat of DE has nonetheless challenged these systems in new ways.

1. First, organizations have struggled to define DE and the boundary between individual freedoms and the need for security.
2. Second, the threat landscape has rapidly evolved, bringing new concerns in the form of online radicalization and a global pandemic.
3. Finally, DE represents an especially high risk to facilities with chemical, biological, radiological, nuclear, or explosive (CBRNE) materials due to the increased risk for violence.

1.1.1 Defining DE

The most obvious issue presented by DE to security measures is the lack of a common term for the threat within law, regulation, and policy (CEP 2021; Clifford 2021; Davies et al. 2021; Striegher 2015). Reviewing documents within the U.S., departments and agencies across the government have used the term DE (Department of Defense Instruction 1325.06), racially or ethnically motivated violent extremism (FBI 2020), domestic violent extremism (DNI 2021), or domestic terrorism (Title 18 United States Code (USC) 2331[5]). This plethora of terms exists not only in the U.S., but internationally; although some organizations define DE in policy, there is often no definition of DE in the legal system (CEP 2021). Notably, many countries (including

[1] Domestic extremism a belief system that exists outside of more broadly accepted societal belief systems, generally because the tactics or ideas are objectionable and involve radical change to society, government, or religion (Anti-Defamation League 2021; Rose et al. 2020). We provide this definition for clarity, although later sections expand on the possible terms for, and definitions of, DE.

the U.S.) do specifically define domestic terrorism; however, the definition of DE, or extremism more generally, is not as clear.

Part of the challenge in the legislative definition of DE stems from the need to protect individuals' civil rights and liberties. Within the U.S., there is a constitutionally protected right to free speech; membership in extremist organizations is not illegal, nor is hate speech (CEP 2021; FBI 2021). Similarly, in Germany, some far-right extremist groups receive protected status under the law due to their registration as political parties (CEP 2021). When addressing the threat of DE, it is critical to develop clear guidance to identify the boundary between an individual's rights to express their beliefs and opinions versus conduct or behavior that might represent a threat or criminal act. The lack of clarity around terms therefore represents a serious concern to consistent regulation or policy. If organizations fail to use consistent language when discussing the threat, then laws, regulations, and policies will also be inconsistent.
To adequately develop consistent responses or penalties to DE, it is critical that states develop common terminology.

Furthermore, it is important that any terms not be limited to contemporary political concerns. The emphasis on different types of extremism has changed over time in the U.S.
Domestic counterterrorism and counter extremism efforts were prioritized after the events of September 11, 2001, and those efforts focused primarily on Islamist extremists and "homegrown jihadists" (German and Robinson 2018; Moghaddam 2005). In recent years, attention in the U.S. has shifted to white supremacists and far-right extremism (Patel 2021; Rose et al. 2020). Regardless of whether extremist beliefs or actions stem from racial, religious, ethnic, environmental, or other extremist ideology, the language in regulation and policy should equally apply. Any terms or definitions used must be adequately expansive to encompass the variety of ideologies that might represent a potential concern to safety and security. The breadth of potential ideologies of concern has challenged institutions to adequately define the threat of DE and to create and enforce policy to counter or prevent it.

Thus, in this effort, we explored the terminology used in academic literature and among experts to better understand the core definition of the threat. Recommendations provide additional guidance to better protect radiological materials and to augment current ORS activities.

1.1.2 Emerging Threats

In addition to the challenges defining the precise threat of DE (and subsequently, regulating it), recent years have changed the threat landscape in a variety of ways. The online world has rapidly developed; social media is now an enduring and prominent part of daily life and provides nearly immediate global communication and reach, even into isolated communities (Zeitzoff 2017). In recent years, social media has played a pivotal role on the global geopolitical stage—for example, featuring prominently in the rise of ISIS (Berger 2014; Gambhir 2016; Zeitzoff 2017). There is, at minimum, a surfeit of anecdotal evidence that social media has had an important role in the radicalization[1] of perpetrators of recent terrorist attacks (Hafez and Mullins 2015; Zeitzoff 2017), and there is no doubt that extremist groups use the internet to advertise, communicate, and recruit new members (Davies et al. 2021; Neumann 2013). Social media has increasingly been a factor in the pathway to radicalization for U.S. extremists, with some data showing that it played a role in the radicalization of nearly 90% of extremists (Jensen et al.

[1] Radicalization is the incremental social and psychological process of commitment to extremist ideology (Horgan and Braddock 2010).

2016; Jensen et al. 2018). There is also evidence that online environments have increased the speed of radicalization (Jensen et al. 2016).

Given the adept use of social media by extremist groups, and its far-reaching capabilities, it has permanently and drastically altered the speed and extent of radicalization (Jensen et al. 2016; Neumann 2013; Zeitzoff 2017; Winter et al. 2020). Individuals can now learn of and be recruited by extremist groups easier than ever before, making it critical that organizations have an unambiguous and immediate response when potential radicalization to extremism is observed within their trusted and vetted personnel. However, this response must be tempered with the need to protect individuals' civil rights and liberties. Obviously, this delicate balancing act requires careful and thoughtful policymaking to assure that the threat is managed without undue adverse impact on individuals' privacy and rights.

The internet has not only provided a tool for communication to extremist groups, but it has also provided a new means of transferring and accessing funds through cryptocurrency (Dion-Schwarz et al. 2019). Although there is no evidence yet that terrorists have made widespread use of this tool, given the possibility for a new cryptocurrency to develop with additional anonymity, security, or usability for terrorist groups, it nonetheless represents a potential emerging threat (Dion-Schwarz et al. 2019). Cryptocurrency could provide the means by which insiders are financed by extremist groups to accomplish violence or extremists plan and fund attacks against sites with critical assets.

Finally, the COVID-19 pandemic has further altered the threat environment, with some scholars referring to it as a "witch's brew of grievances" (Davies et al. 2021). Given the widespread consensus that grievances represent an integral part of the radicalization process, the global disruption of the pandemic provides fertile ground for radicalization (Hafez and Mullins 2015; King and Taylor 2011). Far-right and Islamist extremist groups have redoubled recruiting efforts to take advantage of the chaos created by the pandemic, making the threat of radicalization, extremism, and terrorism even more essential to address swiftly (Davies et al. 2021; Kruglanski et al. 2020). Economic uncertainty, disruption of critical infrastructure, and widespread political unrest have all contributed to a global environment that increases the potential for radicalization.

1.1.3 Radicalization and the Potential for Violence

Although radicalization is not synonymous with the potential for violence, the process of cognitive radicalization is nonetheless a precursor to and risk factor for violent beliefs, plans, or acts (Frissen 2021; Hafez and Mullins 2015; Wolfowicz et al. 2019). That is, endorsement of extremist ideas appears to be an important factor in the decision to engage in violence (Hafez and Mullins 2015). Sites with CBRNE materials might be especially attractive targets for individuals who are interested in committing acts of violence, particularly acts of mass casualty violence, due to their potential for destruction. Thus, it is important that sites with these assets have clear plans in place to counter and prevent extremism to avoid the potential for violence against their facilities, as domestic extremists might target these facilities in particular.

Interestingly, terrorist groups appear to have expressed little special interest in facilities with CBRNE materials (Hegghammer and Dæhli 2017), possibly because these facilities are so well-protected and secured. Particularly with Islamist extremists, scholars have noted that, "jihadi groups have explored multiple ways to kill large numbers of people, and [radiological and nuclear] weapons are only one of them" (p. 14, Hegghammer and Dæhli 2017). Discussion of CBRNE weapons is somewhat more common among far-right extremists (Hegghammer and Dæhli 2017), but still represents a small fraction of the communication within these groups.

Regardless of the emphasis on CBRNE weaponry, however, extremist ideas represent a serious threat to the security of CBRNE materials, as individuals who endorse extremist ideologies are at a much greater risk of committing acts of violence and could use these materials as a means to do so. The lack of prior acts targeting CBRNE facilities is not an indication that extremist groups might not target these facilities in the future.

The increase in the speed of radicalization via the internet is especially concerning for CBRNE facilities, as it increases the risk that a trusted person might radicalize after already being vetted and provided authorized access to a secure facility (i.e., after becoming an insider). Individuals with authorized access to information, facilities, and personnel can become an especially potent threat to their organization by virtue of their knowledge and authority. The possibility for rapid online radicalization makes it particularly important that organizations have robust and ongoing monitoring procedures to identify these radicalized individuals among their trusted personnel. However, in the absence of clear definitions of extremism or specific concerning behaviors (and a consistent organized response), organizations have struggled to differentiate between extreme (but permissible) ideas and potential threats. Organizations need a consistent, coordinated response that is grounded in clear definitions of permissible and prohibited behaviors to adequately prevent or mitigate the threat of DE to critical assets.

1.2 Objectives

The purpose of this effort was to define the threat of DE, to identify best practices, tools, or techniques that are relevant to preventing or countering DE, and to identify potential gaps in security measures that might need to be corrected. Findings focus specifically on recommendations for the CBRNE community to better protect their critical assets against DE, both in the U.S. and internationally. To accomplish these objectives, a literature review and a series of focus groups were conducted to gather expert information on these topics. These processes are described in greater detail in the subsequent sections.

2.0 Methods

Primary methods included focus group discussions with SMEs in critical asset security to understand how organizations refer to and define the threat of DE, best practices in countering the threat, and gaps in security measures that they perceived. In addition, the project team conducted a review of literature to understand the key definitions and terms involved as well as prevention and response practices for countering DE.

2.1 Focus Groups

To gather information from SMEs, five focus group discussions were conducted with SMEs in critical asset security[1]. Detailed information about those discussions is below.

2.1.1 Participants

Participants were contacted via email for participation in this effort using existing professional networks. The initial contact email described the topic and goals of the project and highlighted that participation was voluntary and any comments provided during the focus groups would be kept anonymous. Participants were then instructed to respond to a survey to select a session time if they were interested in participating.

Twenty-two individuals participated in the focus groups sessions. To maintain anonymity, participants were asked to provide only a general description of their role at their organization and the nature of their organization. Table 1 shows a description of the organizational affiliation of the 22 focus group participants.

Table 1: Participant Organizational Affiliation

Organization Type	Frequency	Percent of SMEs
Federal Government	6	27.3
Consultant; Private Practice	5	22.7
Academia; Education	4	18.2
Government Contractor	2	9.1
Medical Facility; Hospital; Health Care	2	9.1
Industry	1	4.5
Local/State/Tribal Government	1	4.5
Local/State/Tribal Law Enforcement	1	4.5
Total	22	100

Participants had a variety of job roles, including private consulting, insider threat professionals within the government, security personnel at universities or medical facilities, academic

[1] Prior to beginning the focus group discussions, a project plan was submitted to the PNNL Institutional Review Board and the project was deemed exempt from human subjects research requirements.

researchers, and practicing clinicians. All participants had experience in critical asset security from either a practical or a research perspective.

2.1.2 Procedures

Five focus group sessions were conducted via Microsoft Teams. Sessions were 90 minutes in length and included between three and seven participants each. At each session, there were at minimum three project team members present. One team member served as the moderator, asking questions and leading the discussion, and two others attended the sessions to observe participant behavior and take notes for later analysis. In some sessions, a fourth team member was present and observed the session.

At the beginning of the conversation, the moderator reminded participants of the topic of discussion (DE and national security), and reinforced that the discussions would remain confidential, and no comments made during the session would be attributed to them or to their organization as the discussion would be conducted under Chatham House Rules. In addition, participants were reminded that the discussion was to be held entirely at the unclassified level. Finally, the moderator reminded participants that participation was voluntary, and that they would be provided a copy of the results for review at the completion of the effort.

After this introduction, the moderator posed questions to the participants, the content of which are shown in Table 2. Because the conversation was interactive, questions varied slightly in phrasing and order in each session, and questions may not have been asked if the information had been addressed in prior conversation.

Table 2: Focus Group Questions

Questions
Does your organization have a consistent term that they use to refer to extreme ideas that groups might hold, such as domestic extremism, domestic violent extremism, racially or ethnically motivated violent extremism, or something else?
Is there a clear definition for that term in your organization’s policy or procedure, or can you describe how you would define that term?
How do you characterize threats posed by domestic extremism to critical asset security?
What do you believe are the key security measures that you have in place at your organization that you think are most relevant to protecting your critical assets from domestic extremist attacks?
Do you have any specific tools that you use in your organization that you find to be especially helpful when protecting against threats like domestic extremism?
How do you share good practices and lessons learned with other similar organizations (e.g., public forum/conferences, private exchange)?
Do you have any security measures that you think are especially critical for organizations to adopt when it comes to the threat of domestic extremism?
How does your organization learn about potential DE threats (e.g., state fusion center, Joint Terrorism Task Force)?
Do you see any changes or trends in the threat posed to your critical assets?

Questions
Do you have any major security concerns that you think need to be addressed? Put differently, what are the things that keep you up at night with regard to securing your critical assets?
What are the gaps in tools, technology, or security management measures that you see, especially as it relates to domestic extremism? For example, do you have technology that you need? Are there policies that you think need to be changed?
Is there anything else you want to mention before we end today's discussion? Are there any others in your network who you think we should include in a future focus group?

During the session, the two team members assigned to take notes recorded responses to the questions using participant initials for later analysis. At the conclusion of the session, the moderator thanked participants for their time and reminded them that they would receive a copy of the findings for review at the close of the effort.

2.1.3 Thematic Analysis

After completion of the focus group sessions, the two team members' notes were consolidated into a single set for thematic analysis. This process assured that the most information possible was captured from the notes. Notes were reviewed by a third team member to verify that information was clear and readable. After consolidation of the notes, three team members ("coders") reviewed notes from all five sessions and conducted a thematic analysis. Thematic analysis is a method of qualitative analysis for identifying, organizing, and describing patterns of meaning in qualitative data (Braun and Clark 2012). Because the primary goal of this effort was descriptive, the thematic analysis was conducted inductively, identifying patterns in the SMEs' responses.

The process of thematic analysis is shown in Figure 1. In summary, coders reviewed the data and created codes to describe the patterns they observed. Using those codes, they began the process by creating themes, which attempt to capture important patterns in the data as they relate to the objectives of the effort. In the final two steps, the coders reviewed the data with those themes in mind to revise them as needed and assure that the key points were captured, and then created names to describe the emergent themes. At the completion of the thematic analysis, the coders captured the key points from SMEs as they related to the objectives of the effort and summarized those themes and the associated SME comments.

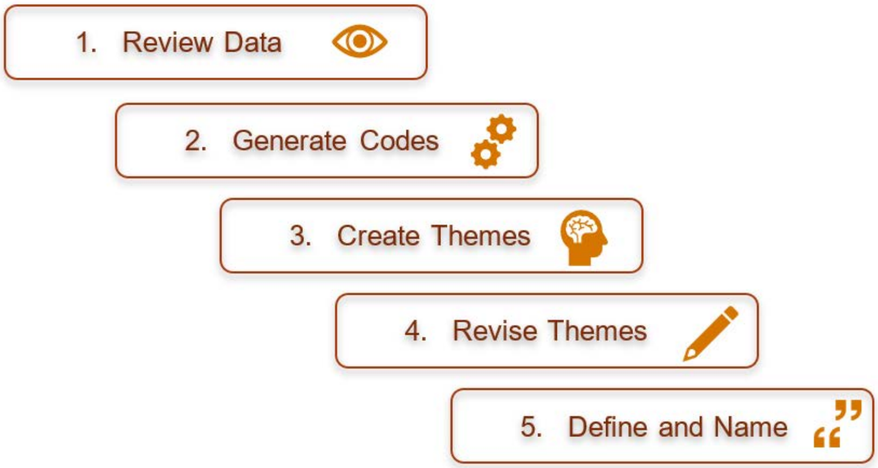

Figure 1: Thematic Analysis Process

2.2 Literature Review

Literature was collected on many topics related to DE, including defining DE, understanding the potential threat (e.g., of violence), understanding the process of radicalization and deradicalization, and identifying best practices in preventing, detecting, and responding to DE threats. An initial set of topics and key words were identified to find articles from academia, industry, relevant nongovernmental organizations (e.g., World Institute for Nuclear Security), and any other publicly available credible sources. Articles were reviewed and key points and relevant information were summarized for future reference and inclusion in this report.

3.0 Themes from Focus Groups

Review of the focus group notes revealed seven primary themes related to the research objectives, presented in Table 3. Each theme is described in greater detail in the sections below.

Table 3: Key Themes from Focus Groups

Theme	Description
Definitions	Definitions of extremism are lacking, ambiguous, or inconsistent.
Culture	The culture of an organization is a critical factor in creating or mitigating the risk of DE.
Privacy	Security must be balanced with the need to protect individual rights to privacy and free speech.
Sociopolitical Environment	The current sociopolitical environment is exacerbating extremism in new ways.
Dynamic Threat	The threat of DE is dynamic and growing, and ongoing threat assessment is needed for security measures to remain effective.
Human Security	Although physical security remains important, the human layer of security is the most critical tool in protecting against DE.
Collaboration	Countering extremism requires collaboration, including outreach to similar organizations, communication with other Federal experts, and community engagement.

3.1 Definitions

During the focus groups, participants were asked whether there were consistent terms used to discuss DE in their organization, and if so, whether there were clear definitions of those terms. Although not universal, most SMEs agreed that confusion remains regarding the appropriate terms to describe the threat and the definitions of those terms. The challenge expressed had to do with differentiating between permissible thoughts and opinions and problematic or illegal behaviors.

In addition, SMEs discussed the inconsistent use of terms, especially between security professionals and the general public, which creates confusion about the nature of the issue at hand. SMEs also mentioned that this creates challenges for law enforcement, because they cannot define an objective point at which a behavior reaches the level for intervention. SMEs mentioned that they occasionally use one term among knowledgeable professionals and another with a general audience, with the focus being on identifying the precise behavior that concerns them within their organization or personnel.

Ultimately, however, SMEs mentioned that the term itself is less important than the clear understanding of the potential threat. Regardless of the term used, SMEs expressed a need to understand the difference between permissible and non-permissible behavior, and to assure that each case of potential threat is handled consistently. To the extent that clearer laws, regulations, or policies support consistent action, they expressed that it was important; well-defined terminology is one part of the practical goal for consistent organizational responses to personnel beliefs or behavior.

3.2 Culture

During the focus groups, SMEs stressed the critical importance of organizational culture in effectively preventing or countering extremist threats. Part of developing a positive culture is underscoring to employees that, if they report their colleagues and coworkers, the organization will not overreact, and that the response will be supportive. For people to feel comfortable providing information to their insider threat mitigation programs, they need to know and believe that the response will be reasonable, and that the organization will not punish employees without cause. If employees fear that the organization will overreact, they are unlikely to report a colleague or to self-report when they observe a potential concern. This is especially problematic in the context of DE, because employee reporting and observation is a useful tool to identify individuals of potential concern before they engage in a problematic act.

As part of the effort to encourage reporting, SMEs also underscored that the focus of insider threat programs needs to change to emphasize wellness and early intervention rather than punishment. Without that support, they argued that it would be unlikely that there will be significant reporting to insider threat and security personnel. Of course, organizations do need to be realistic that there may be negative consequences for employees who are reported (or who self-report) to insider threat programs; however, if the responses of an insider threat program are reasonable, and incorporate employee support rather than sanctions whenever possible, this can have a positive impact on the overall culture and the likelihood of early intervention in cases of potential extremist threat.

Overall, organizational culture was clearly highlighted as a crucial factor in determining the likelihood that an organization will learn of a possible extremist threat before an incident occurs. SMEs emphasized the importance of establishing and maintaining a positive employee culture, in which reporting is encouraged and the organization responds to these reports in a reasonable, measured fashion. To help encourage this culture, SMEs discussed wellness and early intervention as critical parts of the insider threat program, where employees are provided concrete resources—financial, mental health, and other—to help them address issues before they manifest in a damaging insider act.

3.3 Privacy

SMEs discussed that a major challenge when addressing DE is concerns about privacy, civil rights, and liberties. Because DE involves individuals' opinions and beliefs, which may or may not manifest in a concrete threat, SMEs emphasized the importance of balancing the need to secure our facilities, information, and personnel with the need to protect individuals' privacy, civil rights, and liberties. Organizations need to be careful not to overstep and infringe on these rights when implementing insider threat programs.

As one means of doing so, SMEs suggested that insider threat programs should focus on behaviors that indicate the individual might escalate toward a violent or other extremist act, and not just potentially problematic beliefs. If there are indications that an individual is moving toward action, such as attack planning or preparation, then intervention by the organization is warranted. Focusing on concrete, objective behaviors, rather than opinions, beliefs, or ideologies, can help to assure that intervention occurs appropriately and consistently in cases of potential threat.

However, it remains challenging to know when and how to appropriately intervene in instances of potential extremist threat. In addition, because the goal is intervention before a malicious act occurs, the need to balance security with individual rights provides a very short window for action—after there is an indication that an act might occur, but before it actually does. To accomplish this effectively, organizations should strive to have supervisors who are engaged with their employees to identify potential behavioral concerns before they escalate to violence or other malicious acts in the name of extremist ideas.

3.4 Sociopolitical Environment

A frequent topic of discussion during focus groups explored the nature of the current sociopolitical environment in the U.S. When asked about potential changes to the threat of DE, all SMEs agreed that the threat has increased in recent years—something that corresponds with official statements from U.S. government agencies (e.g., DHS, 2021b). In particular, SMEs mentioned the polarized nature of political conversation and the two-sidedness of cultural discourse. SMEs also mentioned an increased rate of misinformation or conspiracy theories as a potential concern. Due to that polarization and misinformation, they expressed concerns about the lack of trust in government institutions, which might lead to a lower likelihood of reporting potentially dangerous situations.

SMEs also mentioned that the pandemic has exacerbated mental health issues, which could increase interest and involvement in extremist groups. That is, individuals may be feeling lonely during periods of isolation, and in many cases, that loneliness may be compounded by financial and other stressors. Individuals might therefore be more vulnerable to—or even seek—extremist groups and be more likely to become entangled with these potentially damaging ideologies.

Overall, SMEs agreed that the current environment in the U.S. creates an increased threat by extremists. This stresses the need for organizations to be prepared to address this threat in their workforce to assure the security of their critical assets.

3.5 Dynamic Threat

When asked about measures that they felt were important to protecting against DE, SMEs discussed the need for organizations to remain apprised of the potential threats in their area. SMEs noted that organizations need to remain informed in order to be prepared to address a changing and growing threat presented by DE. In particular, they discussed how the threat of extremism has merged in recent years, with different organizations learning from each other in new ways. The blending of the threat was a frequent concern: extremist groups are no longer isolated but are communicating and collaborating in new ways. The interference of malicious state actors was also discussed, particularly as it related to funding or supporting domestic actors. Thus, they highlighted the need for organizations to work with local, state, and federal law enforcement agencies to assure that they are aware of the threats in their area and have security measures to address those threats. For instance, a clinic that performs abortions should monitor and create threat scenarios for training against potential anti-abortion extremist groups in their area.

Despite the potential concerns regarding privacy and civil liberties, SMEs also emphasized the need to monitor social media, because extremist groups are using it as a tool to recruit, communicate, and plan attacks. SMEs also discussed the increased speed of radicalization and the decreased window for intervention, again due to social media. Thus, in addition to the need to conduct regular threat assessments to understand the potential threats, they highlighted that organizations need to develop a social media monitoring plan to know the activities of extremist groups around them.

3.6 Human Security

Although SMEs acknowledged the importance of good physical security measures, when asked about key practices to counter DE, the human layer of security was mentioned most often. Similar to discussions on culture, SMEs emphasized that an organization's employees are their best tool to detect potential threats and stop them before they are realized, particularly when the threat comes from another insider.

Again, similar to discussions of culture, SMEs discussed rebranding insider threat to emphasize wellness and support, and prioritizing personnel training so that all employees understand the threat and their role in protecting their organization against it. Doing so can help to encourage employees to participate in security processes through behavior observation programs. One SME also mentioned the importance of vetting in prevention, because once an individual is part of the organization, it is far more difficult to protect against them as a potential threat. Another discussed the value of psychological evaluations and semi-structured interviews at regular intervals to monitor personnel well-being and identify potential extremist ties. Overall, comments in this discussion highlighted the importance of recognizing DE as a human problem requiring human solutions.

3.7 Collaboration

Throughout the conversations, SMEs emphasized the importance of communication and collaboration both between and within organizations. First, for the purposes of learning from others, they discussed having conversations with other similar organizations to understand their security practices. In addition, they discussed professional conferences such as Society for Human Resources Management, Association of Threat Assessment Professionals, and other organization-specific (e.g., healthcare) conventions as important ways to learn best practices in security.

In addition, SMEs emphasized the need to avoid isolating information within specific groups in the organization, and the importance of cross-disciplinary teams. SMEs expressed the importance of ensuring that the insider threat team comprises human resources, security, and communications personnel to facilitate the most effective response to counter extremism. Each of these groups has value when countering extremist threats, and beyond that, may provide additional information or context important to understanding the extent of any given case or situation.

Overall, findings from the SMEs suggested that the threat of DE has grown in recent years. SMEs encouraged organizations to focus on developing a strong organizational culture of support, and to emphasize early intervention and wellness in their insider threat programs. Although these measures are not new, they become especially important in the face of the growing risk of an insider attack by radicalized individuals. The next sections describe these findings in context of the results of the literature review to address the project objectives of defining DE, identifying best practices, and finding potential gaps in security measures.

4.0 Research Synthesis

4.1 Defining DE

One primary objective of this effort was to understand the terms used to describe the threat of DE and the definitions of those terms. In addition to the conversations with SMEs, we conducted a review of the literature to understand how organizations can define DE and the threats it poses to critical assets.

Terrorism

Any activity that:

- Involves an act that is:
  - dangerous to human life or potentially destructive of critical infrastructure or key resources; and
  - a violation of the criminal laws of the U.S. or of any state or other subdivision of the U.S.; and

Appears to be intended to:

- intimidate or coerce a civilian population
- influence the policy of a government by intimidation or coercion
- affect the conduct of a government by mass destruction, assassination, or kidnapping.

Domestic Terrorism

Any activity that:

- Involves acts dangerous to human life that are a violation of the criminal laws of the U.S. or of any state

Appears to be intended to:

- intimidate or coerce a civilian population
- influence the policy of a government by intimidation or coercion
- affect the conduct of a government by mass destruction, assassination, or kidnapping
- occur primarily within the territorial jurisdiction of the U.S.

Figure 2: Criminal Laws Defining Terrorism

In addition to the conceptual issues surrounding the definition of DE, there are legal issues—thus, to begin, we explored some of the relevant laws and regulations that might apply to DE. Within the U.S., individuals are free to express even objectionable thoughts and beliefs; thus, as discussed during the focus groups, organizations have struggled to determine what aspects of those objectionable beliefs can be part of their policy. To help define relevant terms, two definitional statutes are shown in Figure 2.

As Figure 2 shows, within the USC, there are laws defining domestic terrorism and terrorism. The first, 18 USC 2331(5), defines domestic terrorism as acts that occur in the U.S. Domestic terrorism here is described in contrast to international terrorism (defined in 18 USC 2331[1]), which occurs outside of the territory of the U.S. The second statute shown in Figure 2 defines terrorism, regardless of its physical location, in the establishment of the DHS. Highly similar, both statutes describe any destructive acts that are intended to influence the general population or the government to a particular end. Any behaviors that might fit either of these definitions certainly warrant intervention by organizational security or law enforcement personnel. Of course, it is possible that behaviors might be criminal but not fall under these laws; nonetheless, they broadly define the areas of potential law enforcement concern as it relates to DE.

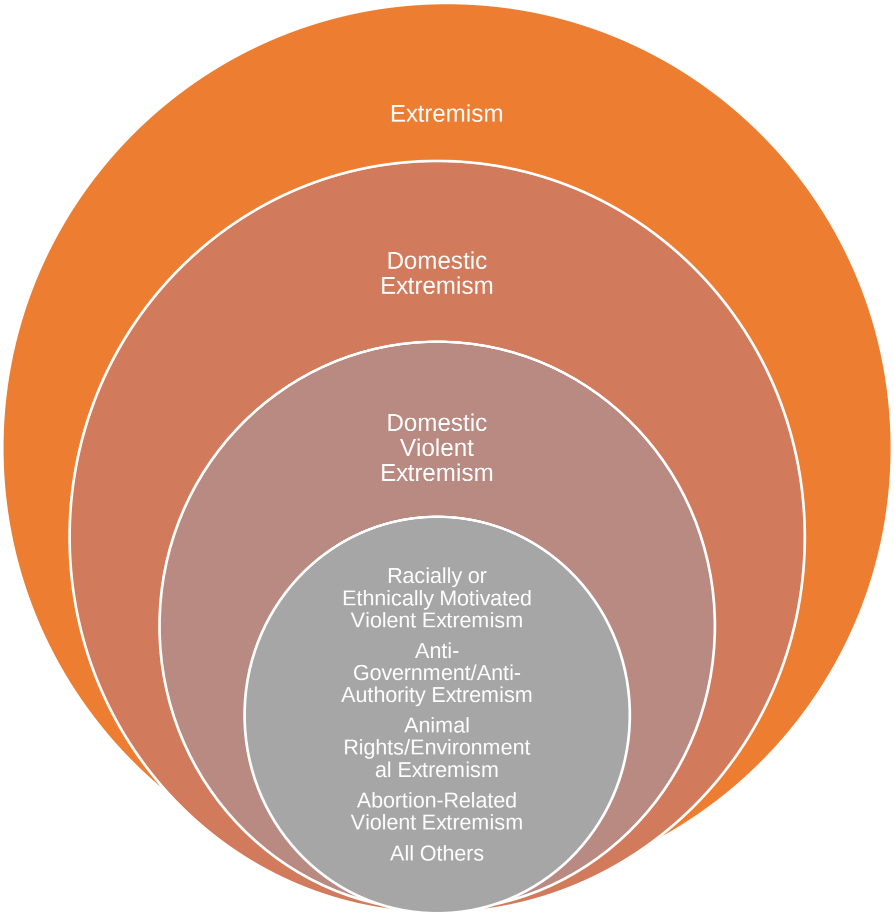
Extremism
Domestic Extremism
Domestic Violent Extremism
Racially or Ethnically Motivated Violent Extremism
Anti-Government/Anti-Authority Extremism
Animal Rights/Environmental Extremism
Abortion-Related Violent Extremism
All Others

Figure 3: Conceptual Map of Extremism Terms

Where the precise definition of DE becomes more challenging is when examining potential threats posed by extremism that might not fall under one of these laws—as discussed during the focus groups. Given the variety of terms used in this space, Figure 3 presents a conceptual map of some key terms, beginning at the highest level (with extremism) down to specific types of extremism that have been outlined as a potential threat (FBI 2020). Again, because these may not involve criminal behavior, they are thought of as threats posed by specific ideologies rather than something that can necessarily be legislated.

Table 4 presents definitions of these terms.

Table 4: Extremism Definitions

Term	Definition
Extremism (Anti-Defamation League [ADL] n.d.)	A religious, social, or political belief system that exists substantially outside of belief systems more broadly accepted in society (i.e., “mainstream” beliefs), generally because their ideas or tactics are objectionable.
Domestic Extremism (ADL n.d.)	A religious, social, or political belief system that exists within the United States and is substantially outside of belief systems more broadly accepted in in the United States (i.e., “mainstream” beliefs), generally because their ideas or tactics are objectionable.
Domestic Violent Extremism (FBI 2020)	The ideas of a group based and operating primarily within the territorial jurisdiction of the United States who seeks to further their ideological goals wholly or in part through unlawful acts of force or violence.
Racially or Ethnically Motivated Violent Extremism (FBI 2020)	This threat encompasses the potentially unlawful use or threat of force or violence in furtherance of ideological agendas derived from bias, often related to race or ethnicity, held by the actor against others or a given population group. Racially or Ethnically Motivated Violent Extremists purport to use both political and religious justifications to support their racially or ethnically based ideological objectives and criminal activities.
Anti-Government or Anti-Authority Violent Extremism (FBI 2020)	This threat encompasses the potentially unlawful use or threat of force or violence in furtherance of ideological agendas, derived from anti-government or anti-authority sentiment, including opposition to perceived economic, social, or racial hierarchies, or perceived government overreach, negligence, or illegitimacy.
Animal Rights/Environmental Violent Extremism (FBI 2020)	This threat encompasses the potentially unlawful use or threat of force or violence in furtherance of ideological agendas by those seeking to end or mitigate perceived cruelty, harm, or exploitation of animals and/or the perceived exploitation or destruction of natural resources and the environment.
Abortion-Related Violent Extremism (FBI 2020)	This threat encompasses the potentially unlawful use or threat of force or violence in furtherance of ideological agendas relating to abortion, including individuals who advocate for violence in support of either pro-life or pro-choice beliefs.
All Other Domestic Terrorism Threats	This category encompasses threats involving the potentially unlawful use or threat of force or violence in furtherance of ideological agendas which are not otherwise defined under or primarily motivated by one of the other domestic terrorism threat categories. Such agendas could flow from, but are not limited to, a combination of personal grievances and beliefs, including those described in the other domestic terrorism threat categories. Some actors in this category may also carry bias related to religion, gender, or sexual orientation.

As Figure 3 shows, extremism is the most general and broadest term, and refers to any extreme idea or belief systems that a group or individual might hold—although some definitions also include fanaticism as a component of extremist beliefs (ADL n.d.; Brown et al. 2021; Kruglanski et al. 2018). Definitionally, those ideas do not need to be problematic or concerning in any way, but colloquially, extremism generally refers to extreme ideas that are in some way objectionable (e.g., involve the subjugation of another group based on race, gender, religion, etc.), and that advocate for radical change to religion, government, or society (ADL n.d.). DE simply refers to extremism that occurs primarily or exclusively within the territory of the U.S.

When the belief system begins to advocate for, condone, or participate in violence as a method of obtaining radical change, within the U.S., it is referred to as domestic violent extremism (DVE; FBI 2020). This is generally where law enforcement agencies within the U.S. become more involved, as domestic violent extremists become a more immediate threat and may engage in criminal behavior. Again, note that not all of these behaviors are illegal; DVE highlights that once extremists begin to advocate for or approve of violence, they become a potential threat, regardless of whether they actually engage in violence.

Finally, the FBI defines several threats that are associated with DVE based on their specific belief system, ideology, or motivations: racially or ethnically motivated violent extremism (RMVE), anti-government/anti-authority violent extremism, animal rights or environmental violent extremism, anti-abortion violent extremism, and any other domestic terrorism threats. Although these are not categories based on criminal laws, they help differentiate the types of groups that might exist and the motivations. This categorization is useful to identify the potential threat posed by different types of DE, particularly as it relates to target selection. The FBI notes that direct threats of violence may be necessary for an individual or group's actions to be in violation of the law; hence, these ideologies are described as violent extremists rather than as domestic terrorists, as mere advocacy of extreme opinions is not a criminal act.

These terms were clarified by the FBI in collaboration with DHS and DNI to help standardize the terminology and the methodology for tracking and preventing domestic terrorist threats (FBI 2020). This is one step toward consensus, at least within the U.S., in the lexicon around extremist threats. These categorizations and definitions, however, need to be adopted at other legal levels (e.g., state, local) for the understanding of the issues at hand to be consistent. Continued communication is necessary to encourage all organizations to discuss the threat of DE in a way that is commonly understand.

In addition, conversations with SMEs suggested that further refinement of these terms might be necessary. In particular, SMEs highlighted that, given globalization, the distinction between international and domestic threats is increasingly arbitrary. Online extremist groups are able to communicate and collaborate in ways that have previously been impossible (CEP 2021; National Security Council 2021; Zeitzoff 2017); furthermore, given the ease of communication between people even at great distances, it no longer matters where individuals are located. This suggests that the distinction between international terrorism and domestic terrorism might be less relevant in today's world, especially as it relates to understanding potential threats.

This perspective is supported in recent documents examining transnational links among extremist groups (CEP 2021). It is further highlighted in the recent U.S. strategy for addressing domestic terrorism, which emphasized as one aspect of the strategic response the importance of recognizing the transnational aspects of terrorism. Future definitions of terrorism might therefore eliminate or reduce the emphasis on international borders when describing the specific actions, although the citizenship of the actors involved remains relevant when determining the appropriate jurisdiction for a response.

However, the transnational connectivity of extremist groups and the increasing globalization of the threat emphasizes the importance of international cooperation in defining and addressing the extremist threat (CEP 2021; Flade 2021; National Security Council 2021). Although the U.S. has made progress at the federal level in defining the terms relevant to the domestic extremist threat, given the global nature of the threat, international cooperation in defining and coordinating responses to extremist threats remains critical. One important future direction mentioned in the literature is to provide a means for countries to meet and share lessons learned and best practices in addressing extremism. This echoes the call by SMEs to engage in collaboration to assure that information is being shared. In addition, given that groups do cross international borders, countries can communicate and inform other relevant nations of intelligence indicating potential threats.

Progress has been made in terms of defining domestic extremist threats, but (as discussed in Section 4.2) organizations will still need to develop their own standards of conduct and policy to outline permissible behaviors for their personnel. Because so much that qualifies as DE is not illegal, efforts should emphasize instead of defining permissible behavior within a specific organization, using recently developed FBI definitions as a potential guide.

4.2 Best Practices in Security

A second objective of this effort was to identify security measures that are most effective when addressing the threat of DE. Security measures to counter DE are divided into those for prevention and those for response. Prevention measures are designed to prevent a domestic extremist threat from occurring; response measures are implemented once a potential threat has been identified.

4.2.1 Prevention

Results of the literature review and SME focus groups highlighted several useful practices in the prevention of domestic extremist threats, including organizational culture; diversity, equity, and inclusion programs; organizational codes of conduct; and behavior observation programs.

4.2.1.1 Organizational Culture

As results of the thematic analysis demonstrated, SMEs highlighted the importance of fostering a strong organizational culture to effectively prevent domestic extremist threats at organizations with critical assets. Specifically, SMEs discussed that organizations should not overreact to potential threats and should provide resources to employees who are experiencing stressors and challenges in their lives to help them manage those stresses effectively. This sentiment was echoed in the literature, where experts discussed the need to foster resilience to help individuals avoid being drawn into extremist groups (Stephens et al. 2021). Similarly, recent guidance from the World Institute on Nuclear Security (WINS) discussed nuclear security culture as one factor in helping organizations prevent the threat of DE (WINS 2020).

In addition, when outlining prevention strategies, WINS emphasized the need to have a program for employees to share concerns. This suggestion is supported in the literature, as studies have repeatedly identified unaddressed grievances as playing a critical role in the radicalization process (e.g., Hafez and Mullins 2015; Moghaddam 2005; Kruglanski et al. 2018). Thus, avoiding unaddressed grievances in the workplace is one way of reducing the risk of domestic extremist incidents. Although organizations cannot address larger societal grievances within the context of employment, they can work to ensure that employees have a voice in the operations of that organization (Stephens et al. 2021; WINS 2020). Providing employees with a means to raise their frustrations can help address their concerns. This can lower the risk of disgruntlement and reduce the likelihood that employees will turn to extreme options to address their issues with the organization (Stephens et al. 2021; WINS 2020). A sense of caretaking and communication within an organization will encourage reporting of potentially anomalous or concerning behaviors in others, providing an opportunity for early intervention.

4.2.1.2 Diversity, Equity, and Inclusion Program

Along with this robust culture of engagement and security, review of the literature also emphasized the need to foster open communication and discussion around issues of diversity, equity, and inclusion (Brown et al. 2021; Mulligan et al. 2021; Stephens et al. 2021). This is important in context of the current sociopolitical environment, which is highly contentious—as mentioned both by experts in the focus groups and in the literature (Davies et al. 2021; Kruglanski et al. 2020).

The findings of this effort suggest that it is important for organizations to develop an open and supportive culture where employees feel that they can embrace their identities, and that they have the opportunity to ask questions and better understand each other in an appropriate way (Stephens et al. 2021). Suppression of those discussions can lead individuals to embrace extreme ideas in the absence of other conversation (Mulligan et al. 2021). All employees should receive training on issues of diversity, equity, and inclusion to support a positive culture around issues of identity and to foster communication about potentially challenging and personal issues.

4.2.1.3 Code of Conduct

SMEs and the literature suggested that a code of conduct is important for organizations to develop and maintain, so that all employees understand what is and is not permissible behavior in their workplace (International Atomic Energy Agency [IAEA] 2020a; WINS 2020). In addition to helping employees understand the standards of behavior, a code of conduct helps to outline the responsibilities and roles of all individuals in the organization, so that employees know what is expected of them (IAEA 2020a). This code of conduct can also help the organization to define and develop their own standards of behavior objectively, so that they can clearly indicate when those standards have been violated.

Thus, when trying to prevent domestic extremist threats, results showed that organizations should create a code of conduct if one does not exist already. If a code of conduct exists, they should review it to ensure that it covers potential behaviors of concern that relate to DE. For example, if the organization has specific standards of conduct around issues of diversity, that conduct should be clearly described. Codes of conduct should be created in communication with the organization’s human resources department and legal counsel to ensure that they are appropriate and enforceable.

4.2.1.4 Behavioral Observation Program

SME discussions repeatedly emphasized the importance of human intelligence in preventing domestic extremist threats. In addition, best practices in the literature highlighted the need to train employees in behavior observation and help them to identify behaviors that might indicate a security concern (Mulligan et al. 2021; WINS 2020). Again, because domestic extremist threats might not involve illegal behavior, human intelligence can be important to prevention by identifying potential threats in the workforce that are still developing, allowing for earlier intervention. Employees and supervisors who interact on a regular basis are best placed to identify if an individual’s behavior might have changed or represent a potential concern. Thus, one best practice is to train all employees in behavior observation and ensure that they are regularly connecting to have opportunities for observation—especially managers with subordinates. Of course, this behavior observation will be most effective in an organization with a robust security culture.

WINS (2020), in its recent guide to countering violent extremism, also underscored more generally the importance of a robust human reliability program in prevention efforts. A well-rounded human reliability program includes pre-employment screening and vetting processes, employee assistance programs, and proper closeout procedures if an employee is terminated. The guide provides specific examples of practices that human reliability programs should use, including interviews, review of financial records, and medical and psychological evaluation, as well as behavioral observation programs. Human reliability programs, along with a robust security culture, can help organizations to leverage their human intelligence as a means to prevent domestic extremist threats.

4.2.2 Response

When responding to threats of DE within their organizations, results of this effort suggested that organizations should leverage a multidisciplinary team, offer employee assistance programs, and respond to threats appropriately. Organizations should also develop realistic DE threat scenarios to assess their insider threat mitigation programs.

4.2.2.1 Multidisciplinary Team

The literature and SMEs emphasized that multidisciplinary teams are key to properly responding to potential domestic extremist threats (Ellis et al. 2020). Not only are these teams important to information-sharing, but different groups have different areas of knowledge and expertise that might be helpful when creating an appropriate response for a specific case. For instance, human resources personnel are especially knowledgeable about employee assistance programs that might be beneficial when addressing a specific concern (e.g., mental health issues). Security personnel can be helpful when responding to more immediate threats, to develop safety and security plans. Of course, insider threat programs within the U.S. should have insider threat programs that implementing sharing policies and procedures in order to meet the National Insider Threat Task Force’s minimum standards (NITTF 2012).

Nonetheless, findings from the literature suggest that multidisciplinary teams are especially important to addressing radicalization and extremism (Ellis et al. 2020). Because the process of radicalization is complex and involves many interacting factors, it is important that the team addressing the potential threat have a variety of skills on which to draw. Doing so will improve the effectiveness of the response by providing additional options and resources to use, above and beyond law enforcement intervention.

4.2.2.2 Employee Assistance Programs

Although not all articles discuss employee assistance programs, articles on deradicalization highlight the need to provide resources to individuals who are a domestic extremist threat—particularly concrete resources, such as counseling (WINS 2020; Ellis et al. 2020). From a practical perspective, financial, mental health, physical health, and other resources can help employees to address stressors in a constructive way, reducing the likelihood that those individuals will explore violent means of resolving their problems. In addition, by providing resources and structure to individuals, organizations can promote employee engagement with families, communities, and their job, all of which can be a barrier to involvement with extremist groups (Simi and Windisch 2020).

When discussing employee assistance programs and extremism, it is important to mention that, although mental health is often discussed as a factor in extremist events, SMEs highlighted that mental health care is not a full solution to the program of insider threat. Although the literature does mention mental health issues as a potential indicator of risk (Brown et al. 2021), most individuals who experience mental health issues do not commit acts of violence. Nonetheless, improved mental health care is frequently cited as an important tool in addressing extremism (Brown et al. 2021; Mulligan et al. 2021).

4.2.2.3 Appropriate Response

Throughout the focus groups, SMEs reiterated that organizations should not overreact when responding to a potential threat (e.g., terminate an employee unnecessarily). There is evidence that overreactions can lead to backlash, creating further damage (Clifford 2021). When those overreactions come from a government institution, they can have the additional impact of supporting an anti-government narrative, making it especially important that responses are graded and reasonable. Again, multidisciplinary teams could be an asset to determining the appropriate response by helping the organization to understand the actual risk of an attack by a given individual. The pathway to violence has been thoroughly explored and discussed; leveraging that knowledge is important to responding appropriately (e.g., Calhoun and Weston 2003; FBI 2015). Because extremism is complex and can involve personal or controversial beliefs, organizations should work to overcome the potential for overreaction out of a desire to avoid risk or liability. Doing so sends a potentially damaging message to the workforce: that even slight missteps will not be tolerated. This might discourage employees from reporting potential concerns.

Of course, organizations do also need to be careful to act on the reports that they receive. It is important to avoid the “not in my organization” bias, where individuals do not believe that an incident could occur at their organization (Bunn and Sagan 2017; WINS 2020). The case of Nidal Hasan illustrates that disbelief and inaction can be extremely damaging, as many individuals had concerns about Hasan prior to the Fort Hood mass shooting in November 2009. Thus, the focus in SME discussions and in the literature was on ensuring that the response was appropriate—i.e., did not overly punish, but also did not ignore potential threats. One way that organizations can attempt to meet this challenge is by identifying, before a case arises, the specific responses they might have to different scenarios to ensure that a consistent plan is in place.

4.2.2.4 DE Insider Threat Scenarios

Although this was not frequently mentioned in the literature, guidance from WINS and from SMEs also discussed the need for organizations to evaluate their current security measures to ensure that they would be effective against domestic extremist threats (WINS 2020). Using intelligence from law enforcement agencies, such as DHS fusion centers, organizations should develop threat scenarios that reflect relevant threats. The WINS guide outlines key considerations when creating realistic DE insider threat scenarios to assess the efficacy of their insider threat mitigation programs (WINS 2020). Ultimately, the critical message is that domestic extremist threats can vary greatly, and so organizations will need to think creatively about the tactics that an attacker might use to ensure effective response measures.

4.3 Potential Gaps in Security Measures

Many of the best practices discussed represent well-established measures in insider threat mitigation. There were two areas of potential concern or gaps in security: social media monitoring and lack of resources. Of course, failing to perform some of the measures already described in insider threat mitigation (e.g., behavior observation, employee vetting) might also present a gap in a specific organization’s security measures; the measures below are systemic concerns expressed in focus groups and the literature.

4.3.1 Social Media Monitoring

There is increasing evidence that social media plays an important role in radicalization processes (Jensen et al. 2016; Jensen et al. 2018), both by increasing the likelihood of radicalization and increasing its speed. However, social media is still not consistently incorporated into the background investigation process in the U.S. (WINS 2020). Much of the literature that discusses social media use in background checks or monitoring focuses not on the use of social media, but instead emphasizes the concerns around privacy and civil liberties (e.g., Ghoshray 2013).

Despite these concerns, SMEs argued that organizations can no longer afford to ignore social media as a source of information on DE and potential threats, and researchers in this area have echoed those concerns, identifying social media as an important source of DE information (Rose et al. 2020). Failing to monitor social media creates a risk that threats will not be identified before they manifest in damaging action against critical assets. Working with legal counsel, the federal government and other organizations should develop processes to incorporate social media into background investigations and monitoring. To address concerns regarding privacy and the potential for bias in the investigation process, organizations may need to think creatively about the use of social media; nonetheless, it is an important data source that needs to be considered when monitoring the domestic extremist threat.

4.3.2 Resource Allocation

SMEs and the literature emphasized that, to effectively prevent domestic extremist threats from manifesting in action, organizations and the federal government need to prioritize the threat in policy and allocate resources accordingly (Mulligan et al. 2021). Although physical protection measures for critical assets have been invested in heavily, and remain important in protecting organizations against extremist threats, SMEs raised concerns that resources have not been sufficiently allocated to insider threat mitigation programs in the area of human intelligence, behavior observation, training, and engagement. SMEs mentioned the need for a team dedicated to analysis of threat information to ensure that intelligence is understood and properly addressed.

Training was emphasized as an important means for protecting against domestic extremist threats, both in the literature and by SMEs (Mulligan et al. 2021; WINS 2020). Organizations should review the allocation of resources to ensure that training and insider threat mitigation programs are adequately staffed and that assigned personnel have sufficient training and tools necessary to complete their jobs. To properly address the threat of DE, insider threat mitigation programs, human resources, and training personnel need time, tools, and funding sufficient to accomplish the task. Although many organizations do this well already, SMEs highlighted this as a potential concern.

4.4 Remaining Challenges

Finally, results of this effort identified two challenges that need to be addressed through additional research and development.

1. First, questions remain regarding the appropriate legislation of DE within the U.S. and internationally.

2. Second, and relatedly, there is a lack of consistent data collection and tracking of extremist incidents.

4.4.1 Legislation

Debate around the need for additional laws around domestic terrorism is ongoing (Clifford 2021; German and Robinson 2018). Within our focus groups, SMEs disagreed about the necessity of a domestic terrorism statute to prosecute relevant cases. As Clifford (2021) and German and Robinson (2018) review, U.S. federal law enforcement generally pursues cases against extremist-related crimes using a variety of charges (e.g., firearms charges, homicide, hate crimes). As a way of prioritizing the prosecution of domestic extremist violence, some groups have recently called for a stand-alone domestic terrorism statute to prosecute relevant crimes (Zabel 2021; Petrow-Cohen 2021). However, there is widespread disagreement about the necessity of a domestic terrorist charge to address the extremist threat. Some argue that the inability to pursue terrorism charges in specific crimes can lead to inequality in the prison sentences for domestic terrorism when compared to similar international cases (Clifford 2021). Others, however, state that the challenge in the U.S. is not one of legislation, but of inequality in prosecutorial application of charges (German and Robinson 2018), and that a domestic terrorism statute is unnecessary (Jenkins 2021).

Regardless of the resolution of this debate, it is clear that there are discrepancies in the way that the law has been applied to domestic and international terrorism cases and the tactics that the federal government uses to investigate and prosecute them (Clifford 2021; German and Robinson 2018). The U.S. needs to prioritize fairness to ensure that similar crimes are handled consistently within the criminal justice system, as broad prosecutorial discretion can perpetuate longstanding issues of social injustice and inequality (German and Robinson 2018). Defining the U.S. criminal justice response to DE and terrorism is an important step in disrupting and deterring terrorist activity—and the recent national strategy highlights the importance of enabling appropriate investigation and prosecution of crimes (National Security Council 2021). Nonetheless, further work in this area is required to reach consensus on the legal framework that is needed. For example, additional analysis of sentencing discrepancies between international and domestic terrorism cases, accompanied by review of the charges involved, might help to elucidate whether an additional domestic terrorism statute is necessary.

4.4.2 Data Collection and Tracking

Throughout the literature, experts highlighted that tracking of extremist violence remains challenging (Mulligan et al. 2021; Rose et al. 2020). Related to the challenge of legislation already discussed, the lack of consistent charging of DE-related offenses makes it difficult to know how many of those incidents have occurred. Because DE cases involve a variety of criminal charges, research and monitoring of the nature, frequency, and intensity of the threat is difficult. Even still, although criminal records represent the likeliest source of information on DE incidents, not all cases will rise to the level of law enforcement involvement; thus, the tracking of the threat becomes challenging and subjective.

Thus, data collection and tracking is one area where a domestic terrorism charging statute could be beneficial, in that it might help to provide a single charge to allow for research and evaluation on the risk and occurrence of DE. It does not, however, eliminate the challenge, as organizations still likely have a large number of cases that are mitigated prior to any actionable event that might enter a record system. This is a challenge not just for DE, but for insider threat in general, in that it is difficult to track the potential threat when success is defined as the absence of an event. To enable research and training in the area of DE, organizations and the federal government should continue to develop ways to track the prevalence and type of DE events occurring in the U.S. One potential option is to leverage the definitions of domestic violent extremism recently published by the FBI and implement a law enforcement reporting system, similar to the system used to collect information on hate crimes since the Hate Crime Statistics Act of 1990 (28 USC 534). Although these hate crime statistics likely still undercount the number of hate crimes that occur in the U.S. (as many crimes go unreported), they provide a baseline from which trends can be identified. Such a system would provide a starting point to determine whether incidents of DE are changing over time in their frequency or nature.

5.0 Discussion

This project strove to define the threat DE poses to critical assets, and to identify any best practices or gaps in security to protect those assets. One promising outcome of this effort is that it demonstrated that the U.S. is beginning to prioritize addressing the threat of DE. In the wake of the January 6 attack on the U.S. Capitol, the Biden administration released a national strategy to counter domestic terrorism; even earlier, DoD held a department-wide stand down to conduct a training and discussion on DE (National Security Council 2021; Office of the Secretary of Defense 2021). Progress is being made domestically to identify ways that the federal government can mitigate the threat of DE; however, there remain opportunities for further development.

1. Section 5.1 describes the implications of these findings for insider threat mitigation programs.
2. Section 5.2 outlines some areas for continued growth and development.
3. Section 5.3 provides specific recommendations for implementation.

5.1 Insider Threat Mitigation Programs

Many of the best practices identified in this effort mirror recommendations for good practice in insider threat mitigation in general (e.g., IAEA 2020b; NITTF 2012; WINS 2020). Despite the fact that they are not novel, many of these measures are especially important in addressing DE. Because of the unique nature of the extremist threat, it is especially important to use these measures to observe and intervene in instances of concerning behavior before it escalates.

Results here emphasized that organizational culture, codes of conduct, and behavior observation are all important measures in prevention of domestic extremist incidents. In addition, when responding to potential threats, a cross-disciplinary team was recommended by SMEs and in the literature. That team should work to assure that the response to a particular incident is graded and appropriate, and incorporates resources provided by employee assistance programs whenever possible. Organizations also need to consider domestic extremist scenarios when evaluating their insider threat programs to determine whether the measures they have in place would be effective against that type of threat.

Overall, many of the findings here emphasize a culture of engagement, wellness, and inclusion as key to preventing extremism at the organizational level. This echoes many of the findings from the literature review that show that resilient individuals who are engaged in the community are less likely to succumb to extreme ideologies, and indeed, community and family engagement can be a barrier to perpetrating acts of mass casualty violence (Ellis and Abdi 2017; Mulligan 2021; Stephens et al. 2021; Simi and Windisch 2020). In the face of recent events that demonstrate the threat of extremism within the U.S. and internationally, development of a dedicated insider threat mitigation program that emphasizes a strong culture of engagement and support can help to mitigate some of the larger societal disruption that has been a consequence of growing sociopolitical tension and a global pandemic (Kruglanski et al. 2020).

Employers have limited ability to intervene in larger societal injustices and social detachment that certainly contribute to the likelihood of extremist violence (Denoeux and Carter 2021; Jasko et al. 2017; Kruglanski et al. 2020). Findings here suggest that creating a culture within the organization that fosters a sense of justice, trust, and fairness can not only reduce the likelihood of DE violence or other damaging acts, but it can also have the beneficial effect of promoting a happy, engaged, and productive workforce. Certainly, each individual organization can have some beneficial impact on society as a whole by promoting those values within that organization. Of course, these factors also promote the security of critical assets and prevention of potentially devastating acts of violence. Security culture has long been identified as key to success in the area of radioactive materials security. When viewing security from the perspective of DE, the need for broad acceptance of security as a priority becomes even more important as the basis for encouraging an open and proactive culture of identifying and reporting issues of concern. Emphasizing and rewarding staff security engagement, while simultaneously demonstrated a balanced approach to addressing reported concerns will be vital.

5.2 Areas for Future Development

In addition to underscoring the importance of good practices in the context of insider threat mitigation, the findings here also identified several areas for continued growth and development in the U.S. and internationally. These areas of growth are described here for awareness purposes; recommendations regarding specific ORS actions are outlined in the next section.

First, the results of this effort highlighted the need for continued international collaboration in countering violent extremism. Although much of the recent federal focus has been on domestic threats, and that was the focus of this effort, results here suggested that the distinction between international and domestic threats is increasingly arbitrary in a world that occurs more and more online. This has implications for the definition of the threat; it also has implications for the capabilities of the threat. That is, as extremist groups communicate and plan online, they have begun to transcend national boundaries and to share tactics. In addition to sharing intelligence, international cooperation also provides an additional venue for sharing best practices in vetting and monitoring that might prevent infiltration of extremists into military and police forces (Flade 2021). In the coming months, the U.S. and its partners should continue to explore ways to communicate and share knowledge with regard to extremism and threats to critical asset security.

Second, the federal government should determine if a domestic terrorism statute would be beneficial. As discussed, there remains widespread debate on this point; regardless of whether an additional domestic terrorism statute is developed, guidance may be issued to law enforcement agencies that supports consistent application of laws to domestic extremist incidents to alleviate any inequities in sentencing. Doing so would help promote fairness in prosecution of domestic and international terrorism (German and Robinson 2018).

Third, as discussed, the literature highlighted the importance of social media in radicalization, making it especially important that organizations with critical assets develop a way to monitor social media in a legal and appropriate manner. In some cases (e.g., for individuals who have eligibility to access classified information or to hold a sensitive position within the federal government) that may involve monitoring of individual activity as authorized (see DNI 2017). For other organizations, that monitoring might take the form of working with law enforcement agencies to identify potential threats to their security in publicly available information. Regardless, the federal government should prioritize the development of social media monitoring tools that organizations can use to support those activities. In order to consistently implement social media in security, tools and technology need to be developed to allow for objective identification of threat-relevant information. Such development is unlikely to occur without federal funding dedicated to that effort. The U.S. will continue to grow in this area, and future discussion on the legal and appropriate incorporation of social media information into vetting processes will likely occur that will impact how facilities with critical assets, such as radiological materials, can use social media in those vetting processes.

Finally, in the context of radiological and nuclear terrorism, one recent paper recommended that the international community make the IAEA Code of Conduct on the Safety and Security of Radioactive Sources a legally binding treaty (Brill and Bernhard 2020). They suggest doing so will increase national accountability in preventing radiological and nuclear terrorism. Although this was not specific to extremist threats, it is a potential area for consideration to support prevention efforts in extremism and terrorism internationally. The international community should consider options to strengthen nuclear and radiological material protection, when possible, particularly focused on the potential risk of insider threat.

5.3 Recommendations

Although much of this paper focuses on outlining good practices and areas for development, we nonetheless provide some detailed recommendations for insider threat mitigation specific to DE prevention and response for ORS partners:

- Domestic Regulatory Requirements
  - ORS should continue to work with partners on developing and maintaining insider threat mitigation programs that meet legal and regulatory requirements. Using existing legal frameworks, ORS should work with partners to enhance those mandated programs with components that relate to prevention and response to DE. For instance, licensees under the Nuclear Regulatory Commission are required to have an insider threat program for clearance holders that complies with the National Industrial Security Program Operating Manual (NISPOM) minimum standards. These programs can be enhanced through an emphasis on the DE threat specifically, such as through additional training on behavior observation to complement current required insider threat training, such as outlined in the recent WINS (2020) best practices guide. Guidance can also include other cultural enhancement activities, such as those outlined in IAEA's recent publication on enhancing nuclear security culture (2021a).
- Domestic Training and Awareness
  - To develop awareness of the DE threat, ORS should conduct a webinar to discuss extremism and its relation to radiological material security. The webinar can cover basic definitions of key concepts in this area, as well as help partners to understand how they can work within their facility or organization to prevent the threat. This webinar will alert facilities to the potential threat and help them to review security measures to ensure their effectiveness against DE threats specifically.
  - The ORS initiative to develop a training course on insider threat topics for its domestic partners is a helpful step to addressing DE. That training course should be reviewed to ensure proper insider threat objectives are addressed and that it incorporates DE strategies and priorities. Employees in critical safety or security positions should receive training in insider threat mitigation and behavior observation that includes behaviors that might indicate a potential DE threat. Recent WINS (2020) guidance outlines many key practices for insider threat mitigation when addressing the DE threat, including human reliability programs and DE scenarios when evaluating the efficacy of insider threat programs.

  - ORS should consider an additional module to its insider threat training that discusses prevention and response measures for the DE threat specifically. In this module, ORS can discuss important factors such as a code of conduct (ORS should identify or develop a model to be shared with partners, similar to the guidance presented in IAEA NSS 38-T), a personnel feedback or suggestion program, a behavior observation program, and employee assistance programs. In addition, ORS should provide greater emphasis to the importance of a broad coalition for meaningful investigation of and response to insider threat cases. Insider threat programs should leverage a cross-disciplinary team that draws from experts in human resources, physical security, cybersecurity, as well as organization leadership. Recent WINS (2020) guidance provides other best practices when countering DE that could be incorporated into this stand-alone DE module.

- International Cooperation

  - ORS should continue to explore ways to collaborate and communicate about extremist threats internationally. Leveraging ORS relationships with INTERPOL, as well as bilateral relationships with partner countries, can improve the mitigation of extremism, both domestically and internationally. Because extremism is a global challenge, it is critical that states share intelligence about potential threats. Furthermore, this collaboration can enhance international response through sharing of information on good practices in prevention of extremism. As ORS works to update its approach to international response engagement, extremism should be included the strategy.

- International Training and Awareness

  - Although this effort focused on domestic concerns, ORS should continue to engage its international partners on insider threats topics and should expand its training efforts to include extremism. Although legal and regulatory frameworks differ internationally, many of the practices outlined in this report and in recent WINS guidance, such as codes of conduct, behavior observation, and design basis threat that include insider adversaries with extremist ties. ORS should incorporate these DE prevention and response measures into conversations with international partners, connecting with existing legal and regulatory frameworks within partner countries when possible.

- Future Directions

  - ORS should contribute to the broader inter-agency discussion regarding the value social media monitoring to address the DE threat. While direct engagement with partners is important to addressing the issue, DE necessitates the development of new mechanisms to help partners succeed.

  - Recent discussions have explored the possibility of creating a legally binding treaty based on the current IAEA Code of Conduct. ORS should contribute to these conversations, potentially through an additional study to explore the potential legal options regarding radiological material security internationally. Such an effort could provide more information about the possible methods by which radiological material security could be enhanced through the application of international law.

5.4 Conclusion

Many of the findings of this effort underscored the value of ORS's current activities in training partners on the importance of insider threat mitigation programs. Given the prominence of the extremist threat domestically and internationally, the findings here suggest that these efforts could be improved through further emphasis on the threat of extremism specifically.

By incorporating prevention and response measures focused on extremism, ORS can support security measures that are robust against this potential threat. These training and awareness efforts should be informed by recent guidance form relevant organizations, such as the IAEA's cultural enhancement measures (2021a) and the recent best practices guide in countering violent extremism issued by WINS (2020). Whenever possible, implementation should leverage existing legal requirements which can help to support the investment of resources necessary by partners to create an effective program.

Finally, although this effort focused on the threat of DE, the threat of extremism is a global one and it will need to be addressed internationally to be effective. Some initial suggestions were provided here for leveraging existing relationships with international partners, but further venues for communication and collaboration will need to be identified. A coordinated global response will support sharing of information regarding potential threats and will accelerate the development of effective measures to prevent and respond to violent extremism and its threat to critical asset security.

6.0 References

Anti-Defamation League (ADL). n.d. Defining Extremism: A Glossary of White Supremacist Terms, Movements and Philosophies. Accessed May 20, 2021 at https://www.adl.org/education/resources/glossary-terms/defining-extremism-white-supremacy.

Berger JM. 2014. “How ISIS Games Twitter.” The Atlantic.

Braun V and V Clark. 2012. “Thematic Analysis.” In APA Handbook of Research Methods in Psychology: Vol. 2, Research Designs, pp. 57 – 71. American Psychological Association.

Brill KC and JH Bernhard. 2020. “Preventing the preventable: Strengthening international controls to thwart radiological terrorism.” Bulletin of the atomic scientists 76(4): 206-209. https://doi.org/10.1080/00963402.2020.1778371.

Brown RA, TC Thi, R Ramchand, AI Palimaru, S Weilant, AL Rhoades, and L Hiatt. 2021. “Violent Extremism in America.” RAND Corporation.

Bunn M and SD Sagan. 2017. "A Worst Practices Guide to Insider Threats." In Insider Threats, pp. 145-174. Cornell University Press.

Calhoun FS and SW Weston. 2003. Threat Assessment and Management Strategies: Identifying the Howlers and Hunter. CRC Press.

Clifford B. 2021. “Racially/ethnically motivated violent extremist (RMVE) attack planning and the United States federal response, 2014-2019.” Program on Extremism, George Washington University.

Counter-Extremism Project (CEP). 2020. Violent Right-Wing Extremism and Terrorism—Transnational Connectivity, Definitions, Incidents, Structures, and Countermeasures. Counter Extremism Project. https://www.counterextremism.com/sites/default/files/CEP%20Study_Violent%20Right-Wing%20Extremism%20and%20Terrorism_Nov%202020.pdf.

Davies G., E. Wu and R. Frank (2021). "A Witch’s Brew of Grievances: The Potential Effects of COVID-19 on Radicalization to Violent Extremism." Studies in Conflict & Terrorism: 1-24.

Davies G., E. Wu and R. Frank (2021). "A Witch’s Brew of Grievances: The Potential Effects of COVID-19 on Radicalization to Violent Extremism." Studies in Conflict & Terrorism: 1-24.

Denoeux G and L Carter. 2009. “Guide to the Drivers of Violent Extremism.” United States Agency for International Development.

DHS National Terrorism Advisory System Bulletin, 14 May 2021.

DHS National Terrorism Advisory System Bulletin, 27 January 2021.

Director of National Intelligence Assessment, Domestic Violent Extremism Poses Heightened Threat in 2021, 01 March 2021.

Director of National Intelligence. 2017. “Security Executive Agent Directive-5: Collection, use, and retention of publicly available social media information in personnel security background investigations and adjudications.”

Department of Defense Instruction 1325.06. 2009. “Handling Dissident and Protest Activities among Members of the Armed Forces.”

Ellis BH and SM Abdi. 2017. “Building community resilience to violent extremism through genuine partnerships.” American Psychologist 72(3): 289-300.

Ellis BH, AB Miller, R Schouten, NY Agalab, SM Abdi. 2020. “The challenge and promise of a multidisciplinary team response to the problem of violent radicalization.” Terrorism and political violence 2020: 1-18. https://doi.org/10.1080/09546553.2020.1777988.

Federal Bureau of Investigation (FBI). 2015. Making Prevention a Reality: Identifying, Assessing, and Managing the Threat of Targeted Attacks. Behavioral Analysis Unit—National Center for the Analysis of Violent Crime.

Federal Bureau of Investigation (FBI). 2020. “Domestic Terrorism: Definitions, Terminology, and Methodology.”

Flade F. 2021. “The Insider Threat: Far-Right Extremism in the German Military and Police.” Combating Terrorism Center at West Point Sentinel 14(5): 1-10.

Frissen, T. 2021. "Internet, the great radicalizer? Exploring relationships between seeking for online extremist materials and cognitive radicalization in young adults." Computers in Human Behavior 114 (2021): 1-13.

Gambhir H. 2016. “The Virtual Caliphate: ISIS’s Information Warfare.” Institute for the Study of War: Alexandria, VA.

German M and S Robinson. 2018. "Wrong Priorities on Fighting Terrorism." New York, NY: Brennan Center for Justice.

Ghoshray S. 2013 "The Emerging Reality of Social Media: Erosion of Individual Privacy Through Cyber-vetting and Law’s Inability to Catch Up." The John Marshall Review of Intellectual Property Law 12(3): 551-582.

Hegghammer T and AH Dæhli. 2017. "Insiders and Outsiders: A Survey of Terrorist Threats to Nuclear Facilities." In Insider Threats, pp. 10-41. Cornell University Press.

International Atomic Energy Agency (IAEA). 2020a. Enhancing Nuclear Security Culture in Organizations Associated with Nuclear and Other Radioactive Material. Technical Guidance. Retrieved from https://www.iaea.org/publications/13405/enhancing-nuclear-security-culture-in-organizations-associated-with-nuclear-and-other-radioactive-material.

International Atomic Energy Agency (IAEA). 2020b. Preventive and Protective Measures against Insider Threats, IAEA Nuclear Security Series No. 8-G (Rev. 1) Implementing Guide. Retrieved from http://www-pub.iaea.org/MTCD/Publications/PDF/PUB1858_web.pdf.

Jasko K, G LaFree, and AW Kruglanski. 2017. “Quest for significance and violent extremism: The case of domestic radicalization.” Political Psychology 38(5): 815-831.

Jenkins BM. 2021. “Five Reasons to be Wary of a New Domestic Terrorism Law.” RAND Corporation, February 24, 2021. https://www.rand.org/blog/2021/02/five-reasons-to-be-wary-of-a-new-domestic-terrorism.html.

Jensen M, P James, G LaFree, A Safer-Lichtenstein, and E Yates. 2018. The Use of Social Media by United States Extremists, College Park: National Consortium for the Study of Terrorism and Responses to Terrorism, University of Maryland.

Jensen M, PA James, and H Tinsley. 2016. “Profiles of Individual Radicalization in the United States - Foreign Fighters (PIRUS-FF): Infographics.” Report to the Office of University Programs, Science and Technology Directorate, U.S. DHS. College Park, MD: The National Consortium for the Study of Terrorism and Responses to Terrorism. https://www.start.umd.edu/pubs/START_PIRUSFF_InfographicSeries_April2016.pdf.

King M and DM Taylor. 2011. “The radicalization of homegrown jihadists: A review of theoretical models and social psychological evidence.” Terrorism and Political Violence 23(4): 602-622.

Kruglanski AW and R Gunaratna, M Ellenberg, and A Speckhard. 2020. “Terrorism in time of the pandemic: exploiting mayhem.” Global security: Health, science and policy 5(1): 121-132.

Kruglanski AW, K Jasko, D Webber, M Chernikova, and E Molinario. 2018. “The making of violent extremists.” Review of General Psychology 22(1): 107-120.

Moghaddam FM. 2005. “The staircase to terrorism: A psychological exploration.” American Psychologist 60(2): 161-169.

Mulligan, K, B Steele, S Clark, A Padmanabhan, and R Hunkler. 2021. “A national policy blueprint to end white supremacist violence.” Center for American Progress & McCain Institute for National Leadership.

National Insider Threat Task Force (NITTF). 2012. Minimum Standards for Executive Branch Insider Threat Programs.

National Security Council. 2021. “National Strategy for Countering Domestic Terrorism.”

Neumann PR. 2013. "Options and Strategies for Countering Online Radicalization in the United States." Studies in Conflict & Terrorism 36(6): 431-459.

Office of the Secretary of Defense. 2021. “Leadership Stand-Down to Address Extremism in the Force.”

Patel F. 2021. “Biden’s Plan to Roll Back Discriminatory Counterterrorism Policies.” New York NY: Brennan Center for Justice.

Petrow-Cohen C. 2021. “To Confront the Reality of Domestic Terrorism, We Need a Federal Law.” Los Angeles Times, July 29, 2021. https://www.latimes.com/opinion/story/2021-07-29/domestic-terrorism-federal-law.

Rose AE, DP Prina, MD Palmer, and B Rapoza. 2020. “Leveraging FBI Resources to Enhance Military Accessions Screening and Personnel Security Vetting.” Defense Personnel and Security Research Center: Seaside, CA.

Simi P and S Windisch. 2020. “Why radicalization fails: Barriers to mass casualty terrorism. Terrorism and political violence” 32(4): 831-850.

Stephens W, S Sieckelinck, and H Boutellier. 2021. “Preventing violent extremism: A review of the literature.” Studies in Conflict and Terrorism 44(4): 346-361.

Striegher JL. 2015. “Violent-Extremism: An Examination of a Definitional Dilemma.” Australian Security and Intelligence Conference. https://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1046&context=asi.

Winter C, P Neumann, A Meleagrou-Hitchens, M Ranstorp, L Vidino, Furst J. 2020. “Online Extremism: Research Trends in Internet Activism, Radicalization, and Counter-Strategies.” International Journal of Conflict and Violence (14(2): 1-20.Dion-Schwarz et al. 2019

Wolfowicz M, Y Litmanovitz, D Weisburd, and B Hasisi. 2019. "What Is the State of the Quantitative Literature on Risk Factors for Radicalization and Recruitment to Terrorism?" In Understanding Recruitment to Organized Crime and Terrorism, pp. 25-53. Springer, Cham.

World Institute for Nuclear Security (WINS). 2020. “Countering Violent Extremism and Insider Threats in the Nuclear Sector.”

Zabel RB. 2021. “Domestic Terrorism is a National Problem. It Should Also be a Federal Crime.” Washington Post, February 2, 2021. https://www.washingtonpost.com/opinions/2021/02/02/domestic-terrorism-federal-crime/.

Zeitzoff T. (2017). "How Social Media Is Changing Conflict." Journal of Conflict Resolution 61(9): 1970-1991.

Appendix A – Literature Review Summary

Table 5: Summary of Literature Reviewed

In-Text Citation	Key Points
Striegher 2015	• Discusses the terms radicalization, violent-extremism, and terrorism and how they are used interchangeably; highlights the confusion around terms. • Provides additional definition of violent extremism, radicalization, and terrorism.
CEP 2020	• Reviews and discusses far-right violent extremism in Finland, France, Germany, Sweden, the UK, and the U.S. • Discusses the structure and drivers of far-right violent extremists across national boundaries. • Provides an overview of the legal definition of terrorism/domestic terrorism within various countries, legal protections, etc. • Discusses the transnational connectedness of far-right groups.
ADL n.d.	• Provides simple, clear definitions of terms relevant to the domestic extremism space, particularly white supremacy.
FBI 2020	• Provides definitions of domestic terrorism, DVE, and threats posed by domestic violent extremists.
DHS 2021a	• Informs law enforcement partners to be especially vigilant against the threat of DE.
DHS 2021b	• Informs law enforcement partners to be especially vigilant against the threat of DE.
DNI 2021	• Outlines and defines the heightened threat posed by DVEs in 2021. – Domestic violent extremists: U.S.-based actors who conduct or threaten activities that are dangerous to human life in violation of the criminal laws of the United States or any state; appearing to be intended to be intimidate or coerce a civilian population; and influence the policy of a government by intimidation or coercion or affect the conduct of a government by mass destruction, assassination, or kidnapping, as per the definition of domestic terrorism in 18 U.S. Code 2331(5). • Uses the same categories as the FBI (2020, 2021).
Congressional Report 2021	• Highlights some failures in preparation for and in response to the U.S. Capitol attack on January 6. • Provides recommendations for changes within Department of Defense, DHS, FBI, and U.S. Capitol Police to improve preparedness and to help prevent similar issues from arising again.
Flade 2021	• Reviews cases of far-right extremists among Germany's military and police. • Emphasizes the need for international collaboration to share lessons learned and best practices in detection and monitoring to prevent infiltration of security and military forces by extremists.

In-Text Citation	Key Points
Dion-Schwarz et al. 2019	• Reviews the use of cryptocurrency by terrorist groups. • Discusses the changes that might make cryptocurrency more attractive to terrorist groups in the future.
National Security Council 2021	• Highlights the threat posed by DVEs in 2021 and onward, and provides a description of the threat, focusing especially on RMVEs. • Outlines the key strategies to address the threat.
Koehler and Popella 2020	• Uses a data set of right-wing chemical, biological, radiological, and nuclear (CBRN) incidents to demonstrate the potential threat. • Identifies 31 far-right CBRN incidents in the U.S., UK, and South Africa between March 1970 and May 2017. – Overall, CBRN terrorism is very rare and generally unsophisticated; even if the plots were successful in acquiring the material, they were unlikely to be able to use it in a mass casualty attack.
Guarrieri and Meisel 2019	• Determines whether there are individual differences between attackers who choose chemical/biological agents as their method for terrorist attack. – Older extremists are more likely to pursue CB weapons. – Jobless/student extremists are more likely to pursue CB weapons. – No relationship with gender.
Kruglanski et al. 2020	• Reviews the ways that terrorist/extremist groups have taken advantage of the COVID-19 pandemic and associated disruption.
McCann 2020	• Attempts to identify the factors that influence the likelihood of CBRN terrorism. • Creates a novel database of CBRN terrorist acts using the Profiles of Incidents Involving CBRN and Non-state Actors, Extended Data on Terrorist Groups (Hou et al. 2020), and the Global Terrorism Database. – Lone actors were more likely to pursue CBRN/BRN than groups. – Religious groups were more likely to pursue CBRN/BRN than other groups.
Zeitzoff 2017	• Highlights how social media has impacted politics and conflict. – Social media reduces the cost of communication and increases the speed and dissemination of information.
Davies et al. 2020	• Reviews the ways that extremist groups have capitalized on the pandemic to further participation in their case. • Demonstrates that posting behavior increased online on some extremist forums.
Berger 2014	• Talks about Islamic State in Iraq and Syria (ISIS) and the ways that they've used social media to recruit new members. • Outlines the tactics/techniques used on Twitter by ISIS to spread their message and to increase engagement from potential recruits through "Dawn of Glad Tidings" and use of hashtags.
Gambhir 2016	• Talks about ISIS's strategy online in their information operations campaigns Describes strategic goals and tactics used to achieve them.

In-Text Citation	Key Points
Frissen 2021	• Examines the rates at which different types of extremist media are sought online. • Explores the associations between different factors and cognitive radicalization. – Although shocking forms of media (i.e., beheading videos) are most sought, other types of media (magazines) are more strongly associated with cognitive radicalization and its precursors (juvenile delinquency, moral disengagement).
Hafez and Mullins 2015	• Serves as an excellent summary of the different factors that contribute to radicalization. – This is important, as it outlines the potential “risk factors” for radicalization, or potentially, indicators of radicalization. Can help us to consider how or why organizations or societies might be at risk.
Wolfowicz et al. 2019	• Quantitative review of risk factors for radicalization within democratic countries – Reviews 53 papers published between 2007 and 2018, most of which focused on cognitive radicalization in the form of attitudes as the dependent variable. 12 examined radical behaviors through self-report (5) or terrorist activity (7). This paper identifies the key risk and protective factors for cognitive radicalization and radical attitudes, known precursors to behavioral radicalization and risk factors for violence.
King and Taylor 2011	• Reviews theoretical models of terrorism and radicalization. • Provides an excellent overview of the ways that individuals might become radicalized and therefore behaviors you might see at various points along that process or pathway (if it is in fact linear; see Hafez and Mullins).
Jasko et al. 2017	• Explores the association between demographic factors and the likelihood of violence within a set of ideologically motivated crimes. – Economic failure, social detachment, and traumatic/abusive experiences predicted the likelihood of violence.
Kruglanski et al. 2018	• Describes the significance quest theory, which argues that individuals engage in violent extremism as part of an ongoing search for meaning and importance in their lives.
Moghaddam 2005	• Describes the "staircase to terrorism" model, which consists of six steps: – Psychological interpretation of material condition (unfair) – Perceived options to fight unfair treatment (few options) – Displacement of aggression (blaming a specific group) – Moral engagement (engaging with the idea of committing violence) – Solidification of categorical thinking (us vs. them; dehumanization) – Terrorist act
Denoeux and Carter 2009	• Examines societal and social factors that influence the potential growth of violent extremism. – Most relevant here as it underscores the importance of a sense of justice in prevention of violent extremism.

In-Text Citation	Key Points
Doosje et al. 2016	• Outlines a model of radicalization process with three phases: – Sensitivity – Group membership – Action • Describes the micro-, meso-, and macro-level factors that influence each of these steps.
Moghaddam 2009	• Describes deradicalization as the process of taking steps down the staircase from terrorism. • Discusses what deradicalization should entail based on where the individual was on the staircase to terrorism.
Stern 2016	• Describes the risk factors for radicalization, specifically focused on ISIS. • Discusses recommendations for countering ISIS in the U.S.: – Amplify stories of real wives of ISIS and other defectors – Take on ISIS's version of Islam in a way that appeals to potential ISIS recruits – Highlight ISIS's hypocrisy – Publicize ISIS's atrocities against Sunnis – Suspend ISIS's social media accounts
Brown et al. 2021	• Interviews 24 former extremists and 12 of their family members/friends, representing 32 cases of radicalization/deradicalization – 24/32 were white supremacists – Eight were Islamist extremists – Has an excellent summary of the factors influencing radicalization and deradicalization, as well as detailed recommendations for what communities can do to counter radicalization and research needed.
Stephens et al. 2021	• Reviews the literature and identifies four key themes in preventing violent extremism: – Developing resilience in individuals – Creating space to explore and validate identities – Engaging in open dialog and allowing individuals to have a voice – Creating engagement between communities and institutions (e.g., police) and strengthening social ties within/between communities ○ Many of the suggestions could be modified/applied to an organizational context to improve organization resilience against extremism.
Ellis and Abdi 2017	• Discusses how to build community resilience to prevent violent extremism (VE) through partnerships with community organizations. • Summarizes the ways that these community partnerships can increase bonds and decrease susceptibility to extremism.
Brill and Bernhard 2020	• Argues for making the International Atomic Energy Agency (IAEA) Code of Conduct a legally binding agreement using some impactful statistics regarding incidents of trafficking and misuse of radioactive material.

In-Text Citation	Key Points
	• Provides three options for doing so: making it a stand-alone treaty, adding it to the Convention on the Physical Protection of Nuclear Material and Nuclear Facilities, or adding it to the Joint Convention on the Safety of Spent fuel.
Simi and Windisch 2020	• Uses a sample of white supremacists who did not engage in mass casualty violence but were part of groups that might use that as a tactic, examines barriers to mass casualty violence. • Barriers included: – Belief that mass casualty violence is counterproductive – Preference for interpersonal violence – Change in focus/availability for movement – Internal organizational conflict – Moral apprehension
Ellis et al. 2020	• Provides an example of a community engagement program to prevent radicalization to violence. • Suggests not focusing on extremism specifically but instead focusing on violence prevention overall and integrating violent extremism prevention efforts into those programs but highlights that interventionists should be aware and knowledgeable about relevant ideologies and motivations.
Mulligan et al. 2021	• Provides a detailed policy blueprint for countering white supremacist violence. • Recommends leveraging federal government resources, developing new research through data sharing, improving reporting and tracking of white supremacist violence, providing resources to communities, and legislating/prioritizing hate crimes. • Provide recommendations for preventing infiltration of or recruitment of military, law enforcement, and veterans, all of whom are targeted by white supremacist groups.
Clifford 2021	• Reviews data on 40 individuals who engaged in racially or ethnically motivated violent extremist (RMVE) acts between 2014 and 2019 to identify a demographic description and understand any gaps in legislation. – Perpetrators were around 30 years of age, all male; 10 had served in the military; 13 had prior criminal offenses. – Most common targets were religious institutions, distantly followed by large public events. Charges were generally federal laws around firearms, interstate violations, weapons of mass destruction, etc. – RMVEs generally received slightly shorter sentences than homegrown violent extremists with ties to terrorist organizations (e.g., ISIS). – One way to alleviate the sentencing gap is to introduce an additional statue under 18 USSC 2332(b) to cover acts of terrorism without an international connection.
Jugl et al. 2020	• Conducts meta-analysis of evaluations of VE/radicalization prevention programs. • Concludes that programs varied widely in their techniques, but all were generally effective.

In-Text Citation	Key Points
	– Authors suggest that VE/radicalization programs should be broad and offer opportunities to strengthen social and cognitive skills, drawing from crime prevention programs, which have consistently been shown to be effective.
Neumann 2013	• Online radicalization can occur through online disinhibition, a sense of moral outrage, extremist forums as criminogenic environments, mortality salience, mobilization through role-playing, and links to terrorist organizations. • Three ways that online radicalization can be countered: eliminate content, reduce demand, or exploit cyberspace for evidence/intelligence. • Explores and describes these methods in more detail.
World Institute for Nuclear Security (WINS) 2020	• Introduces the concept of insider threat. • Gives guidance on creating realistic VE insider threat scenarios Outlines key preventive measures to VE insiders. • Describes the elements of a good human reliability program in detail, including measures that should be taken before, during, and after employment. • Includes list of "red flag" behaviors for VE concerns.
Rose et al. 2020	• Looks at the potential ways that Department of Defense (DoD) can leverage FBI resources for the vetting of military accessions. • Provides an overview of relevant DoD policies and definitions in the introduction. • Reviews different databases as sources of information on DE. • Domestic terrorism (DT): A criminal or federal violation that involves the threat of or use of force or violence in furtherance of a political or social ideology.
Jensen et al. 2018	• Outlines the role of social media in radicalization. • Results showed that lone actors were more active on social media and it played a greater role in their radicalization. – Social media did not, however, increase the success rate of U.S.-based extremists seeking to join foreign groups. – Social media did contribute to the speed of radicalization.
Jensen et al. 2016	• Provides some overview statistics regarding individuals in the U.S. who attempt to leave or have expressed interest in leaving the U.S. to support a foreign armed group or foreign regime. – Gives some descriptive information about the role of the internet in radicalization of foreign fighters: in 86% if cases, the internet played a role; in 50%, social media played a role. – The average time frame for radicalization reduced from 16.3 months in 2002 to 9.8 months in 2015; this corresponded to an increase in the percentage of individuals for whom the internet played a role in their radicalization.

Pacific Northwest
National Laboratory

902 Battelle Boulevard
P.O. Box 999
Richland, WA 99354
1-888-375-PNNL (7665)

www.pnnl.gov