INSTITUTE FOR DEFENSE ANALYSES

Prohibited Extremist Activities in the U.S. Department of Defense

Peter K. Levine
Joseph F. Adams
Amy A. Alrich
Rachel G. Augustine
Margaret D.M. Barber
Sujeeta B. Bhatt
Kathleen M. Conley
Dave I. Cotting
Alan B. Gelder
Jeffery M. Jaworski
Mark F. Kaye
Carrington A. Metts
Neil V. Mithal
Matthew J. Reed

December 2023*
Approved for public release; distribution unlimited.
IDA Paper P-33076
Log: H 22-000175

INSTITUTE FOR DEFENSE ANALYSES
730 E. Glebe Road
Alexandria, Virginia 22305

The Institute for Defense Analyses is a nonprofit corporation that operates three Federally Funded Research and Development Centers. Its mission is to answer the most challenging U.S. security and science policy questions with objective analysis, leveraging extraordinary scientific, technical, and analytic expertise.

About This Publication
This work was conducted by the Institute for Defense Analyses under contract HQ0034-19-D-0001, project BE-6-5006, "Study on Extremist Behavior within DoD Total Force," for the Office of the Under Secretary of Defense for Personnel and Readiness (USD(P&R)). The views, opinions, and findings should not be construed as representing the official position of either the Department of Defense or the sponsoring organization.

For More Information:
Mr. Peter K. Levine, Project Leader
plevine@ida.org, 703-845-2516
Ms. Jessica L. Stewart, Director, SFRD
jstewart@ida.org, 703-575-4530

***This research was conducted from June 2021 to June 2022.**

INSTITUTE FOR DEFENSE ANALYSES

IDA Paper P-33076

Prohibited Extremist Activities in the U.S. Department of Defense

Peter K. Levine
Joseph F. Adams
Amy A. Alrich
Rachel G. Augustine
Margaret D.M. Barber
Sujeeta B. Bhatt
Kathleen M. Conley
Dave I. Cotting
Alan B. Gelder
Jeffery M. Jaworski
Mark F. Kaye
Carrington A. Metts
Neil V. Mithal
Matthew J. Reed

This page is intentionally blank.

Executive Summary

***This research was conducted from June 2021 to June 2022.**

On 5 February 2021, Secretary of Defense Lloyd Austin issued a memorandum directing a one-day stand-down to discuss and address extremism in the Department of Defense (DOD). On 9 April 2021, the Secretary issued a second memorandum, directing immediate actions to counter prohibited extremist activities in the Department and establishing a working group to implement those actions and develop additional recommendations. One of the immediate actions called for by the April 9 Memorandum was an independent study on extremist behavior in the Total Force. On June 21, 2021, this study was awarded to the Institute for Defense Analyses (IDA).

The objective of the IDA study was to gain greater fidelity on the scope and nature of extremist ideologies and behaviors in the military community (including service members, former service members, DOD civilians, and contractor employees); identify the sources of such ideologies and behaviors; assess their impact; and develop strategies for preventing, countering, and neutralizing that impact. To that end, IDA formed three sub-teams: a social and behavioral sciences team, a law and policy team, and a data and technology team. The three teams built a library of governance documents, studies, articles, and data regarding extremist activities and related behaviors. Together, the teams conducted 57 interviews, including more than one hundred DOD officials and outside experts, and conducted site visits at geographically diverse Marine Corps, Navy, Air Force, and Army installations.

There are many forms of extremist ideologies and motivations. The academic literature describes left-wing extremism, right-wing extremism, single-issue extremism, and politico-religious extremism. Law enforcement agencies describe racially or ethnically motivated extremism, anti-government or anti-authority extremism, animal and environmental rights extremism, abortion-related extremism, and other domestic terrorism threats. Extremist activities range from advocacy to threats of force to violent action. To avoid constitutional concerns, law enforcement agencies must investigate specific criminal acts, and not someone's membership in extremist groups. DOD has greater leeway with regard to regulating and investigating the conduct of service members, but still seeks to define extremism in terms of conduct, not beliefs.

IDA's review found no evidence that the number of violent extremists in the military is disproportionate to the number of violent extremists[*] in the United States as a whole, although there is some indication that the rate of participation by former service members is slightly higher and may be growing. IDA also found no evidence of violent extremist behavior by DOD civilians.

[*] It does not appear to be possible to compare military and civilian participation rates for nonviolent forms of extremist activities that are prohibited for service members, because these forms of conduct are not prohibited for the civilian population.

The participation in violent extremist activities of even a small number of individuals with military connections and military training, however, could present a risk to the military and to the country as a whole.

DOD has used a wide variety of terms, phrases, and concepts to describe prohibited extremist behaviors and activities. As a result, service members at all levels told the IDA team that they are unaware of or confused about existing definitions and standards. In the absence of a clear and consistent message, there is a risk that misinterpretations could lead to a significant division in the force along political and ideological lines, with some members of the military believing that they are being targeted for their views. IDA found reason to believe that the risk to the military from widespread polarization and division in the ranks may be a greater risk than the radicalization of a few service members. For this reason, IDA's recommendations focus more on steps that could be taken to address underlying causes of extremist behavior than on punitive responses to such behavior.

The Department recently published an improved definition of prohibited extremist activities, which broadly encompasses the use or advocacy of unlawful force or violence to deprive individuals of their rights, or to achieve goals that are political, religious, discriminatory, or ideological in nature.** However, other DOD, Military Department, and service policies contain language that is inconsistent with the new definition and the Department does not appear to have developed a clear message in support of the new guidance. *IDA recommends that DOD take steps to ensure that the new definition is consistently applied throughout the Department. The Department should also develop a communication plan that informs the force of the new policy in as non-divisive a manner as possible by presenting restrictions on prohibited extremist activities as a logical constituent of widely-accepted military values.*

The IDA team determined that easy access to online information and social networks can serve as a conduit for disinformation, extremist content, and hate speech, which can lead to radicalization. Although pathways to radicalization vary and there is no single profile of a radicalized individual ready to take violent action, many of the factors that make individuals susceptible to radicalization also drive other maladaptive behaviors such as suicidal inclinations and other forms of violence. For the Veterans' community in particular, loss of military identity appears to have a strong association with difficult adjustments to civilian life that can in turn contribute to negative behaviors.

Military core values help build greater connectedness and may serve as a bulwark to build and sustain resistance to radicalization. For this reason, *IDA recommends that the Department focus its efforts to prevent prohibited extremist conduct in ongoing education and training in core values such as loyalty, respect, duty, honor, and mission, emphasizing from recruitment all the way to separation that these values are inconsistent with prohibited extremist activities. The*

** DOD Instruction 1325.06, "Handling Protest, Extremist, and Criminal Gang Activities Among Members of the Armed Forces," December 20, 2021, p. 9–11.

Department should also work to counter false information campaigns and build critical thinking in the force by providing training and instruction on how to be a critical consumer of information.

The Department could also support service members by expanding on comprehensive threat assessment teams to identify at-risk behaviors, activities, and vulnerabilities at multiple levels. Risk assessment teams should have connectivity to the full range of resources and assistance that are available to the Department. *In addition, the Department should leverage available opportunities to foster strengthened post-separation group identity for former service members.* Although the Department does not have jurisdiction over veterans (with a limited exception for retirees who can be recalled to active duty for certain purposes), it does have an opportunity in the separation process to connect departing service members to available resources, including community and support groups. The Department of Veterans Affairs (VA) should also play a vital role.

The IDA team found that multiple legal and policy regimes applicable to prohibited extremist activities by service members provide DOD with a broad range of prevention, mitigation, and disciplinary options to forestall and respond to problematic conduct. Legal and policy regimes include suitability and credentialing processes, security clearance processes, insider threat programs, equal opportunity and anti-harassment systems, command discipline systems, the military justice system, and the federal criminal justice system. Available options under these regimes range from feedback and counseling to informal and formal letters of counseling, admonition, or reprimand; non-judicial punishment; administrative discharge; and criminal sanctions.

In light of the inherent gray areas in any definition of extremism, the IDA team concluded that a punitive approach to all forms of prohibited extremist activities would risk alienating a significant part of the force. For this reason, *IDA recommends a consistent and carefully modulated approach that matches the response to the offense and seeks restorative interventions such as mentoring and counseling before punishment for behaviors that are not obviously criminal in nature.* Although this is the current practice of most military commanders and their legal advisors, the Department's messaging has not always been consistent with this practice. *IDA also recommends against escalating the punitive focus on extremist activities by making prohibited extremist activities a separate criminal offense under the Uniform Code of Military Justice. Instead, the Department should expressly make evidence of extremist motivations an aggravating factor in sentencing for other criminal offenses.*

The Department has a narrower set of tools to address extremist activities in its civilian and contractor workforces (to the extent that such activities, which do not appear to have been documented, take place). DOD civilians work under the government-wide civil service system, with strong procedural protections that cannot generally be waived or modified by the Department. The Department can impose requirements on contractor employees through mandatory contract provisions, but both civilian employees and contractors enjoy the full range of First Amendment rights without any of the limitations that may apply to members of the Armed Forces. As a result,

the most effective legal tools available to reach prohibited extremist activities in the broader Total Force are the Department's processes for authorizing access to information, systems, and facilities.

DOD's processes for awarding security clearances, assessing suitability, and granting access to facilities still focus to a significant extent on Cold War threats and threats related to the Global War on Terrorism rather than the threat of home-grown extremism. For this reason, *IDA recommends that the Department update and standardize security and suitability questions to directly ask about prohibited extremist activities; develop guidance on security clearance, access, and suitability determinations, explaining how active participation in prohibited extremist activities will be considered pursuant to existing criteria; and update insider threat training and related materials to provide definitions and examples of prohibited extremist activities and to expressly encourage early reporting of potential concerns.* Updating some of these processes (and incorporating them into new continuous evaluation procedures) may require a whole-of-government approach beyond what the Department can unilaterally accomplish.

IDA was also directed to review and evaluate current DOD information collection, tracking, and data sharing systems (including military justice systems, equal employment opportunity systems, command discipline systems, hotline response systems, insider threat programs, and law enforcement/security systems). This requirement runs parallel to section 554(b) of the National Defense Authorization Act for Fiscal Year 2021, which required the Department to develop standard mechanisms for tracking supremacist, extremist, and criminal gang activities across the Armed Forces.

The IDA team found that a number of DOD information systems, including the military justice, criminal investigative, and equal opportunity systems of the military departments, have begun to incorporate mechanisms for flagging extremism cases in the past few years. However, these flagging systems are not linked or standardized, and lack clear and consistent definitions. As a result, they have produced inconsistent data at best. *IDA recommends that the Department take steps to ensure that the new definition of prohibited extremist activities is consistently applied to all extremism flagging systems, ensure that flagging capabilities can differentiate between substantiated cases and unsubstantiated allegations, and implement quality control checks to ensure that cases are recorded consistently and appropriately.*

Finally, the IDA team learned that the Department is considering how to use existing authority to screen publicly available social media to identify prohibited extremist activities by service members and others in the military community (including DOD civilians and contractor employees). Any such effort must overcome significant technical challenges as well as legitimate concerns about overly intrusive surveillance that could alienate a significant part of the force. These challenges and concerns are exacerbated by a lack of clarity regarding the types of online behavior that are potentially subject to disciplinary action in the Department. For these reasons, *IDA recommends that the Department clarify its guidance regarding expectations for online behavior and social media activities, and exercise great caution in fielding systems and technologies for screening the social media activities of members of the military community.*

Many of the recommendations in this report call for comprehensive cultural change that cannot be accomplished through a single action but will require a concerted effort over a period of time. While IDA is not in a position to design a comprehensive course of action for each recommendation, this report suggests a number of implementation steps that the Department could take. The Department has already taken a number of these steps as a result of the Secretary's direction and the review conducted by the Secretary's Countering Extremist Activities Working Group (CEAWG).

Anecdotal accounts of military participation in violent extremist events, like the events of 6 January 2021, draw public attention and may create the impression that the military has "an extremism problem." Such accounts magnify the actions of a few and provide little information on the overall scope of the problem. Moreover, these accounts frequently fail to differentiate between those who are currently serving in the military and those who have left the military (often many years earlier) or have been removed from the military for cause with less than honorable discharges. As the Department responds to such events, it should remain cognizant of the fact that violent extremism does not appear to be any more prevalent among service members than it is in American society as a whole, and avoid steps that risk unnecessary polarization or division in the ranks.

This page is intentionally blank.

Contents

1. Introduction

At a time when public confidence in major public and private institutions has been seriously undermined by deep cultural and political divisions in American society, support for the U.S. military has declined slightly, but remains relatively unscathed. For example, Gallup's most recent poll on institutional trust shows that only 38 percent of Americans have confidence in the presidency, 12 percent have confidence in Congress, 16 percent have confidence in television news, 37 percent have confidence in organized religion, 20 percent have confidence in the criminal justice system, and 32 percent have trust in the public schools. By contrast, 69 percent of Americans reported having "a great deal" or "quite a lot" of confidence in the military.[1]

There are many reasons for the American public's continued confidence in the Armed Forces. These likely include: the military mission of defending the nation and serving the national interest; the military commitment to a consistent set of American values; the competence shown by the Armed Forces in responding to crises of all kinds; and the obvious sacrifice made by so many service members over the course of 20 years of conflict in the Middle East and Central Asia (as well as sacrifices in previous conflicts). One factor that should not be overlooked in maintaining the military's popularity in the face of societal divides is the military tradition of nonpartisanship and the steadfastness of the Armed Forces—from the leadership down—in resisting the efforts from all sides to draw them into the political fray.

Against this background, there have been a number of recent incidents of violent extremism involving service members and veterans. Most recently, on 6 January 2021, supporters of a defeated presidential candidate stormed the Capitol Building in "a violent insurrection for the purpose of trying to prevent the peaceful transfer of power after a legitimately certified election, from one administration to the next."[2] Soon thereafter, media reports began to emerge that a significant number of participants in this event had served in the military.[3] Even if the number of violent extremists with military connections is not disproportionate to the number of service members and veterans in American society as a whole, significant participation of military-

---

1 Jack Marshal, "Gallup's Institutional Trust Poll," *Ethics Alarms,* July 18, 2021, https://ethicsalarms.com/2021/07/18/gallups-institutional-trust-poll/.

2 Jonathan Weisman and Annie Karni, "McConnell Denounces R.N.C. Censure of Jan. 6 Panel Members," *New York Times,* February 8, 2022, https://www.nytimes.com/2022/02/08/us/politics/republicans-censure-mcconnell.html (quoting Senate Republican Leader Mitch McConnell).

3 E.g., Olivia Rubin, "Number of Capitol Riot Arrests of Military, Law Enforcement and Government Personnel Rises to 52," *ABC News,* April 23, 2021, https://abcnews.go.com/US/number-capitol-riot-arrests-military-law-enforcement-government/story?id=77246717.

connected individuals in violent activities that are inconsistent with the military's tradition of nonpartisanship could undermine the military's positive image and widespread public support.

On 5 February 2021, Secretary of Defense Lloyd Austin issued a memorandum directing a one-day stand-down to discuss and address extremism in the Department of Defense.[4] On 9 April 2021, the Secretary issued a second memorandum, directing immediate actions to counter prohibited extremist activities in the Department and establishing a working group to implement those actions and develop additional recommendations.[5] One of the immediate actions called for by the April 9 Memorandum was an independent study on extremist behavior in the Total Force. On 21 June 2021, this study was awarded to the Institute for Defense Analyses (IDA).

The objectives of the IDA study are to gain greater fidelity on the scope and nature of extremist ideologies and behaviors in the Department; identify the sources of such ideologies and behavior; assess their impact; and develop strategies for preventing, countering, and neutralizing that impact. To that end, the project description calls for IDA to:

1. Document the range of known extremist ideologies and behaviors that are contrary to U.S. law and policy;
2. Identify existing definitions of extremism and prohibited extremist activities;
3. Identify pathways of extremist ideology and behavior broadly and within the Department in particular;
4. Assess why the DOD workforce and others in the military community (including veterans, DOD civilians, and contractor employees) might be susceptible to extremist recruiting efforts;
5. Survey DOD approaches to the prevention of other forms of violence (including suicide, domestic violence, assault, sexual assault, and hate crimes) to identify strategies that might be adopted;
6. Assess policies and initiatives of other federal agencies that might be helpful to the Department;
7. Identify existing legal frameworks for addressing prohibited extremist activities in the Total Force;

---

[4] Secretary of Defense, "Memorandum for Senior Pentagon Leadership Defense Agency and DOD Field Agency Activity Directors: Stand-Down to Address Extremism in the Ranks," (Memorandum, Washington. DC: Department of Defense, February 5, 2021), https://media.defense.gov/2021/Feb/05/2002577485/-1/-1/0/STAND-DOWN-TO-ADDRESS-EXTREMISM-IN-THE-RANKS.PDF.

[5] Secretary of Defense, "Memorandum for Senior Pentagon Leadership Commanders of the Combatant Commands Defense Agency and DOD Field Activity Directors: Immediate Actions to Counter Extremism in the Department and the Establishment of the Countering Extremism Working Group," (Washington, DC: Department of Defense, April 9, 2021), https://media.defense.gov/2021/Apr/09/2002617921/-1/-1/1/MEMORANDUM-IMMEDIATE-ACTIONS-TO-COUNTER-EXTREMISM-IN-THE-DEPARTMENT-AND-THE-ESTABLISHMENT-OF-THE-COUNTERING-EXTREMISM-WORKING-GROUP.PDF.

8. Evaluate current DOD efforts to counter extremist ideologies and behaviors in the ranks, identifying gaps and strengths; and
9. Review and evaluate current DOD information collection, tracking, and data sharing systems (including through the military justice, equal employment opportunity, command discipline, hotline response systems, insider threat, and law enforcement/security systems).

The project description also calls for IDA to provide recommendations for steps that the Department could take to prevent, address, and neutralize the spread of prohibited extremist activities in the Armed Forces, and in the broader military community (including veterans, civilian personnel, and contractor employees).

Chapter 2 explains the methodology used by IDA to develop this report.

Chapter 3 of this report provides background on the historic context for extremist activities in the Armed Forces, together with an assessment of the current state of knowledge on the prevalence of such activities in the military community.

- Part A discusses historic context, showing that the military reflects American culture and society and shares a parallel history of violent extremist events.
- Part B discusses prevalence, showing that the level of participation of service members in violent extremist activities remains low and is not disproportionate to levels of violent extremism in the United States as a whole.

Chapter 4 discusses definitions of extremism, addressing requirements (1) and (2) of the project description.

- Part A addresses scholarly definitions and law enforcement categories, which describe stages of radicalization and categories of extremist ideologies.
- Part B addresses DOD definitions, showing that the Department has used many different words and phrases to describe prohibited extremist activities, heightening the risk of confusion and misinformation.

Chapter 5 discusses pathways to extremist ideology and behavior, addressing project requirements (3) and (4).

- Part A identifies risk factors and indicators for extremism and shows commonalities with risk factors and indicators for other forms of violence and destructive activities.
- Part B discusses false information and conspiracy theories and summarizes scholarly discussion of possible responses.

Chapter 6 discusses existing interventions and strategies to counter radicalization, addressing project requirements (5) and (6).

- Part A discusses lessons from outside DOD, focusing on the resiliency model utilized by the Federal Bureau of Investigation (FBI) and Department of Homeland Security (DHS) and the threat assessment model utilized by the National Threat Assessment Center and local law enforcement agencies.
- Part B addresses DOD efforts to build resiliency in service members through education, training, and the inculcation of military values.
- Part C addresses DOD efforts to implement a threat assessment model through the primary prevention workforce and the DOD Insider Threat Management and Analysis Center.
- Part D addresses mechanisms for reaching veterans.

Chapter 7 discusses legal and policy mechanisms for responding to extremist activities in the military community, addressing project requirements (7) and (8).

- Part A shows that a broad range of mechanisms are available to address prohibited extremist activities in the military, and makes the case that an excessively punitive focus on such activities would be counterproductive.
- Part B shows that a narrower range of mechanisms are available to address extremist activities among DOD civilians and contractor employees, but that some of these mechanisms have been underutilized.

Chapter 8 discusses data and technology aspects of DOD efforts to counter extremist behaviors and activities, addressing project requirement (9).

- Part A discusses DOD systems for tracking data on prohibited extremist activities and shows that these systems are still incipient stages of development.
- Part B discusses non-government systems for tracking data on extremism and describes continuing limitations on available data.
- Part C discusses legal and technical issues raised by efforts to screen social media for prohibited extremist activities.

Chapter 9 summarizes IDA's conclusions and recommendations.

While the primary focus of the IDA review was on members of the Armed Forces, this report contains sections addressing the broader military community, including veterans, DOD civilians, and defense contractor employees. Chapter 3.B.2. shows that the level of participation of veterans in violent extremist activities appears to be increasing, while Chapter 6.D. discusses the limited toolset available to the Department to address extremist activities among former service members. Chapter 7.B. addresses legal and policy mechanisms for addressing extremist activities among DOD civilians and contractor employees (although no such cases have been identified) and shows that the Department is not making full use of the tools available to it. In addition, Chapter 7.A.4. addresses issues unique to the reserve components, finding that although the same standards of conduct apply, they may be difficult to enforce in some cases.

2. Methodology

A. The Sub-Team Approach

The IDA project description called for a wide-ranging study that would help the DOD gain greater fidelity on the scope and nature of extremist ideologies and behaviors in the military community, identify the sources of such ideologies and behavior, assess the tools available to the Department for addressing prohibited extremist activities, and develop strategies for preventing, countering, and neutralizing the impact of such activities.

To address these issues, IDA formed three separate sub-teams: a social and behavioral sciences (SBS) team, a law and policy (L&P) team, and a data and technology (D&T) team. The SBS team was responsible for assessing pathways of extremist ideologies and behaviors, the range of such ideologies and behaviors, and why the military community might be susceptible to these ideologies and behaviors. The L&P team was responsible for addressing legal frameworks for confronting extremist activities and current DOD efforts to respond to such activities. The D&T team was responsible for addressing current DOD information systems and data on extremist activities. The three teams worked together to discuss DOD approaches to other types of violence and the resources, policies, and initiatives of other agencies.

In addition, the three teams worked together on a set of interviews with senior DOD officials and conducted four site visits to military installations, the results of which supported the work of all three teams.

1. Social & Behavior Sciences

The SBS team began the task by creating a library of existing empirical studies, meta-analyses, and literature reviews regarding radicalization, extremism, and terrorism. Additionally, the team collected materials regarding the history of extremism and radicalization both in the United States and abroad. They also collected literature on existing Federally-developed threat assessment programs (e.g., National Threat Assessment Center (NTAC)) and on the state and local law enforcement programs that emerged from NTAC's work. Finally, the SBS team worked with the other teams to conduct interviews with government officials (DOD, federal, state, and local law enforcement) with responsibilities associated with prevention and response to radicalization and terrorism, as well as engaging in site visits at Army, Navy, Air Force, and Marine military installations.

Using the information gathered as a foundation, the SBS team developed a brief historical context to radicalization and terrorism. The team then described the various terms associated (and often confounded) with extremism as they are operationalized in the academic literature and by

Federal law enforcement. The team followed this with a summary of the literature on the process of radicalization, the role of false information in radicalization, approaches to assessing the risk of radicalization, and a review of current programs for countering violent extremism (CVE). Because of the focus on service members, the team reviewed the self/identity development process, the related internalization of military values as a protective factor in radicalization prevention, and the potential to leverage the transition to veteran process and veterans support organizations to counter radicalization post-service. Finally, the SBS team reviewed the DOD's prevention strategies for other forms of violence within the services and the broad threat assessment approaches taken by other governmental organizations.

2. Law & Policy

The L&P team began by creating a library of existing statutes, regulations, directives, and instructions addressing prohibited extremist activities and related behaviors. The library included government-wide statutes and regulations, DOD-wide statutes and regulations, and service-specific guidance. It also included studies and articles regarding extremist activities and related behaviors inside and outside the military community. The L&P team then worked with the other teams to conduct a series of interviews of government officials with relevant responsibilities, including senior leaders, leaders of DOD personnel systems, leaders of DOD security and investigative organizations, leaders of the DOD legal community (including the military justice system), and representatives of other federal agencies with responsibilities for countering extremist activities and related behaviors. These interviews were supplemented by a series of site visits, in which the three teams engaged with a cross-section of service members and DOD civilians from all three Military Departments.

On the basis of this information, the L&P team identified existing definitions of extremism, assessed the elements of these definitions, and identified gaps and inconsistencies among them. The team identified legal frameworks for addressing extremist activities and related behaviors, identified gaps and inconsistencies in these frameworks, and used this analysis to assess the effectiveness of current DOD efforts in this area. Finally, the L&P team worked with the other teams to assess policies and resources of other federal agencies and assess the extent to which these policies and resources might be helpful to the Department.

3. Data & Technology

The data and technology team conducted a variety of efforts to assess the types of data for tracking and monitoring prohibited extremist activity that are available within and outside of DOD. For data sources outside of DOD, this included surveying data repositories on radicalization, terrorism, and other sources connected to prohibited extremist activities and behaviors. The team gave extra attention to data sources that included information about the potential involvement in these activities of those with current or previous military experience. For instance, the team examined publicly available, but largely anonymous social media repositories (e.g., Reddit,

Telegram) where extremist ideologies may be present in combination with groups or individuals who self-identify with the military in some way.

Within DOD, the team participated in interviews with senior leaders and subject matter experts. This included discussions and correspondence with individuals who are familiar with many of the data systems used in DOD for tracking disciplinary actions. These discussions focused on exploring how prohibited extremist activities are tracked, policies and practices that have been successful, limitations, and suggestions for future improvement.

The team examined a large set of studies that the DOD has produced on efforts to incorporate publicly available social media information into the security background process. The team also participated in interviews with senior leaders and subject matter experts on this and other technologies that may be pertinent for monitoring electronic content related to prohibited extremist activities.

To identify the relative prevalence of more serious prohibited extremist activities within DOD, the team conducted a search of all publicly available military appellate court opinions issued by the Military Department courts of criminal appeals, as well as the U.S. Court of Appeals for the Armed Forces, from 2011 to 2021. The team also explored the relative prevalence of individuals with and without military experience who were charged in relation to the U.S. Capitol events of 6 January 2021. Given the relative size of the male veteran population, male service member population, population of females with current or prior military experience, the corresponding population sizes for the general populace, and the rates of individuals being charged, this analysis examined the number of individuals from the military populations that would be expected to be charged if individuals with military experience are charged at the same rate as the general population.

B. Common Resources

1. Interviews

The IDA team conducted 57 interviews with senior officials in the DOD and in other federal agencies. Most of these interviews included more than one individual, so the total number of officials interviewed by the IDA team was well in excess of one hundred. Some interviews were conducted in person and others were conducted by video conference or telephone. Interviews took about an hour each and were mostly conducted in the period from July to October 2021. All interviews were conducted on a not-for-attribution basis to ensure free and open discussion; as a result, interviewees are not identified by name or position in this report. Figure 1 identifies the interviewees and the organizations that they represent in a manner consistent with IDA's non-attribution commitment.

	LEADERS/ MISC	PERSONNEL	SECURITY	IT/COMMS	LEGAL	IG/CID	TOTAL
OSD/JS	CEWG J5	IRC CPP DPSO ODEI/DMOC OFR SAPRO	USD(I&S)	CIO JAIC		DODIG	12
DAFAS		OPA MEPCOM PERSEREC TAP MCFP	DCSA				6
ARMY	TRADOC	G-1			JAG	CID	4
NAVY	N2/N6 MCPON Chief of Chaplains	CNP Veterans' Transition		CRMD	JAG	IG NCIS	9
AF/SF	CMSAF	A1 AFPC AFRS AETC			JAG	IG AFOSI	8
USMC	Chief of Chaplains	M&RA MCRC MCTP Marine for Life		Wolverine DASH	JAG		8
NG	ARNG						1
OTHER FED.	VA			START/ARLIS		FBI DHS NTAC Local LE (3) DoJ NSD	9
TOTAL	10	22	2	6	4	13	57

Figure 1. Summary of IDA interviews[6]

[6] Acronyms in table: OSD/JS = Office of the Secretary of Defense and the Joint Staff; DAFAS = Defense Agencies and Field Activities; AF/SF = Air Force and Space Force; USMC = United States Marine Corps; NG = National Guard; CEWG = Secretary's Countering Extremism Working Group; J5 = strategies, plans and policy directorate of the Joint Staff; TRADOC = Army Training and Doctrine Command; N2/N6 = Navy staff office for intelligence and communications; MCPON = Master Chief Petty Officer of the Navy; CMSAF = Chief Master Sergeant of the Air force; ARNG = Army National Guard; VA = Department of Veterans Affairs; IRC = Secretary's Independent Review Commission on sexual assault in the military; CPP = office of Civilian Personnel Policy; DSPO = Defense Suicide Prevention Office; ODEI/DMOC = Office of Diversity, Equity and Inclusion and the Diversity Management Operations Center; OFR = Office of Force Resiliency; SAPRO = Sexual Assault Prevention and Response Office; OPA = Office of People Analytics; MEPCOM = Military Entrance Processing Command; PERSEREC = Defense Personnel and Security Research Center; TAP = Transition Assistance Program; MCFP = office of Military Community and Family Policy; G-1 = Army staff directorate for personnel policy; CNP = Chief of Naval Personnel; A1 = Air Force Staff office for personnel policy; AFPC = Air Force Personnel Center; AFRS = Air Force Recruiting Service; AETC = Air Education and Training Command; M&RA = office of the Assistant Secretary of Defense for Manpower and Reserve Affairs; MCRC = Marine Corps Recruiting Command; MCTP = Army Mission Command Training Program; USD(I&S) = Under Secretary of Defense for Intelligence and Security; DCSA = Defense Counterintelligence and Security Agency; CIO = DOD Chief Information Officer; JAIC = Joint Artificial Intelligence Center; CRMD = Navy Commander's Risk Mitigation Dashboard; Wolverine = Marine Corps court-martial tracking system; START/ARLIS = National Consortium for the Study of Terrorism and Reponses to Terrorism; ARLIS = Applied Research Laboratory for Intelligence and Security; JAG = Judge Advocate General of a military Service; DODIG = Department of Defense Inspector General; CID = Army Criminal Investigative Division; IG = Inspector General of a military department; NCIS = Navy Criminal Investigative Service; AFOSI = Air Force Office of Special Investigations; NTAC = National Threat Assessment Center of the Secret Service; Local LE = State, County, or Municipal Law Enforcement Agency; DoJ NSD = National Security Division of the Department of Justice.

Almost every interview included a set of questions regarding the interviewee's views on the extent to which the Department has a problem with extremist behaviors and activities, and the extent to which prohibitions on such behaviors and activities are well-defined and well-understood in the military community. Other questions varied from interview to interview depending on the position, knowledge, experience, and areas of expertise of the interviewee. Over the course of the interviews, IDA attempted to collect information on the nature and extent of extremist behaviors and activities in the military community, pathways to extremist behaviors and activities, views on policy issues regarding such behaviors and activities, tools for identifying and addressing prohibited extremist activities and related behaviors, and data systems that are or could be used for tracking extremist behaviors and activities.

Common themes arising out of the interviews included:

- Most senior officials believe that the Department lacks a clear definition of extremism ("The first question is what even *is* extremism?");
- Most believe that extremism in the military is very rare ("In 35 years in uniform, I have never met an extremist"), although a few speculate that they may not see all extremist activities;
- A few express the concern that the current effort to address extremism could be perceived as politically-motivated ("a finger in the chest, blaming people and saying what wasn't acceptable");
- Several speculate that individuals who are isolated or unconnected may be vulnerable to extremist recruiting;
- Many believe that extremism is more of a problem for former service members than for those currently serving;
- Some speculate that the guard and reserve may be more vulnerable than active duty service members because of their greater exposure to community influences; and
- Many emphasized the importance of a positive message of shared mission, shared identity, and shared values ("We don't do a good job of teaching civics in school anymore; the military has to make up for that deficiency in its own training").

These issues and other results from the IDA interviews are discussed in more detail in the balance of the report.

2. Site Visits

In addition to interviews, the IDA team conducted site visits at Marine Corps, Navy, Air Force, and Army bases. The intent of the site visits was to speak with members of the force, uniformed and civilian, in geographically dispersed regions regarding how their organizations approach and address the topic of extremist behaviors and activities. These site visits enabled the

IDA team to collect observations regarding leader, subordinate, and peer perceptions of the topic, together with information about prevalence and the extent to which organizational approaches for addressing the topic have been effective. Participants were also asked about how organizational approaches, training, and education could be strengthened.

As with the interviews of senior leaders, all discussions were conducted on a "not for attribution basis;" no names, ranks, or units of participants were documented. IDA coordinated these discussions with service and installation points of contact. Site visits included discussion groups of junior enlisted, junior officer, mid/senior noncommissioned officers, senior officers, and DOD civilians. The vast majority of the civilian research participants were military veterans and retirees, providing an additional lens to the discussions.

Figure 2 shows the composition of the participants in group discussions during IDA's site visits.

	Junior Enlisted	Mid-Senior Enlisted	Junior Officers	Senior Officers	DoD Civilians	Total
Marine Corps Base Camp Lejeune	4	8	8	8	12*	40
Naval Station Norfolk	11	9	9	9	23**	61
Fort Sill	7	10	6	8	7**	38
Kirtland Air Force Base	11	10	8	7	15***	51****
TOTAL	33	37	31	32	57	190

Figure 2. Summary of IDA Site Visits

Note: *Vast majority military Veterans/military Veteran retirees; **Broken into two groups; ***Broken into three groups; ****Additional military attempted to participate via video teleconference

In addition to the individuals who physically appeared for discussions, a number of military members participated or attempted to participate via video teleconferencing from remote locations. While installation bandwidth and technology challenges did not let these members fully participate

like those who participated in-person, comments posted in chat rooms were captured by the IDA research team.

Themes emerging from the site visits were consistent with those from the interviews:

- The lack of a standardized definition of extremist behaviors and activities, with boundaries for what is and is not permissible, was a common theme regardless of rank; many participants saw "intolerance of others' views" as an important element of inappropriate extremist behavior;
- While junior participants appeared tolerant of different views and reluctant to engage in potentially polarizing conversational topics (politics, religion, etc.), more senior participants and civilians were more likely to express their strong views;
- Senior participants felt that extremist behaviors and activities were not as big a problem in the force compared to other challenge areas, including racism, discrimination, and bias;
- According to participants, clear messaging and communication from leadership are critical to the morale of the force; and
- The majority of participants, to include instructors, viewed the stand-down training as ineffective. Many perceived it as unbalanced, and some felt targeted by the training.

Specific information obtained from the site visits are included as appropriate in the discussion of specific issues throughout the report.

This page is intentionally blank.

3. Background

A. Historic Context

The events of the last few years are far from the first encounter that the DOD and its predecessor organizations have had with violent extremist activities in the military community. The American military always reflects the culture and society from which it springs and shares a parallel history of violent extremist events. Much of this history centers on the divisive history of racism in the United States. This section traces some of the most significant episodes of military-connected violent extremism from the beginning of the 20th century to the present. While these events are in no way representative of the behavior and conduct of the millions of Americans who have served with honor in the Armed Forces over the last hundred years, they do demonstrate how the actions of a few can besmirch the image of the many.

After World War I, a number of armed service members and veterans actively participated in violent race riots in dozens of cities such as Charleston, South Carolina; Houston, Texas; New London/Groton, Connecticut; Washington D.C.; and other locations. In many cases, service member and veteran participants engaged in racially-motivated acts of violence, including lynching.[7] Service members organized some of these events, recruiting veterans and members of the public; in other cases, service members and veterans participated in, but did not lead the event.[8] A few key examples provide an idea of the scope of these events:

- In 1917, in Houston, black soldiers played a primary role in planning and carrying out a violent riot which has been described as "aggressive retaliation for treatment which they deemed unpardonable."[9] Following extreme brutality by a white Houston policeman against two black soldiers (one of whom died), approximately 100 armed black soldiers departed their camp, unauthorized, and headed for Houston with the intent to kill the policeman.[10] The riot lasted two hours, leaving fifteen white citizens, among them four

---

7 Mark Ellis, "J. Edgar Hoover and the "Red Summer" of 1919." *Journal of American Studies* 28, no. 1 (1994): 42, https://history.msu.edu/files/2010/04/Mark-Ellis.pdf; John Darrell Sherwood, *Black sailor, White Navy: Racial Unrest in the Fleet During the Vietnam War Era* (New York City, NY: NYU Press, November 2007): 5; David Krugler, "A Mob in Uniform: Soldiers and Civilians in Washington's Red Summer, 1919," *Washington History* 21 (2009): 48-77. https://www.jstor.org/stable/25704908?pq-origsite=360link?pq-origsite=360link.

8 Krugler, "A Mob in Uniform: Soldiers and Civilians in Washington's Red Summer, 1919," 52.

9 Edgar A. Schuler, "Race Riots During and After the First World War," *Negro History Bulletin* 7, no. 7 (1944): 156, http://www.jstor.org/stable/44212138; Robert V. Haynes, "The Houston Mutiny and Riot of 1917," *The Southwestern Historical Quarterly* 76, no. 4 (1973): 435, http://www.jstor.org/stable/30238208.

10 Fred Borch, "The Largest Murder Trial in the History of the United States: The Houston Riots Courts-Martial of 1917," Department of The Army. *The Army Lawyer* (March 2012): 1, https://www.loc.gov/item/75615419_02-2011/.

Houston police officers, dead. Four black soldiers died; the fifth, the alleged leader, was found dead by suicide before he could be apprehended.[11]

- The riot resulted in the "largest court-martial in American military history" followed by "the mass execution of thirteen soldiers at Camp Travis at dawn on 1 December 1917, and by the sentencing of 41 others to life in prison."[12] In a subsequent court-martial, 16 additional soldiers received death sentences and 12 were sentenced to life in prison. President Woodrow Wilson commuted the sentences of ten soldiers from death to life in prison.[13]
- In May 1919, hundreds of white men, including demobilized sailors stationed at Charleston, South Carolina, looted rifles from two indoor shooting ranges and entered the city's predominately black neighborhood. Local police were unable to control the situation that unfolded. The mayor requested that marines from the local Navy Yard be dispatched alongside additional Navy military police reinforcements to quell the violence. The rioting left seven people dead and 93 people severely wounded. Many white service members were arrested. Two white sailors were "tried and acquitted for the manslaughter" of two black citizens, although the Navy court of inquiry found them "guilty of rioting." Both sailors were sentenced to one year in prison.[14]
- For four days in mid-July 1919, in Washington, D.C., several hundred armed white soldiers, sailors, marines and veterans banded together, forming an "all-White, male mob" that stormed the Southwest part of the city, destroying property and attacking black citizens living there.[15] During the riot, at least seven people were killed, more than a dozen were severely wounded, and hundreds were injured. The government mobilized approximately 2,000 service members from nearby bases to quell the violence and gain control of the mob.[16]

---

[11] Borch, "The Largest Murder Trial in the History of the United States: The Houston Riots Courts-Martial of 1917," 1.

[12] Robert V. Haynes, "The Houston Mutiny and Riot of 1917," 438.

[13] Haynes, "The Houston Mutiny and Riot of 1917," 438. A subsequent review by the Acting judge Advocate General, Brigadier General Samuel Ansell, resulted in "General Orders No. 7, promulgated by the War Department on 17 January 1918, which ultimately led to the creation of a "Board of Review with duties" to examine "records of trial in all serious general courts-martial;" this Board of Review formed the legislative foundation "and is the basis for today's Army Court of Criminal Appeals." Borch, "The Largest Murder Trial in the History of the United States: The Houston Riots Courts-Martial of 1917," 3.

[14] Theodore Hemmingway, "Prelude to Change: Black Carolinians in the War Years, 1914-1920." The Journal of Negro History 65, no. 3 (1980): 223, https://www.journals.uchicago.edu/doi/10.2307/2717096; Nick Butler, "The Charleston Riot of 1919," Charleston County Public Library, May 10, 2019, https://www.ccpl.org/charleston-time-machine/charleston-riot-1919#_edn3.

[15] David F. Krugler, "1919: Defending Black Lives," *Washington History* 32, no. 1/2 (Fall 2020): 28, https://www.jstor.org/stable/26947511.

[16] Krugler, "A Mob in Uniform: Soldiers and Civilians in Washington's Red Summer, 1919," 49.

During the World War II era, the United States experienced a smaller wave of race riots, with white and African-American service members playing an active role. Again, specific examples provide an idea of the role played by the military community:

- The 1935 Harlem race riot was sparked by the death of an black soldier who was shot and killed by a white police officer after the soldier tried to intervene in the arrest of an black woman accused of disturbing the peace. As with earlier riots, service members and veterans who were involved engaged in racially-motivated acts of violence.[17]
- In the 1943 Zoot Suit Riots[18] in Los Angeles, a sailor was beaten in a fight between white service members and Mexican American youth. A few days later, approximately 50 sailors from the nearby U.S. Naval Reserve Armory, armed with clubs and similar weapons, attacked anyone wearing a zoot suit. Over the following days, mobs of service members and military personnel from Southern California joined those stationed in Los Angeles to engage in attacks in which Hispanic men were beaten and stripped of their suits. The riots died down nine days after they began, when service members and military personnel were barred from leaving their barracks.
- In 1944, at Fort Lawton, in Seattle, Washington, between 50 and 100 armed black soldiers departed their housing area and entered barracks that housed Italian prisoners of war (POWs). After a period of fighting, Military Police arrived, ordered the black soldiers back to their barracks, and then transported injured soldiers and POWs to the infirmary.[19] Following an investigation by the Army's Inspector General, 43 black soldiers were charged with rioting and tried by court martial in which 28 were convicted. In 2007, the Army's Board of Corrections of Military Records "found the trial, held in the segregated Army of the time, was 'fundamentally unfair' to the African-American soldiers." The Army subsequently overturned the convictions of the 28 court-martialed soldiers, only two of whom were still living at that time.[20]

The military's ongoing racism problem was also evident when the body of a black private was found hanging from a tree in a wooded area at Fort Benning, Georgia, in 1941. Despite evidence that the private's hands and legs had been bound behind him, authorities on post asserted

---

17 John A. Williams, "The Long Hot Summers of Yesteryear," *The History Teacher* 1, no. 3 (March 1968): 19-20. http://users.clas.ufl.edu/davidson/HistArch/Week%2014/williams%201968.pdf.

18 Zoot suits were popular among young minorities during that time, thus the name. Eduardo Obregón Pagán, "Los Angeles Geopolitics and the Zoot Suit Riot, 1943," *Social Science History* 24, no. 1 (2000): 223-256, https://www.cambridge.org/core/journals/social-science-history/article/abs/los-angeles-geopolitics-and-the-zoot-suit-riot-1943/88C78F0516856B0B8157585685882E06; John J. Chiodo, "The Zoot Suit Riots: Exploring Social Issues in American History," *The Social Studies* 104, no. 1 (2013): 3, doi:10.1080/00377996.2011.642421.

19 Beth Kraig, "The Unquiet Death of Guglielmo Olivotto," *Peace & Change* 30, no. 3 (July 2005): 303, doi:10.1111/j.1468-0130.2005.00322.

20 Jonathan Martin, "U.S. Army Overturns Convictions of Fort Lawton Soldiers Court-Martialed in 1944 After Riot, Lynching," *Seattle Times*, October 26, 2007, https://www.seattletimes.com/seattle-news/us-army-overturns-convictions-of-fort-lawton-soldiers-court-martialed-in-1944-after-riot-lynching/.

that the death was a suicide.[21] A Fort Benning doctor ruled otherwise, determining that the death was a homicide. Even though an FBI investigation confirmed the doctor's findings and identified suspects, no prosecution took place. In July 2021, the Army erected a historic marker near where the soldier was last seen on Fort Benning.[22]

During the Vietnam War era, the military was not free of the wide-range of protests—anti-war, anti-draft, anti-service—that divided American society. Vietnam was the first major conflict in which black service members served in fully integrated units, and the first conflict after the civil rights movement.[23] Once again, racial tensions were evident in the ranks both during and after the war. Several major incidents took place in Vietnam:

- In 1967, Staff Sergeant Clide Brown found a burning cross outside his tent after he was featured on the cover of *Time* magazine for a story on "The Negro in Vietnam."[24]
- After the 1968 assassination of Dr. Martin Luther King Jr., some white service members stationed in Vietnam openly celebrated the death. Witnesses reported that they saw service members parading around in "makeshift Ku Klux Klan robes," burning crosses at an American Air Force base in Cam Ranh Bay, and flying the Confederate flag over the military facilities headquarters buildings in Da Nang.[25] Morale problems related to these racial tensions, as well as drug use, resulted in an increase in incidents of fragging (that is, deliberately killing fellow soldiers).[26]

Other events took place in the United States in the years after the end of the war. For example:

- In 1976 at Camp Pendleton, white marines regularly held KKK meetings on base, openly held membership in the KKK, and possessed unauthorized weapons and literature. Black marines complained to their leadership regarding abusive treatment,

---

21 Ronald C. Griffin, "A Black Perspective of the Military," *Negro History Bulletin* 36, no. 6 (October 1973): 135, https://www.jstor.org/stable/44175572?seq=1.

22 Laura James, "Army Unveils Memorial to a Black Soldier Lynched on Military Base 80 Years Ago," *CNN*, August 4, 2021, https://www.cnn.com/2021/08/03/us/felix-hall-soldier-lynched-memorial-fort-benning/index.html.

23 In July 1948, President Harry S. Truman issued an "executive order banning segregation in the Armed Forces." "Executive Order 9981: Desegregation of the Armed Forces (1948)" *National Archives Milestone Documents*, https://www.archives.gov/milestone-documents/executive-order-9981. Despite the issuance of that Executive Order, "many units remained segregated until late 1954." Gerald F. Goodman, "Black and White in Vietnam," *The New York Times*, July 18, 2017, https://www.nytimes.com/2017/07/18/opinion/racism-vietnam-war.html.

24 Terry Wallace, "Bringing the War Home," *The Black Scholar* 2, no. 3 (November 1970): 11, https://www.jstor.org/stable/41202864.

25 The author of this article "spent more than two years in Vietnam as a correspondent for *Time* magazine," during which time he conducted surveys of 833 service members stationed there, as well as interviews with hundreds of survey respondents, both black and white (p. 7). Wallace Terry, "Bringing the War Home," *The Black Scholar* 2, no. 3 (November 1970): 11, http://www.jstor.org/stable/41202864; James E. Westheider, *Fighting on Two Fronts: African Americans and the Vietnam War* (New York City, NY: NYU Press, 1997): 5, 68, 83.

26 George Lepre, *Fragging: Why U.S. Soldiers Assaulted Their Officers in Vietnam* (Lubbock, TX: Texas Tech University Press, 2011): 100-112.

receiving no recourse. On 13 November 1976, black marines engaged in a "bloody racial assault" to seek justice.[27]

- In 1979, white sailors openly wearing KKK robes on the U.S.S. Independence sparked multiple incidents of racial violence.[28]

Over the next decade, similar events took place at Camp LeJeune, Fort Bragg, Fort Benning, Fort Monroe, and other bases.[29] In these incidents, there was evidence of white supremacism—such as pictures of uniformed Soldiers holding KKK signs with racist and anti-Semitic messaging—and racial violence followed.[30]

Over the last thirty years, the military leadership has consistently emphasized that racism in the ranks will not be tolerated. During this period, the number and scope of violent racial incidents in the military has dropped significantly, but isolated incidents continue to pop up. For example:

- In 1993, in Anchorage, Alaska, a senior enlisted white soldier at Fort Richardson directed a mock hanging of a subordinate, the only black "in their 15-member explosives unit." The white soldier was both demoted and fined for his role in organizing and executing the mock lynching.[31]
- In 1995, white soldiers stationed at Fort Bragg killed two black private citizens in Fayetteville, North Carolina. Two of the soldiers were sentenced to life in prison. Another 19 Soldiers were discharged for engaging in extremist, neo-Nazi activities. Police found Nazi paraphernalia, as well as written materials regarding bomb-making in the primary accomplice's off-base apartment.[32]

Over the same period, a handful of individuals with military connections, generally Veterans rather than active service members, engaged in violent extremist activity of other kinds. For example:

---

27 Everett R. Holles, "Marines in Klan Openly Abused Blacks at Pendleton, Panel Hears," *The New York Times*, January 9, 1977, https://www.nytimes.com/1977/01/09/archives/marines-in-klan-openly-abused-blacks-at-pendleton-panel-hears.html?searchResultPosition=1.

28 Blaine Harden, "Sailors Wearing Sheets Create Racial Incident Aboard Aircraft Carrier," *The Washington Post*, September 6, 1979, https://www.washingtonpost.com/archive/local/1979/09/06/sailors-wearing-sheets-create-racial-incident-aboard-aircraft-carrier/cbc97c28-ff49-4221-9fbb-ffd1977905f7/.

29 William E. Schmidt, "Soldiers Said to Attend Klan-Related Activities," *The New York Times*, April 15, 1986, https://www.nytimes.com/1986/04/15/us/soldiers-said-to-attend-klan-related-activities.html.

30 Dave Philipps, "White Supremacism in the U.S. Military, Explained," *The New York Times*, February 27, 2019, https://www.nytimes.com/2019/02/27/us/military-white-nationalists-extremists.html.

31 T.A. Badger, "Soldier Punished for Racial Incident at Army Base," *The Associated Press*, April 6, 1993, https://apnews.com/article/84b02b8c599f783fce1185f851d13c72.

32 William Branigan and Dana Priest, "3 White Soldiers Held in Slaying of Black Couple," *The Washington Post*, December 9, 1995, https://www.washingtonpost.com/archive/politics/1995/12/09/3-white-soldiers-held-in-slaying-of-black-couple/1f11ca9f-9fe2-4e28-a637-a635007deeaf/.

- In April 1995, Timothy McVeigh, an Army combat veteran turned anti-government extremist, parked a rented truck filled with homemade explosives outside of the Alfred P. Murrah Federal Building in Oklahoma City, Oklahoma. The ensuing explosion killed 168 people—among the deceased were 16 children. Many hundreds of individuals were injured. McVeigh had associations with the National Alliance, an extremist, Neo-Nazi organization.[33]
- Following a series of bombings from 1996 to 1998, Eric Rudolph, an Army veteran discharged after two years of service for marijuana use, was placed on the FBI's list of Ten Most Wanted Fugitives. Rudolph's targets included the 1996 Olympic Summer Games in Atlanta's Centennial Olympic Park; an abortion clinic in Atlanta in January 1997; an Atlanta lesbian bar, the Otherside Lounge; and in 1998, the New Woman All Women Health Care in Birmingham, Alabama. Rudolph was captured, tried, and sentenced to multiple consecutive life terms.[34]
- In March 2003, Army Sergeant Hasan K. Akbar was arrested for attacking service members from the brigade command section of the 101st Airborne Division of Camp Pennsylvania in Kuwait "using stolen grenades and a rifle, because he was concerned that troops would kill Muslims in Iraq." Akbar was convicted of killing two service members and wounding fourteen others. He was sentenced to death by a court-martial.[35]
- On 5 November 2009, Army psychiatrist Major Nidal Hasan entered the Soldier Readiness Processing Center on Fort Hood, Texas, armed with two weapons and "20-30 magazines, each containing around 20 bullets." Hasan shouted "Allahu akbar" and began shooting. The duration of the attack was just under 30 minutes. Hasan killed 13 people and wounded 32 others; most of the casualties were soldiers.[36] In 2013, a military jury convicted him of 13 counts of murder and 32 counts of attempted murder. He was subsequently sentenced to death.[37]
- During the Unite the Right rally in Charlottesville in August 2017, Marine Corps Lance Corporal Vasillios Pistolis, a member of Atomwaffen Division, a Neo-Nazi group, was

---

33 "Oklahoma City Bombing," FBI.gov Website, accessed June 16, 2022, https://www.fbi.gov/history/famous-cases/oklahoma-city-bombing.

34 History.com Editors, "Olympic Park Bomber Eric Rudolph Agrees to Plead Guilty," History.com, last updated April 8, 2022, https://www.history.com/this-day-in-history/olympic-park-bomber-eric-rudolph-agrees-to-plead-guilty.

35 The Associated Press, "Soldier Convicted in Deadly Attack on His Camp," *The New York Times*, April 22, 2005, https://www.nytimes.com/2005/04/22/us/soldier-convicted-in-deadly-attack-on-his-camp.html.

36 Katherine Poppe, *Nidal Hasan: A Case Study in Lone-Actor Terrorism* (Washington, DC: George Washington University, Program on Extremism, October 2018): 2, https://extremism.gwu.edu/sites/g/files/zaxdzs2191/f/Nidal%20Hasan.pdf.

37 History.com Editors, "Army Major Kills 13 People in Fort Hood Shooting Spree," History.com, last updated November 2, 2021, https://www.history.com/this-day-in-history/army-major-kills-13-people-in-fort-hood-shooting-spree.

photographed clubbing a man with a wooden flagpole.[38] On the day of the event, Pistolis bragged on social media that he "cracked 3 skulls open with virtually no damage to myself." He was subsequently discharged from the Marine Corps and convicted on charges of "disobeying orders and making false statements."[39]

- In early 2021, Private First Class Cole Bridges was charged with "attempting to provide materiel support to a designated foreign terrorist organization and attempting to murder service members." Specifically, he was charged with plotting "to blow up New York City's 9/11 Memorial and provide the Islamic State group with tactics and information for killing U.S. service members overseas." Bridges reportedly engaged in communications with a covert operative, who was actually an FBI agent and exposed his plans.[40]

These events do not show that the military has a unique problem with violent extremism; rather, they appear to show that the military reflects the pressures and divisions in American society. From the virulent racism of the early 20th century to the deeply divisive period during and after the Vietnam War, to the "lone wolf" terrorists and extremists of more recent times, trends in the military reflect changes in social and political norms, and cultural and demographic shifts in American society as a whole. Nonetheless, this history shows that the military community, like the nation as a whole, must continue to work hard to live up to its high ideals.

B. Prevalence

Anecdotal accounts of military participation in violent extremist events, like those described in the previous section, draw public attention and may create the impression that the military community as a whole has "an extremism problem." Such accounts magnify the actions of a few and provide little information on the overall scope of the problem. Moreover, these accounts frequently fail to differentiate between those who are currently serving in the military and those who have left the military (often many years earlier) or have been removed from the military for cause with less than honorable discharges. An assessment of the actual prevalence of prohibited extremist activities in the Department and the military community requires data, which can be difficult to come by.

---

[38] Shawn Snow, "Marine with Alleged Neo-Nazi Connections Booted from the Marine Corps" *Marine Corps Times*, August 1, 2018, https://www.marinecorpstimes.com/news/your-marine-corps/2018/08/01/marine-with-alleged-neo-nazi-connections-booted-from-the-marine-corps/.

[39] A. C. Thompson and Ali Winston, "U.S. Marine to be Imprisoned Over Involvement with Hate Groups," *Frontline*, June 20, 2018, https://www.pbs.org/wgbh/frontline/article/u-s-marine-to-be-imprisoned-over-involvement-with-hate-groups/.

[40] Harm Venhuizen, "US Soldier Arrested for Planning Attacks on NYC 9/11 Memorial and Troops Overseas," *ArmyTimes*, January 19, 2021, https://www.armytimes.com/news/your-army/2021/01/19/us-soldier-arrested-in-plot-to-blow-up-nyc-911-memorial/.

Senior DOD military and civilian leaders interviewed by the IDA team generally expressed the view that extremist activities are extremely rare in the Department. One leader told IDA, ". . . 35 years in uniform, I have never met an extremist." A second stated, "I have seen immature, inappropriate behavior that needs to be corrected, but nothing that would be considered extremist." A third noted the lack of data, stating, "We don't think this is wide-spread, but . . . we don't know if we have complete comprehension."

Service members and civilians of all ranks generally reflected these views during IDA's site visits with most saying that they had never seen evidence of prohibited extremist activities. Several white service members were aware of incidents in which individuals had displayed swastikas (and appropriate disciplinary action had been taken). One black service member reported having received a death threat after President Obama was elected. Other members of racial and ethnic minority groups stated that they had experienced or observed instances of racism or discrimination but hesitated to describe this conduct as "extremist." "It seems like we are trying to create a divide with this issue," one participant told the IDA team. "It's not very useful to spend our time talking about a topic that is so far under the radar."

Although interviews and site visits appeared to show that extremist activities in the military are infrequent, these discussions were largely focused on active duty service members and currently employed DOD civilians. Several senior leaders cautioned that national guard and reserve members may be both more vulnerable to extremist radicalization and more difficult to monitor. Because members of these components spend more time away from their units, they may require more time to become fully acculturated to DOD values. Additionally, norms for acceptable behavior vary by region, which could make it difficult to implement uniform standards of behavior across the country. Many of these factors also apply to veterans, who live and work in communities around the country and are likely to reflect local values.

Any degree of participation in prohibited extremist activities by those are serving or have served in the military can be problematic. The CEAWG stated in its December 2021 report that "even a small number of cases can pose a significant problem, challenging safety and unit cohesion."[41] However, to the extent the military community is a microcosm of society, it is pertinent to consider whether individuals with military experience participate in prohibited extremist activities at a higher or lower rate than the general U.S. population.

In an effort to shed light on the prevalence of prohibited extremist activities in the military, IDA reviewed available data from both DOD and non-DOD sources. While available data are limited, they generally appear to confirm the view of senior leaders that violent extremism in the military remains relatively rare, and is not disproportionate to rates of violent extremism in the

[41] DOD, *Report on Countering Extremist Activity Within the Department of Defense*, (Washington, DC: Department of Defense, December 2021): 8, https://media.defense.gov/2021/Dec/20/2002912573/-1/-1/0/REPORT-ON-COUNTERING-EXTREMIST-ACTIVITY-WITHIN-THE-DEPARTMENT-OF-DEFENSE.PDF.

population as a whole. Notably, while this data provided some information on extremist activities by service members and by veterans, IDA was unable to identify any data on extremist activities by DOD civilians or contractors. IDA notes that the absence of data does not mean the absence of prohibited conduct, only that to the extent that such conduct has taken place, if at all, it has not been well documented.

1. Information on the Prevalence of Extremism from DOD Data Systems

DOD's capability to track incidents of prohibited extremist activities involving service members has improved in recent years. Each of the Military Departments maintains multiple data systems to track disciplinary infractions committed by service members. As described in Chapter 8 of this report, many of these systems have implemented flagging protocols to specifically identify cases of prohibited extremist activity. While there remains a need to standardize reporting practices across systems and organizations to ensure that the cases being flagged in each system meet the same definition of prohibited extremist activities, these systems now provide useful information on the number of disciplinary actions based on prohibited extremist activities.

IDA's review revealed that a relatively small number of such cases appear to have been flagged to date. The Marine Corps' system for equal opportunity cases, the first to start flagging potential extremism cases, has reportedly identified 28 cases involving "dissident and protest activities" since 2018, of which 17 have been substantiated. The flagging system of the Naval Criminal Investigative Service (NCIS) has reportedly identified incidents in the "low dozens" since it started flagging cases in 2019. The case tracking system of the Navy and Marine Corps Judge Advocate General and Staff Judge Advocate to the Commandant has reportedly identified 11 cases since March 2021. A comparable flagging system established by the Air Force at about the same time had reportedly identified only three cases at the time that IDA completed its field work. Overall, IDA determined that even with the fairly broad definitions used by some of the flagging systems, there appeared to be fewer than 100 substantiated cases per year of extremist activity by members of the military in recent years.

These low numbers are generally consistent with a report compiled by the Inspector General of the Department of Defense (DOD IG) at the end of 2021, which identified 92 documented cases of extremist and gang activities between 1 January and 30 September 2021 that were substantiated and subject to official action.[42] The DOD IG report states:

> The Military Departments reported a total of 294 allegations, 281 investigations and inquiries, 92 instances where action was taken, zero instances where no action was taken, and 83 referrals to civilian law enforcement agencies . . .. The Military

[42] DoD OIG, *Department of Defense Progress on Implementing Fiscal Year 2021 NDAA Section 554 Requirements Involving Prohibited Activities of Covered Armed Forces* (Washington, DC: DoD OIG, December 1, 2021), https://media.defense.gov/2021/Dec/02/2002902153/-1/-1/1/DoDIG-2022-042.PDF.

> Departments also reported incidents of criminal gang activity involving military members [and those incidents are included in these numbers].[43]

Nearly all of these cases were addressed through administrative action, non-judicial punishment, or referral to command for appropriate action, indicating that likely, most of the violations were relatively minor infractions. Based on IDA's interviews with senior leaders and military lawyers, it appears likely that the vast majority of prohibited extremist activity cases centered on the display of extremist or gang symbols, offensive speech, and/or connections with inappropriate organizations. Few, if any of those cases, included evidence of violent action or plans for violent action.

The DOD OIG report noted many shortcomings in the Department's data collection systems and processes. For example:

- "We found that data collection across the Military Departments is inconsistent."[44]
- "The Military Departments reported issues with compiling and validating their data and, in some cases, the reported numbers were conflicting."[45]
- "We did not independently verify the reliability of the data from each Department."[46]
- "The Secretary of Defense "has not yet established or implemented standard policies to report and track prohibited activities, including supremacist and extremist activity."[47]

Since the practice of explicitly flagging cases involving prohibited extremist activities is in its infancy and has yet to be standardized, IDA sought to perform an independent check on the scale of prohibited extremist activities in the Department by reviewing court-martial opinions. Since court-martial opinions from each service's Court of Criminal Appeals are typically archived, searchable, and available to the public, these documents provide a unique window into the prevalence of prohibited extremist activities over a longer time horizon. The IDA team conducted an analysis of more than ten years of publicly-facing court-martial opinions and identified those that included key words suggesting that a particular case involved prohibited extremist activities.

The path from an offense to a court-martial opinion often begins when an allegation is brought to the attention of a military criminal investigative organization (MCIO). The organization then investigates to determine whether the report is founded or unfounded, and whether the case involves a criminal violation (or at least credible evidence of one). Non-criminal violations of military policy are typically referred to commanders for further action. Criminal violations are passed to the servicing military justice office, where the accused service member may be tried by

---

[43] Ibid, 5–6.

[44] Ibid, 4.

[45] Ibid, 6.

[46] Ibid.

[47] Ibid, 4.

court-martial. The trial may result in an acquittal, a minor sentence, or a major sentence. All cases involving a major sentence are automatically reviewed by the service's Court of Criminal Appeals and appeals from some less severe sentences are also reviewed by this court. It is at this stage that a military appellate court opinion is produced. The U.S. Court of Appeals for the Armed Forces is the next highest level of appeal from the decisions of all services' Courts of Criminal Appeals, and we likewise include the opinions issued by this court in our analysis.

There are several limitations to this approach. First, minor offenses and cases that are resolved through plea agreements are unlikely to result in military appellate court opinions; hence, there are a significant number of courts-martial excluded from our analysis. Second, the Uniform Code of Military Justice (UCMJ) does not include a separate offense for "extremism." Violations of DOD or Military Department and service extremism regulations may be prosecuted under Article 92 of the UCMJ for "Failure to obey order or regulation." However, not all Article 92 cases are extremism cases, and not all extremism cases are prosecuted under Article 92. Extremist behaviors may also be charged as a violation of the article of the UCMJ reflective of the underlying conduct (e.g., "Assault" (Article 128); "Communicating Threats" (Article 115)). The IDA analysis depends on the issuance of written opinions by the military appellate courts and on the use of terms in those opinions that take note of some aspect of prohibited extremist behavior. Finally, there is a lag in the data, as there may be a lapse of one or more years between a prohibited action and the publication of an opinion by a military appellate court.

The IDA team identified 6,315 military appellate court opinions that were published between 1 January 2011, and 31 December 2021, of which 5,803 were machine readable. Of the 5,803 machine-readable opinions, 78 (approximately 1.3%) included at least one keyword signifying possible extremist or gang activity.[48] After manual review, IDA determined that 17 of these 78 opinions (approximately 0.3% of the total number of opinions) involved a prohibited extremist or gang activity.[49] Of these, seven involved gang activity, and only ten involved prohibited extremist activity—a rate of about one case per year. Figure 3 reflects the distribution of opinions by court and year and shows no clear increase or decrease in the number of cases over time. The larger number of cases in 2014 and 2017 is partially attributable to the identification of multiple service members' involvements in the same extremist organization or criminal gang.

[48] The methodology used in this review, including the keywords selected to signify possible extremist or gang activity, are described in Appendix C.

[49] The remaining 61 cases identified in the initial keyword search were determined to not represent instances of extremist activity. Six involved the use of racial slurs without further advocacy for widespread unlawful discrimination, which does not alone appear to constitute an extremist activity in violation of DoDI 1325.06. Another six opinions were duplicates of opinions that were previously considered. The remaining 49 included the triggering word in a different context (such as quotes from previous trials, references to the 9/11 terrorist attacks, or determinations that the appellant was not a member of a criminal gang).

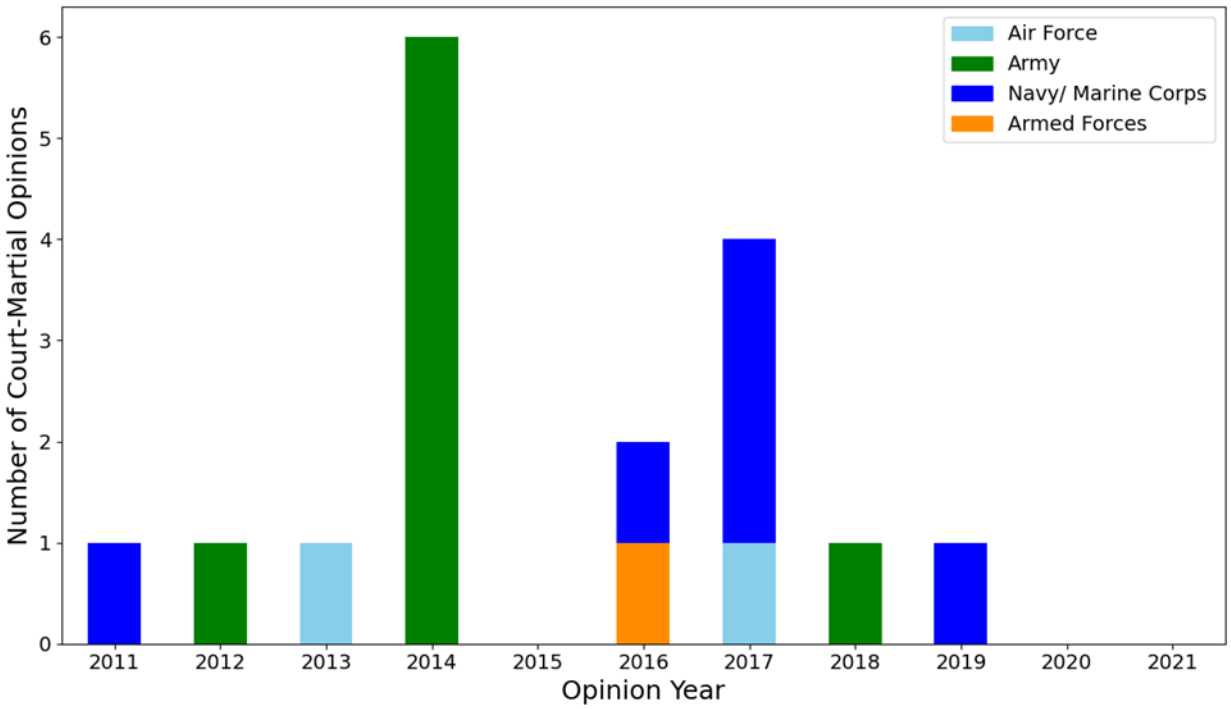


Figure 3. Written Court Martial Opinions per year including Evidence of Prohibited Gang and Extremist Activities

Table 1 presents more detailed information about the identified extremism and gang-related cases. The cases reflect a broad range of offenses, including several types of extremist activities that are prohibited by DODI 1325.06.[50]

[50] For three of the 17 opinions, the only arguable violation of DoDI 1325.06 is paragraph 8.c.1.e, which includes "advocating or encouraging military, civilian, or contractor personnel … to violate the laws of the United States … or to disobey lawful orders or regulations, for the purpose of disrupting military activities (e.g., subversion), or personally undertaking the same." The keywords used in the IDA search are inadequate to recover the breath of possible activities that could fall under this definition. These three opinions happen to contain one or more of the keywords, but these opinions should not be interpreted as an exhaustive search for subversion and related activities. Each of these three opinions involves an individual "personally undertaking" an effort to disrupt military activities (rather than "advocating or encouraging" others).

Table 1. Court-Martial Opinions Involving Prohibited Extremist or Gang Activities

Court of Appeals	Case Number	Opinion Date	Connection to Prohibited Extremist or Gang Activities	DoDI 1325.06, Encl. 3 violation
Air Force	38864	2017-07-06	Formed a “Crips” gang in Minot, North Dakota	10.b
Air Force	37528	2013-01-29	Participated in a gang initiation ritual that resulted in the death of the new initiate	10.b
Army	20130739	2018-05-31	Released classified documents to Wikileaks	8.c.1.e[51]
Army	20130451	2014-06-02	Member of extremist organization ("20th Infantry") in El Paso, Texas	8.c.1.a-b, d, f, 8.c.2.a, h
Army	20090166	2014-05-29	Participated in a gang initiation	10.b
Army	20130419	2014-05-19	Member of extremist organization ("20th Infantry") in El Paso, Texas	8.c.1.a-b, d, f, 8.c.2.a, d, h
Army	20110986	2014-05-02	Found guilty of "wrongfully participating in an extremist organization"[52]	8.c.1.d
Army	20130523	2014-04-30	Member & leader of extremist organization ("20th Infantry") in El Paso, Texas	8.c.1.a-b, d, f 8.c.2.a, d, f, h
Army	20110975	2014-03-31	Advocated mutiny, participated in a group advocating overthrow of U.S. government	8.c.1.d-e, 8.c.2.a, d, f
Army	20050514	2012-07-13	Intentionally killed and injured members of his brigade while deployed	8.c.1.e[53]
Navy/ Marine Corps	201800071	2019-06-19	“Targeted and abused three Muslim recruits from three separate platoons"	8.c.1.b
Navy/ Marine Corps	201500400	2017-06-06	Member of a criminal motorcycle gang	10.b
Navy/ Marine Corps	201500415	2017-04-27	Member of a criminal motorcycle gang; participated in a violent assault of a Marine	10.b
Navy/ Marine Corps	201600375	2017-03-17	Member of a criminal motorcycle gang; participated in a violent assault of a Marine	10.b
Navy/ Marine Corps	201500381	2016-11-15	Intended to build a bomb to cripple or damage his ship	8.c.1.e
Navy/ Marine Corps	201100187	2011-11-29	Sold weapons to gang members	10.b
Armed Forces	15-0476	2016-03-18	Threatened the U.S. President	8.c.1.d

[51] Subversion is included as an extremist activity in 8.c.1.e, and this case reflects conduct that is arguably a form of subversion. Subversion is defined in DoDI 1325.06 as “Actions designed to undermine the military, economic, psychological, or political strength or morale of a governing authority.”

[52] This opinion finds that the organization did not meet the criteria to be considered an extremist group. However, its purpose was to “defend the constitution by force if necessary, in case the government became corrupt.”

[53] Included herein as an act of subversion (the appellant conducted a lethal attack on his brigade’s leadership).

Overall, this analysis demonstrates that the prevalence of extremist and gang-related activity that are reflected in court-martial opinions is limited to fewer than 20 cases over since 2012. The identified cases represent a wide range of prohibited extremist and criminal gang activity. If gang cases are excluded, the total number of extremist cases amounts to just one case per year over the period studied. The extremely low number of published court-martial cases involving prohibited extremist activities appears consistent in overall scale with the relatively low number of cases tracked in DOD criminal and investigative data systems.

Although this analysis was conducted as comprehensively as possible, there are some limitations. First, as previously stated, this analysis only focuses on military appellate court opinions and thus excludes all incidents that were addressed by other than court-martial (such as at the command level or by adverse administrative action). Second, not all courts-martial are the subject of a military appellate court opinion. Third, the manual review of opinions may have excluded some opinions that should have been included or vice versa. Finally, as is the case with all keyword searches, it is possible that some cases did have a nexus to prohibited extremist activities and conduct but did not contain one of the keywords used in the initial screening.

2. Prevalence Information from External Data Systems

Although the DOD data provides some measure of the scale of prohibited extremist activity within the Department, it provides no information at all on extremist activity in the larger military community (including veterans, civilian employees, and contractors) and no basis for assessing whether levels of activity in this community are proportionate or disproportionate to levels of activity in the population as a whole.

In this regard, it is important to keep in mind that DOD tracking systems include a range of activities that would not be prohibited if committed by civilians. For instance, military members are prohibited from knowingly displaying "paraphernalia, words, or symbols in support of extremist activities," including "flags, clothing, tattoos, and bumper stickers, whether on or off a military installation." [54] Outside of the military, such actions are protected by the First Amendment and are not prohibited. This is a pertinent distinction when considering the DOD's reported numbers of prohibited extremist actions involving service members because there is not necessarily a clear civilian benchmark with which to compare them.

Law enforcement officials responsible for monitoring incidents of domestic violent extremism told the IDA team that the rate at which individuals with military connections participate in such incidents appears to be roughly proportionate to the percentage of individuals in society as a whole. However, these officials also indicated that the rate of participation by individuals with military connections in incidents of domestic violent extremism appears to have

[54] DOD, "Handling Protest, Extremist, and Criminal Gang Activities Among Members of the Armed Forces," DODI 1325.06.

been increasing in recent years, perhaps even doubling from about five percent of all incidents to about ten percent of such incidents.

IDA did not have access to law enforcement databases and could not independently identify these trends. However, IDA was able to examine several databases external to DOD, including data and reports collected in the Profiles of Individual Radicalization in the United States (PIRUS) database maintained by the National Consortium for the Study of Terrorism and Responses to Terrorism (START). These data and reports generally appear to confirm that both participation rates of service members in violent extremist activities are not disproportionate to overall participation rates in the nation as a whole, and that participation rates for former service members appear to be growing.

A challenge in comparing participation rates between those with and without military experience comes down to a lack of data. Data on isolated incidents can provide meaningful insights and case studies, but unless data are tracked more systematically, it is challenging to say anything about participation rates. An ideal data source would be a comprehensive collection of all incidents of a defined set of prohibited extremist activities within the U.S. over a specified period of time. Such an ideal data set would track all incidents, whether or not the offender had military experience. For those who do have military experience, it would ideally track the amount and type of military experience that each offender had and how relevant that experience was in the incident.[55] Such a data set does not exist at present.

In the absence of comprehensive data, a representative sample of incidents of a given type, occurring in a particular location and time, would be sufficient to identify participation rates for those with and without military experience. This too is challenging. Perhaps the best effort to date is the PIRUS dataset. Its curators have made "every effort . . . to maximize the representativeness of the data using random sampling techniques."[56] However, they also note that their data may not be representative due to factors outside their control. The PIRUS data are based on publicly available sources, and to the extent that these sources are not representative, the data will not be representative. For example, the representativeness of the PIRUS sample can be impacted by the types of extremist activities that attract news media attention at a given point in time (e.g., Islamist extremism in the wake of 9/11), and the availability of digital historical sources that can be searched (which can result in "a disproportionate number of more recent cases").[57]

---

[55] Military training may increase the potential damage, risk, or lethality associated with some more violent forms of prohibited extremist activities. However, military training and experience may not give the offender any special advantage in other less violent forms of prohibited extremist activities, such as advocacy and cyberspace activities.

[56] See "PIRUS - Frequently Asked Questions," "Is the PIRUS dataset a *representative* sample of individuals radicalized in the United States?" National Consortium for the Study of Terrorism and Responses to Terrorism Website, accessed June 16, 2022, https://www.start.umd.edu/pirus-frequently-asked-questions#q12.

[57] Ibid.

A factor further complicating an examination of the relative prevalence of prohibited extremist activities among those with military experience is that the composition of the U.S. population with military experience has shifted dramatically in recent years. In 1990, 30 percent of adult males in the U.S. were veterans. This dropped to 25 percent in 2000. By 2010, the number had dropped to 18 percent, and was down further to 13 percent in 2018.[58] This changing composition makes it difficult to identify a reasonable comparison population. PIRUS, for instance, has collected data on prohibited extremist activities for individuals with military experience going back to at least 1990. If these data were determined to be adequately representative of prohibited extremist activities over such a longitudinal period—both for those with and without military experience—then a comparison of participation rates would need to account for the changing composition of those with military experience.

The PIRUS database includes information on 2,226 de-identified individuals who were radicalized "to the point of violent or nonviolent ideologically motivated criminal activity, or ideologically motivated association with a foreign or domestic extremist organization" in the United States from 1948 to 2018.[59] Following Secretary Austin's 5 February 2021, memorandum on prohibited extremist activities in DOD, researchers at START investigated the incidents of individuals in PIRUS with a military background. The resulting brief, "Extremism in the Ranks and After," was first released in July 2021, with the most recent update in December 2021, looking at all individuals in PIRUS with military ties from 1990 through 2021.[60] The brief explores both past extremists with military backgrounds and the specifics of all individuals known to have military service and connected to the 6 January 2021, breach of the U.S. Capitol.

As of the December 2021 update, there are 458 individuals in PIRUS with military ties who committed criminal acts of an extremism from 1990 through 2021. 118 of these persons are associated with the Capitol breach. The vast majority of the military-connected individuals (383, or 83.6 percent) were no longer serving in the military when arrested.[61] Nearly three-quarters (73 percent) had been separated from the military for six years or more, and almost two-fifths (38 percent) had been separated for 15 years or more at the time of their arrest. Roughly 13 percent of those who committed an extremist crime after leaving the military had received an "other than

---

58 See p. 5 of Jonathan Vespa, *Those Who Served: America's Veterans from World War II to the War on Terror*, Washington, DC: U.S. Census Bureau, Department of Commerce, June 2020, https://www.census.gov/content/dam/Census/library/publications/2020/demo/acs-43.pdf.

59 START also maintains and curates more recent data, but the publicly released database is only updated through 2018. ("PIRUS – Frequently Asked Questions, What is PIRUS?" National Consortium for the Study of Terrorism and Responses to Terrorism (START) Website, accessed June 16, 2022, https://www.start.umd.edu/pirus-frequently-asked-questions#q12).

60 Michael Jensen, Elizabeth Yates, and Sheehan Kane. *Extremism in the Ranks and After* (College Park, MD: National Consortium for the Study of Terrorism and Responses to Terrorism (START), July 2021), https://www.start.umd.edu/news/start-releases-new-data-extremism-among-us-service-members-and-veterans.

61 Michael Jensen, Elizabeth Yates, Sheehan Kane, *Extremism in the Ranks and After* (College Park, MD: National Consortium for the Study of Terrorism and Responses to Terrorism (START), December 2021), https://www.start.umd.edu/publication/extremism-ranks-and-after.

honorable, bad conduct, or dishonorable discharge"—a rate that is four times higher than the roughly 3 percent of all service members who receive such a discharge characterization.[62]

According to the report, the rates of military service among extremists in the PIRUS database are roughly comparable to the rates of military service in the public, with 8.3 percent of PIRUS subjects in 2018 having served in the military, while 7 percent of adults in the United States in 2018 had military service. Women, however, are far underrepresented in this group. There are only nine women out of the 458 individuals in the database (2.0 percent), while women comprise 9 percent of the U.S. adult population with military experience. [63]

About 68 percent of the individuals in PIRUS with a military background served in the Army or Marine Corps. The Army is the largest branch, so this may be expected, but the Marine Corps is the smallest, which means that the Marine Corps has the largest per capita rate of participation in extremism cases. When those in the National Guard or Reserves are also counted, the Army and Marine Corps make up 78.2 percent of all military-connected individuals in the database.[64]

Nearly half of all PIRUS individuals with a military background were categorized as individuals who had "adhered to anti-government views or were members of organized militias." Of these, more than 30 percent were reported to have racist ideologies, and about 10 percent were connected in some way to foreign Salafi Jihadists.[65] Although 59 percent of the 458 individuals in PIRUS with military ties were reported to have plotted violence, only 35 percent of these attempts were successful. Despite the concern that military-connected individuals could bring dangerous skills to extremist groups, this reported success rate is substantially lower than the 55 percent rate of successful violent actions by individuals in the PIRUS dataset without a military background.[66]

The rate of arrests tracked by PIRUS for offenders with a military background has also been increasing over time. The report states:

> "From 1990–2010, an average of 6.9 subjects per year with U.S. military backgrounds were included in the PIRUS data. Over the last decade, that number has more than quadrupled to 28.5 subjects per year. Not including Capitol offenders, an average of 17.7 subjects per year with military backgrounds have been added to the PIRUS data since 2010."[67]

---

62 Michael Jensen, Elizabeth Yates, and Sheehan Kane, *Radicalization in the Ranks: An Assessment of the Scope and Nature of Criminal Extremism in the United States Military* (College Park, MD: National Consortium for the Study of Terrorism and Responses to Terrorism (START), April 2022): 10–11, https://www.start.umd.edu/publication/radicalization-ranks.

63 Jensen, *Extremism in the Ranks and After,* July 2021, 2.

64 Jensen, *Extremism in the Ranks and After*, December 2021, 3.

65 Ibid, 4.

66 Ibid, 3.

67 Ibid, 2.

In other words, the rate of military participation in violent extremist incidents, as tracked within PIRUS, has roughly quadrupled from the two decades before 2010 to the decade after 2010 (or more than doubled, if the events of 6 January 2020, are excluded).

The trend is, at least in part, driven by only three years: 2017, 2020, and 2021. As the report explains, "each of these years were marked by issues that mobilized comparatively large numbers of U.S. extremists. These include the Unite the Right rally in Charlottesville in 2017; the COVID-19 pandemic, racial justice protests, and U.S. Presidential election in 2020; and the Capitol breach of 6 January 2021."[68] The overall level of violent extremism registered in the PIRUS database has also increased from an average of 40.4 individuals per year from 1990–2010 and an average of 84.6 per year from 2010–2020. Although the increase in the overall rate of violent extremist incidents roughly doubled, this rate of increase is lower than the increase for individuals with a military affiliation. Although the data are limited, the larger increase seen for military-connected individuals is in line with assessments provided to IDA by senior law enforcement officials.

A 2021 study published by the Center for Strategic & International Studies' (CSIS) Transnational Threats Project (TNT) based on data from several publicly-available databases and news sources reaches similar conclusions.[69] The CSIS study reports that "A small number of military and law enforcement[70] personnel have been involved in domestic extremism over the years." Military-connected individuals were responsible for a significant share of such events from the 1970s forward, the report states, but this share dropped precipitously after the terrorist attacks of 11 September 2001:

> According to FBI data, 37 percent of lone offender terrorists between 1972 and 2015 served in the military. But in the decade after September 11, 2001, there were few attacks by active-duty, reservist, or law enforcement personnel, although extremist groups attempted to infiltrate the military and law enforcement.[71]

In the last few years, this trend has been reversed and the rate of participation by military-connected individuals has risen again (although not to earlier levels). The report states:

> In 2020, 6.4 percent of all domestic terrorist attacks and plots (7 of 110 total) were committed by one or more active-duty or reserve members—an increase from 1.5 percent in 2019 (1 of 65 total) and none in 2018. While the attacks in 2021 account for only one month, the numbers in January 2021 showed another increase: 17.6

---

68 Jensen, *Extremism in the Ranks and After*, July 2021, 2.

69 The databases used by the CSIS study are described later in this report. Seth Jones, Catrina Doxsee, Grace Hwang, and Jared Thompson, *The Military, Police, and the Rise of Terrorism in the United States* (Washington, DC: Center for Strategic & International Studies (CSIS), April 12, 2021): 4, https://www.csis.org/analysis/military-police-and-rise-terrorism-united-states.

70 A brief review of law enforcement participation in violent extremist incidents is provided in Appendix E.

71 Seth Jones, Catrina Doxsee, Grace Hwang, and Jared Thompson, *The Military, Police, and the Rise of Terrorism in the United States*, 4.

percent of domestic terrorism plots and attacks (3 of 17 total) were committed by active-duty or reserve personnel.[72]

In light of data indicating the possibility of a trend in military participation over a very recent period that has been punctuated by a few salient events, IDA examined the prevalence of military service members who have been charged in relation to the U.S. Capitol events of 6 January 2021. Of the more than 700 federal cases in which charges were publicly available a year after these events, fewer than ten were for individuals who were serving in the military at the time. Based on the size of the military relative to the general population and considering the rate of charges for males and females, we find no evidence that service members were charged at a different rate than the members of the general population. However, the picture becomes much more complicated when individuals who formerly served in the military are included in the analysis.

As of 1 January 2022, nearly a year after the incident, there were "704 federal cases where charges are publicly available."[73] Although hundreds more were present and participated to varying degrees in the events of 6 January 2021, most available analysis focuses on these 704 cases, as the demographics of uncharged participants is largely unknowable.[74] These 704 cases represent considerable geographic diversity, including individuals from more than 350 different counties within the U.S., and 45 different states and the District of Columbia.[75] The individual participants ranged in age from 18 to 80, with an average age of 39. They were also overwhelmingly male—613 of the 704 individuals were male (87 percent).[76]

Clifford and Lewis report that 82 of the 704 individuals "had some confirmed form of prior U.S. military service."[77] Of these, one was on active duty, two were in the National Guard, four were in the Reserves, one was in Basic Training, and 73 were veterans.[78] These numbers are partially corroborated by analysis performed by START, which identifies one individual on active duty, two in the National Guard, and four in the Reserves.[79] Hence, these two reports identify

---

72 Ibid.

73 Bennett Clifford, Jon Lewis, *"This is the Aftermath:" Assessing Domestic Violent Extremism One Year After the Capitol Siege* (Washington, DC: Program on Extremism at George Washington University, January 2022): 12, https://extremism.gwu.edu/sites/g/files/zaxdzs2191/f/This%20is%20the%20Aftermath.pdf.

74 Not all who were present at or near the U.S. Capitol grounds engaged in unlawful behavior, which can complicate the comparison between the participation rates for those with and without military experience. If a current member of the military were present, but not engaging in unlawful behavior, the act of being present at such an event may result in a military investigation or punishment that a civilian would not be subject to. Focusing on those with federal charges provides a common threshold for severity of conduct that extends to those with and without military experience.

75 350 counties represent more than 10 percent of all counties in the U.S.

76 See Clifford and Lewis, *"This is the Aftermath,"* 12.

77 Ibid, 15.

78 These numbers add to 81, and it is not clear from the report whether the remaining individual was currently serving in the military or was a Veteran. See Ibid, 15–16.

79 Jensen, *Extremism in the Ranks and After*, December 2021. START specifically notes two in the Army National Guard, two Army Reservists, two Marine Reservists, and a Marine on Active Duty. START also reports two

either seven or eight individuals with federal charges for incidents at the Capitol who were serving in the military in some capacity at the time. The reports differ in terms of the number of veterans they identify. Clifford and Lewis identify 73 veterans while START identifies 107 veterans.[80] START also reports that "on average, the subjects who are facing charges for the Capitol breach have been separated from military service for nearly 15 years."[81]

IDA used these reported numbers to assess the rate of participation among military-connected individuals and compare it to the rate of participation in the overall population. To address differences in the composition of the military and non-military populations, IDA assessed three separate groups: male veterans, male service members, and females with military experience (either past experience as a veteran or experience in some capacity as a current service member)[82]. For each of these groups, IDA developed multiple comparison sets for the general population based on different age ranges.

For example, there are roughly 112.6 million males in the U.S. between the ages of 20 and 79. Of these individuals, roughly 15.2 million or 13.5 percent are veterans. If male veterans are equally likely to receive federal charges for participation in the events of 6 January 2021 as males who are not veterans, then we would expect roughly the same 13.5 percent of the males between the ages of 20 and 79 with charges would be veterans. Of the 704 total federal charges across all demographics, an estimated 603 are for males between the ages of 20 and 79.[83] Thus, if male veterans were charged at the same rate as males who are not veterans, we could expect that 81 male veterans (that is, 13.5 percent of 603) would face federal charges for participation in the U.S. Capitol events of 6 January 2021.[84] This number is roughly on par with the 73 to 107 veterans who

---

individuals "who enlisted after January 6, 2021" and two Civil Air Patrol Cadets. However, these four individuals arguably do not count as having military experience prior to the events at the Capitol. The Civil Air Patrol "is a 501(c)3 non-profit organization that serves as the civilian auxiliary to the U.S. Air Force" and Cadets are under no obligation to serve in the military (see "Cadet FAQs," "Do cadets have to join the military?" Civil Air Patrol Website, accessed June 16, 2022, https://www.gocivilairpatrol.com/join/youth-in-cadet-program/cadet-faqs); for quoted text, see "Youth," Civil Air Patrol Website, accessed June 16, 2022, https://www.gocivilairpatrol.com/join/youth-in-cadet-program.

80 A later START report indicates 109 Veterans (Jensen, *Radicalization in the Ranks*, 19-20).

81 Ibid, 20.

82 Females were combined into a single category because the small number of females included was insufficient to support analysis of separate categories for veterans and current service members.

83 The ages for 72 of the 704 individuals are unknown. Clifford and Lewis, *"This is the Aftermath,"* give the age distribution overall, but not broken out by gender. Table 2 herein shows the number of estimated charges by age and gender, assuming the age distribution is the same across gender, and also that the age distribution of the 72 individuals whose ages are unknown (from publicly available sources) is the same as the age distribution for the 632 whose ages are known. See Appendix E for details.

84 We can also estimate a statistical range for the number of male Veterans who would likely be charged. If the number of male veterans between the ages of 20 and 79 who are charged is between 67 and 96, then the proportion of Veterans charged is not statistically different (at the 10 percent significant level) from the proportion charged from the general population. This statistical test could be shaped multiple ways. The proportion of the Veteran population charged (i.e., the number of Veterans charged divided by the total Veteran population) could be compared to the proportion charged in the total population (i.e., the number charged

were actually charged (depending on the source), indicating that the participation rate of male veterans in the Capitol breach was generally proportionate to the participation rate of the overall male population. [85]

However, the veteran population in the United States tends to be older than the population as a whole. Since elderly individuals may be less likely to participate in violent activities, the rate of veteran participation in the events of January 6th may be understated in the absence of some age adjustment for the relevant populations. Of course, it is worth noting that the active duty population is considerably younger than the U.S. population as a whole, so that unadjusted participation rates for those currently serving are likely to be overstated in the absence of an age adjustment.

Table 2 shows the number of male veterans who would be expected to be charged based on a variety of age range assumptions for purposes of comparison to males from the general population. For example, if we limit the comparison to male veterans whose ages are between 20 and 69, we expect 64 veterans to be charged. If the focus is on male veterans between the ages of 20 and 59, we would expect 50 to be charged. If the criteria that Clifford and Lewis use to identify 73 veterans with "some confirmed form of prior U.S. military service" is correct, then this number is roughly in line with expectations if veterans were charged at the same rate as males from the general population.[86] If instead the criteria used by START to identify 107 veterans is correct, then the number of veterans charged is somewhat higher than for the general male population. If the 20 to 79 age range is the appropriate comparison, then male veterans may be about one-third more likely to be charged than males in the general population. If the 20 to 59 age range is the appropriate

---

divided by the total population). This comparison can be done with a one-proportion test or a binomial test. Both yield the range of 67 to 96 at the 10 percent significance level. Alternatively, a two-proportion test could be conducted between the proportion of the Veteran population charged and the proportion of the non-Veteran population charged (i.e., non-Veterans charged divided by the total non-Veteran population, that quotient treated as a random variable in its own right). This yields a range of 68 to 95 at the 10 percent significance level. These tests were implemented in R using binom.test() and prop.test(). For example, a one-proportion test of 67 Veteran charges out of a population of 15,195,000 veterans, compared with a hypothesized probability of 603 charges divided by a population of 112,610,000 (i.e., a probability of 0.00000535476) can be tested with the following: prop.test(x = 67, n = 15195000, p = 0.00000535476, alternative = "two.sided"), which has a p-value of 0.1202. The binom.test() follows the same syntax. A two-proportion test between 68 Veterans charged out of a population of 15,195,000 veterans against 535 non-Veterans charged (i.e., a total of 603 charged minus 68 Veterans charged) out of a non-Veteran population of 97,415,000 (i.e., a total population of 112,610,000 minus a Veteran population of 15,195,000) can be implemented with prop.test(x = c(68, 535), n = c(15195000, 97415000), alternative = "two.sided"). This has a p-value of 0.1251.

[85] As shown in Table 2 and explained in the above footnote, there is an expected range of 67 to 96 Veterans who would be charged if Veterans were charged at a rate equal to the corresponding non-Veteran population. The number of 73 Veterans charged as reflected by Clifford and Lewis, *"This is the Aftermath,"* is in line with this expectation. The number of 107 veterans charged from the PIRUS data in Jensen, *Extremism in the Ranks and After*, December 2021, is slightly higher than this statistical range. In that sense, it is statistically different. However, in terms of order of magnitude, it is different by only a few percentage points.

[86] Clifford and Lewis, *"This is the Aftermath,"* do not provide an age range broken out for those with military experience, so we cannot break down the 73 by the various age ranges. It may be on the high side if the relevant comparison is to those between the ages of 20 and 59 and all (or nearly all) of those charged fall within that age range.

comparison, then male veterans may be about twice as likely to be charged as males in the general population.[87]

Table 2. Expected Number of Male Veterans Charged for the 6 January 2021 Events if Male Veterans are Charged at the Same Rate as the General Population

Group	Estimated charges in group (Numerator)	Group size in U.S. (Denominator)	Proportion of group charged in U.S. (Quotient)	Group size in U.S. who are Veterans	Expected charges for Veterans (Quotient X Veterans)	Expected Range
Males, Ages 20 to 79	603	112,610,000	0.00000535476	15,195,000	81	67 to 96
Males, Ages 20 to 69	597	101,686,000	0.00000587101	10,816,000	64	50 to 76
Males, Ages 20 to 59	563	83,669,000	0.00000672890	7,442,000	50	39 to 62

Notes: Based on the 704 individuals with federal charges that were publicly available as of 1 January 2022, as cited in Clifford and Lewis (2022). The expected range represents the number of male Veterans who could be charged without a statistically significant difference from the rate for males in the general population at the 10 percent significance level (under the more conservative of a one-proportion test or binomial test comparing the proportion of male Veteran charges to the proportion of male charges in the general population; results are similar with a two-proportion test comparing the proportion of male Veteran charges to the proportion of male non-Veteran charges).

Sources:

U.S. population by age and gender, 2019, from U.S. Census Bureau at https://www2.census.gov/programs-surveys/demo/tables/age-and-sex/2019/age-sex-composition/2019gender_table1.xlsx

Veteran population by age and gender, 2019 forecasts from VETPOP2018, from Veterans Affairs at https://www.va.gov/vetdata/docs/Demographics/New_Vetpop_Model/1L_VetPop2018_National.xlsx

Publicly available federal charges for 6 January 2021 U.S. Capitol events by age and gender, as of 1 January 2022, estimated from Clifford and Lewis (2022, p. 12–13). Further details on estimates are in Appendix E.

Table 3 shows the number of expected charges for males currently serving in the military (whether on active duty, in the Reserves, or in the National Guard), based on a different set of age assumptions. Since the vast majority of those serving in the military are under the age of 60, we focus on the age ranges of 18 to 59, 18 to 49, and 18 to 39.[88] Across these age ranges, if male

[87] START also does not provide an age distribution, so we cannot break down the 107 by the various age ranges.

[88] In contrast to the veteran age ranges in Table 2, which have a minimum age of 20, we include 18- and 19-year-olds for the comparison of those who are currently serving in the military to account for the many who enlist at

service members are just as likely to be charged as males in the general population, the expected number of male service members to be charged is around 11 to 14.[89] Both Clifford and Lewis (2022) and START identified seven or eight service members who were charged, which is in line these expectations. Based on these numbers, we find no evidence that male service members were charged at a different rate than males from the general population. Because roughly two-thirds of currently serving members of the military are part of the active force, the number of males charged from the active force would appear significantly lower than the rate for the general population.

Table 3. Expected Number of Male Service Members Charged for the 6 January 2021 Events if Male Service Members are Charged at the Same Rate as the General Population

Group	Estimated charges in group (Numerator)	Group size in U.S. (Denominator)	Proportion of group charged in U.S. (Quotient)	Group size in U.S. who are Service Members	Expected charges for Service Members (Quotient X Service Members)	Expected Range
Males, Ages 18 to 59	571	87,887,000	0.00000649698	2,105,000	14	8 to 20
Males, Ages 18 to 49	460	67,911,000	0.00000677357	1,922,000	13	7 to 18
Males, Ages 18 to 39	323	48,290,000	0.00000668876	1,682,000	11	6 to 16

Notes: Based on the 704 individuals with federal charges that were publicly available as of 1 January 2022, as cited in Clifford and Lewis (2022). The expected range represents the number of male service members who could be charged without a statistically significant difference from the rate for males in the general population at the 10 percent significance level (under the more conservative of a one-proportion test or binomial test comparing the proportion of male service member charges to the proportion of male charges in the general population; results are similar with a two-proportion test comparing the proportion of male service member charges to the proportion of male non-service member charges).

Sources: U.S. population by age and gender, 2019, from U.S. Census Bureau at https://www2.census.gov/programs-surveys/demo/tables/age-and-sex/2019/age-sex-composition/2019gender_table1.xlsx. Since counts are reported in five-year age increments, the count for those in the age 15 to 19 increment is multiplied by 2/5 to get estimated counts for those ages 18 to 19.
Service member populations by age and gender, December 2020, from the Defense Manpower Data Center.

those ages. In most cases, former service members must have at least minimal military experience before achieving the status of veteran, so a higher minimum age is appropriate to capture the vast majority of veterans.

[89] Table 3 includes all reserve categories. Excluding members of the individual ready reserve, standby reserve, and retired reserve, the expected number of service members charged drops from 14 to 12 for the 18- to 59-year-old age range, from 13 to 12 for the 18- to 49-year-old age range, and from 11 to 10 for the 18- to 39-year-old age range.

These counts include the active duty, Reserves, and National Guard, including all reserve categories. Excluding members of the Individual Ready Reserve, Standby Reserve, and Retired Reserve, the expected number of charges is 12 (ages 18 to 59), 12 (ages 18 to 49) and 10 (ages 18 to 39).
Publicly available federal charges for 6 January 2021 U.S. Capitol events by age and gender, as of 1 January 2022, estimated from Clifford and Lewis (2022, p. 12–13). Further details on estimates are in Appendix E.

Table 4 examines the expected number of charges for females with military experience. Females constitute a much smaller portion of the total number of individuals charged (13 percent). Additionally, females with any military experience—either as a current service member or previously as a veteran—make up only about two percent of the adult female population (compared with roughly 15 percent for the adult male population). Assessing the expected number of female charges may therefore be less precise because the proportion of female charges and the size of the female population with military experience are both much smaller. If females with military experience are charged at the same rate as females without military experience, then we could expect one or two females with military experience being charged. Statistical ranges expand the window to somewhere between zero and four females with military experience being charged. START reports three females with military experience "participated in the Capitol breach."[90] A separate source reports two females with military experience who had been indicted for events at the U.S. Capitol on 6 January 2021.[91] Both of these are in line with the expected number of females with military experience to be charged. We find no evidence that females with military experience were charged at a different rate than females from the general population.

[90] Jensen, *Extremism in the Ranks and After*, December 2021, 2.

[91] From a December 9, 2021 presentation from Daniel Milton and Andrew Mines, *"This is War:" Examining Military Experience Among the Capitol Hill Siege Participants* (Washington, DC: Program on Extremism at George Washington University, Combatting Terrorism Center at West Point, April 12, 2021, https://ctc.usma.edu/this-is-war-examining-military-experience-among-the-capitol-hill-siege-participants/.

Table 4. Expected Number of Females with Military Experience Charged for the 6 January 2021 Events if Females with Military Experience are Charged at the Same Rate as the General Population

Group	Estimated charges in group (Numerator)	Group size in U.S. (Denominator)	Proportion of group charged in U.S. (Quotient)	Group size in U.S. with Military Experience	Expected charges for those with Military Experience (Quotient X Military Experience)	Expected Range
Females, Ages 18 to 59	85	89,805,000	0.00000094650	1,891,000	2	0 to 4
Females, Ages 18 to 49	68	68,263,000	0.00000099615	1,402,000	1	0 to 3
Females, Ages 18 to 39	48	47,956,000	0.00000100092	936,000	1	0 to 2

Notes: Military Experience is the sum of service members and veterans. Based on the 704 individuals with federal charges that were publicly available as of 1 January 2022, as cited in Clifford and Lewis (2022). The expected range represents the number of females with military experience who could be charged without a statistically significant difference from the rate for females in the general population at the 10 percent significance level (under the more conservative of a one-proportion test or binomial test comparing the proportion of female charges for those with military experience to the proportion of female charges in the general population; results are similar with a two-proportion test comparing the proportion of female charges for those with and without military experience).

Sources: U.S. population by age and gender, 2019, from U.S. Census Bureau at https://www2.census.gov/programs-surveys/demo/tables/age-and-sex/2019/age-sex-composition/2019gender_table1.xlsx. Since counts are reported in five-year age increments, the count for those in the age 15 to 19 increment is multiplied by 2/5 to get estimated counts for those ages 18 to 19.
Service member populations by age and gender, December 2020, from the Defense Manpower Data Center. These counts include the Active Duty, Reserves, and National Guard, including all reserve categories.
Publicly available federal charges for 6 January 2021 U.S. Capitol events by age and gender, as of 1 January 2022, estimated from Clifford and Lewis (2022, p. 12–13). Further details on estimates are in Appendix E.

In addition to January 6th participants with military experience, "a further 24" of the 704 individuals with publicly available federal charges "had experience in law enforcement," and "a handful of defendants . . . had previously worked for federal government agencies." [92] None of the sources make mention, however, of any past or present DOD civilian employees being charged.

In sum, IDA's review found no evidence that the number of violent extremists in the military is disproportionate to the number of violent extremists in the United States as a whole. Extremism

[92] Clifford and Lewis, *"This is the Aftermath,"* 15.

in the veterans' community has seen peaks and valleys over recent decades, and currently appears to be on the increase. IDA found no evidence of participation in violent extremist events by DOD civilians or defense contractor employees.

4. Definitions of Extremism

A. What is Extremism?

The Académie Française drafted the first official definition of 'terrorist' in reference to the actions of the Jacobins (a far-left group opposing the rule of the new First Republic government) during a period of the French Revolution known as the Reign of Terror (1793-1794).[93] In the centuries since the Reign of Terror, researchers have identified more than 260 different definitions of terrorism.[94] In fact, the General Assembly of the United Nations has been trying to reach an agreement on a legal definition of terrorism since 1972 and has yet to do so.[95]

A wide range of definitions of extremism and the myriad of terms associated with it (e.g., terrorism, domestic terrorism, violent extremism, homegrown violent extremism, hate crime) have been used by social and behavioral scientists and by the law enforcement and intelligence agencies (LEIA) tasked with keeping the public safe from extremist activity. This issue was a key theme explored during a 2019 conference held by the National Counterterrorism Center, during which participants identified the need for a common set of terms and associated definitions that can apply across U.S. government agencies and departments with domestic terrorism investigative, intelligence, or prevention missions.[96]

Complicating matters is the fact that academics, federal authorities (e.g., law enforcement, policy makers, leadership), and extremists themselves define extremism and extremist behaviors differently. The challenge of defining extremism and extremist behavior should not be surprising, as the thoughts, beliefs, and actions considered to be extremist are highly subjective and depend on a number of factors, including the nature of the political system, prevailing political culture,

---

93 Although the actual count is unknown, the French government killed an estimated 16,000 to 40,000 citizens over the course of the year. See Joseph S. Tuman, *Communicating Terror: The Rhetorical Dimensions of Terrorism*, 2nd edition (Thousand Oaks, CA: Sage Publications, Inc., 2010), doi: https://dx.doi.org/10.4135/9781452275161.

94 Joseph J. Easson and Alex Schmid, "250+ Academic, Governmental and Intergovernmental Definitions of Terrorism," in *The Routledge Handbook of Terrorism Research*, edited by Alex Schmid, 99-200 (New York City, NY: Routledge, 2011), https://www.routledge.com/The-Routledge-Handbook-of-Terrorism-Research/Schmid/p/book/9780415520997.

95 Alex Schmid, "The Definition of Terrorism," in *The Routledge Handbook of Terrorism*, edited by Alex Schmid (New York City, NY: Routledge, 2011).

96 National Counterterrorism Center, Department of Justice, Department of Homeland Security, *Domestic Terrorism Conference Report* (n.p.: January 2020), https://www.dni.gov/files/2020-01-02-DT_Conference_Report.pdf.

system of values, ideology, personal characteristics, experiences, and ethnocentrism.[97] Walter Laqueur, when discussing the ability to develop an objective and internationally accepted definition of terrorism, stated: "one man's terrorist is another man's freedom fighter [or patriot]."[98] In other words, the definition of extremism can be in the eye of the beholder.

In this section, we provide descriptions of the various terms associated (and often confounded) with extremism as they are operationalized in the academic literature and in federal law enforcement. We then examine the extremism-related terms used by DOD with regard to how DOD defined them, both historically and in recently updated DOD Instructions. We end this section with recommendations on addressing the definitional challenges associated with extremism.

1. Extremism and Extremist Ideology: Scholarly Definitions

In general, radicalization may be defined as the transformational cognitive and behavioral *process* of adopting to, changing, or strengthening a set of ideas that are outside, or in opposition to, mainstream societal ideas or the status quo. In other words, radicalization is the process by which an individual develops extremist ideologies, beliefs, and emotions, which can then lead to extremist actions or behaviors (e.g., an act of terrorism).[99] Radicalization does not necessarily mean that the radicalized individual will engage in violent action;[100] there are far more radicalized individuals in the world than there are individuals who will engage in an act of terrorism. However, almost all individuals who engage in terrorist acts have gone through a radicalization process.[101] Pathways to radicalization are described in detail in Chapter 5.A of this paper.

Many definitions of extremism combine ideological motivations with their associated violent actions, effectively blending extremism with terrorism. In general, however, extremism refers to ideologies, beliefs, and convictions that oppose the fundamental values of society, the laws of democracy, and common notions of human rights. In many cases, such ideologies, beliefs, and

---

97 Andrej Sotlar, "Some Problems with a Definition and Perception of Extremism within a Society," *Policing in Central and Eastern Europe*, edited by Gorazd Meško, M. Pagon, & B. Dobovšek (Ljubljana, Slovenia: Faculty of Criminal Justice, University of Maribor, December 2004), https://www.ojp.gov/pdffiles1/nij/Mesko/208033.pdf.

98 Walter Lacqueur, *The Age of Terrorism* (New York City, NY: Little Brown and Company, 1987): 7.

99 This process can take place over a period ranging from a few weeks to several years. See Jamie Bartlett, Jonathan Birdwell, and Michael King, *The Edge of Violence: A Radical Approach to Extremism*, (London, UK: Demos, 2010); and Randy Borum, "Radicalization in Violent Extremism I: A Review of Social Science Theories," *Journal of Strategic Security* 4, no. 4 (Winter 2011): 7-36, https://www.jstor.org/stable/26463910?seq=1.

100 Roger Scruton, *The Palgrave Macmillan Dictionary of Political Thought*, 3rd edition (New York City, NY: Palgrave Macmillan, February 7, 2007); Peter R. Neumann, "The Trouble with Radicalization," *Internal Affairs* 89, no. 4 (July 2013): 873-893, doi:10.1111/1468-2346.12049.

101 Michael Wolfowicz, Yael Litmanovitz, David Weisburd, Badi Hasisi, "Cognitive and Behavioral Radicalization: A Systematic Review of the Putative Risk and Protective Factors," *Campbell Systematic Reviews* 16, no. 3 (September 9, 2020): e1102, doi:10.1002/cl2.1102.

convictions advocate the supremacy of a particular group (racial, religious, political, economic, social, etc.). The term extremism has also been used to refer to the methods (though not the specific acts) through which extremist actors try to achieve their aims.[102]

The academic literature categorizes extremism by the fundamental ideology or motivation for extremist actions and behaviors. Researchers generally agree on four main types of extremist (violent and nonviolent) ideologies, as shown in Table 5: left-wing, right-wing, single-issue, and politico-religious. Although there are only a few categories of extremist ideologies, each is associated with a variety of groups. We note that these categories are not as clear-cut as described in Table 5, as some groups fit into multiple ideological categories. For example, the Aryan Nations could be considered both a right-wing and politico-religious extremist group because it was founded on the Christian Identity and white supremacist movement.

Table 5. Literature-based Categories of Extremist Ideologies

Typology	Description of Ideology	Examples
Left-Wing	Emphasis on class struggles and a desire to change political systems that cause social inequalities; often focused on anti-capitalist ideals	Anarchists, Maoist, Trotskyists, Marxist-Leninist
Right-Wing	Supports fascism, racism, supremacism, ultranationalism, survivalism, and radical hostility towards state authorities, minorities, immigrants, left-wing political groups	KKK, Black Separatists, Neo-Nazis, Neo-Confederates, White Nationalists
Single-Issue	Motivated by a single issue and therefore cover a diverse set of ideologies and goals	Radical environmentalists, animal rights groups, anti-abortion groups, anti-LGBTQ, anti-feminist groups (Incels)
Politico-Religious	Motivated by political interpretation of religion and defense of religious identity perceived to be under threat; any religion may lead to this type of extremist ideology	Al Qaeda, Red Army Faction, Army of God, Aum Shinrikyo

One driver pushing violent ideologies into action is the idea of accelerationism. As a force amplifier, accelerationism can both push mainstream ideas towards a violent end and further radicalize those already radicalized to engage in violent action. Accelerationism was originally conceptualized as the idea that social processes such as capitalist growth and technological change could be expanded or drastically sped up to bring about radical social change. However,

[102] Kristen Klein & Arie Kruglanski, "Commitment and Extremism: A Goal Systemic Analysis," *Journal of Social Issues* 69, no. 3 (September 9, 2013): 419-435, https://spssi.onlinelibrary.wiley.com/doi/abs/10.1111/josi.12022; Simona Trip et al., "Psychological Mechanisms Involved in Radicalization and Extremism: A Rational Emotive Behavioral Conceptualization," *Frontiers in Psychology* 10 (March 6, 2019): 1-8, doi:10.3389/fpsyg.2019.00437.

accelerationism has been adopted by individuals and groups across the spectrum of extremist ideologies as a justification for violent action.[103]

Although the definitions of radicalization and extremism focus on transformation and ideology, respectively, the definition of terrorism focuses on action. Terrorism may be described as an expression or manifestation of a violent ideology. While extremism can be expressed through violent or nonviolent action, terrorism, by definition, requires violence or the threat of violence. One definition of terrorism from the academic literature is –

> an act or threat of violence to persons or property that elicits terror, fear, or anxiety regarding the security of human life or fundamental rights and that functions as an instrument to obtain further ends. This instrumentality relies upon either an explicit or implicit threat of separate acts of future violence.[104]

An individual can espouse violent extremist ideology without committing a crime, however, once the threshold of planning, preparation, and/or execution of a criminal act has been crossed, an act of terrorism has occurred.[105]

Terrorism and political violence are closely linked, but they are not synonymous. Terrorism is a violent act motivated by extremist ideology. Political violence, on the other hand, includes any use of force to achieve a political purpose, including justifiable military action. However, the distinction between terrorism and political violence is not always clear, as "freedom fighters and terrorists are not mutually exclusive categories. Terrorists can also fight for national liberation,

---

[103] Alex Newhouse, "The Threat is the Network: The Multi-Node Structure of Neo-Fascist Accelerationsim," *CTC Sentinel* 14, no. 5 (June 2021): 17-25, https://ctc.usma.edu/wp-content/uploads/2021/05/CTC-SENTINEL-052021.pdf. In recent times, anti-government and far-right extremist are most commonly linked to accelerationism, with two of the most well-known groups being Atomwaffen and The Base. These groups see Western governments as deeply corrupt and do not perceive value in seizing power through the political process (i.e., running for office, serving in government, or voting). Instead, they prefer to spread chaos and create political tension through violent actions and actions that are perceived as violent, with the ultimate goal of bringing about the collapse of "liberal" government to make way for a future that is in line with extremist ideologies. For example, white supremacist accelerationists believe that the government is systematically targeting the demise of the white race though its immigration policies, multiculturalism, and by other means. The only way to prevent such perceived injustices, in this view, is to replace modern social and political systems with a new approach based in ethnonationalism. Accelerationism is not an ideology, in that it is ideologically agnostic. Instead, it drives strategic orientation towards violence as a means to an end. Institute for Strategic Dialogue, *Accelerationism: An Overview of Extremist Narratives about the Need for Societal Collapse to Preserve the White Race* (London, UK: Institute for Strategic Dialogue, 2021) https://www.isdglobal.org/wp-content/uploads/2021/09/Accelerationism-External-May-2021.pdf; Brian Hughes and Cynthia Miller-Idriss, "Uniting for Total Collapse: The January 6 Boost to Accelerationism," *CTC Sentinel* 14, no. 4 (April/May 2021): 12-17, https://ctc.usma.edu/uniting-for-total-collapse-the-january-6-boost-to-accelerationism/; Jade Parker, "Accelerationism in America: Threat Perceptions," *Global Network on Extremism & Technology*, February 4, 2020, https://gnet-research.org/2020/02/04/accelerationism-in-america-threat-perceptions/.

[104] Shawn Kaplan, "A Typology of Terrorism," *Review Journal of Political Philosophy* 6, no. 1 (2008): 1-38, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1460938.

[105] Gregory D. Miller, "Blurred Lines: The New 'Domestic' Terrorism," *Perspectives on Terrorism* 13, no. 3 (June 2019): 63-75, https://www.researchgate.net/publication/333676937_Blurred_Lines_The_New_Domestic_Terrorism.

and freedom fighters can also carry out inhuman atrocities."[106] The justification of the violent action can be in the eye of the beholder.

While the typologies of extremism typically focus on ideological motivation, typologies of terrorism focus on categories of action. Terrorist actions may be categorized based on the discrimination of legitimate and illegitimate targets, the degree of force used, the agency of the perpetrator (e.g., state vs. non-state actors), the context of the terrorist act (e.g., domestic vs. international),[107] and whether the violent act was committed by an extremist group or by a single individual who is neither part of a group nor directed by an outside organization.

Analysts describe individual actors as lone-wolf or lone-actor terrorists.[108] The rise of the internet and social media have contributed to a parallel rise in the number of lone-actor attacks worldwide. Individuals share extremist ideologies and templates for violence online, enabling individuals who may not have the means, opportunities, or desires to join an extremist organization, to engage in lone-actor attacks. Even if an individual acts alone, extremist and terrorist groups often claim responsibility, reaping the benefits of free dissemination of their ideology.[109] Despite the increase in lone-actor attacks, most result in a small number of casualties,[110] often because the perpetrators are untrained in carrying out their violent plans. Prior combat or terrorism experience by the lone-actor may dramatically improve the odds of success,[111] increasing the stakes associated with the potential radicalization of members of the military community.

Commonly, terrorism scholars use three variables to classify terrorism as "domestic" or "international:" the nationality of the perpetrator, the nationality of the human and non-human victim(s), and the location of the attack. If all three of these variables align, an event is typically

---

[106] Alex Schmid, "Terrorism-The Definitional Problem," *Case Western Reserve journal of International Law* 36, no. 2 (2004): 414 https://scholarlycommons.law.case.edu/jil/vol36/iss2/8/.

[107] Kaplan, "A Typology of Terrorism."

[108] For example, Ted Kaczynski (known as the Unabomber) killed three and injured more than 20 people using mail bombs as part of a self-driven plan of terrorism that was unaffiliated with any extremist group. However, lone-actor terrorists rarely act in complete isolation—often, these individuals feel a connection to a broader cause or the extremist ideology motivating their violent actions. A terrorist attack on December 2015 in San Bernardino, CA, is such a case. Specifically, a married couple by the names of Syed Rizwan Farook and Tashfeen Malik carried out an attack at a Christmas party held by Farook's employer. The two sought information about and were influenced by al Qaeda (i.e., they self-radicalized) and although they had no direct contact with ISIS, pledged loyalty to the group's leader during the attack. Daniel L. Byman, "How to Hunt a Lone Wolf: Countering Terrorists who Act on their Own," *Brookings*, February 14, 2017, https://www.brookings.edu/opinions/how-to-hunt-a-lone-wolf-countering-terrorists-who-act-on-their-own/.

[109] For example, had Farook and Malik not pledged their loyalty to ISIS, law enforcement and the media might have classified the attack as an act of workplace violence, not terrorism.

[110] Ibid.

[111] Thomas Hegghammer, "Should I Stay or Should I Go? Explaining Variation in Western Jihadists' Choice between Domestic and Foreign Fighting," *American Political Science Review* 107, no. 1 (January 28, 2013): 1-15, https://doi.org/10.1017/S0003055412000615.

identified as domestic terrorism—all other cases are classified as international terrorism (Miller, 2019). Using this analysis, the 1995 Oklahoma City bombing is a prototypical domestic terrorist act: Timothy McVeigh (a U.S. citizen) engaged in a terrorist act against the U.S government, resulting in the deaths of U.S. citizens.

The use of the internet and social media by extremist organizations to spread their ideologies and influence individuals on a global level has blurred the distinction between domestic and international terrorism. For example, there is debate on the classification of the San Bernardino attack: Farook was a U.S. citizen who attacked fellow citizens in California, but whose attack was inspired by the global Islamic extremist movement. One leading scholar suggests that the alignment of the perpetrator and victim nationality with the location of the attack is an insufficient means to classify terrorism as domestic or international. Instead, he suggests examining the motivation of the attack. If the underlying ideology and motivation is based on national issues (e.g., racial divides, ethnonationalism, issues with specific policies or laws), he suggests that the associated violent acts are best labeled as domestic terrorism.[112]

2. Extremism and Extremist Ideology: Law Enforcement Categories

The definitions and typologies of radicalization, extremism, and terrorism used by law enforcement differ from those described in the academic literature.

In response to the Fiscal Year 2020 National Defense Authorization Act (FY 2020 NDAA), the Federal Bureau of Investigations (FBI), U.S. Department of Homeland Security (DHS), and the Director of National Intelligence (DNI) jointly developed standardized definitions of terminology relating to domestic terrorism and provided typologies of domestic terrorism threats. The LEIA use the term "violent extremism" because it is the aspect of violence, rather than the underlying extremist ideology or the advocacy of this ideology that can be prohibited by law.

Using this approach, the LEIA developed a list of domestic threat typologies, including racially or ethnically motivated extremism, anti-government or anti-authority extremism, animal rights or environmental extremism, abortion-related extremism, and other domestic terrorist threats. These categories are described in Table 6. However, the LEIA acknowledge that the motivations of actors vary, are nuanced, and can arise from a blend of ideologies.[113]

[112] Miller, "Blurred Lines."

[113] Federal Bureau of Investigation (FBI) and Department of Homeland Security (DHS), *Strategic Intelligence Assessment and Data on Domestic Terrorism* (Washington, DC: FBI and DHS, May 2021), https://www.fbi.gov/file-repository/fbi-dhs-domestic-terrorism-strategic-report.pdf/view.

Table 6. U.S. Government Categories of Extremist Motivations

Violent Extremism Typology	Description of Ideology
Racially or Ethnically Motivated	Potentially unlawful use or threat of force/violence to further ideological agenda based on bias (usually race/ethnicity) against others; use political and religious justifications to support ideological objectives and criminal activities
Anti-Government or Anti-Authority	Potentially unlawful use or threat of force/violence to further ideological agenda based on anti-government or anti-authority sentiment, to include perceived economic, social, or racial hierarchies or perceived government overreach, negligence, or illegitimacy; includes individuals, militias, anarchists, and sovereign citizen movements that advocate violence to achieve their agendas[114]
Animal Rights/Environmental	Potentially unlawful use or threat of force/violence to further ideological agenda to end or mitigate perceived cruelty or harm to, or exploitation of animals, or the exploitation/destruction of natural resources and the environment
Abortion-Related	Potentially unlawful use or threat of force/violence to further ideological agenda relating to abortion, both in regard to pro-life or pro-choice beliefs
All Other Domestic Terrorism Threats	Potentially unlawful use or threat of force/violence to further ideological agenda not defined under the aforementioned categories; the belief/agenda can arise from personal grievances and beliefs from one of the other categories and may include biases regarding religion, gender, or sexual orientation

The U.S. Government does not compile lists of groups affiliated with violent extremist ideology because "advocacy of associated political or social positions, political activism, use of strong rhetoric, or generalized philosophic embrace of violent tactics may not constitute violent extremism, and may be constitutionally protected."[115] FBI policy is not to investigate, collect, or maintain information on U.S. citizens to monitor extremist groups that advocate violent and nonviolent action unless there is reason to believe that a federal crime has been committed or is about to be committed. In these cases, the FBI and other law enforcement organizations are allowed to obtain information regarding the activity and the role of an individual, group, or organization in the criminal activity.[116]

[114] We note that although the U.S. Government does not compile lists of groups affiliated with violent extremist ideologies, the joint report from the FBI, DHS, and DNI identifies subcategories of anti-government and anti-authority violent extremist categories. Militia violent extremists are individuals who take steps to violently resist or overthrow the U.S. Government based on their belief that the Government is intentionally exceeding its Constitutional authority and trying to establish a totalitarian regime. These individuals oppose many state and local laws/regulations, particularly those regarding firearms ownership. Anarchist violent extremists oppose all forms of capitalism, corporate globalism, and governing institutions, as they perceived them as harmful to society. Sovereign citizen violent extremists believe they are immune from government authority and laws.

[115] FBI and DHS, *Strategic Intelligence Assessment and Data on Domestic Terrorism,* 4.

[116] Ibid.

The FBI and DHS use the term, "homegrown violent extremism (HVE)" to describe U.S. persons who are motivated by ideologies of foreign terrorist organizations. Specifically, an HVE is "a person of any citizenship who has lived and/or operated primarily in the United States or its territories who advocates, is engaged in, or is preparing to engage in ideologically-motivated terrorist activities (including providing support to terrorism) in furtherance of political or social objectives promoted by a foreign terrorist organization, but is acting independently of direction by a foreign terrorist organization."[117] Both the FBI and DHS make a distinction between HVEs and domestic violent extremists, as the latter group support the achievement of political or social goals using unlawful force or violence, but is not directed or inspired by foreign terrorist goals.[118]

Section 2331(5) of Title 18, United States Code defines international terrorism and domestic terrorism. Both categories of terrorism include violent acts or acts that are dangerous to human life that would be criminal law violations if committed in U.S. jurisdiction. Both include acts designed to intimidate or coerce civilian populations, influence governmental policy through intimidation or coercion, or engage in mass destruction, assassination, or kidnapping as a means to affect governmental functions.

In international terrorism, these acts take place primarily outside U.S. territorial jurisdiction or are considered transnational due to the manner in which the acts are accomplished, the persons they appear intended to intimidate or coerce, or the location where the perpetrator resides (or operates from). On the other hand, domestic terrorism occurs primarily within U.S. territorial jurisdiction and does not include these transnational factors. Under these definitions, a U.S. citizen who is inspired by al Qaeda (or other internationally based extremist ideology) could be engaging in an act of international terrorism, even if he or she has no actual international ties and carries out an attack on U.S. soil.[119] For this reason, the FBI has classified the San Bernardino attack of 2015 as an incident of international terrorism. The distinction is an important one because, as explained later in this report, domestic terrorism is not, in itself, a criminal offense.

Individuals who are radicalized or motivated by extremist ideologies may also commit hate crimes. Hate crime statutes apply when an offender willfully causes (or attempts to cause) bodily injury using a dangerous weapon because of victim's perceived or actual race, color, religion, or national origin. Federal hate crime statutes include The Matthew Shepard and James Byrd Jr. Hate Crimes Prevention Act of 2009 (18 U.S.C. § 249), Damage to Religious Property, Church Arson

---

[117] Director of National Intelligence, *US Violent Extremist Mobilization Indicators* (Washington, DC: Director of National Intelligence, 2021), https://www.dni.gov/files/NCTC/documents/news_documents/Mobilization_Indicators_Booklet_2021.pdf.

[118] Lisa N. Sacco, "Sifting Domestic Terrorism from Hate Crime and Homegrown Violent Extremism" (Washington, DC: Congressional Research Service, January 15, 2021), https://www.everycrsreport.com/files/2021-01-15_IN10299_572203b7de901830d66301cbd676c81a3cab67b9.pdf.

[119] Shirin Sinnar, "Separate and Unequal: The Law of "Domestic" and "International" Terrorism," *Michigan Law Review* 117, no. 7 (May 2019): 1333-1404, doi:10.36644/mlr.117.7.separate.

Prevention Act (18 U.S.C. § 247), and Violent Interference with Federally Protected Rights (18 U.S.C. § 245).

Because hate crimes can involve an ideological motivation, the distinction between a hate crime and an act of domestic terrorism can become blurry. For example, the following cases could be considered either hate crimes or acts of domestic terrorism:

- In June 2015, Dylan Roof entered a Charleston, South Carolina church and after sitting with a bible study group, began shooting, killing nine people. In a manifesto discovered after his arrest, Roof declared a racial and ideological motivation for his crime, stating:

  > …I chose Charleston because it is the most historic city in my state, and at one time had the highest ratio of blacks to Whites in the country. We have no skinheads, no real KKK, no one doing anything but talking on the internet. Well someone has to have the bravery to take it to the real world, and I guess that has to be me . . . Black people are racially aware almost from birth, but White people on average don't think about race in their daily lives. And this is our problem. We need to and have to.[120]

- Wade Michael Page, a military Veteran involved with white supremacy groups and a founding member of a new-Nazi band, entered a Sikh temple in Wisconsin on 5 August 2012, and opened fire, killing six worshipers and injuring seven. Wade committed suicide without leaving behind a manifesto, however, he was tattooed with racist symbols that could also be indicative of alignment with a terrorist motivation.[121]

Each of these cases involved a U.S. citizen who executed a violent attack against U.S. persons on American soil at institutions of worship, but they were classified differently. A federal grand jury in South Carolina brought a 33-count indictment against Dylan Roof, including federal hate crimes and firearms offenses, but was not charged with domestic terrorism.[122] In Page's case, by contrast, local police stated that they were treating the act as a "domestic terrorist incident" and the FBI noted that they were looking into whether the act could be classified as domestic terrorism.[123]

---

[120] Dylann Roof, *The Last Rhodesian: The Manifesto's of Dylann Roof* (n.p.: Create Space Independent Publishing Platform, October 5, 2017).

[121] Megan Sullaway, "Hate Crime, Violent Extremism, Domestic Terrorism—Distinctions Without Difference?" In *The Psychology of Hate Crimes as Domestic Terrorism: U.S. and Global Issues*, edited by A. B.-M. Edward Dunbar (Santa Barbara, CA: Praeger, 2017), 89-121, https://psycnet.apa.org/record/2016-51715-003.

[122] Ibid.

[123] Steven Yaccino, Michael Schwirtz, and Marc Santora, "Gunman Kills 6 at a Sikh Temple near Milwaukee," *The New York Times*, August 5, 2012, https://www.nytimes.com/.

One approach to distinguishing between hate crimes and domestic terrorism focuses on the element of motivation for domestic terrorism, as defined in title 18 of the U.S. Code, §2331.[124] That statute provides that an act of domestic terrorism is one that is carried out to "influence the policy of a government by intimidation or coercion or to affect the conduct of government by mass destruction." Because the motivation for the terrorist act is to influence government policy, it may be perpetrated for reasons other than the bias or hatred that motivate hate crimes. In practice, however, this distinction may be difficult to make, as violent extremist ideologies that motivate acts of terrorism also may include elements of bias and hatred.

B. What are Prohibited Extremist Activities?

1. Principles and Considerations

The Department has a legitimate interest in regulating extremist behaviors and activities because violent and divisive actions are inconsistent with core military values such as dignity and respect, and risk undermining the military mission. Even advocacy and association with abhorrent ideologies can be destructive of the cohesiveness of the force and have the potential to weaken public support for the armed forces. For these reasons, the Department seeks to get "left of the bang" by identifying and addressing extremist behaviors and activities before they express themselves in specific criminal actions.

It is not easy to define "extremism" in terms that draw a clear line between behaviors and activities that are commonly viewed as unacceptable on the one hand, and acceptable participation in the disputes of a deeply divided society on the other. The problem is that "extremism" can be in the eye of the beholder, so that what may appear "extreme" to a person with one set of political or ideological beliefs may appear perfectly normal to a person of opposing beliefs. As described above, social and behavioral scientists have historically defined the term in reference to cultural norms and prevailing societal values—but what happens when society is deeply divided, and cultural norms appear to be either changing or in dispute?

Senior DOD officials interviewed by the IDA team generally described a spectrum of extremist behaviors and activities that could raise concerns, ranging from bigotry and intolerance to violent action. These leaders were less certain, however, as to which categories of the behaviors and activities they described should be prohibited by law or regulation. For example, some interviewees indicated that force or violence (or the advocacy of force or violence) is an essential element of any prohibition on extremism. Others disagreed. Some stated that mere membership in an extremist group should be prohibited, while others disagreed again. Figure 4 shows some of the

[124] E. Lee, "Hate Perspective on Terror: Domestic and International," Chap. 2 Vol. 3 in *The Psychology of Hate Crimes as Domestic Terrorism: U.S. and Global Issues*, edited by Edward Dunbar, Amalio Blanco, and Desirée. A. Crèvecoeur-MacPhail (Santa Barbara, CA: Praeger, November 2016): 37-62.

behaviors and activities described by senior officials, arranged on a scale from those that are seen as merely a cause for concern, to those that should be expressly prohibited.

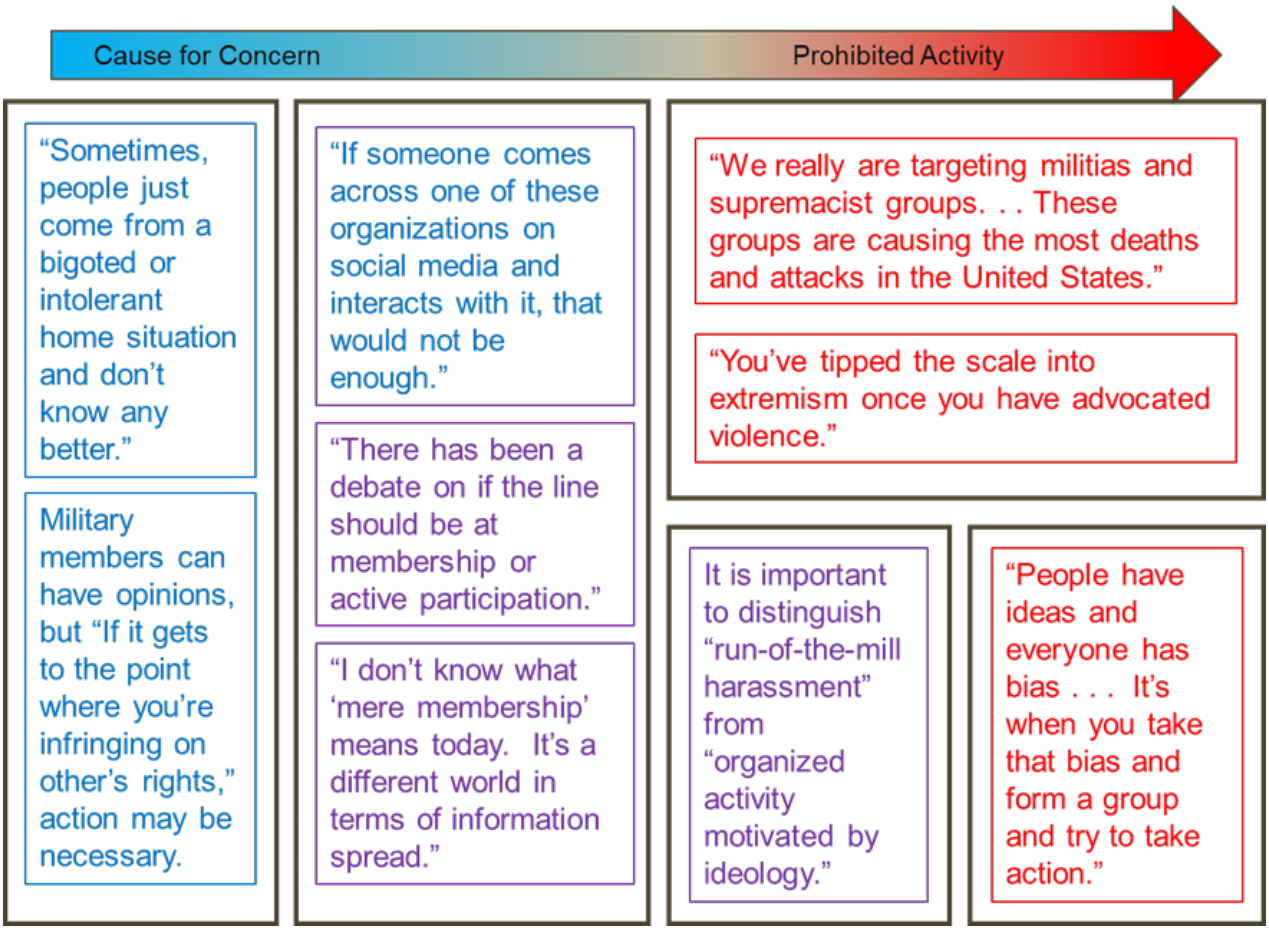


Figure 4. Spectrum of Potentially Extremist Behaviors and Activities

The difficulty in defining prohibited extremist behaviors and activities is exacerbated by the First Amendment to the United States Constitution, which protects freedom of speech and freedom of association. Largely because of the sensitivity of these fundamental rights and freedoms, violent extremism is not an enumerated crime in the United States, and even domestic terrorism statutes lack the teeth of statutes addressing international terrorism. Although the Supreme Court has determined that the "different character of the military community and of the military mission" require a unique application of these rights, the Court also concluded that "members of the military are not excluded from the protection granted by the First Amendment."[125]

Some DOD personnel interviewed by IDA suggested that First Amendment concerns could be avoided by defining extremist prohibitions in terms of conduct rather than the content of the views that serve as the basis for the conduct. For example, a definition could focus on the element of violence or force, prohibiting actions directed at achieving political or ideological objectives

[125] Parker v. Levy, 417 U.S. 733 (Supreme Court. 1974).

through unlawful force or violence without regard to the substance of the objectives or the views on which they are based.

Even a definition based on the element of violence raises difficult questions, however. Violent attacks on people or property are generally illegal, regardless of whether they are committed for political or ideological reasons, so what would be added by a separate crime of violent "extremism" that covers the same offenses? If advocacy of violence and membership in groups that advocate the use of violence are also prohibited (as they have been by DOD regulations) then a series of additional questions must be answered. For example:

- How far can DOD go in prohibiting advocacy or membership activities, even for members of the military, without violating First Amendment rights of speech and association?
- What level of intent is required for advocacy to be prohibited? Does the advocacy have to be knowing, willful, or committed with specific intent to lead to violence?
- Does the display of symbols (such as flags and tattoos) of organizations that are associated with violence constitute prohibited advocacy? If so, what constitutes a prohibited symbol and under what circumstances is it off limits?[126]
- What constitutes "membership" in a group that advocates or uses violence? Is passive attendance at events or is viewing of group websites enough?
- Does it matter whether the group is singularly dedicated to violence, or sometimes justifies violence in pursuit of a broader agenda (as has been the case with some environmental, animal, and anti-abortion rights groups)?

Other interviewees associated extremism with White Supremacism and other ideologies that advocate systematic discrimination. This emphasis is understandable in light of the Department's historic concerns about the penetration of the military by the Ku Klux Klan and other violent supremacist groups. White Supremacism poses a particular danger for the armed forces, which were integrated years before other major American institutions and rely on a racially diverse force to meet their military mission. While a prohibition directed at White Supremacist groups serves a legitimate military purpose, such a prohibition adds an element of content regulation to the Department's otherwise ideologically neutral regulations. Under a definition of extremism that includes ideological racism, members of the military who advocate depriving others of rights on

[126] Defining prohibited symbols can be as challenging as defining extremism. As an example, if displaying the Confederate flag is determined to be off limits, how far does that extend? Until January 2021, the Mississippi state flag included the flag of the Confederacy in its canton. If a service member from Mississippi had one of these recently retired state flags, would that be off limits? Taken to an extreme, one of the six historic flags of Texas was the Confederate flag, so would the logo of the Six Flags theme park (which was originally named for these six historic flags) be off limits? There is a spectrum of symbols from the problematic to the benign. Drawing a meaningful line between what is off limits and what is not, while also respecting First Amendment rights, is not a trivial task.

the basis of race, unlike advocates of other "extreme" political or ideological views, could be found to have engaged in prohibited behavior, even if they are entirely nonviolent.

The regulation of nonviolent speech on the basis of content becomes more extensive if the definition of prohibited extremist behaviors and activities is expanded to include hate-based activism on the basis of sex, sexual orientation, gender, and gender identity. The extension of prohibited extremist behaviors and activities to include advocacy offenses associated with sex and gender might also undermine some of the societal consensus on which extremism prohibitions have historically been based. While American society appears to broadly reject racism and sexism, societal views on issues of sexual orientation and gender identity remain deeply divided.

The inclusion of racist and sexist conduct in a definition of prohibited extremist behaviors and activities also raises a question about where the lines are between: (1) incidents of discrimination or harassment that invoke equal opportunity statutes and regulations; (2) individual hate crimes that are motivated by racism and sexism; and (3) and potentially criminal violations of prohibitions on extremist behaviors and activities. Discrimination and harassment on the basis of race and sex remain widespread to a troublesome extent in the military, as they are in American society as a whole.[127] By contrast, the number of documented extremist incidents in the military, as described in Chapter 3 of this report, appears to be quite low. One military interviewee told the IDA team:

> With what I see daily [from an internal military] reporting stream, I can see racial or sexually problematic behaviors. I see those regularly. . . . We have seen some racially-charged graffiti, but that's not labeled as extremism. The issues I dealt with as a commander have all been: (1) inappropriate hazing, but not usually bad hazing, (2) racial issues like inappropriate language, (3) inappropriate behavior like writing a nasty note about female colleagues . . . . I can't recall anything that would be considered extremist. You're making me think about what extremism actually is.[128]

One way to delineate extremism-based offenses from incidents of discrimination and harassment and hate crimes is to focus on the ideological component of the offense: extremist behaviors and activities can be viewed as those that are intended to propagate a world view or to achieve goals that are political, religious, discriminatory, or ideological in nature. For this reason, organization and advocacy could be seen as a key element of an extremist offense. This approach would help exclude individual hate-based offenses and discrimination cases, but excessive reliance on the element of motivation could also drive the Department closer to the risky ground of content regulation and prohibitions that are based as much on beliefs as actions.

---

[127] E.g., Blue Star Families, *2020 Military Family Lifestyle Survey Comprehensive Report: Finding 1* (Encintas, CA: Blue Star Families, Syracuse University, 2020), https://bluestarfam.org/wp-content/uploads/2021/03/BSF_MFLS_CompReport_FINDING_1.pdf, finding that 26% of non-white service members surveyed reported having experienced racial discrimination in their units and 48% of female service members surveyed reported having experienced gender-based discrimination in their units.

[128] Confidential Interview with IDA team.

In the absence of a consistently communicated definition that draws clear lines around prohibited extremist behaviors and activities, there is a risk that misinterpretations could lead to a significant division in the force along political and ideological lines. Several senior DOD officials interviewed by the IDA team reported that some of their subordinates believe that the Department's current focus on extremism is driven by "political correctness" and an unbalanced approach that targets only one side of the political spectrum. One senior officer worried that parts of the force view a campaign against extremism as "a finger in the chest, blaming people and saying what [isn't] acceptable." A second stated, with regard to the National Guard, "If you're in Idaho, you probably think this is targeting you. If you're an African American in Chicago, you may think it's about time."

The risk of misinterpretation is exacerbated by the fact that large sectors of the American public (and the military) rely heavily on partisan news sources and have become vulnerable to false information campaigns that are conducted through social media. For example, one participant in a discussion group told the IDA team, "According to a training guide from the government, I'm an extremist because I'm an evangelical Christian." He added, "What are we identifying? Who are we targeting? Why are we even doing it if the people in the room don't think it is an issue?" On further examination, it turned out that the "government training guide" to which the service member was referring was a 10-year-old briefing that did not reflect DOD policy at the time and has been forcefully disavowed by the Department.

2. Historic Definitions

DOD has made numerous efforts to develop policy, doctrine, and implementation tools addressing extremist activities in the force in response to a series of incidents over the last two decades. The IDA research team compiled 30 documents across the Office of the Secretary of Defense (OSD), the military services, and the Joint Staff that provide direction on behaviors related to extremism, on interventions, and/or on mitigation approaches. Together, these documents demonstrate the complexity of the problem, and the range of solutions DOD has chosen to pursue.

Despite the existence of these policy, doctrine, and implementation tools, DOD officials at all levels continue to express uncertainty as to the definition of extremism and the scope of activities that are prohibited. One senior DOD official told the IDA team, "The first question is what even *is* extremism?" A second began a discussion of extremism in the Department by saying, "If we could just get a damned definition . . ." A third stated, "There is a general frustration in the force—they want a definition." A fourth, when asked whether the definition of extremism is well-understood in the force, responded, "Absolutely not."

Concern about the lack of a standardized definition of extremism, with boundaries, was also a common theme for all ranks participating in discussion groups during IDA's visits to military installations. One participant stated, "The term 'extremist' is not helpful. Somebody should be telling us what the definition is. It's not a very helpful term." A second told IDA, "Even when they did the training, they didn't really have a definition." A third complained that extremism is difficult

to address because "There is not enough agreement about where the line is between strongly held opinions and extremism." Other participants agreed with these comments and added similar statements of their own.[129]

This section uses DOD policy, doctrine, and implementation tools to describe a spectrum of extremist activities and related behaviors. It also captures the range of interventions available across DOD to address these behaviors. We then break down the treatment of extremism into conceptual themes and analyze how common the themes are across these DOD documents. Finally, we explore how the concept of extremism has evolved over the last ten years. For the purpose of this analysis, the IDA team used a set of 30 DOD documents, of which 23 were machine-readable.

a. Spectrum of Extremism, Extremist Activities, and Related Behaviors

Taken together, DOD policies, doctrine, and tools cover an extremism spectrum that flows from ideology to expression to membership and active participation in extremist groups. On one end of the spectrum, constitutionally-protected rights make regulation of ideology and expression difficult. In particular:

- Military personnel are limited in the views that they may express in uniform or when the expression could be construed to represent the views of the military, but are generally free to have, and to express, their own political views in a personal capacity. While current policy documents do not generally seek to regulate privately-held beliefs or opinions, they do address ideologies that seek to deprive individuals of their rights.
- Generally speaking, regulations on speech and writing apply to social media as well, but with caveats specific to the kinds of information social media sites might contain. Military personnel may express private views on political issues, for example, so long as their affiliation with the military is not listed on the social media platform in which they are engaging.
- Military members may also host blogs, including blogs that permit comments. Service members remain unable to make disparaging comments against local, state, or federal leaders or engage in any discussion that is detrimental to the morale, discipline, or good order of the military; this rule applies across media types.
- A final type of expression addressed in policy documents is body markings/ornamentation. Gang or extremist markings or other ornamentation are expressly forbidden. Recruits are screened for such markings, and if they have them, they are either disqualified from service or subject to additional investigation to discern their level of fidelity to such organizations. Obscene or prejudicial markings may also be banned.

On the other end of the spectrum, violent behavior and active participation in violent organizations are much more readily prohibited. Based on the documents we surveyed, five different types of active participation in extremist organizations are likely to be prohibited:

- Proselytizing: Advocating for extremist organizations, distribution of materials, display of related paraphernalia;
- Fundraising: Raising money for extremist organizations, accepting donations in support of such organizations, donating to such organizations;
- Recruiting: Assisting extremist organizations in building the membership pool, training members, assuming a leadership role, or other means of growing the number and expertise of group members;
- Protesting/Demonstrating: Participating in demonstrations or protests in support of extremist groups or extremist causes, participating in any protest or demonstration while on duty, in uniform, or in a foreign country that breaches law and order or could result in violence; and
- Violence: Engaging in sabotage, sedition, violence against persons.

However, the policy documents appear to diverge when it comes to the question of membership in extremist organizations. In some documents "mere membership" is permitted, but "active participation" is not. In other documents, membership is cause at least for further investigation, and in some cases denial of service or revocation of security clearance. Several senior officials pointed out to the IDA team that it is not even entirely clear what "membership" in an extremist organization means, given that such organizations rarely have formal membership criteria or membership lists. Figure 5 shows the range of behaviors addressed in the policy documents.

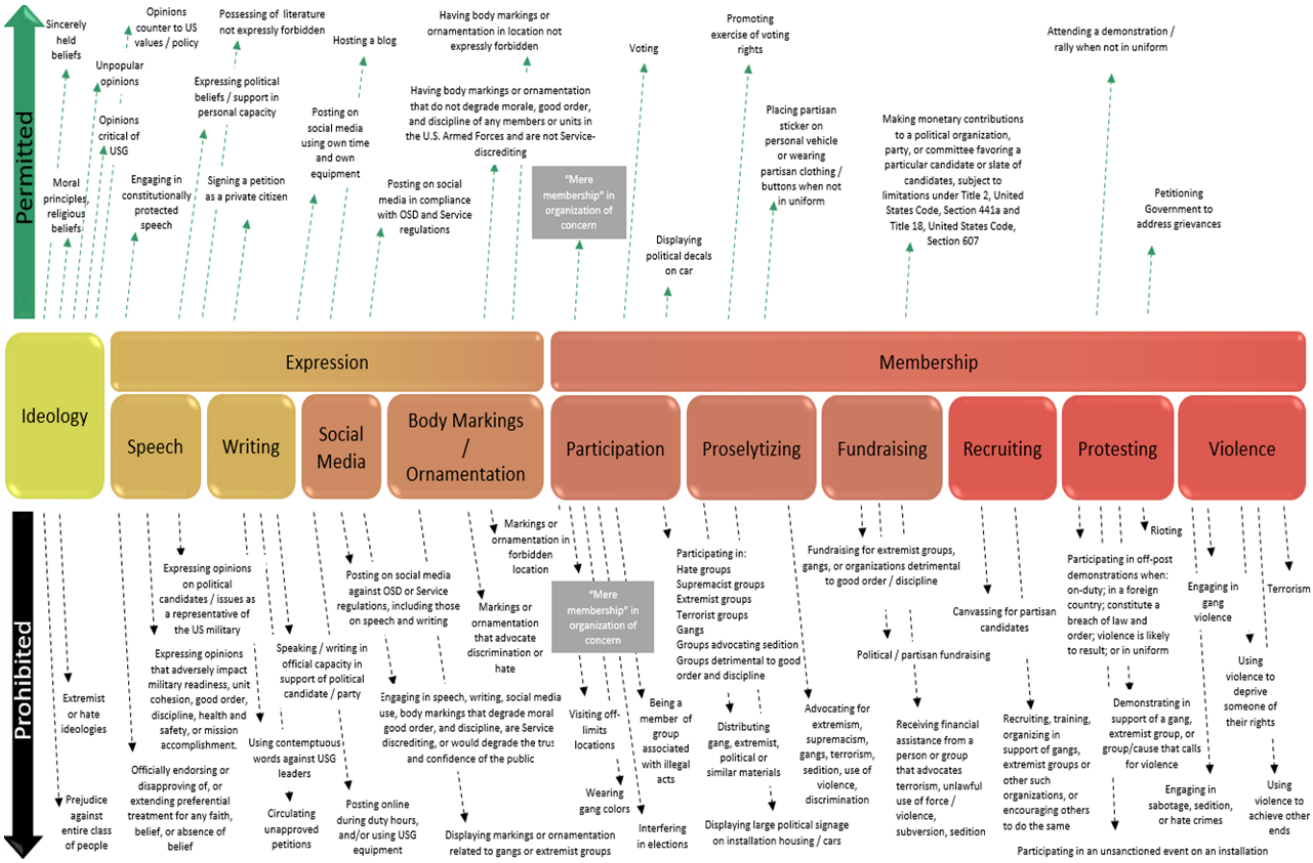


Figure 5. Spectrum of Extremist Activities

Existing policy, doctrine, and implementation tools also reference a range of interventions available to DOD and to service members. Formal mechanisms start at the time of recruitment with a series of screening activities designed to identify signs of extremist behavior or allegiance prior to enlistment. The outcome of these screening activities may include additional interviews, denial of security clearance, denial of service suitability, or all such actions. Members of the force are subject to periodic reviews, most frequently via the clearance renewal process, as well as encouragement to report extremism-related behavior. There are far fewer interventions aimed at the end of a service member's career to prepare them for transition out of the service.

Informal interventions are also available to commanders to respond to or prevent behaviors of concern. Preventive interventions include limitations on participation in events, travel to specific locations, or publications. Remedial interventions include counseling or reporting. These less formal approaches lack clear guidelines for when they ought to be implemented. Commanders are also responsible for reinforcing service values and building a culture in which extremist behaviors are not considered appropriate. A lack of clarity in the line between formal and informal interventions leaves commanders with significant discretion and could result in the uneven enforcement or application of intervention mechanisms.

Figure 6 shows the range of formal and informal interventions available in DOD policy documents.

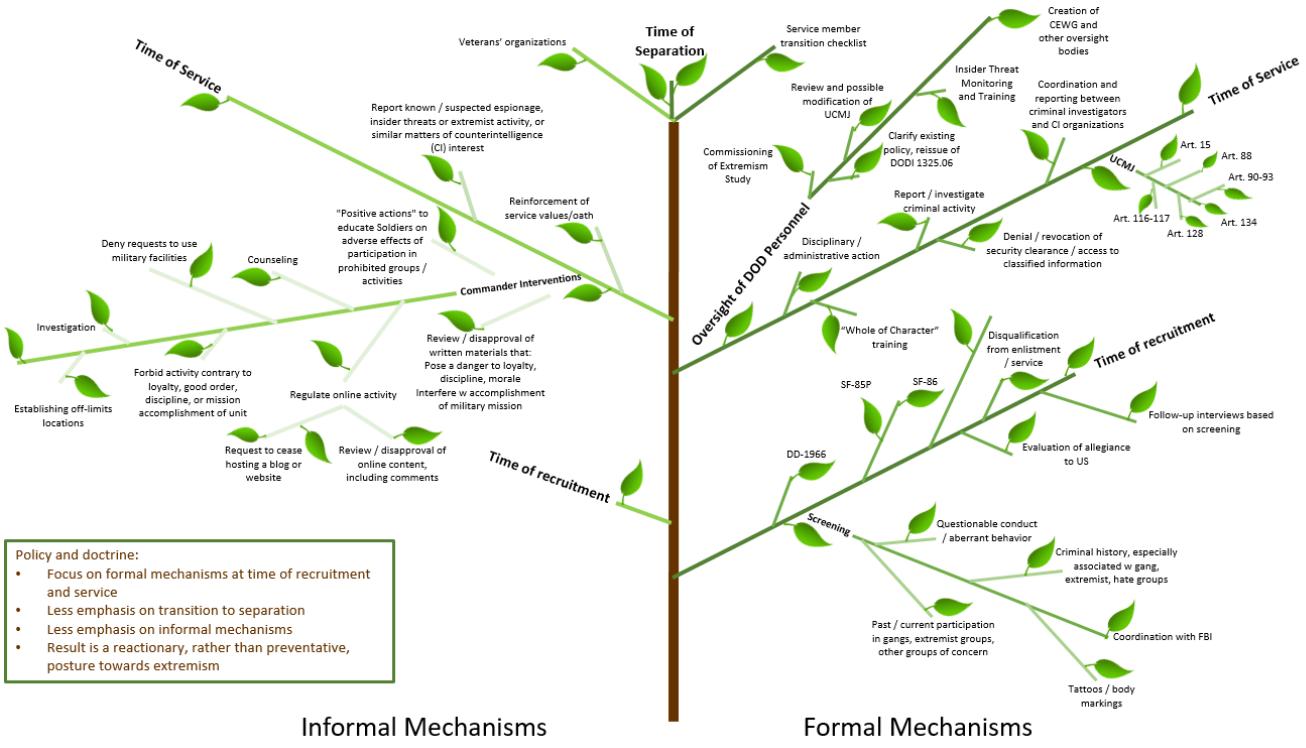


Figure 6. Extremism Interventions over the Career Life of Military Service Members

b. Consistency and Change across Policy Documents

While the themes addressed in DOD policy documents have been relatively consistent, the terminology used in those documents has been all over the map. For example, some documents require knowing or willful conduct (or even specific intent), while others are silent on the issue of state of mind. Some documents address individuals who "associate or sympathize with" extremist groups, while others address those who "support or advocate for," "participate actively in," or "help to organize" such groups. Some documents broadly address illegal efforts to "influence a policy" or "affect the conduct of government," while others focus more narrowly on "sabotage, espionage, treason, terrorism or sedition," and "efforts to overthrow or destroy the government."

Some of these terms are used in a single document; others are used in multiple documents. As far as IDA was able to determine, however, the only theme that is common to the full set of DOD policy documents is a prohibition on the use of unlawful violence.

The inconsistent terminology used by DOD policies on prohibited extremist activities is most likely a logical consequence of the manner in which these policies were developed. An Army policy is written in response to an event that takes place in the Army; a Marine Corps policy is written in response to a problem in the Marine Corps; a DOD-wide policy is written in response

to an event that captures the attention of senior DOD leaders. Because the policies were written at different times, by different leaders, in response to different events, it is not surprising that they use different terminology.

IDA analyzed DOD policy for thematic consistency and change over time to understand the many ways in which the Department has defined extremism. To do this, IDA identified 32 key themes divided into seven buckets that are addressed in the policy documents. The seven buckets are:

1. State of mind,
2. Nature of participation,
3. Type of group,
4. Desired outcomes,
5. Type of nonviolent activity addressed,
6. Type of violent activity addressed, and
7. Type of intervention authorized.

The seven buckets are shown in Figure 7, with the 32 themes arrayed in columns under the heading for each bucket. Within each bucket, bins are vertically sorted from most to least prevalent. Lighter colors are used for themes that are used more often, while darker colors are used for themes that are used less often. Of the 32 key themes, only one ("lone actors") is not present in any of the surveyed documents. This omission is illustrated in the figure with a gray color and a label of "0 Documents."

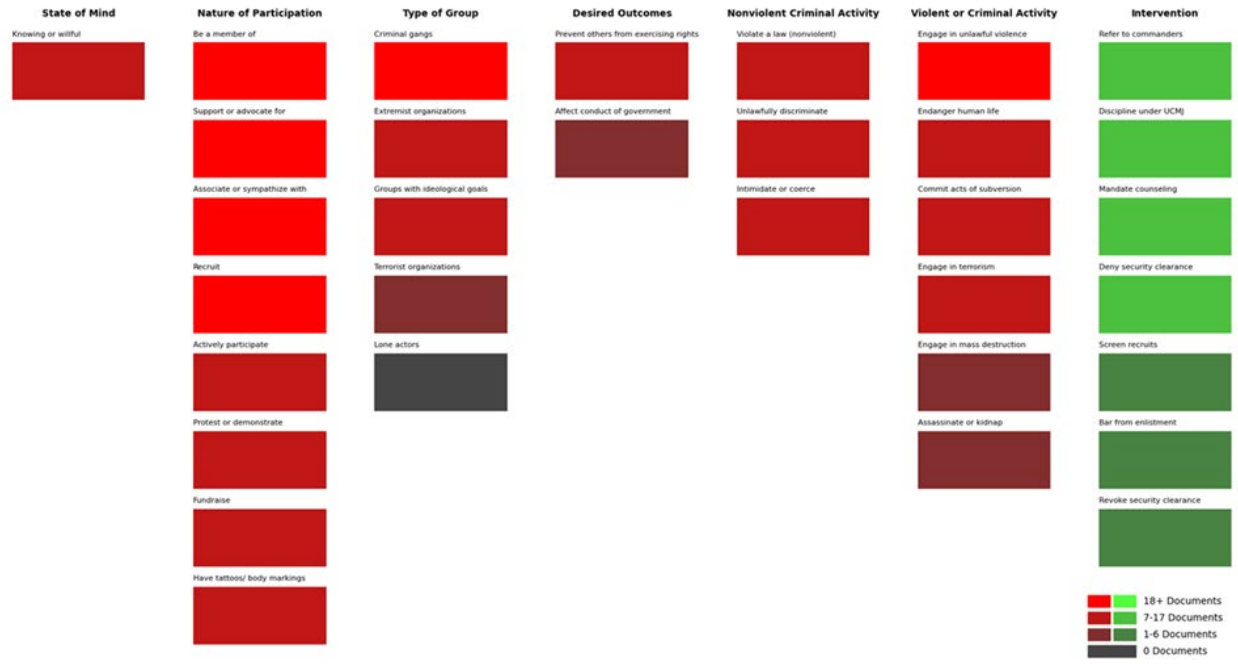


Figure 7. Extremism Themes in Policy Documents

While activities that might be labeled "extremist" can be discerned across the body of DOD policy documents we surveyed, these behaviors are not addressed uniformly or consistently. As the bin counts suggest, each nonviolent and violent activity bin is only covered by around half of the documents we surveyed. Buckets associated with the treatment of participation in gatherings, fundraising, and tattoos are also covered by only about half of the documents surveyed.

The types of interventions or consequences for engaging in a prohibited activity are similarly disjointed. 17 policies state that violations may be referred to commanders for further action (although it is worth noting that referral to the commander could lead to any or all of the other types of interventions listed). No other interventions appear in more than half of the documents. Only 11 state that service members may be either referred for counseling or prosecuted under the UCMJ, and fewer than ten mention denial or revocation of a security clearance. Some of the documents are specifically targeted to recruiters; in total, seven refer to the practice of screening prospective recruits, but only four explicitly state that applicants with known associations to extremist groups or activities may be barred from service.

IDA further reviewed the documents to assess the extent to which the Department's treatment of extremism has evolved over time. For each of the 32 themes, IDA developed a grid including the 23 documents in the IDA review that were published in a format with searchable text.[130] The order of documents is chronological (from bottom left to top right) and consistent across all grids.

[130] IDA reviewed 30 policy documents, of which 23 were searchable. The documents used in this analysis are listed in Appendix F.

A square is colored red for prohibited conduct (or green for interventions) if the given document references the topic and gray if not.[131] Note that the grid tracks documents, not years—with the eight most recent documents all being generated in 2021.[132]

The most dramatic change is seen in the approach to an actor's state of mind. Figure 8 illustrates which documents specify that participation in an extremist cause is only prohibited if it is knowing or willful. Before 2021, nearly every document addressed this issue. However, in the past year, limitations regarding state of mind have largely been omitted. As a result, certain activities may be prohibited even if they are conducted negligently or inadvertently; the Department may respond without having to demonstrate the actor's intent.

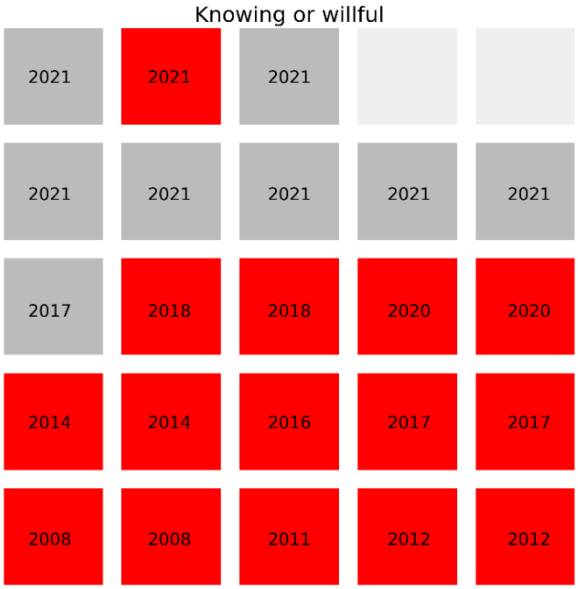


Figure 8. Treatment of State of Mind over Time

In other areas, the pattern is more difficult to discern, with the appearance of a patchwork approach continuing over time. Figure 9 shows the type of group or organization that is prohibited by each document. The majority of the policies specifically mention criminal gangs and extremist organizations, and nearly half make mention of groups with specific political, religious, or

[131] The key words and phrases used to develop this analysis are listed in Appendix G.

[132] Of the eight published in 2021, two are memoranda concerning the events of January 6, 2021 and the subsequent stand-down trainings. The remaining six documents are new or reissued organization policies or training materials, such as the revised version of DODI 1325.06. While the context of these six documents is similar to the documents published in earlier years, the increased number may be indicative of a shift in the Department's focus.

ideological goals. However, only one document specifically mentions terrorist organizations, and none discuss lone actors.[133]

Figure 9. Groups and Organizations of Concern over Time

Figure 10 illustrates the types of participation addressed in each policy. Almost all of the documents outline guidance regarding support or advocacy for extremist or supremacist causes. The majority also prohibit actively participating, supporting, or advocating for extremist causes, in addition to recruiting new members to join an extremist organization. Fewer documents address fundraising in support of an extremist cause or having tattoos or other body markings with extremist or supremacist themes. Approximately half of the policies outline guidelines regarding permitted and prohibited participation in protests or demonstrations. Five of the documents cover all of the topics examined in this category. Overall, the prohibited types of actions are defined fairly comprehensively across the entire corpus.

[133] A number of the documents broadly prohibit acts of terrorism without the stipulation that the actor must be a member of a known terrorist group or organization. Because this figure only concerns groups, those documents are not included here. Figure 13 includes a broader perspective of the policies that mention terrorism in any capacity.

Figure 10. Nature of Participation – Prohibited Activities and Behaviors

Figure 11 addresses the intended outcomes of prohibited extremist activities. More than half of the documents specified that any action taken with the intention of depriving other people of their rights is prohibited. A smaller number of documents also stated that any attempt to overthrow the government or otherwise disrupt government operations is prohibited. When compared to how these documents address participation and violence, it is clear that policy concerns itself with observables—the actions and behaviors that may suggest extremist tendencies—rather than what outcomes those actions are designed to affect. In other words, policy documents are more likely to focus on the what rather than the why.

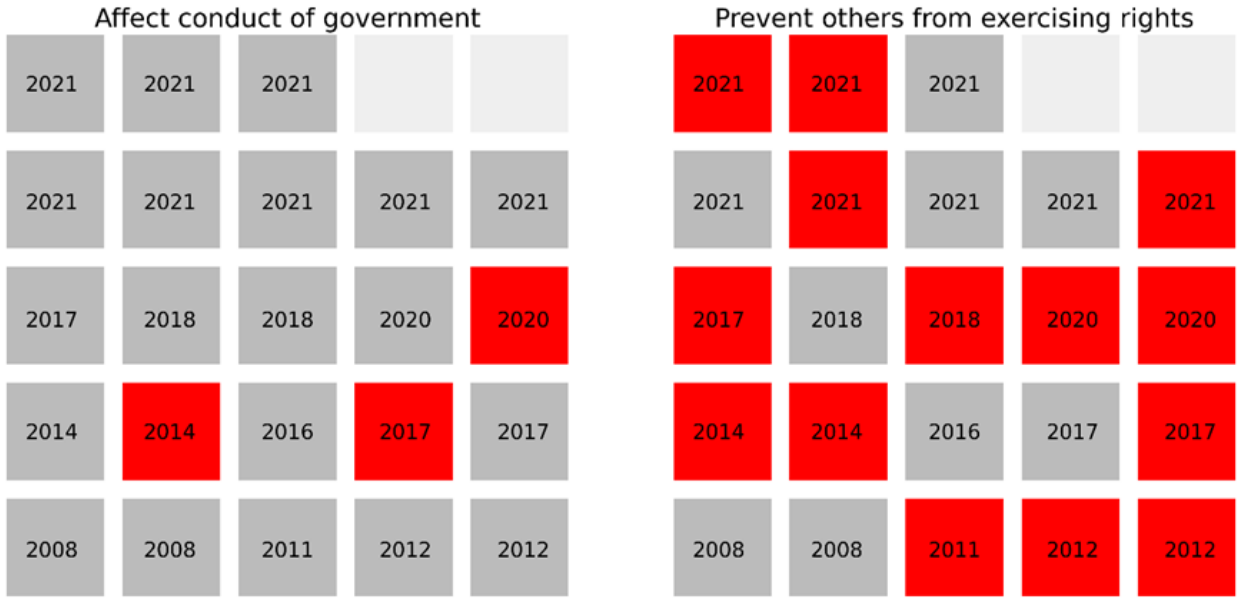


Figure 11. Intended Outcomes over Time

Figures 12 and 13 address two categories of prohibited actions: nonviolent criminal activities and acts of violence. In the case of nonviolent criminal activities (Figure 12), the majority of the documents include an overarching prohibition of any nonviolent illegal activity. A smaller number of policies also prohibit any form of unlawful discrimination, a focus that appears to have increased in policy documents over the last five years. A handful of earlier documents address intimidation and coercion, but this emphasis appears to have been virtually eliminated in 2021. Coverage of violent activities (Figure 13) is similarly disjointed. Though all documents prohibit the use of unlawful violence, the documents are inconsistent in their coverage of other actions, including assassination, kidnapping, subversion/treason/sedition, terrorism, mass destruction, and other acts that endanger human life.

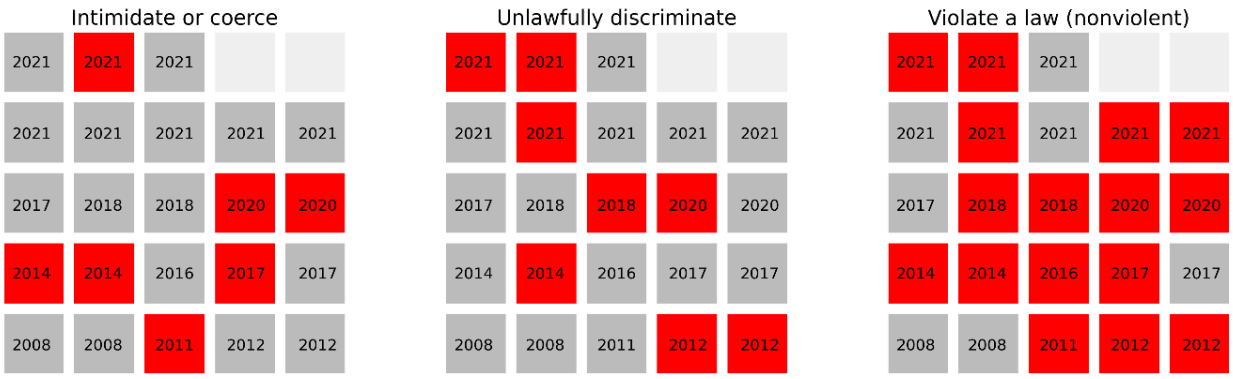


Figure 12. Prohibited Nonviolent Criminal Activity

Figure 13. Violent Activities

Finally, Figure 14 shows the range of potential interventions that are authorized in response to a violation of policy. Roughly two-thirds of the documents authorize referral to commanders for further action, but beyond that the policy is inconsistent. About half reference prosecution under the UCMJ, and about half provide that the commander may mandate counseling for the service member. A smaller number of policy documents reference actions such as barring enlistment or denying security clearances. This inconsistency in the document does not mean that the measures available to the services vary in practice, but it does show that the Department has failed to send clear signals as to its expectations.

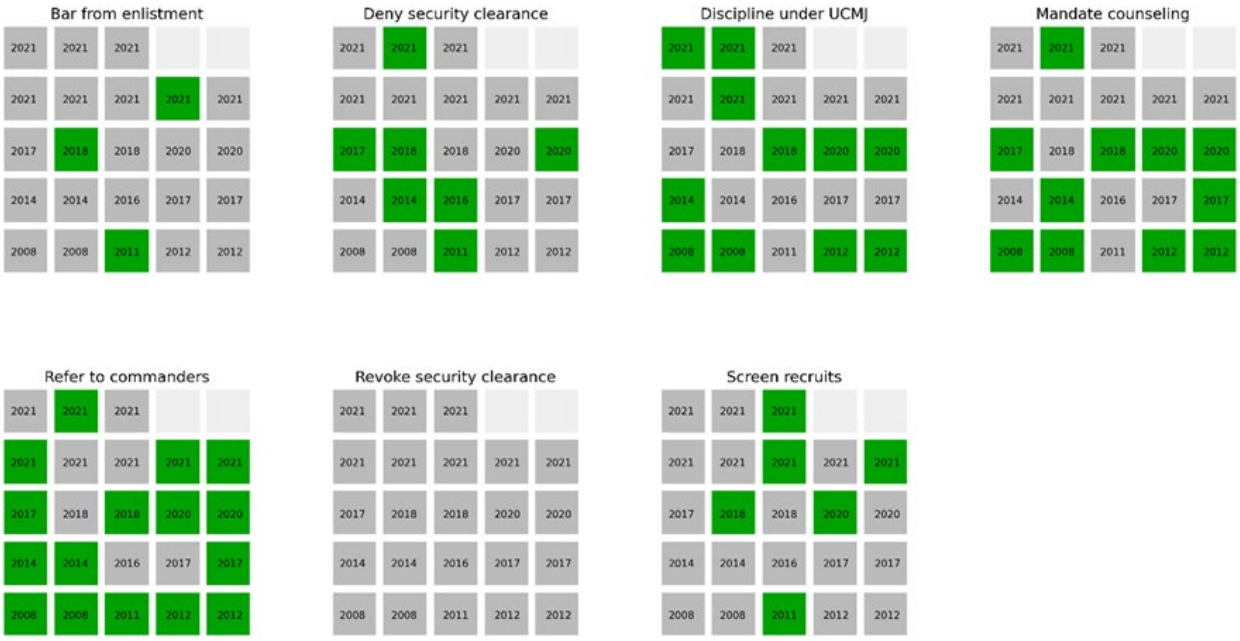


Figure 14. Range of Interventions to Counter Extremist Activity

The bottom line is that although the DOD has a large number of policies regarding extremist conduct and affiliations, the content of these policies has been an inconsistent patchwork. The discrepancies among these documents create a risk that prohibitions against extremist activities will be unevenly enforced across the Department. An even greater risk may be that the Department's message is muddied by the inconsistency in its policies. In the absence of a clear and consistent message from the Department, members of the Armed Forces are left in doubt as to what is prohibited and may be more susceptible to messaging from outside entities with their own agendas.

3. The New DOD Definition

Over the last year, the Department responded to uncertainty over the definition of extremism and the scope of prohibited behaviors and activities by establishing a cross-functional team comprised of senior officials from the OSD, the Joint Staff, and the military services to review and update the DOD Instruction that defines prohibited extremist activities. The revised DODI 1325.06, published on 20 December 2021, provides a comprehensive definition of prohibited extremist activities that is much improved from previous definitions.[134]

[134] The full text of the definition is as follows: "The term 'extremist activities' means:

"(a) Advocating or engaging in unlawful force, unlawful violence, or other illegal means to deprive individuals of their rights under the United States Constitution or the laws of the United States, including those of any State, Commonwealth, Territory, or the District of Columbia, or any political subdivision thereof."

The new definition includes four types of actions that constitute "prohibited extremist activities" when they have the objective of promoting several categories of improper or illegal objectives. Figure 15 shows the relationship between the four categories of actions (shown on the left) and the illegal objectives (shown in the middle and on the right).

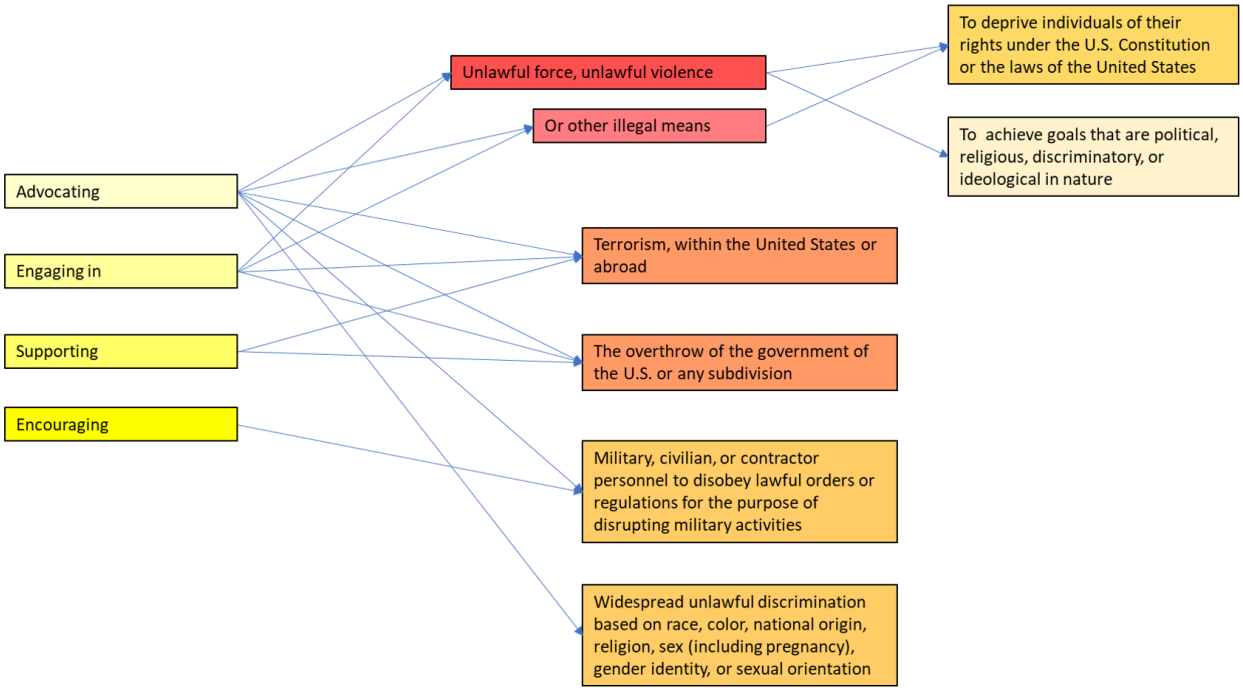


Figure 15. Schematic of DODI 1325.06 Definition of Prohibited Extremist Activities

Of the four types of covered actions, three are advocacy activities implicating rights of speech and association ("advocating," "supporting," and "encouraging"), while the fourth ("engaging in") entails direct participation in illegal activities. Of the categories of illegal objectives, two are violent in nature (use of "unlawful force and violence" and "terrorism"), and two are by nature

---

"(b) Advocating or engaging in unlawful force or violence to achieve goals that are political, religious, discriminatory, or ideological in nature."

"(c) Advocating, engaging in, or supporting terrorism, within the United States or abroad."

"(d) Advocating, engaging in, or supporting the overthrow of the government of the United States, or any political subdivision thereof, including that of any State, Commonwealth, Territory, or the District of Columbia, by force or violence; or seeking to alter the form of these governments by unconstitutional or other unlawful means (e.g., sedition)."

"(e) Advocating or encouraging military, civilian, or contractor personnel within the DOD or United States Coast Guard to violate the laws of the United States, or any political subdivision thereof, including those of any State, Commonwealth, Territory, or the District of Columbia, or to disobey lawful orders or regulations, for the purpose of disrupting military activities (e.g., subversion), or personally undertaking the same."

"(f) Advocating widespread unlawful discrimination based on race, color, national origin, religion, sex (including pregnancy), gender identity, or sexual orientation."

inconsistent with the duties and responsibilities of service members ("overthrow of the government" and disobeying orders "for the purpose of disrupting military operations (e.g., subversion)").

The remaining categories of illegal objectives are directed at White Supremacism and other forms of systematic discrimination. These include the use of "other illegal means" to deprive individuals of their legal rights, and advocacy of "widespread unlawful discrimination based on race, color, national origin, religion, sex (including pregnancy), gender identity, or sexual orientation." These categories reveal the difficulty of defining inappropriate supremacist activities in a manner that distinguishes such conduct from individual hate crimes and other acts of bias and discrimination. With regard to the first category, it is not immediately clear what "illegal means," other than force or violence, the provision is intended to address. With regard to the second category, the phrase "widespread unlawful discrimination" may successfully differentiate advocacy for systematic actions against a protected class from individual acts of bias or discrimination, but also risks being interpreted broadly to bar some forms of legitimate public discourse.

A recent commentary in *Breaking Defense* noted that there is currently an active public debate on the legitimacy of a number of historic policies based on sex, sexual preference, gender, and gender identity. As the law has changed in more than one direction over time, the characterization of some forms of discrimination as "unlawful" is not likely to put an end to the debate:

> Would a statement questioning the role of transgender individuals in the military be considered "violent extremism?" The Biden administration regards discrimination against transgender people as illegal. What about a statement arguing that pregnancy hurts readiness? Discrimination against pregnant women is illegal. Such sentiments have been legitimate topics for discussion in the past, even if today official policy and most senior officials disagree.
>
> "Military journals are full of articles questioning and even opposing current policies. That's how militaries adapt to changing circumstances. Thus, how this provision is applied will be important to the intellectual life of the military services. One overzealous censor could stifle a lot of intellectual activity.[135]

In order to violate the new policy, a service member must "actively participate" in an extremist activity. As noted above, the Department seeks to get to "the left of the bang" by identifying and addressing extremist behaviors and activities before they express themselves in specific criminal acts. For this reason, the revised DODI 1325.06 defines "active participation"

[135] Mark Cancian, "A Year After January 6, DoD's Vague Extremism Definition Could set up New Problems," *Breaking Defense,* January 6, 2022, https://breakingdefense.com/2022/01/a-year-after-jan-6-dods-vague-extremism-definition-could-set-up-new-problems/. The concerns expressed in this article could be mitigated by the glossary in DoDI 1325.06, which defines the phrase "widespread unlawful discrimination" to exclude "lawful efforts to overturn, amend, or enact laws applicable to discrimination or lawful support for causes or organizations that engage in such efforts." In practice, however, it may be difficult to distinguish between prohibited advocacy (e.g., "people like you shouldn't be allowed to serve in the military") and protected advocacy (e.g., "there should be a law saying that people like you shouldn't be allowed to serve in the military").

broadly to prohibit individuals not only from personally advocating or engaging in extremist activities, but also from 14 different categories of encouragement or support to extremist endeavors, as shown in Figure 16.[136]

[136] The full text of the definition is as follows: "For purposes of this section, the term "active participation" means the following, except where such activity is within the scope of an official duty (e.g., intelligence or law enforcement operations):

"(a) Advocating or engaging in the use or threat of unlawful force or violence in support of extremist activities."

"(b) Advocating for, or providing material support or resources to, individuals or organizations that promote or threaten the unlawful use of force or violence in support of extremist activities, with the intent to support such promotion or threats."

"(c) Knowingly communicating information that compromises the operational security of any military organization or mission, in support of extremist activities."

"(d) Recruiting or training others to engage in extremist activities."

"(e) Fundraising for, or making personal contributions through donations of any kind (including but not limited to the solicitation, collection, or payment of fees or dues) to, a group or organization that engages in extremist activities, with the intent to support those activities."

"(f) Creating, organizing, or taking a leadership role in a group or organization that engages in or advocates for extremist activities, with knowledge of those activities."

"(g) Actively demonstrating or rallying in support of extremist activities (but not merely observing such demonstrations or rallies as a spectator)."

"(h) Attending a meeting or activity with the knowledge that the meeting or activity involves extremist activities, with the intent to support those activities:"

"(1) When the nature of the meeting or activity constitutes a breach of law and order;"

"(2) When a reasonable person would determine the meeting or activity is likely to result in violence; or"

"(3) In violation of off-limits sanctions or other lawful orders."

"(i) Distributing literature or other promotional materials, on or off a military installation, the primary purpose and content of which is to advocate for extremist activities, with the intent to promote that advocacy."

"(j) Knowingly receiving material support or resources from a person or organization that advocates or actively participates in extremist activities with the intent to use the material support or resources in support of extremist activities."

"(k) When using a government communications system and with the intent to support extremist activities, knowingly accessing internet web sites or other materials that promote or advocate extremist activities."

"(l) Knowingly displaying paraphernalia, words, or symbols in support of extremist activities or in support of groups or organizations that support extremist activities, such as flags, clothing, tattoos, and bumper stickers, whether on or off a military installation."

"(m) Engage in electronic and cyber activities regarding extremist activities, or groups that support extremist activities – including posting, liking, sharing, re-tweeting, or otherwise distributing content – when such action is taken with the intent to promote or otherwise endorse extremist activities. Military personnel are responsible for the content they publish on all personal and public Internet domains, including social media sites, blogs, websites, and applications."

"(n) Knowingly taking any other action in support of, or engaging in, extremist activities, when such conduct is prejudicial to good order and discipline or is service-discrediting."

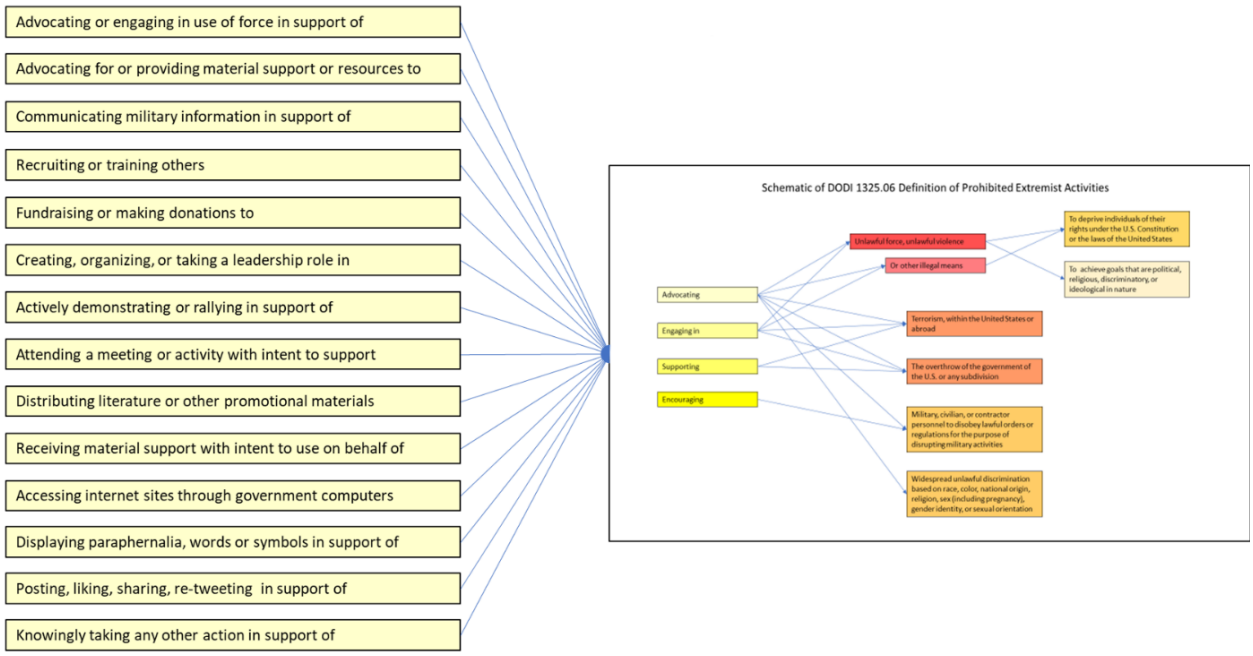


Figure 16. Schematic of DODI 1325.06 Definition of Active Participation

These categories cover a broad range of participatory actions, including:

- A high-end of violent action ("use of force in support of") and leadership ("creating, organizing, or taking a leadership role");
- A middle-tier of active membership-type activities ("attending a meeting or activity with intent to support;" "distributing literature or other promotional materials"); and
- A low-end of what appear to be mere expressions of support ("displaying paraphernalia, words, or symbols . . . such as flags, clothing, tattoos, and bumper stickers;" "posting, liking, sharing, re-tweeting" in support of).

The inclusion of low-end expressions of active participation gives the Department the ability to identify and address extremist behaviors and activities before they express themselves in specific criminal acts. For example, it is not hard to see why the Department would want to act against a service member who posts electronic communications in favor of terrorism or the overthrow of the United States government before the individual takes concrete steps to act on those beliefs.

When layered on top of the broad definition of extremist activities, however, these low-end categories of active participation risk over-broad interpretation. For example, the prohibition on electronic communications appears to cover "liking" a social media site that advocates widespread illegal discrimination on the basis race, color, national origin, religion, sex (including pregnancy), gender identity, or sexual orientation. An argument could be made that such sites could include

websites of major political parties and well-established religions that oppose gay marriage or the use of gendered restroom and shower facilities by transgender males and females.

While there is little risk that members of the military will be punished for expressing support for a mainstream political party or religion, the fact that the regulation *could* be read this way demonstrates the acute difficulty of developing any definition that draws clear lines between extremist activities that threaten good order and discipline and the expression of views that is the right of every American, including members of the military. It also exacerbates the risk that some members of the force could feel targeted by the Department's focus on prohibited extremist activities. These continuing issues should not be taken as an indication that the new definition is defective, but rather as an indication that *any* definition that seeks to codify prohibited extremist activities in the absence of a strong societal consensus on social and political issues is likely to be problematic.

While the comprehensive definitions in revised DODI 1325.06 are a substantial improvement on the definitions included in earlier regulations, most of the old patchwork remains in place. As of the time that IDA concluded its field work, the extremism policies of the military services had yet to be updated to incorporate the new definitions. Similarly, defense-wide policies pertaining to security clearances, suitability determinations, access to facilities insider threats, use of social media, and related topics remain unchanged and may continue to contain language inconsistent with the new definitions. Until these policies are appropriately updated, they are likely to contribute to continued confusion over the scope of prohibited activities.

C. Findings and Recommendations

The IDA team concludes that DOD policies have used a wide variety of words, phrases, and concepts to describe prohibited extremist behaviors and activities. As a result, service members and employees at all levels who participated in IDA interviews and discussion groups are unaware of or are confused about existing definitions and standards. In the absence of a clear definition, there is also a risk that some members of the military will feel "targeted" by the Department's focus on extremism. The Department recently published an improved definition of prohibited extremist activities in revised DODI 1325.06. Although the new instruction appears to provide as clear of a definition as is possible, this definition has yet to be reflected in other policies of the Department.

While the Department has published new guidance on prohibited extremist activities, it does not appear to have developed a comprehensive plan for communicating that guidance to the force. The absence of a strong communication plan creates a risk of misunderstanding that could result in continued confusion and concern in the force. IDA's site visits revealed that many service members develop their own understandings of what "extremism" means, and that those understandings are sometimes influenced by outside sources. As a result, the new DOD policy could be viewed by segments of the force as a "politically correct" effort to tell them what they can and cannot think.

For these reasons, the IDA team recommends that the Department take steps to:

- Ensure that prohibited extremist behaviors and activities are consistently defined throughout the Department.
- Consistently link prohibitions on extremist behaviors and activities to a broader context, emphasizing the need to bridge differences and build a united, disciplined fighting force comprising of individuals with diverse backgrounds and opinions.
- Clarify the line between individual racist/harassment/bullying offenses and cases of prohibited extremist behavior.

The implementation of these recommendations cannot be accomplished through a single action but will require a concerted effort over a period of time. While IDA is not in a position to design a comprehensive course of action for each recommendation, the IDA team has developed a number of implementation options for the Department's consideration. These options are described below.

Recommendation 1: Build on the new definition of prohibited extremist activities in DODI 1325.06 to ensure that prohibited extremist behaviors and activities are consistently defined throughout the Department.

To implement this recommendation, the Department should consider the following options:

- The Secretary could direct the Secretaries of the Military Departments to ensure that the new definition of prohibited extremist behaviors and activities in DODI 1325.06 is fully and accurately reflected in the policies and directives of the military services (and require that the new policies be reviewed by the Under Secretary of Defense for Personnel and Readiness (USD(P&R)) for consistency with the DOD policy).
- The Secretary could direct the Principal Staff Assistants to ensure that policies and directives under their respective purviews pertaining to security clearances, suitability determinations, access to facilities, insider threats, use of social media, and related topics are updated to fully and accurately reflect the new definition of prohibited extremist behaviors and activities in DODI 1325.06.

Recommendation 2: Consistently link prohibitions on extremist behaviors and activities to a broader context, emphasizing the need to bridge differences and continue to build a united, disciplined fighting force comprising of individuals with diverse backgrounds and opinions.

To implement this recommendation, the Department should consider the following options:

- The Secretary could develop a comprehensive communication plan to educate the force on the new definition and place it in the appropriate context of core military values.
- The Secretary could direct the military services, in consultation with the Secretary's Senior Advisor for Human Capital and Diversity, Equity, and Inclusion, to promote inclusion, tolerance, and respect in the force by opening channels of communication through a series of "necessary conversations," along the lines set forth by the Chief of

Naval Operations (CNO) in July 2020. As described in the Navy publication, such conversations would not be one-time occurrences, would be planned but open-ended, would take place in an environment that encourages sharing, and would be conducted pursuant to ground rules that ensure respect for a variety of perspectives.

- The Secretary could ask that senior DOD officials –
  - Refer to "prohibited extremist behaviors and activities" rather than simply "extremism" in legal or policy documents, testimony, training, or discussions with the force to emphasize actions that are inappropriate (rather than viewpoints that although different may be within Constitutionally-protected bounds); and
  - Make every effort to put prohibitions on extremist behaviors and activities in a broader context of the need to uphold core military values, preserve the value of a diverse fighting force to national security, maintain good order and discipline, and treat service members of all backgrounds and opinions with dignity and respect.
- The USD(P&R) could draft a simple one- or two-paragraph explanation of the basis for prohibitions on extremist behaviors and activities that places the prohibitions in the broader context of the need to uphold core military values, preserve the value of a diverse fighting force to national security, maintain good order and discipline, and treat service members of all backgrounds and opinions with dignity and respect. An explanation along the following lines could be considered:

  The U.S. military appropriately reflects the full range of backgrounds and opinions that shape American society. Service members have every right to their own opinions, including opinions that may appear extreme or even distasteful to others, as long as those views do not express themselves in behaviors and activities that undermine good order and discipline or other core military values.

  However, the actual or threatened use of unlawful force or violence in an effort to change government policy is inconsistent with a service member's oath of office and the core value of loyalty to the Nation. The use or advocacy of illegal means to deprive others of their rights on the basis of race, gender, or ethnicity is inconsistent with the core values of teamwork and respect and undermines efforts to build a cohesive force. DOD Directive 1325.06 prohibits extremist behaviors and activities that conflict with these core values.
- The Secretary could ask that senior DOD leaders incorporate the policy explanation into their communications regarding prohibited extremist behaviors and activities to the maximum extent appropriate.
- The Secretary could direct the military services and other DOD components to ensure that the policy explanation is incorporated into their training materials on prohibited extremist behaviors and activities to the maximum extent practicable.

Recommendation 3: Clarify the line between individual offenses of prejudice/harassment/bullying and cases of prohibited extremist behavior. Not all misconduct is extremist and reporting individual incidents as prohibited extremism may give a distorted picture of the role and influence of extremist groups in the Department.

To implement this recommendation, the Department should consider the following options:

- The USD(P&R) could develop guidance, including a set examples of cases, describing conduct that should be addressed as prohibited extremist activities, and cases that constitute racist/harassment/bullying, but fall short of prohibited extremist activities. For example, the guidance and examples could illustrate the distinctions:
  - Between opinions and actions,
  - Between individual behaviors and organized activities,
  - Between advocacy and violent action, and
  - Between one-off actions and concerted systematic behaviors.
- The Under Secretary could develop guidance, including a set of examples of cases, describing actions that do not rise to the level of prohibited extremist activities, but suggest the potential for future violations. Such examples could include:
  - Insensitive or offensive use of language,
  - Aggressive or harassing speech, and
  - Intolerance or disrespect for the views of others.
- The Under Secretary could direct the military services to use the examples in training and education materials, and in guidance to those who collect and report information on cases of prohibited extremist activities.
- The Under Secretary could establish a cross-functional team from across the Department to assist in the development, validation, and updating of the examples.

5. Pathways to Extremist Ideology and Behavior

The Project Description for this study calls for IDA to "identify pathways of extremist ideology and behavior broadly and within the Department in particular," and to "assess why the DOD workforce and the military community (including veterans) might be susceptible to recruiting by extremists." The hope is that research that increases our understanding of the various pathways to radicalization may serve as a guidepost to the development of tools and approaches to prevent or mitigate the likelihood for radicalization and incidents of extremist behaviors and activities.

This chapter provides an overview of the risk and vulnerabilities to radicalization by first examining potential risk factors for radicalization and the development of risk assessment tools based on these risk factors. Further, because of the increased role that social media and the internet play in in communication, we describe how false information and conspiracy theories can lead to radicalization. Next, we consider strategies to counter radicalization by leveraging lessons from outside DOD on how to build resiliency within communities and the role of threat assessment teams in mitigating radicalization and risk of violence. Then, we apply these lessons to DOD by exploring how to increase resiliency in service members and the role risk assessment plays in mitigating both forms of violence and insider threats within the Department. We extend these findings to mitigating the risk of radicalization post-service by focusing on transition and support systems for veterans. Finally, we summarize the findings of this chapter and provide evidence-based recommendations for reducing the risk of radicalization in the Armed Forces.

A. Risks and Vulnerabilities to Radicalization and Extremist Action

1. Push, Pull, and Personal Factors

Radicalization is a dynamic cognitive and behavioral process through which individuals develop extremist ideologies, beliefs, and affect, which can lead to extremist actions or behaviors.[137] More than 50 years of research shows that there is no single pathway or explanatory theory for radicalization that can apply to all individuals (or groups) and that radicalization is influenced by a number of factors.[138] Radicalization is not "the product of a single decision but the

[137] Bartlett, Birdwell, & King, *The edge of violence*; Borum, "Radicalization in Violent Extremism I."

[138] Randy Borum, *Psychology of Terrorism* (Tampa, FL: University of South Florida., 2004); Borum, "Radicalization in violent extremism I."

end result of a dialectical process that gradually pushes an individual towards a commitment to violence over time."[139]

As a dynamic, multi-stage, and multi-faceted process, radicalization is influenced by individual push, pull, and personal factors in an enabling environment.

- *Push factors* are real or perceived factors external to the individual that serve as drivers that push the individual towards radicalization. Push factors include structural, political, and sociological contexts such as lack of socioeconomic opportunities, marginalization and discrimination, prolonged and unresolved conflicts, and poor governance.
- *Pull factors* are group-level socio-cognitive factors that draw the individual to seek information, experiences, and other individuals that align with extremist ideology, thus pulling the individual towards radicalization. Pull factors include extremist ideology, group belonging, and other incentives that make adhering to extremist ideologies or joining extremist groups appealing to some people.
- *Personal factors* are individual characteristics and experiences (psychological and biographical) that make some individuals more vulnerable to radicalization than their peers. Personal factors include psychological disorders, personality traits, and traumatic experiences.[140]

Push, pull, and personal factors are interrelated: the structural and contextual conditions identified by push factors can also serve as a root cause for pull and personal factors.[141] For example, poverty (a push factor) might contribute to an individual's low self-esteem (a personal factor), which might boost the desire to belong to a group (a pull factor).

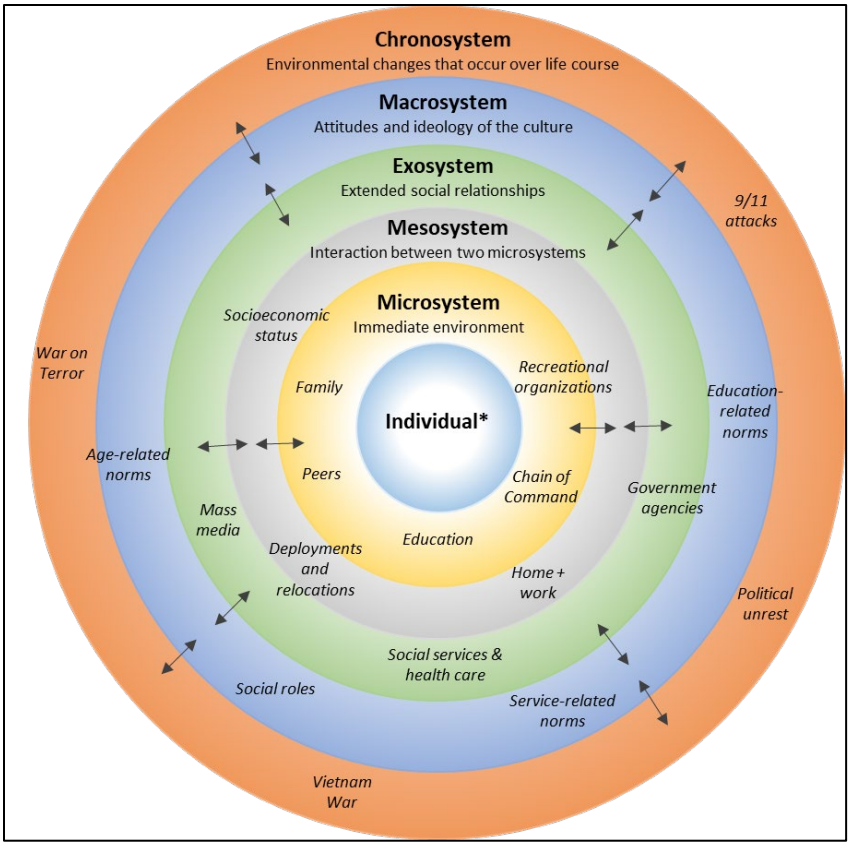
These drivers of radicalization operate at the level of the individual, group/community, and society, and some drivers can resonate and operate across all three levels. Figure 17 shows a modified version of Bronfenbrenner's diagram of his bioecological model for human development to show the relationships between drivers and the levels at which they operate.

---

[139] Gordon H. McCormik, "Terrorist Decision Making," *Annual Review of Political Science* 6 (June 2003): 492, doi:10.1146/annurev.polisci.6.121901.085601.

[140] Adrian Cherney, Idhamsyah E. Putra, Vici Sofianna Putera, et al., (2021). "The Push and Pull of Radicalization and Extremist Disengagement: The Application of Criminological Theory to Indonesian and Australian cases of Radicalization," *Journal of Criminology* 54, no. 4 (July 30, 2021): 407-424, doi:10.1177/26338076211034893; Rositsa Dzhekova, Mila Mancheva, Nadya Stoynova, and Dia Anagnostou, *Monitoring Radicalization: A Framework for Risk Indicators* (Sofia, Bulgaria: Center for the Study of Democracy, February 2017); Matteo Vergani, Muhammad Iqbal, Ekin Ilbahar, and Greg Barton, (2020). "The Three Ps of Radicalization: Push, Pull and Personal. A Systematic Scoping Review of the Scientific Evidence about Radicalization into Violent Extremism," *Studies in Conflict & Terrorism* 43, no. 10 (2020): 854-885, doi:10.1080/1057610X.2018.1505686.

[141] Vergani, Iqbal, Ilbahar, and Barton, "The Three Ps of Radicalization."



Note: * Indicates personal factors such as motivation, beliefs, and self-identity.
Source: Figure modified from Bronfenbrenner (1977).

Figure 17. Drivers of Risk to Radicalization by Levels of Influence.

At the center of this diagram is the individual, with all aspects of motivation, belief, self-identity, and the like. The successive outer circles show the familial, societal, and cultural factors that influence each aspect of that individual, indicating that the factors that affect one aspect, such as self-identity, may differ from those that influence another aspect of the individual, such as beliefs. The process of radicalization, which may engage some or all of these aspects and levels, is neither deterministic nor linear—it is a complex context-dependent phenomenon that follows an unplanned path that is influenced by sociological, political, ideological, and psychological drivers over time.[142] Vulnerability to radicalization may develop as a snowball effect (in which small changes combine to form a larger change) or a spiral pattern (in which small changes incrementally impact other layers, resulting in larger changes).

[142] Dzhekova, Mancheva, Stoynova, Anagnostou. *Monitoring Radicalization*.

Although Figure 17 shows five levels of influence surrounding the individual, some researchers have categorized drivers to radicalization into a three-level model, including "macro," "meso," and "micro" level factors.[143]

- Macro level or structural factors are those that are external to the individual and include experiences such as social marginalization/exclusion or discrimination, poverty, effects of international politics, or conflicts;
- Meso level or group-based factors are those related to group, community, and social networks and include experiences such as identity dynamics at the group level, group dynamics, social influence, social rules, and social media (role in social networks and opinion formation); and
- Micro level factors are those at the individual level (i.e., personal factors) and include an individual's psychological characteristics, personal experiences, and motivations.

A number of factors can increase or decrease a service member's vulnerability to radicalization, however, the time at which the service member is influenced by these factors is critical. For example:

- At the meso level, an individual may be strongly influenced by his or her family and by his or her chain of command. The factors that influence radicalization may also interact, as in the experiences that one has with family and command during deployments and relocations can impact each other and influence the radicalization process. For veterans, the support one receives after service from military support organizations such as Veterans Affairs might be a push/pull factor in radicalization.
- At the macro level, cultural attitudes and ideologies can play a role in belief development, as can larger global issues such as any active political situation or an ongoing war; individual participation in terrorism is commonly rooted in lived or perceived collective experiences and framed by narratives that draw on these events.

Any one or more of these factors can make one more (or less) vulnerable to radicalization and any of these factors can serve as a catalyst for radicalization. The process can be slow, taking place over a lifetime, or it can be quick, triggering real-time efforts to seek information on extremist groups and/or engage extremist activities.

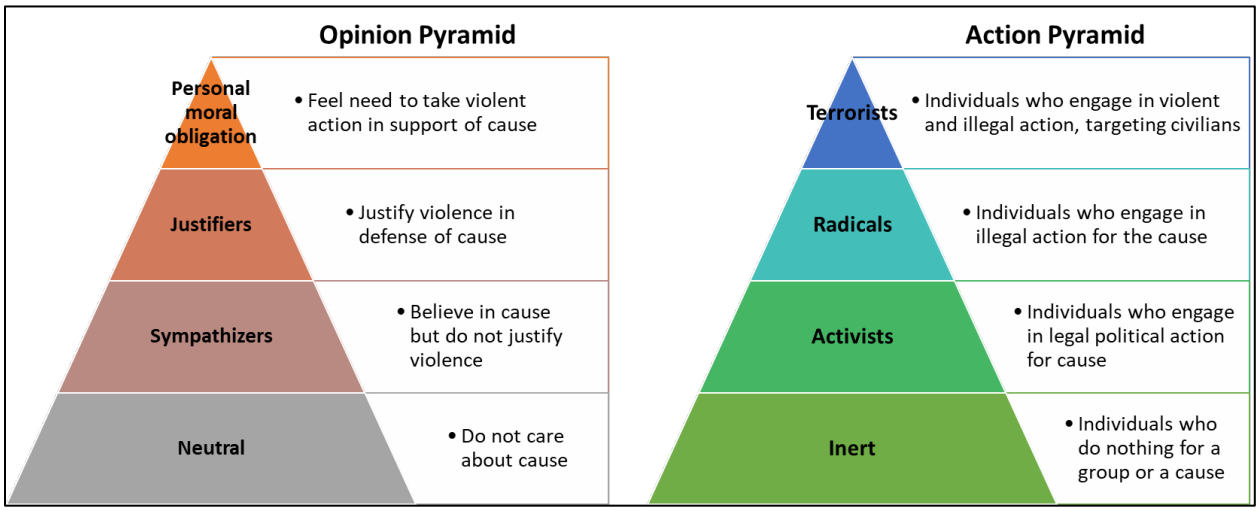
The literature of radicalization also distinguishes between cognitive and behavioral radicalization.

---

[143] Schmid, A. (Ed.). (2011). The Routledge Handbook on Terrorism Research. New York: Routledge; Martha Crenshaw, *Explaining Terrorism: Causes, Processes and Consequences* (New York City, NY: Routledge, November 2010); Marc Sageman, *Understanding Terror Networks* (Philadelphia, PA: University of Pennsylvania Press, May 14, 2004); Arie Kruglanski, Michele Gelfand, Jocelyn Belanger, et al., "The Psychology of Radicalization and Deradicalization: How Signifance Quest Impacts Violent Extremsim," *Political Psychology* 35, no. 1 (February 2014): 69-93, https://onlinelibrary.wiley.com/doi/10.1111/pops.12163.

- Cognitive radicalization (radicalization of opinion) is the process through which an individual adopts an extremist ideology. Radical beliefs are considered to be an antecedent to behavioral radicalization.[144]
- Behavioral radicalization (radicalization of action) is the process through which an individual decides to take action (violent or otherwise) in support of radical beliefs.

Figure 18 shows a two-pyramid model developed by McCauley and Moskalenko[145] to separate and individually represent radicalization of opinion from radicalization of action.



Source: Adapted from McCauley and Moskalenko (2017).

Figure 18. Two-pyramid Model of Radicalization

All individuals undergoing behavioral radicalization have undergone cognitive radicalization, but not all individuals who have undergone cognitive radicalization will become behaviorally radicalized.[146] This separation can be important, as a very small percentage of individuals with radicalized ideas ever act in support of those ideas. It is also consistent with the DOD effort to separate extremist beliefs from extremist activities, prohibiting only activities. The approaches and resources needed to counter radicalized opinion differ significantly from those

[144] Lorenzo Vidino, *Countering Radicalization in America* (Washington, DC: United States Institute for Peace, 2010), https://www.usip.org/sites/default/files/resources/SR262%20-%20Countering_Radicalization_in_America.pdf.

[145] Clark McCauley, Sophia Moskalenko, "Understanding Political Radicalization: The Two-Pyramids Model," *American Psychologist* 72, no. 3 (April 2017): 205-216, doi:10.1037/amp0000062.

[146] Adrienne Ou, "Hearts and Minds: A Comparison of the Counter-Radicalization Strategies in Britain and the United States," *Cornell International Affairs Review* 9, no. 2 (2016): 1-3. http://www.inquiriesjournal.com/articles/1413/hearts-and-minds-a-comparison-of-counter-radicalization-strategies-in-britain-and-the-united-states. Social psychology research has shown that there is a weak relationship between attitudes and behaviors. In fact, Borum (2011) argued the need to distinguish the process of radicalization (or the development of extremist ideologies and beliefs) from the action pathways through which individuals engage in terrorism or violent extremism.

needed to counter radicalized action (or terrorism). For example, research shows that efforts to counter radicalization of opinion may require addressing a sector of society, while responses to radicalization of action are more likely to require focusing on individuals and small groups.[147]

2. Identifiable Risk Factors for Radicalization

A key consideration for the prevention of radicalization is knowledge of its causes; contributing push, pull, and personal factors; and the environmental context that enables it. Current research on interventions to radicalization seeks to identify the micro, meso, and macro level factors to help explain how an individual became radicalized and why those push or pull factors had the specific psychological and behavioral impacts. At the macro level, surveys are often used to identify threats and trends across extremist activities, actors, drivers, and known determinants to radicalization (e.g., grievances, polarization, tension, activism) within the general population. At the micro level, first line practitioners (i.e., police officers, psychologists, social workers, teachers) assess risk using empirically based tools to identify risk of radicalization and/or terrorism.[148] Some research identifies risk factors by comparing extremists who engaged (or attempted to engage) in terrorism with extremists who did not, while other studies examine the frequency with which factors appear in known extremists who engaged in terrorism.[149]

Since 2012, the National Institute of Justice (NIJ)'s Domestic Radicalization to Terrorism program has sponsored research to identify factors associated with radicalization and to develop prevention and intervention efforts based upon this research[150]. A 2018 report by Allison Smith[151] summarized the findings of four such efforts sponsored by NIJ that examined potential risk factors associated with engaging or attempting to engage in terrorism for group-based and lone-actor extremists in the United States. Similarly, a 2021 report by LaFree and Schwarzenbach examined a variety of micro- and macro-level factors that are associated (both positively and negatively)

---

[147] McCauley and Moskalenko, "Understanding Political Radicalization."

[148] Dzhekova, Mancheva, Stoynova, and Anagnostou, *Monitoring Radicalization*.

[149] The inclusion of a nonviolent comparison group increases the validity and strength of the findings and are thus a more reliable method to develop risk factors for radicalization.

[150] Risk factors are a set of characteristics identified in known offenders (in the case of radicalization, characteristics of known extremists). These factors are only correlated with and may not be causally related to radicalization. Risk factors should not be confused with indicators. Risk factors indicate the likelihood of a given outcome while indicators help signal presence of that outcome. Allison G. Smith, *Risk Factors and Indicators Associated with Radicalization to Terrorism in the United States: What Research Sponsored by the National Institutes of Justice Tells Us* (Washington, DC: National Institute of Justice, June 2018), https://www.ojp.gov/pdffiles1/nij/251789.pdf.

[151] Ibid.

with radicalization and terrorism.[152] Table 7 summarizes the findings of these two studies, assessing the association of ten major demographic factors with radicalization and terrorism.[153]

Table 7. Micro-level Risk Factors for Radicalization and Terrorism

Risk Factor	Findings
Gender	Males are overrepresented as perpetrators of terrorism; proportion of women engaging in terrorism is increasing over time; a majority of lone-actors are male.[154]
Age	Although youth is associated with engagement in violent crime, the average age of those engaging in terrorism is older and spans a broader age range; in the U.S. however, younger individuals are radicalized to terrorism.[155]
Radical Peers	Having (and being in contact with) radical peers (including in social networks) significantly increases likelihood of developing violent extremist ideologies and engaging in terrorism but contact with nonviolent peers protects against participation in terrorism.[156]
Employment	Historically, most individuals were gainfully employed while engaging in terrorism, but lack of stable employment is a strong risk factor for radicalization and engaging in political terrorism, particularly for lone-actors.[157]

[152] Gary LaFree and Anina Schwarzenbach, "Micro and Macro-Level Risk Factors for Extremism and Terrorism: Towards a Criminology of Extremist Violence," *Monatsschrift für Kriminologie und Strafrechtsreform* 104, no. 3 (August 18, 2021): 184-202, doi:10.1515/mks-2021-0127.

[153] The researchers examined relationship of each factor listed with engaging or attempting to engage in terrorism independently. In other words, neither the interactions of the potential risk factors nor the role of a combination of risk factors was not examined.

[154] Gary LaFree, Michael Jensen, Patrick James, and Aaron Safer-Lichtenstein, "Correlates of Violent Political Extremism in the United States," *Criminology* 56, no. 2 (February 2, 2018): 233-268, https://onlinelibrary.wiley.com/doi/abs/10.1111/1745-9125.12169; Candice D. Ortbals and Lori Poloni-Staudinger, *Gender and Political Violence: Women Changing the Politics of Terrorism* (Cham, Switzerland: Springer, 2018).

[155] Jytte Klausen, Tyler Morrill, and Rosanne Liberetti, "The Terrorist Age-Crime Curve: An Analysis of American Islamist Terrorist Offenders and Age-Specific Propensity for Participation in Violent and Nonviolent Incidents," *Social Science Quarterly* 97, no. 1 (February 26, 2016): 19-32, https://onlinelibrary.wiley.com/doi/10.1111/ssqu.12249; David C. Pyrooz, Gary LaFree, Scott H. Decker, and Patrick A. James, "Cut from the Same Cloth? Comparing Gangs and Violent Political Extremists," *Justice Quarterly* 35, no. 1 (May 18, 2017): 1-32, https://www.tandfonline.com/doi/full/10.1080/07418825.2017.1311357.

[156] Lösel Friedrich, Sonja King, Doris Bender, and Irina Jugl, "Protective Factors Against Extremism and Violent Radicalization: A Systematic Review of Research," *International Journal of Developmental Science* 12, no. 1-2 (2018): 89-102, https://content.iospress.com/articles/international-journal-of-developmental-science/dev170241.

[157] Sageman, *Understanding Terror Networks*.

Risk Factor	Findings
Marriage	Marital status is a factor, but its relationship to terrorism is mixed; marriage itself is not a protective factor as spouse is likely supportive of extremist behavior; vast majority of lone-actors were single, lived alone, or socially-isolated.[158]
Military Service	Findings are mixed—military training serves as a protective factor from some extremist ideologies, but military training is a highly desired expertise for which some extremist groups recruit; there is a 33% likelihood that lone-actors had prior military service.[159]
Prior Criminal Activity	Pre-radicalization violent and/or nonviolent behavior is strongest non-ideological predictor of post-radicalization violence; far-right extremist more likely to engage in crime before radicalization than other ideologies; those engaging in criminal activity before age 18 more likely than non-juvenile offenders to engage in violent extremist acts after radicalization.[160]
Imprisonment	Past incarceration is associated with a higher likelihood of engagement in terrorism; findings increase twofold when individuals radicalized to extremist ideology while incarcerated.[161]
Ideology	Extreme ideology is associated with a higher likelihood of engaging in extremist actions (including terrorism) and aggressive attitudes and behaviors.[162]
Mental Illness	There is no consensus in the research, but mental illness may combine with other causal factors to produce a pathway to terrorism. This finding is more consistent for lone-actor terrorists (e.g., of far-right extremists who committed homicides, 40% of lone-actor terrorists vs. 8% of other far-right extremists had a reported history of mental health issues) than for other violent actors.[163]

Source: Adapted from Smith (2018) and LaFree and Schwarzenbach (2021).

[158] Mary Beth Altier, Emma Leonard Boyle, John G. Horgan, "Returning to the Fight: An Empirical Analysis of Terrorist Reengagement and Recidivism," *Terrorism and Political Violence* 18 (November 18, 2019): 1-25, https://www.tandfonline.com/doi/full/10.1080/09546553.2019.1679781.

[159] Mohammed Hafez, "Radicalization in the Persian Gulf: Assessing the Potential of Islamist Militancy in Saudi Arabia and Yemen," *Dynamics of Asymmetric Conflict* 1, no. 1 (July 28, 2008): 6-24, https://www.tandfonline.com/doi/full/10.1080/17467580802034000; Department of Homeland Security, Office of Intelligence and Analysis, *Rightwing Extremism: Current Economic and Political Climate Fueling Resurgence in Radicalization and Recruitment* (Washington, DC: Department of Homeland Security, April 7, 2009), https://irp.fas.org/eprint/rightwing.pdf.

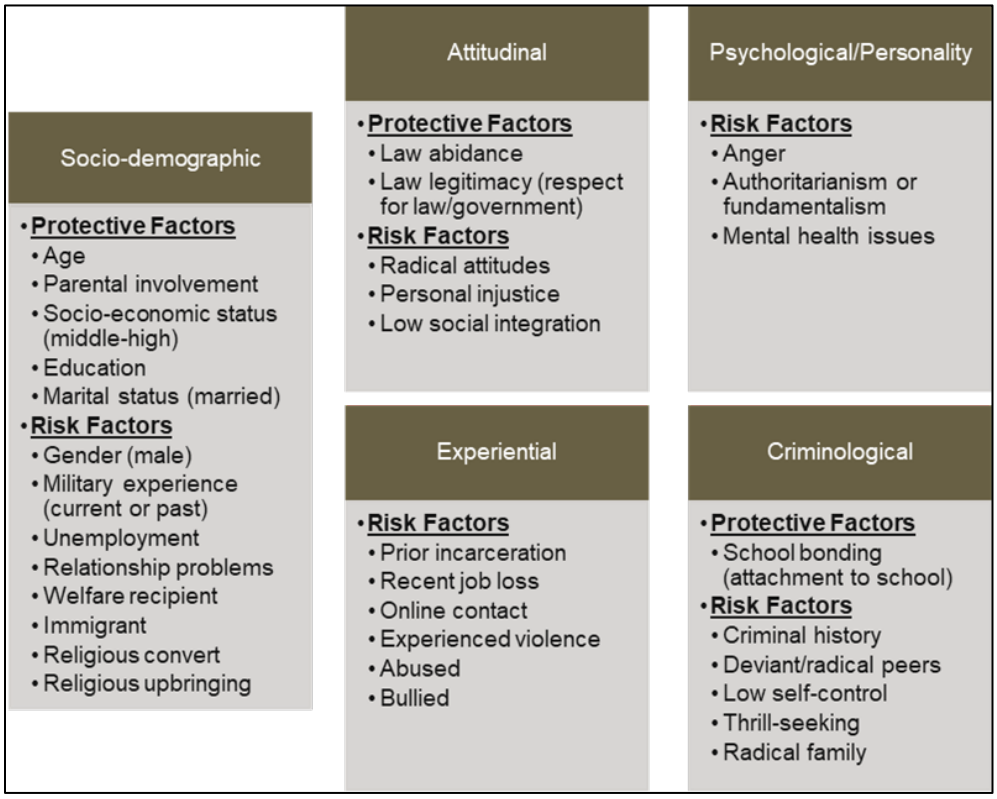
[160] Michael Jensen, Anita Seate, and Patrick James, "Radicalization to Violence: A Pathway Approach to Studying Extremism," *Terrorism and Political Violence* 32, no. 5 (April 9, 2018): 1067-1090, https://www.tandfonline.com/doi/full/10.1080/09546553.2018.1442330.

[161] Gary LaFree, Bo Jiang, and Lauren Porter, "Prison and Violent Political Extremism in the United states," *Journal of Quantitative Criminology* 36, no. 3 (April 16, 2019): 1-26, https://link.springer.com/article/10.1007/s10940-019-09412-1.

[162] Alain van Hiel, Emma Onraet, Dries H. Bostyn, et al., "A Meta-Analytic Integration of Research on the Relationship Between Right-Wing Ideological Attitudes and Aggressive Tendencies," *European Review of Social Psychology* 31, no. 1 (December 2020): 183-221, doi: 10.1080/10463283.2020.1778324.

[163] Steven Chermak, Joshua Freilich, and Michael Suttmoeller, "The Organizational Dynamics of Far-Right Hate Groupsin the United States: Comparing Violent to Nonviolent Organizations," *Studies in Conflict and Terrorism* 36, no. 3 (February 14, 2013): 193-218, https://www.tandfonline.com/doi/full/10.1080/1057610X.2013.755912; Paul Gill and Emily Corner, "Lone-Actor Terrorist Target Choice," *Behavioral Sciences & the Law* 34 (November 20, 2016): 693-705, https://onlinelibrary.wiley.com/doi/10.1002/bsl.2268.

A more systematic and comprehensive review, by Wolfowicz et al. (2020) identified 101 individual-level factors associated with radical attitudes, 45 associated with radical intentions, and 33 associated with radical behaviors across five domains.[164] The risk and protective factors identified by the Wolfowicz study included socio-demographic factors, attitudinal factors, experiential factors, psychological/personality factors, and criminological factors.[165] Although research can identify potential risk factors that may generally increase the likelihood of radicalization, each case must be examined individually to determine which characteristics and experiences served as drivers to radicalization for that individual and also to understand how the drivers interact with each other. The contributing factors identified in the Wolfowicz study are summarized in Figure 19.



Source: Adapted from Wolfowicz et al. (2020).

Figure 19. Protective and Risk Factors for Development of Radical Attitudes, Intentions, and Behaviors

[164] Wolfowicz, Litmanovitz, Weisburd, and Hasisi, "Cognitive and Behavioral Radicalization."

[165] Variables that work opposite to risk factors are protective factors. Protective factors shield and defend an individual's resilience to radicalization. Nevertheless, as Borum (2015) has noted, research has not adequately identified an empirical list of protective factors that mitigate against extremist violence although there is a corpus of research on risk and protective factors in other forms of violence.

This more detailed list of risk factors includes a number of factors that have been linked to other violent and problem behaviors such as suicidal tendencies, sexual assault, and drug and alcohol abuse. For example:

- The list of socio-demographic risk factors includes unemployment and relationship problems;
- The list of attitudinal risk factors includes low social integration;
- The list of experiential risk factors includes past experience of violence, abuse, and bullying; and
- The list of psychological and personality risk factors includes anger and mental health issues.

These common factors are also consistent with the anecdotal accounts of senior DOD leaders, who told the IDA team that the rare service members they encountered who engaged in prohibited extremist activities appeared to be isolated actors who were cut off from their peers. The identification of such risk factors may be particularly helpful for DOD, because the Department's comprehensive authorities with regard to military personnel may enable it to identify and address some of these factors through mentoring, counseling, and peer support mechanisms without waiting for the factors to express themselves through prohibited extremist activities or other negative behaviors.

It is worth noting that these studies provide no solid empirical evidence to support the idea that service members are more vulnerable to extremist radicalization than their civilian counterparts. There is some evidence that military training is linked to participation in terrorist violence among extreme Islamists, but similar linkage has not been demonstrated for other violent ideologies. Some studies suggest that previous participation in combat or military training experience could be a potential risk factor for radicalization,[166] but other research suggests that military service can serve as a protective factor against criminal trajectories.[167] In the PIRUS dataset (discussed in Chapters 2.B.2 and 8.B), 11.5% of individuals engaging in extremist crimes had a military background and a vast majority of these individuals (83.7%) committed those crimes after leaving military service.[168] This data is generally consistent with IDA's finding on the prevalence of extremist activities in the military community presented in Chapter 3.B.2.

Risk factors for radicalization alone are insufficient to provide a basis for successful prevention and intervention programs and policies; a sole reliance on risk factors could lead to the identification of the wrong targets for intervention. While risk factors increase the likelihood of a given outcome, indicators help signal the presence of that outcome. For example, smoking is a risk

[166] Per Dzhekova et al., *Monitoriing Radicalization*; and Smith, *Risk Factors and Indicators Associated iwth Radicalization to Terrorism in the United States*.

[167] Hafez, "Radicalization in the Persian Gulf."

[168] Jensen, Yates, and Kane, *Radicalization in the Ranks*.

factor for lung cancer because it increases the likelihood of an outcome of cancer, but difficulty breathing could be an indicator that cancer may be present. The existence of an indicator does not necessarily mean that the outcome is occurring—just because an individual is suffering from impaired breathing does not necessarily mean they have lung cancer, even if he or she is a smoker. The detection of indicators for radicalization can help to narrow scope and better target prevention and intervention programs.

At an individual level, the development of radicalization indicators is based on the idea that the radicalization process is likely to reveal itself in the actions, behaviors, and attitudes of an individual and might be identified by other individuals who encounter them.[169] These individual level indicators can be behavioral or cognitive (and violent or nonviolent), but as we have noted previously, these indicators may be associated with nonviolent or violent ideologies and/or actions. Micro (or individual) level behavioral indicators are observable behaviors such as practices, actions, and appearance; cognitive indicators are expressions of opinions, beliefs, and attitudes.[170]

Unfortunately, the literature on potential indicators of violent extremist (or terrorist) action remains thin. Smith's review of NIJ sponsored terrorism research identified only one potential indicator: the number of extremist group meetings an individual attended was associated with an increased likelihood of attempting or engaging in terrorism,[171]—which is not a surprising finding. As noted in a separate study,[172] the NIJ research indicated that individuals who displayed this indicator to radicalization often broadcasted or verbalized their intentions to act in a violent manner before acting. Stockpiling of weapons is another potential indicator of planning and preparing to engage in acts of terrorism—but since stockpiling weapons is an act of preparation, this also appears to be a truism.

The list of potential indicators for radicalization of belief is more complete, including potential indicators such as actively conveying information about grievances, extremist ideologies, and/or desires to hurt others.[173] A leading study divides behavioral and cognitive indicators into three categories: indictors suggestive of vulnerability to radicalization, potential red flags of radicalization, and high-risk indicators of radicalization, as shown in Figure 20.[174]

---

[169] Dzhekova, Mancheva, Stoynova, and Anagnostou, *Monitoring Radicalization*.

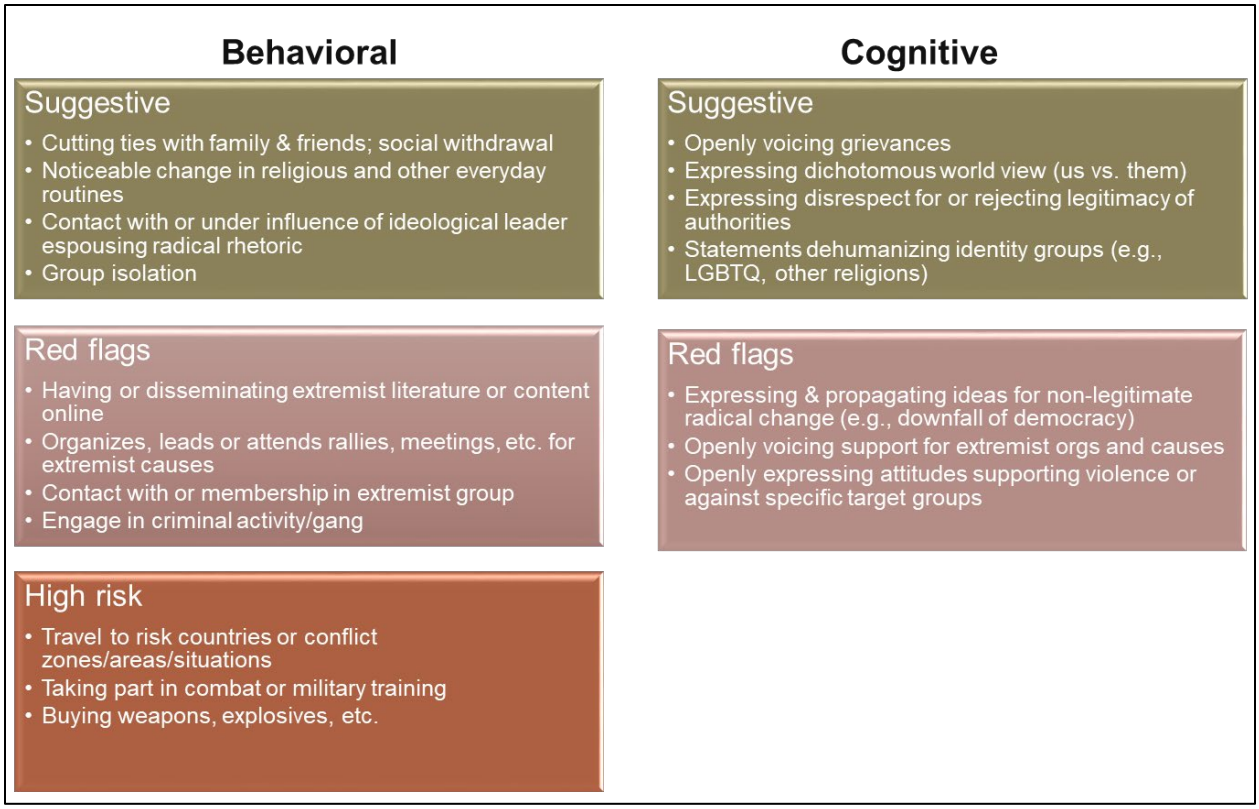
[170] Ibid.

[171] Smith, *Risk Factors and Indicators Associated with Radicalization to Terrorism in the United States*.

[172] Dzhekova, Mancheva, Stoynova, and Anagnostou, *Monitoring Radicalization*.

[173] Smith, *Risk Factors and Indicators Associated with Radicalization to Terrorism in the United States*.

[174] Dzhekova, Mancheva, Stoynova, and Anagnostou, *Monitoring Radicalization*. While the Smith (2018) review focused on potential or executed cases of terrorism in the U. S., the Dzhekova et al. (2017) indicators list was generated by cases in Europe. Dzhekova et al. (2017) do not provide details regarding the origins of these indicators and thus, it is unclear whether the indicators are based on frequency counts from known terrorism cases or if comparison cases were used.



Source: Adapted from Dzhekova et al. (2017).

Figure 20. Observable Behavioral and Cognitive Risk and Vulnerability to Radicalization Indicators

Suggestive indicators are signs of vulnerability to radicalization, but are not definitive on their own, although they may suggest the need for in-depth professional assessment. Red flag indicators are stronger indicators of risk-relevant behaviors and attitudes, but even so, professional review is needed to assess risk on an individual basis.

3. Risk Assessment Tools

Risk assessment tools are frameworks for collecting data to examine the likelihood of harm based on available information. Such tools have been used in criminology since the 1920s to measure vulnerability to violent crime as a means for criminal justice agencies to make informed decisions about resource allocation, sentencing, release, and parole.[175] A leading study defines risk assessment as:

> …the process of collecting and considering information about a person and the situations and context that person is likely to encounter in order to describe and

[175] RTI International, *Countering Violent Extremism: The Application of Risk Assessment Tools in the Criminal Justice and Rehabilitation Process* (Research Triangle Park, NC: RTI International, February 2018), https://www.dhs.gov/sites/default/files/publications/OPSR_TP_CVE-Application-Risk-Assessment-Tools-Criminal-Rehab-Process_2018Feb-508.pdf.

> evaluate the potential that the person will engage in jeopardous behavior and prevent or mitigate the behavior and its adverse consequences.

Risk assessments can be used to predict the likelihood that an individual will engage in actions of concern, to inform decisions regarding risk management and interventions, to provide a historical account for decision-making, and to improve understanding both within and across multidisciplinary teams tasked with risk mitigation.[176]

Unfortunately, researchers have yet to produce widely accepted risk assessment tools for violent extremism. The problem, like the problem of identifying risk and factors and indicators for radicalization, stems from the heterogeneity of extremists (although most have been male and many have been relatively young), low base rates of radicalization and violent extremist action, and the periodic ebb and flow of radicalization.[177] Although there is now a large body of research examining the root causes of radicalization, it appears to be a dynamic, non-linear process requiring the assessment of a number of factors spanning sociological, political, ideological, and individual drivers.[178] Further, there is no guarantee that a radicalized individual will engage in nonviolent or violent action. Given that there is no single path (or even several paths) to radicalization and/or to terrorism and that these paths can change over time, risk assessment tools to identify vulnerabilities to radicalization cannot predict future behavior. Instead, these tools can identify an individual's characteristics, which when considered together with his or her life history and disposition, may provide some indication of the likelihood of radicalizing or engaging in terrorism.[179]

There are three major approaches to risk assessments:

- Unaided professional judgement risk assessments are based on only the professional assessor's experience and knowledge of the assessed individual.[180]
- Structured professional judgement (SJP) tools combine actuarial and unaided professional judgement approaches, using evidence-based risk factors to guide the assessor in systematically identifying and interpreting risk associated with the individual within defined contexts.[181]

---

[176] Leslie Helmus and David Thornton, "Stability and Predictive and Incremental Accuracy of the Individual Items of Static-99r and Static 2002r in Predicting Sexual Recidivism: A Meta-Analysis," *Criminal Justice and Behavior* 42 (February 12, 2015): 917-973. doi:10.1177/0093854814568891.

[177] LaFree and Schwarzenbach, "Micro and Macro-Level Risk Factors for Extremism and Terrorism."

[178] Dzhekova, Mancheva, Stoynova, and Anagnostou, *Monitoring Radicalization*.

[179] RTI International, *Countering Violent Extremism*.

[180] Ashimesh Roychowdhury and Gwen Adshead, "Violence Risk Assessment as a Medical Intervention: Ethical Tensions," *Psychiatric Bulletin* 38, no. 2 (April 2014): 75-82, doi:10.1192/pb.bp.113.043315.

[181] Laura Guy, Ira Packer, and William Warnken, "Assessing Risk of Violence Using Structured Professional Judgment Guidelines," *Journal of Forensic Psychology Practice* 12 (May 24, 2012): 270-283, doi:10.1080/15228932.2012.674471.

- Actuarial tools use an inflexible approach based on a checklist of risk indicators.

In general, experts appear to support the use of SJP tools over unaided professional judgement or inflexible checklists for purposes of risk assessment for radicalization. SJP tools take both risk assessment and management strategies into consideration but are more flexible and person-centered than a check-list approach.[182]

While tools for risk assessment originally focused on static measures of lifetime risk of generic violence, researchers have pointed out the inadequacies of using traditional tools developed for managing risk of violence in the general criminal justice context, for risk for terrorism. For example, traditional tools to identify risk of violence omit variables related to the backgrounds and motivations of ideologically motivated individuals. Further, risk management for violent extremism must account for a complex set of variables and their interactions including the potential of actual, attempted, or threatened attacks with a variety of weapons (e.g., explosives, guns, knives, vehicles) on both government agencies (and their employees) and members of the public, and whether the actor is acting alone or with a group.[183]

Several risk assessment tools have been designed specifically to address the risk of terrorism. These tools include a number of globally developed measures such as the Violent Extremism Risk Assessment-2[184] and the Terrorist Radicalization Assessment Protocol.[185] Unfortunately, these terrorism-specific risk assessment tools have focused on assessments of known terrorists (i.e., after the individual has become radicalized and taken violent action) to inform the criminal justice context (e.g., sentencing, rehabilitation, reintegration of individual into society).

Risk assessment tools that focus on known terrorists may be helpful, but they provide little insight into the radicalization process, and so may not provide sufficient early warning of developing problems. Risk assessment in the prevention of violent radicalization into terrorism has received far less attention, but governments within the United Kingdom and European Union have funded a number of guidelines developed for the prevention context. These guidelines are described in Table 8.

---

[182] Kevin Douglas, Stephen Hart, Christopher Webster, et al., "Historical-Clinical-Risk Management-20, Version 3 (HCR-20V3): Development and Overview," *International Journal of Forensic Mental Health* 13 (May 19, 2014): 903-108, doi:10.1080/14999013.2014.906519.

[183] Caroline Logan and Monica Lloyd, "Violent Extremism: A Comparison of Approaches to Assessing and Managing Risk," *Legal and Criminological Psychology* 24, no. 1 (August 29, 2018): 141-161. doi:10.1111/lcrp.12140.

[184] Elaine D. Pressman and John Flockton, "Calibrating Risk for Violent Political Extremists and Terrorists: The VERA 2 Structured Assessment," *British Journal of Forensic Practice* 14, no. 4 (November 16, 2012): 237-251, doi:10.1108/14636641211283057.

[185] (TRAP-18 (J. R. Meloy, K. Roshdi, J. Glaz-Ocik, and J. Hoffmann, "Investigating the Individual Terrorist in Europe," *Journal of Threat Assessment and Management* 2, no. 3-4 (September 2015): 140-152, doi:10.1037/tam0000036)(see Dzhekova et al., *Monitoring Radicalization*; RTI International, *Countering Violent Extremism*; and Smith, *Risk Factors and Indicators Associated with Radicalization to Terrorism in the United States*, for a review of the existing tools for violent extremism risk assessment and their limitations).

Table 8. Developed Guidelines for Prevention of Violent Radicalization

Guideline	Benefits	Limitations
Vulnerability Assessment Framework (Government of the United Kingdom 2012)	Used to identify vulnerability by examining: (1) factors that promote engagement and emotions/cognitions that allow susceptibility to recruitment; (2) intent factors indicating readiness to use violence and dehumanization of terrorist targets; (3) capability to cause harm (individual skill/competency and access to networks/weapons)	Lacks details on how factors were isolated; no reference to empirical evidence on violent radicalization included with guidance
Observable Indicators of Possible Radicalization (Pilner 2013)	21 indicators clustered by thematic area: identity and identity seeking; in-group-outgroup differentiation; pro-violence social interactions (including distancing from friends/family); change in persona; association with extremist groups	Based on consultation with individuals involved in counter-radicalization work (e.g., first line responders). Unclear if the indicators are evidence based.
Identifying vulnerable People (Cole 2014)	List of empirically based indicators; identifies red flag behaviors (i.e., membership of nonviolent radical groups, contact with known extremists, advanced military training, overseas combat experience) and other factors (e.g., cultural and/or religious isolation, isolation from family, risk-taking behaviors, isolated peer group, hate rhetoric, political activism)	Unclear if the indicators are based on frequency counts in cases of known terrorists or if developed against a comparison group

These guidelines are in line with an SJP approach, but they do not specify the risk being predicted, do not provide a clear theoretical link between the risk factors and terrorism, and each sets a relaxed threshold for categorizing individuals as being at risk (which may result in a large number of false positive risk assessments).[186]

Both risk assessments for radicalization and risk assessments for terrorism face similar challenges and limitations due to the low base-rate problem and limited data set available for the study of radicalization and violent extremist activities. In general, there is insufficient evidence to support the use of risk assessment tools for prediction of future behavior. For example, there are insufficient data to develop tools with adequate specificity (i.e., true negative rates; accurately identifying those not at risk) or sensitivity (i.e., true-positive rates; accurately identifying those at risk). Before operationalizing any risk assessment tool, its performance should be validated. The tool should demonstrate strong statistical and empirical confidence that it is correctly assessing what it is designed to do. The low rate of radicalization, together with the heterogeneous nature of

[186] Kiran M. Sarma, "Risk Assessment and the Prevention of Radicalization from Nonviolence into Terrorism," *American Psychologist* 72, no. 3 (April 2017): 278-288, doi:10.1037/amp0000121.

radicalization and terrorism makes validation difficult because such small sample sizes often lack the statistical power on which to derive any empirically meaningful conclusions.[187]

Despite these challenges, currently available and emerging risk assessment tools for radicalization and/or terrorism are improving with more study and improved data sets. New studies are beginning to address gaps in validation through the development of targeted research agendas and will play a critical role in the development of improved risk assessment tools. The limited tools now available are better than no tools at all, and there is a prospect of improved tools in the near future.

B. False Information and Conspiracy Theories

Self-radicalization is a form of cognitive radicalization where an individual embraces extremist beliefs without direct affiliation with any particular extremist group.[188] In most cases, self-radicalized individuals experience a "cognitive opening" where some catalyst (e.g., discrimination, job loss, social isolation) leads them to seek out extremist ideas and individuals as a means to address a turbulent situation.[189] With the advent and growth of digital communication and social media, including online hate forums, individuals can become self-radicalized to engage in accelerationist violence on their own without a connection to an extremist group, an extremist leader, or an organized plot of any kind.[190] The ubiquity of social media poses a particular risk for DOD because it not only exposes service members to influences from outside the bubble of the military environment, but it may also make it more difficult for leaders and peers to detect the presence of malign influences.

The internet allows for individuals with extreme beliefs and ideologies to become bolstered in their beliefs because they seek out and share materials only in support of those beliefs, thus developing an echo chamber through cognitive bias.[191] The internet also enables the sharing of goals, tactics, and rhetoric on message boards and through informal online networking, allowing

---

[187] RTI International, *Countering Violent Extremism*.

[188] Roger Bradbury, Terry Bossomaier, and David Kernot, "Predicting the Emergence of Self-Radicalization Through Social Media: A Complex Systems Approach," pages 379-389 in *Terrorists' Use of the Internet*, edited by Maura Conway, Lee Jarvis, Orla Lehane, Stuart Macdonald, and Lella Nouri (IOS Press, 2017). doi:10.3233/978-1-61499-765-8-379.

[189] Trip, Bora, Marian, Halmajan, and Drugas, "Psychological Mechanisms Involved in Radicalization and Extremism."

[190] Jakob Guhl and Jacob Davey, *A Safe Space to Hate: White Supremacist Mobilisation on Telegram* (London, UK: Institute for Strategic Dialogue, June 26, 2020), https://www.isdglobal.org/isd-publications/a-safe-space-to-hate-white-supremacist-mobilisation-on-telegram/.

[191] Georgia Hollewell and Nicholas Longpré, "Radicalization in the Social Media Era: Understanding the Relationship between Self-Radicalization and the Internet," *International Journal of Offender Therapy and Comparative Criminology* 66, no. 8 (June 30, 2021), doi:10.1177/0306624X211028771.

multiple groups to adopt similar strategic orientations.[192] Because the internet allows for fragmented individuals and groups to organize around shared objectives, accelerationist strategies and motivations have gained transnational traction.[193] As a result, extremist organizations and ideologies have been able to leverage the internet and social media for recruitment, radicalization, and even the planning of terrorist acts.[194]

Internet and online platforms and their algorithms that make navigation of the online world easier for users (e.g., access to information, communication, social connectedness) come with a cost. These algorithms can also enable echo chambers that distort reality and serve as a diffusion mechanism for extremist content and hate speech.[195] Oftentimes, the viral spread of information also goes hand-in-hand with the production of information cascades in which users share information without fully understanding or knowing (or caring) about the accuracy of that information. The proliferation of such misinformation and disinformation make the internet a potent breeding ground for extremist radicalization.[196]

Both misinformation and disinformation involve the sharing of false information, but the intent or motivation for sharing the false information is different.

- In misinformation, false (and potentially harmful) information is shared without malicious intent, i.e., the individual either believes the information is true or has not evaluated the veracity of the information.
- In disinformation, the source knows that the information is false and shares it with malicious intent (e.g., deliberately seeking harm or seeking political personal or financial gain).[197]

---

[192] Arie Perliger, "CARR Policy Insight Series: Deciphering the Second Wave of the American Militia Movement," *Centre for Analysis of the Radical Right*, January 7, 2021, https://www.radicalrightanalysis.com/2021/01/07/carr-policy-insight-series-deciphering-the-second-wave-of-the-american-militia-movement/.

[193] Hughes and Miller-Idriss, "Uniting for Total Collapse."

[194] For a review of how extremist groups manipulate the social media ecosystem, see Alice Marwick and Rebecca Lewis, Media Manipulation and Disinformation Online (New York City, NY: Data & Society, May 2017), http://www.chinhnghia.com/DataAndSociety_MediaManipulationAndDisinformationOnline.pdf.

[195] Zach Bastick, "Would you Notice if Fake News Changed your Behavior? An Experiment on the Unconscious Effects of Disinformation," *Computers in Human Behavior* 116, no. 106633 (March 2021), doi:10.1016/j.chb.2020.106633.

[196] For a comprehensive review of the psychology (accepting, sharing, and correcting false information), see Rainer Greifeneder, Mariela Jaffé, Eryn Newman, and Norbert Schwartz, *The Psychology of Fake News: Accepting, Sharing, and Correcting Misinformation* (New York City, NY: Routledge, 2021); and Ullrich Ecker, Stephan Lewandowsky, John Cook et al., "The Psychological Drivers of Misinformation Belief and its resistance to Correction," *Nature Reviews Psychology* 1 (January 12, 2022): 13-29, https://www.nature.com/articles/s44159-021-00006-y.

[197] Jennifer Jerit and Yangzi Y. Zhao, "Political Misinformation," *Annual Review of Political Science* 23 (May 2020): 77-94, doi:10.1146/annurev-polisci-050718-032814.

Because it is often difficult to determine the knowledge and intent of an individual who shares false information, misinformation and disinformation are often lumped together under the label of sharing "false information." Table 9 shows eight categories of false information identified by researchers.[198] These types of false information overlap such that some information may fall into multiple categories.

Table 9. Types of False Information

Type	Definition
Fabricated	Completely fictional narrative disconnected from real facts
Propaganda	Fabricated story, often within a political context, aimed to harm interests of a particular party
Conspiracy Theory	Narratives that try to explain a situation or event as orchestrated by a covert group or a group with malevolent intentions, but do so without proof; narrative is usually unsourced information presented as fact or as evidence for explanation
Hoaxes	News stories containing facts that are false or inaccurate but are presented as legitimate
Biased or one-sided	Stories that are hyper-partisan or extremely biased towards a person/party/situation/event
Rumors	Stories where the accuracy is ambiguous or never confirmed
Clickbait	Deliberate use of misleading headlines and thumbnails on the internet
Satire	Stories that contain irony and humor, but which are obfuscated, overlooked, or ignored by users who take the story at face value without further validation of the information

Some extremist and accelerationist groups intentionally spread misinformation and disinformation to propagate dissent and build support for their radical agendas. This strategy may take the form of endorsing or spreading conspiracy theories.[199] A conspiracy theory generally alleges the existence of secret plots by multiple actors who are working to seize political or economic power, violate rights, infringe upon established agreements (e.g., the Constitution), withhold critical secrets or information, or alter foundational institutions. Although a conspiracy theory may reference some actual facts and/or events, it generally relies upon questionable connections and linkages that may or may not be true.[200]

[198] Savvas Zannettou, Michael Sirivianos, Jeremy Blackburn, and Nicolas Kourtellis, "The Web of False Information: Rumors, Fake News, Hoaxes, Clickbait, and Various other Shenanigans," *Journal of Data and Information Quality* 11, no. 3 (September 2019): 1-37, doi:10.1145/3309699.

[199] Anna Levinsson, Diana Miconi, Zhiyin Li, Rochelle L. Frounfelker, and Cécile Rousseau, "Conspiracy Theories, Psychological Distress, and Sympathy for Violent Radicalization in Young Adults During the COVID-19 Pandemic: A Cross-Sectional Study," *International Journal of Environmental Research and Public Health* 18, no. 15 (July 24, 2021): 7846-7858, doi:10.3390/ijerph18157846.

[200] Karen Douglas, Joseph Uscinski, Robbie Sutton, et al., "Understanding Conspiracy Theories," *Political Psychology* 40, Suppl. 1 (February 2019): 1-33, doi:10.1111/pops.12568.

Some conspiracy theories seek to attack or discredit specific individuals or groups such as minorities. Because conspiracy theories are associated with an overall distrust of mainstream narratives and governing institutions, they also play a role in the development and spread of anti-government ideologies. In addition, conspiracy theories that condone the use of violence as a means to rectify perceived grievances may normalize terrorism, helping to move individuals from radicalization to terrorism.[201] One review of the literature, ideology, and propaganda of more than 50 extremist groups in Europe and the United States determined that extremist groups use conspiracy theories to increase threat perception and in-group identification, which leads to exacerbated "us" versus "them" rhetoric, increased group polarization and group think, and intensified extremist beliefs.[202]

Conspiracy theories providing a unified narrative focused on malicious enemies can serve as a catalyst and reinforcer of extremist ideologies and behaviors. The starting point to radicalization often includes a real or perceived event that negatively affects an individual's sense of personal significance. Individuals who experience such a negative event may seek to restore their sense of purpose, leading to a cognitive opening for extremist narratives.[203] Conspiracy theories can be a source of narratives to aid in this process. In fact, research on susceptibility to conspiratorial narratives shows that the quest for significance, specifically, searching for and relying on narratives as an explanation for and as a means for rectifying one's negative sense of purpose is a common theme in radicalization literature.[204]

Conspiracy theories work, in part, because people are susceptible to the truth-by-repetition effect, even for highly improbable statements. Due to processing fluency, repetition makes it easier to cognitively process information, which is misinterpreted as a signal that the information is true.[205]

---

[201] Gregory Rousis, Dan Richard, and Dong-Yuan Debbie Wang, "The Truth is out There: The Prevalence of Conspiracy Theory use by Radical Violent Extremist Organizations," *Terrorism and Political Violence*, (November 19, 2020):1-19, doi:10.1080/09546553.2020.1835654.

[202] Jamie Bartlett and Carl Miller, *The Power of Unreason: Conspiracy Theories, Extremism and Counterterrorism* (London, UK: Demos, August 2010).

[203] Arie Kruglansi, Katarzyna Jasko, David Webber, Marina Chernikova, and Erica Molinario, "The Making of Violent Extremists," *Review of General Psychology* 22, no. 1 (March 1, 2018): 107-120, https://journals.sagepub.com/doi/10.1037/gpr0000144. In Smith's review of NIJ-supported terrorism research findings, she noted that 80% of lone-actors examined across the four studies held some form of grievance.

[204] Federico Vegetti and Levente Littvay, "Belief in Conspiracy Theories and Attitudes Toward Political Violence," *Italian Political Science Review* 52, no. 1 (May 10, 2021): 18-32, doi:10.1017/iop.2021.17.

[205] Doris Lacassagne, Jeremy Béna, and Olivier Corneille, "Is Earth a Perfect Square? Repetition Increases the Perceived Truth of Highly Implausible Statements," *Cognition* 223 (June 2022), https://www.sciencedirect.com/science/article/pii/S0010027722000403.

Recent research indicates that conspiracy mentality is associated with stronger intentions of engaging in extremist violence.[206] Figure 21 shows the complex relationship between conspiracy theories and psychological and attitudinal receptivity on the part of an individual.

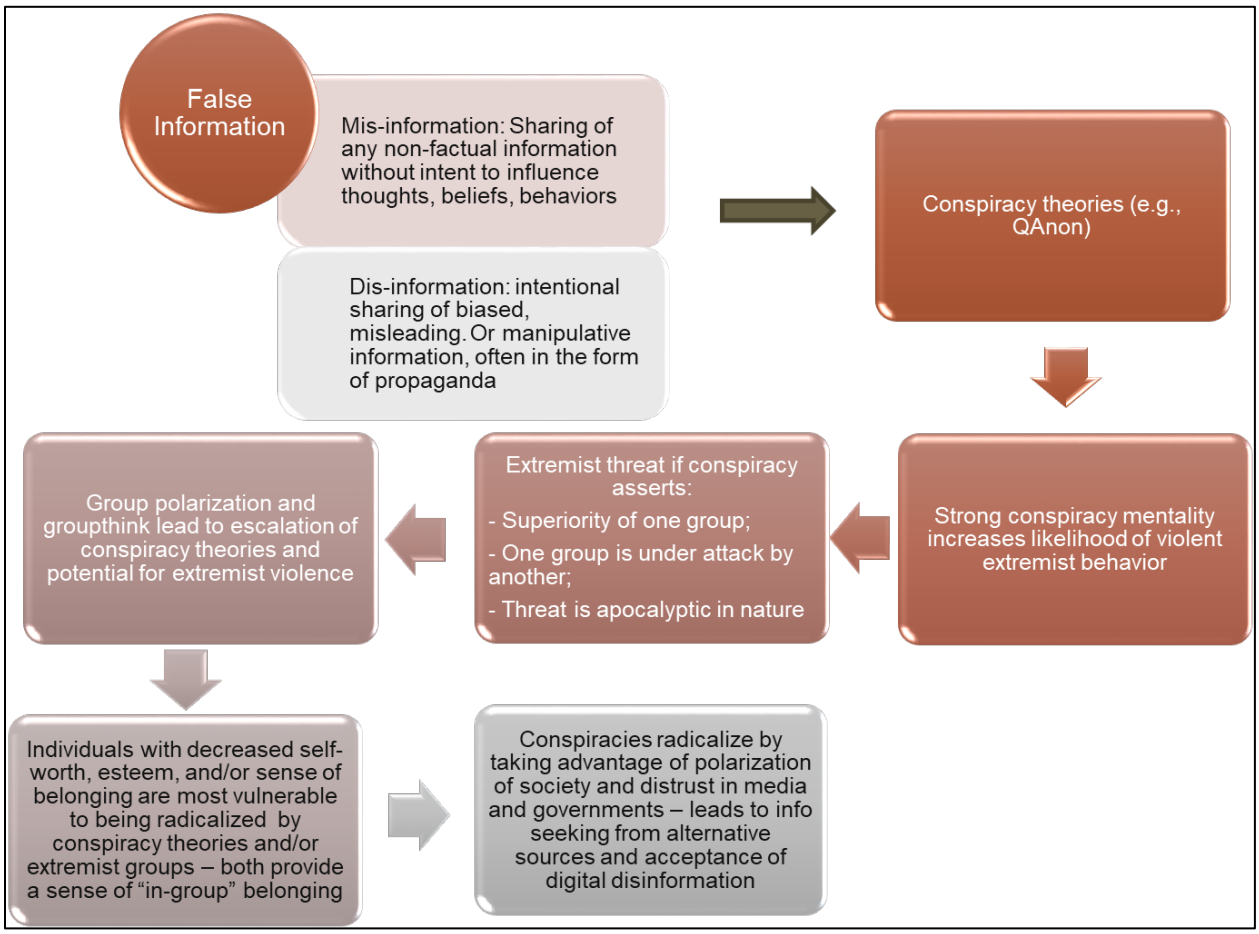


Figure 21. Role of False Information such as Conspiracy Theories on Radicalization

The risk of radicalization toward violence is exacerbated when a conspiracy mentality is associated with high self-confidence or self-efficacy[207] and/or low self-control. Those with high levels of both self-efficacy and conspiracy beliefs report that they are more likely to engage in violent action. In other words, increased confidence in one's own abilities, combined with other factors associated with radicalization, can potentially increase the likelihood that an individual

[206] Bettina Rottweiler and Paul Gill, "Conspiracy Beliefs and Violent Extremist Intentions: The Contingent Effects of Self-Efficacy, Self-Control, and Law-Related Morality," *Terrorism and Political Violence* (October 20, 2020): 1-20, https://www.tandfonline.com/doi/full/10.1080/09546553.2020.1803288.

[207] Self-efficacy effects behavioral intentions and thus is considered a predictor of human behavior. It refers to the belief that one has it in his or her ability (based on perceptions of his/her capabilities) to successfully perform an action or achieve a desired outcome. Research shows that higher levels of self-efficacy are associated with positive outcomes in terms of mental and physical health and normative prosocial intentions and behaviors. As such, self-efficacy has been examined as a potential protective factor to radicalization (Bandura 1997).

engages in violent extremism.[208] Similarly, high self-control mitigates the impacts of conspiracy beliefs, while having both conspiracy mentality and low self-control is a risk factor for radicalization to violent action.[209] Together, these findings suggest that debunking conspiracy theories alone may be insufficient to prevent potential violent action. Instead, CVE approaches need to incorporate the psychological, attitudinal (or emotional), and cognitive factors that allow individuals to adhere strongly to conspiracy theories, particularly those focused on political or societal imbalances.[210]

False information campaigns (including those involving conspiracy theories) are not easily reversed. Acquired beliefs may be extremely difficult to correct, even when individuals acknowledge that their views are based on incorrect, false, or erroneous information, or if the information was openly labeled a conspiracy theory.[211] Tactical responses, such as deploying fact-checking tools or adjusting social media algorithms to disincentivize false information and prevent it from appearing on newsfeeds, have shown mixed efficacy. Many media literacy approaches fall short because it is impossible to correct every false story, and even when corrections are issued, many individuals continue to rely on false information, especially when the messages involve a political context.[212]

Social and behavioral scientists have experimented with efforts to counter the spread of false information by fostering critical and well-informed consumers of online information. The goal of these approaches is to leverage behavioral science and education to empower the public at the individual level and thereby decrease the effectiveness of false information online (and presumably offline as well).

---

[208] These findings suggest that although higher self-efficacy is associated with increased resiliency, care must be taken when developing CVE intervention programs leveraging self-efficacy as a potential means to decrease vulnerability to radicalization.

[209] Rottweiler and Gill, "Conspiracy Beliefs and Violent Extremist Intentions." Legal cynicism is the cognitive process that leads to the desire (and decision) to deny the legitimacy of the law and support behaviors that are in opposition to laws and social norms. It can emerge in response to perceptions of persistent injustices and deprivations; Robert J. Sampson and Dawn Jeglum Bartusch, (1998). "Legal Cynicism and (Subcultural?) Tolerance of Deviance: The Neighborhood Context of Racial Differences," *Law & Society Review* 32, no. 4 (1998): 777–804, https://doi.org/10.2307/827739.

[210] Ibid. For political issues, assessing what constitutes a false story and false information has an added layer of complexity since many media outlets have political leanings and may be selective about what they cover, how much prominence it receives, and the context in which it is presented. The information in a news story may indeed be factual, but without providing an adequately broad and neutral context, the story may appear to someone holding opposing views to be more of a half-truth or an editorial. An assertion by a news organization with a known political leaning that a piece of information opposing their political view is "false information" may consequently be discounted or fall on deaf ears.

[211] Karen Douglas, Jan-Willem van Prooijen, and Robbie Sutton, "Is the Label 'Conspiracy Theory' a Cause or a Consequence of Disbelief in Alternative Narratives?" *British Journal of Psychology* 00 (December 17, 2021): 1-16, doi:10.1111/bjop.12548; Jerit and Zhao, "Political Misinformation."

[212] Stephan Lewandowsky, Ullrich K. H. Ecker, Colleen M. Seifert, Norbert Schwarz, and John Cook, "Misinformation and its Correction: Continued Influence and Successful Debiasing," *Psychological Science in the Public Interest* 13, no. 3 (September 17, 2012): 106-131, doi:10.1177/1529100612451018.

An inoculation approach developed by McGuire and Papageorgis[213] has been shown to be effective across a number of domains, such as health and politics.[214] The inoculation approach consists of two components: (1) an affective element that provides a warning to elicit and activate threat (or stress) in the message recipient to motivate them to protect their existing beliefs; and (2) a cognitive element that utilizes the counterargument process and provides specific content that can be used to resist persuasion attempts via information and education.[215] Research suggest that inoculation against false information does provide some protection for the recipient in terms of belief in the information and subsequent spread of that information.[216]

An alternative approach is to train readers of online content to evaluate information for consistency, congruence, and coherence. This method of evaluation for accuracy relies on the reader's ability (and willingness) to compare new and previously known information. Evaluation methods such as instructions to edit text for accuracy help readers identify false information and become less susceptible to the falsehood, but due to the level of effort required to engage in this type of evaluation, the reader must be motivated to engage in the evaluation process.[217] Further, although providing readers with substantial prompts to evaluate accuracy has been shown to decrease the likelihood that individuals will share the information online, drawing attention to inaccuracies also increases the reader's exposure to false information; in the absence of careful focus on the evaluation of accuracy, such added exposure could have negative results.[218]

---

[213] W. J. McGuire and D. Papageorgis, "The Relative Efficacy of Various Types of Prior Belief-Defense in Producing Immunity Against Persuasion," *Journal of Abnormal and Social Psychology* 62, no. 2 (March 1961): 327-337, doi: 10.1037/h0042026.

[214] Josh Compton, Ben Jackson, and James A. Dimmock, "Persuading Others to Avoid Persuasion: Inoculation Theory and Resistant Health Attitudes," *Frontiers in Psychology* 122, no. 7 (February 9, 2016), https://psycnet.apa.org/record/2016-19527-001; Michael Pfau, David Park, R. Lance Holbert, and Jaeho Cho, "The Effects of Party-and PAC Sponsored Issue Advertising and the Potential of Inoculation to Combat its Impact on the Democratic Process," *American Behavioral Scientist* 44, no. 12 (August 2001): 2379-2397, https://www.researchgate.net/publication/247751775_The_Effects_of_Party_and_PAC-Sponsored_Issue_Advertising_and_the_Potential_of_Inoculation_to_Combat_its_Impact_on_the_Democratic_Process.

[215] John A. Banas and Stephen A. Rains, "A Meta-Analysis of Research on Inoculation Theory," *Communication Monographs* 77, no. 3 (September 22, 2010): 281-311, https://doi.org/10.1080/03637751003758193.

[216] Sander van der Linden and Jon Roozenbeek, "Psychological Inoculation Against Fake News," Chap 9. In *The Psychology of Fake News*, edited by Eryn Newman, Mariella Jaffé, Norbert Schwarz, and Rainer Greifeneder (New York City, NY: Routledge, 2020), https://www.taylorfrancis.com/chapters/oa-edit/10.4324/9780429295379-11/psychological-inoculation-fake-news-sander-van-der-linden-jon-roozenbeek.

[217] David N. Rapp, Scott R. Hinze, Kristine Kohlhepp, and Rachel A. Ryskin, "Reducing Reliance on Inaccurate Information," *Memory & Cognition* 42 (June 13, 2013): 11-26, doi:10.3758/s13421-013-0339-0; Tobias Richter and David N. Rapp, "Comprehension and Validation of Text Information: Introduction to the Special Issue," *Discourse Processes* 51, no. 1-2 (January 9, 2014): 1-6, doi:10.1080/0163853X.2013.855533; Murray Singer, "Challenges in Processes of Validation and Comprehension," *Discourse Processes* 56, no. 5-6 (April 19, 2019): 1-19, doi:10.1080/0163853X.2019.1598167.

[218] Lisa Fazio, "Pausing to Consider why a Headline is True or False can Help Reduce the Sharing of False News," *The Harvard Kennedy School Misinformation Review* 1, no. 2 (February 10, 2010): 1-8, doi:10.37016/mr-2020-

The use of metacognitive prompts, or asking readers to reflect on past experiences with false information seems to help individuals think about the role false information has played (or could play) in their personal experiences and thus, can motivate them to engage in deeper evaluation of statement accuracy.[219] A simpler prompt is to ask readers to explain why a headline to a story is true or false.[220] One benefit of such accuracy prompts is that the decision regarding who is the arbiter of the truth is taken out of the equation. Accuracy and metacognitive prompts rely on the individual reader to make the determination for him or herself regarding which information is true and which is false, thus reducing pushback regarding "who decides" what information is false. Another benefit is that these approaches can be scaled up to large groups and populations of users.[221]

These inoculation approaches may be effective because they encourage readers to slow down and think more deeply about their actions rather than automatically sharing information after a cursory glance at it. It may be that readers initially plan to share information regardless of its accuracy, but when made to pause, they are able to resist this tendency and reevaluate their actions.[222] It is possible that these prompts may shift readers' motivations for sharing information, increasing the value of accurate information to outweigh that of information that is merely

009; Andrea Eslick, Lisa Fazio, and Elizabeth Marsh, "Ironic Effects of Drawing Attention to Story Errors," *Memory* 19, no. 2 (February 2, 2011): 184-191, doi:10.1080/09658211.2010.543908.

[219] (Johanna Abendroth and Tobias Richter, "How to Understand What you don't Believe: Metacognitive Training Prevents Belief-Biases in Multiple Text Comprehension," Learning and Instruction 71 (February 2021): 1-16, https://www.sciencedirect.com/science/article/pii/S095947521930739X.) Nikita A. Salovich and David N. Rapp, "Misinformed and Unaware? Metacognition and the influence of Inaccurate Information," *Journal of Experimental Psychology: Learning, Memory, and Cognition* 47, no. 4 (April 2021): 608-624, doi:10.1037/xlm0000977, asked study participants to think about instances in which they have encountered inaccurate information in their own lives and to generate ideas regarding how they could improve their evaluation when reading in order to avoid being influenced by false information in the future. They found that participants who did not receive metacognitive prompts made twice as many judgement errors regarding the accuracy of information than participants who received the metacognitive prompts.

[220] Fazio conducted a study in which she engaged some participants in this very exercise. Prior to rating how likely they were to share a political news story based on the headline alone, she asked participants to explain how the reader determined whether the headline was true or not. This accuracy prompt led to a reduction in participants' intentions to share false headlines but had no effect on true headlines. This effect was largest when participants were seeing the headline for the first time. Liz Fazio, "Pausing to Consider why a Headline is True or False can Help Reduce the Sharing of False News," *Harvard Kennedy School Misinformation Review*, February 10, 2020, https://doi.org/10.37016/mr-2020-009.

[221] For example, Instagram installed a prompt asking users, "Are you sure you want to post this?" before they are able to post comments that are identified as possibly being bullying in nature (Dave Lee, "Instagram now asks Bullies "Are you Sure?" BBC News, July 8, 2019, www.bbc.com: https://www.bbc.com/news/technology-48916828?).

[222] Bence Bago, David Rand, and Gordon Pennycook, "Fake News, Fast and Slow: Deliberation Reduces Belief in False (but not true) News Headlines," *Journal of Experimental Psychology: General* 149 (January 9, 2020): 1608-1613, doi:10.1037/xge0000729.

entertaining.[223] The effectiveness of interventions designed to counter belief in and spread of false information (also known as media literacy efforts) varies across individuals.[224]

While this research is promising, it remains limited. The current body of literature is often focused on specific subpopulations (e.g., users of a single digital communication medium) and/or issues (e.g., politics) and randomized controlled trials (the gold standard in empirical research) are rare.[225] Another limitation is that although extensive efforts are being made on these initiatives, there are only a few large-scale studies supporting the use of media literacy as a response to false information. Finally, although media literacy interventions have been successful in improving critical thinking outcomes regarding false information, they have been less successful in behavioral outcomes (e.g., change in practice). This is likely due to the fact that most media literacy interventions focus on cognitive and not behavioral change.

---

[223] Fazio, "Pausing to Consider why a Headline is True or False can Help Reduce the Sharing of False News."

[224] For example, Mohsen Mosleh, Gordon Pennycook, Antonio A. Arechar, and David G. Rand, "Cognitive Reflection Correlates with Behavior on Twitter," *Nature Communications* 12 (February 10, 2021): 921, doi:10.1038/s41467-020-20043-0 investigated the relationship between individual difference in cognitive reflection and behavior on Twitter. They found that those scoring higher on the Cognitive Reflections Test (a well-known measure of reflective thinking) were more judicious in their social media use based upon the type and number of accounts they followed on Twitter and the reliability of the news sources they shared with other users. Specifically, those who engaged in more cognitive reflection shared higher quality content from more reliable sources and tweeted about weightier subjects. In general, it appears that more reflective thinking, which serves as a barrier to misinformation and disinformation, may be positively associated with disbelief in religion, the paranormal, and conspiracy theories (Gordon Pennycook, James Allen Cheyne, Paul Seli, Derek J. Koehler, and Jonathan A. Fugelsang, "Analytic Cognitive Style Predicts Religious and Paranormal Beliefs," *Cognition* 123, no. 3 (June 2012): 335-346, doi:10.1016/j.cognition.2012.03.003; Viren Swami, Martin Voracek, Stefan Stieger, Ulrich S. Tran, and Adrian Furnham, "Analytic Thinking Reduces Belief in Conspiracy Theories," *Cognition* 133, no. 3 (December 2014): 572-585, doi:10.1016/j.cognition.2014.08.006) and with an increased acceptance of science (Pennycook, Cheyne, Koehler, and Fugelsang, "Analytic Cognitive Style Predicts Religious and Paranormal Beliefs"). Reflectionistic perspective taking is also positively associated with a decreased likelihood of believing false new stories, decreased sharing of false news, and decreased trust in hyper-partisan news sources (Bago, Rand, and Pennycook, "Fake News, Fast and Slow"; Gordon Pennycook and David G. Rand, "Lazy, not Biased: Susceptibility to Partisan Fake News is Better Explained by Lack of Reasoning Than by Motivated Reasoning," *Cognition* 188 (July 2019): 39-50, doi:10.1016/j.cognition.2018.06.011; Gordon Pennycook and David G. Rand, "Fighting Misinformation on Social Media Using Crowdsourced Judgments of News Source Quality," *Proceedings from the National Academies of Sciences of the United States of America* 116, no. 7 (January 28, 2019): 2521-2526, doi:10.1073/pnas.1806781116.

[225] Andrew Guess, Michael Lerner, Benjamin Lyons et al., "A Digital Media Literacy Intervention Increases Discernment between Mainstream and False News in the United States and India," *Proceedings from the National Academies of Sciences* 117, no. 27 (June 22, 2020): 15536-15545, https://www.pnas.org/doi/10.1073/pnas.1920498117; Alice Huguet, Jennifer Kavanagh, Garrett Baker, and Marjory Blumenthal, *Exploring Media Literacy Education as a Tool for Mitigating Truth Decay* (Santa Monica, CA: RAND Corporation, 2019), https://www.rand.org/pubs/research_reports/RR3050.html.

6. Strategies to Counter Radicalization

A. Lessons from Outside the Department of Defense

Countering terrorism has become a common feature of national security strategies for the United States and other Western nations over the past decade. The United States established formal CVE objectives in a 2011 *Strategic Implementation Plan for Empowering Local Partners to Prevent Violent Extremism in the United States* (SIP).[226] The national CVE strategy focused on three primary lines of effort: (1) preventing radicalization, (2) disengagement from extremist groups, and (3) de-radicalization programs that focus on altering the extremist beliefs that individuals hold. Generally, these programs focus on affecting large groups, as compared to disengagement and de-radicalization programs, which have an individually-tailored focus.[227] All three lines of effort prioritize preventative actions using community-based approaches to bring together government, law enforcement, and local communities to counter recruitment, radicalization, and mobilization by potential violent extremists.[228]

In 2017, the U.S. Government Accountability Office (GAO) released a report assessing domestic federal CVE efforts. Although the SIP was released in 2011, GAO reported that an interagency task force led by DHS and the FBI to coordinate federally-funded CVE efforts was not created until 2016. The Task Force updated the SIP and sharpened its focus on empowering communities and society, messaging and counter-messaging, and addressing drivers to radicalization and extremism. The GAO review found that these efforts failed to provide stakeholder agencies with specific direction and metrics by which to identify program successes and implementation gaps. As a result, GAO reported, "we could not determine the extent to which the United States is better off today as a result of its CVE effort than it was in 2011." It appears that the Task Force was disbanded before it could address any of the GAO recommendations.[229]

---

[226] Executive Office of the President, *Strategic Implementation Plan for Empowering Local Partners to Prevent Violent Extremism in the United State* (Washington, DC: Executive Office of the President, December 2011), https://obamawhitehouse.archives.gov/sites/default/files/sip-final.pdf.

[227] Caitlin Mastroe, and Susan Szmania, *Surveying CVE Metrics in Prevention, Disengagement and De-Radicalization Programs* (College Park, MD: START, March 2016), https://www.start.umd.edu/pubs/START_SurveyingCVEMetrics_March2016.pdf.

[228] Sarah Chaney Reichenbach, "CVE and Constitutionality in the Twin Cities: How Countering Violent Extremism Threatens the Equal Protection Rights of American Muslims in Minneapolis-St. Paul," *American University Law Review* 69, no. 6 (2020): 1989-2046, https://digitalcommons.wcl.american.edu/cgi/viewcontent.cgi?article=2222&context=aulr.

[229] Government Accountability Office (GAO), *Countering Violent Extremism: Actions Needed to Define Strategy and Assess Progress of Federal Efforts* (Washington, DC: GAO, April 6, 2017), https://www.gao.gov/assets/gao-17-300.pdf.

Although the whole of government approach to CVE has not been fully successful to date, continued study in the academic community and experimentation by government agencies have resulted in the development of two approaches that show some promise for the Department and the military community: (1) a resiliency model; and (2) a comprehensive threat assessment model.

1. Building Resiliency

a. Approaches in the Scholarly Literature

The concept of a "resilient individual" is that radicalization might be prevented through the development of capacities, skills, or characteristics that serve as a protective factor at the individual level.

One approach to building the "resilient individual" focuses on helping individuals build the capacity to assess and question messages, ideas, and propaganda (i.e., false information), by identifying and accessing a wider range of their own values. This approach seeks to move individuals from rapid, inflexible, and closed black and white thinking to a more deliberate, flexible, open thinking style that allows them to see the benefit of other opinions without diminishing their own values.[230] Cognitive capacity may also be increased by focusing on the development of critical thinking skills or the ability to evaluate information by questioning and analyzing its source. It is important that any critical thinking or cognitive capacities skill building training and education avoid telling individuals what to think—the focus must be on the individual's abilities to think for themselves.

Another approach focuses on developing character traits that might serve as protective factors that might be stronger than possible pull factors in radicalization. It is theorized that in order to engage in violent radicalization, individuals undergo a process of dehumanizing the "other" such that they disengage from their internal moral standards that would normally serve to prevent violent engagement. The Beyond Bali intervention addresses this issue by focusing on the development of empathy for terrorism victims and the perspective that violent extremism is morally unjust and cruel.[231] It may also be possible to develop character traits as protective factors by promoting values that serve as a preventative framework against radicalization. For example,

---

[230] Eloene M. Boyd-MacMillan, "Increasing Cognitive Complexity and Collaboration Across Communities: Being Muslim Being Scottish," *Journal of Strategic Security* 9, no. 4 (Winter 2016): 79-110, doi:10.5038/1944-0472.9.4.1563; Jose Liht and Sara Savage, "Preventing Violent Extremism Through Value Complexity: Being Muslim Being British," *Journal of Strategic Security* 6, no. 4 (2013): 44-66, doi:10.5038/1944-0472.6.4.3.

[231] Anne Aly, Elisabeth Taylor, and Saul Karnovsky, "Moral Disengagement and Building Resilience to Violent Extremism: An Educational Intervention," *Studies in Conflict & Terrorism* 37, no. 4 (March 11, 2014): 369-385, doi:10.1080/1057610X.2014.879379.

focusing on citizenship, diversity, and human rights might offer groups of individuals a shared value base on which to build moral development.[232]

Tied to the concept of developing a "resilient individual" is the idea that radicalization occurs when there is a real or perceived threat to, or marginalization of, one's group identity.[233] For this reason, identity development may play a role in preventing radicalization. The self-concept (i.e., the conception and evaluation individuals form of themselves) serves as an organizing and planning mechanism for individuals to understand both who they are and how to relate to others so as to make their social environment more predictable. An approach that dominates the rich theoretical traditions that describe self and identity processes proposes that the sense of self is greatly affected by group memberships, defining social identity as "that part of the individual's self-concept which derives from his [her] membership of a social group (or groups) together with the value and emotional significance attached to that membership."

In the development of a self-concept, groups can represent a powerful source for self-enhancement (i.e., positive image of self), but groups also help reduce uncertainty about who one is and how one should behave, particularly with others. Self-enhancement and uncertainty reduction however, serve as distinct motivators; whereas self-enhancement helps understand the pull of in-group and intergroup status and prestige, the aversive feeling associated with self-related uncertainty has been found to be more potent and more stable in motivating group identification. Further, some types of groups are better suited than others to reduce self-related uncertainty.

The need for both the opportunity and space to discuss the issues of radicalization and extremism without fear of condemnation has also been highlighted in the literature. Disparaging radical views or groups might lead to an individual feeling targeted and/or may prevent productive communication that could lead to change. Further, similar opportunity and space must be created in order for individuals to discuss grievances and frustrations related to perceptions of power[234] rather than passively receiving a message from leadership. Grievances play a role in the susceptibility to conspiracy theories and false information, so supporting the opportunity for individuals to share their grievances and feel that they are being heard may help counter push and pull factors for radicalization.

---

[232] Joyce Miller, "REsilience, Violent Extremism, and Religious Education," *British Journal of Religious Education* 35, no. 2 (November 23, 2012): 188-200, doi:10.1080/01416200.2012.740444.

[233] William Stephens, Stijn Sieckelinck, and Hans Boutellier, "Preventing Violent Extremism: A Review of the Literature," *Studies in Conflict & Terrorism* 44, no. 4 (January 2, 2019): 346-361, doi:10.1080/1057610X.2018.1543144.

[234] Angela Quartermaine, "Discussing Terrorism: A Pupil-Inspired Guide to UK Counterterrorism Policy Implementation in Religious Education Classrooms in England," *British Journal of Religious Education* 38, no. 1 (September 5, 2014): 13-29, doi:10.1080/01416200.2014.953911; Adrian Cherney and Jason Hartley, "Community Engagement to Tackle Terrorism and Violent Extremism: Challenges, Tensions and Pitfalls," *Policing and Society* 27, no. 7 (October 5, 2015): 750-763, doi:10.1080/10439463.2015.1089871.

Finally, advocates of resilient communities seek to build on features and characteristics of communities, such as the quality of relationships and social connections, that prevent their members from being drawn to extremism.[233] Some of the work on resilient communities focuses on communities that have faced disasters to better understand what it means to be a resilient community. This literature examines the relationship between individuals in communities (i.e., social bonding), between communities (i.e., social bridging), and between communities and institutions (i.e., social linking). Together, these relationships are indicative of the community's social capital, or the "existence of trust-based relationships and networks among local actors, including the government."[235] The research suggests that strengthening these relationships leads to increased resiliency within communities, which may reduce vulnerability to radicalization.

Taken together, the literature on Preventing and Countering Violent Extremism (P/CVE) emphasizes resilience building, both at the individual and community levels—a strength-based approach that builds on societal strengths rather than a deficits-oriented or punitive approach. The attention to building identity using core values and cognitive approaches to develop a deliberate, flexible, open-thinking style, while supporting open dialogue within the context of a resilient community, is a way to reduce individual and group vulnerabilities to radicalization and avoid the marginalization of individuals, groups, or ideas.

b. Approaches taken by Other Federal Agencies

Within the federal government, two agencies have taken the lead in efforts to build resiliency against radicalization and terrorism: DHS and the FBI.

Within the FBI, the Behavioral Analysis Unit (BAU) and the National Center for the Analysis of Violent Crime (NCAVAC) help to coordinate investigative and operational support functions, criminological research, and training to assist Federal, State, Local, Tribal, and Territorial (SLTT) law enforcement in investigating and preventing violent crimes. The FBI's Behavioral Threat Assessment Center (BTAC) is a multi-agency, multi-disciplinary task force[236] focused on the prevention of terrorism and targeted violence, leveraging behavioral science-based support, training, and research to address these issues. BTAC routinely conducts case studies to enhance and improve prevention efforts and provides law enforcement agencies with threat assessment and management consultations, communication analysis, interview and investigative strategies, and training.[237]

---

[235] Anja Dalgaard-Nielsen and Patrick Schack, "Community Relience to Militant Islamism: Who and What?: An Explorative Study of Resilience in Three Danish Communities," *Democracy and Security* 12, no. 4 (October 13, 2016): 309-327, doi:10.1080/17419166.2016.1236691.

[236] Members of BTAC include the FBI; U.S. Capitol Police; Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF); analysts; and psychiatrists.

[237] Federal Bureau of Investigation. *News*. Retrieved from FBI Behavioral Threat Assessment Center Releases Lone Offender Terrorism Report, November 13, 2019, https://www.fbi.gov/news/pressrel/press-releases/fbi-behavioral-threat-assessment-center-releases-lone-offender-terrorism-report. In 2019, BTAC released its Lone

DHS is charged with engaging in preventative and protective actions against terrorism and targeted violence.[238] DHS has addressed this responsibility with a preventative approach that supports the integration of programs to increase community resiliency to reduce radicalization. The DHS approach to community resiliency relies on a number of findings identified earlier in this report, such as that grievances can play a role in radicalization, close friends and family might be best positioned to recognize individuals exhibiting signs of radicalization, and false information can play a role in radicalization. DHS seeks to support community resiliency to radicalization by working with community organizations to share up-to-date findings regarding risk factors and behavioral indicators of radicalization, the threat environment, what bystanders can do when an individual is exhibiting concerning behavior, and counter-messaging and educational efforts to combat radicalization via false information.[239]

To this end, the DHS Science and Technology Directorate sponsors data collection and analysis from empirical studies in order to characterize threats and opportunities for prevention and to evaluate terrorism and targeted violence prevention programs and interventions. Additionally, DHS's Center for Prevention Programs and Partnerships (CP3) provides technical, financial, and educational assistance to local (societal/community-based) efforts to prevent radicalization. For example, CP3 provides funding for communities to expand their prevention and intervention activities or to address gaps in their current radicalization prevention capabilities through the replication of existing practices or the exploration of new or innovative approaches. CP3 also hosts a Digital Forum on Prevention series in which community leaders are convened to discuss prevention services and approaches, emerging trends in radicalization, and to build community relationships to strengthen radicalization prevention efforts. Finally, CP3 provides communities with briefings and publications focused on prevention efforts and tools to combat radicalization and targeted violence.[240]

Although these approaches may be difficult to scale to American society as a whole, they are likely to have significant applicability to a military organization that benefits from an

---

Offender Terrorism Report. In this report, BTAC compared offender motivational factors with their backgrounds, family and social networks, behavioral characteristics, radicalization ideologies, planning of the attack, and bystander observations. The findings of the report are consistent with the findings regarding risk factors to radicalization described above, however, the report provides information regarding these attacks that can be leveraged by threat assessment programs. Federal Bureau of Investigation Behavioral Threat Assessment Center, *Lone Offender: A Study of Lone Offender Terrorism in the United States (1972-2015)* (Washington, DC: U.S. Department of Justice, Federal Bureau of Investigation, Behavioral Analysis Unit, National Center for the Analysis of Violent Crime, November 13, 2019, https://www.fbi.gov/file-repository/lone-offender-terrorism-report-111319.pdf/view.

[238] Department of Homeland Security, *Strategic Framework for Countering Terrorism and Targeted Violence* (Washington, DC: Department of Homeland Security, September 2019): 2, https://www.hsdl.org/?abstract&did=829572.

[239] Ibid.

[240] Department of Homeland Security Website. "Center for Prevention Programs and Partnerships," accessed June 16, 2022, https://www.dhs.gov/CP3.

encompassing personnel system and a comprehensive training and education program that together could provide a natural framework for the incorporation of resiliency training.

2. The Threat Assessment Model

The NTAC, a part of DHS that is overseen by the United States Secret Service (USSS), has taken a different approach to CVE. NTAC was established in 1998 to provide research and guidance in support of the USSS and public safety. The USSS has long maintained that threat assessment is the most effective practice for preventing acts of violence against the President and other public officials. Through its research efforts, NTAC has begun to apply this approach to preventing other forms of violence affecting U.S. communities.

Since its inception, NTAC has conducted research that has resulted in briefings and reports on behavioral case studies of terrorists and individuals who engaged in targeted violence, school/campus attacks, mass attacks in public spaces, and mass attacks against the government.[241] Of particular relevance to the current report is NTAC's research on threat assessments for preventing targeted school violence. Although targeted school violence and extremism in the military may not seem related, NTAC has found that students often display a variety of observable concerning behaviors as they escalate towards violence, similar to those observable concerning behaviors of individuals who become radicalized towards violent action. Further, many of the risk factors to radicalization described earlier in this report are common to students who plotted and/or perpetrated school attacks. Specifically, many of these students had histories of school discipline and contact with law enforcement, experienced bullying or had mental health issues, used drugs or alcohol, and had been impacted by adverse childhood experiences.

A 2021 NTAC report analyzing plots against schools (i.e., thwarted attacks) concluded that a comprehensive threat detection system is the key to forestalling violent events.[242] NTAC identified a number of key findings that resonate with findings from radicalization and terrorism case studies. For example:

- Because the primary function of threat assessment is not a criminal investigation or conviction, communities should seek to identify and intervene with students (or individuals) in distress before the behavior escalates to a criminal act.

---

[241] United States Secret Service Website, "National Threat Assessment Center," accessed June 16, 2022, https://www.secretservice.gov/protection/ntac.

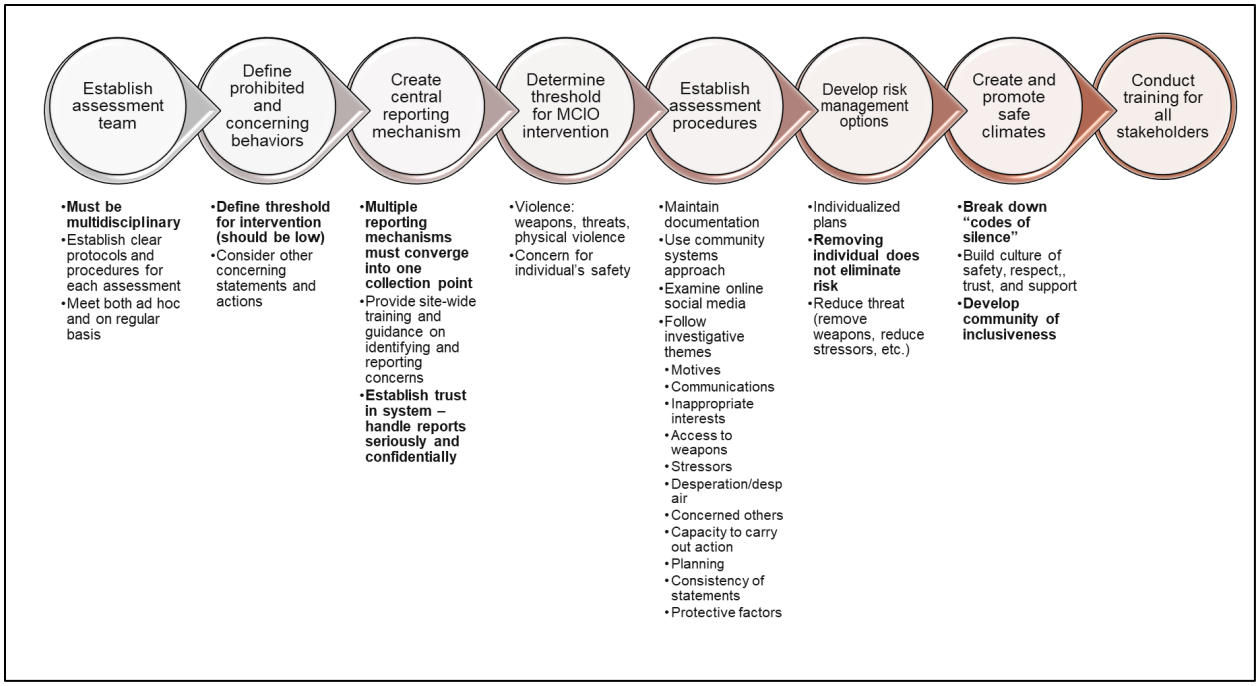
[242] Lina Alathari, Diana Drysdale, Steven Driscoll, et al., *Averting Targeted School Violence: A U.S. Secret Service Analysis of Plots Against Schools* (Washington, DC: U.S. Department of Homeland Security, United States Secret Service, National Threat Assessment Center, March 2021), https://www.secretservice.gov/sites/default/files/reports/2021-03/USSS%20Averting%20Targeted%20School%20Violence.2021.03.pdf.

- A strong motivating factor for students who planned and carried out school attacks was a grievance with classmates, indicating a need for de-escalation programs focused on addressing grievances.
- Peers (friends and family) are best positioned to identify and report concerning behaviors; thus, their roles in recognizing such behavior are critical to prevention (and speaks to DHS's support of community resiliency).
- Immediate assessment and intervention should be provided to students (or individuals) displaying an interest in violent or hate-filled topics—this includes both an interest in prior acts of terrorism and targeted violence and in violent extremist ideology.

This list makes clear that regardless of age or context of the planned violent attack, many of the risk and contextual factors that might drive an individual to engage in terrorism (due to radicalization) are the same as those that might lead to an act of targeted violence.

NTAC has been supporting research and training on the safety of children in American schools since 2002; however, in 2018, NTAC first provided guidance to schools on the development of targeted violence prevention programs. NTAC maintains that an individual's risk of violence can best be understood by engaging in the threat assessment process, which allows for the collection of the most relevant information about the individual's communications and behaviors, negative or stressful events that he or she has experienced, and the resources that she or he may have to overcome negative events (i.e., protective factors). The NTAC guidance outlines eight actionable steps, listed in Figure 22, that schools can use to identify individuals exhibiting behaviors that may be of concern, collect information to assess risk, and provide risk management strategies to ensure positive outcomes for the at-risk individuals and community.[243]

[243] National Threat Assessment Center, *Enhancing School Safety Using a Threat Assessment Model: An Operational Guide for Preventing Targeted School Violence* (Washington, DC: U.S. Department of Homeland Security, United States Secret Service, National Threat Assessment Center, July 2018), https://www.cisa.gov/sites/default/files/publications/18_0711_USSS_NTAC-Enhancing-School-Safety-Guide.pdf.



Source: adapted from National Threat Assessment Center, 2018.

Figure 22. NTAC Threat Assessment Model

Because schools are embedded in communities, NTAC has developed training programs for and provides consultations to both schools (including administration, school boards, resource officers, teachers) and SLTT law enforcement entities. NTAC also provides corporate security training and consultation to reduce the risk of workplace violence and has provided consultation to military services to develop workplace violence prevention policies.

Similar threat assessment programs, although still relatively small in number, have been established at city, county, and state levels (often with the assistance of NTAC). For instance, the city of Aurora, Colorado, has a Targeted Violence Prevention program to "identify behaviors exhibited by a person suffering from a mental illness or mental health, which are indicative of being on a pathway to future act(s) of targeted mass violence." Members of the Rochester (New York) Threat Advisory Committee (ROCTAC), Pinellas County (Florida) Sheriff's Office Threat Management Section, and North Carolina State Bureau of Investigation's Behavioral Threat Assessment Unit described similar programs to the IDA team.

The Pinellas County Sheriff's Threat Management Section (P/TMS) is described in detail here because it appears to be the strongest program, having implemented a continuous monitoring and reassessment approach, with the goal of removing individuals from the pathway to violence. The program was developed as part of efforts to prevent school shootings after the Marjory Stoneman Douglas High School shooting on 14 February 2018, in Parkland, Florida. Prior to the existence of the P/TMS, reports of concerning behaviors would be made to a school official; the school's principal would speak to teachers and perhaps to the at-risk student before issuing some

punishment to the student. The Pinellas County Sherriff's Office reported that the usual process for addressing behaviors of concerns was informal and inconsistent, such that students with involved parents might receive a suspension or detention, while other students would receive harsher punishments for exhibiting the same behaviors.

The P/TMS consists of a mix of law enforcement officers (lieutenants, sergeants, detectives, and uniformed officers), analysts, threat management professionals, and behavioral health specialists who cover the Section 15 hours per day, seven days per week. The P/TMS evaluates individuals exhibiting behaviors of concern based on three principles: identification, assessment, and management. Seven sources of information are consulted to identify at-risk individuals:

- School-based threat assessments (transient and serious: serious go to the school board for threat assessment and trigger mandatory threat assessment by the P/TMS).
- Risk protection orders (triggers mandatory threat assessment by the P/TMS).
- Domestic violence arrests (more than two arrests in 90 days).
- Directed reports by public officials (e.g., public defenders; report triggers mandatory threat assessment by the P/TMS).
- Florida Department of Law Enforcement firearms non-approvals (reported to the state; triggers mandatory threat assessment by the P/TMS).
- Baker Act Incidents (anyone who has been the subject of three or more mental health evaluations in 90 days and poses a threat to themselves or others).
- Law Enforcement reports (analysts review each incoming report to determine if the incident meets the criteria for assessment; criteria include targeted/planned violence, threats of violence, intimidation or bullying, comments about harming others, stalking, arson, animal cruelty, fixation on mass murder/weapons/violence, fixation on hate groups).

The P/TMS engages in a systematic evidence-based approach to determine if the person of concern is on the pathway to engage in a violent act and assigns a "Level of Concern" for that individual (e.g., low, moderate, elevated, critical)[244]. Specifically, the P/TMS—

- Determines whether an immediate action should be implemented to mitigate the threat.
- Pulls together background information in a report to distribute it to the team.
- Conducts witness interviews (with neighbors, friends, and family) and determines if another intermediate threat assessment needs to be conducted based on this information.

[244] The Threat Management Section reported that from March 10th to September 4th, 2021, the team reviewed 26,290 reports against criteria list which led to 753 assessments. Of these assessments, 86.4% were assessed as low levels of concern, 11.6% moderate, 1.1% elevated, and 0.8% critical.

- Conducts interviews with the person of concern and determines if another intermediate threat assessment needs to be conducted based on this information.
- Reviews the case with the entire team and conducts another immediate action assessment.
- Assigns a Level of Concern that informs the threat management process.

Finally, the P/TMS develops a coordinated management plan with direct and indirect interventions based on all of the information gathered and assessments conducted regarding the person of concern. They assemble a behavioral threat management team comprising a wide range of expertise (e.g., Child Protection Investigators, School Resources Officers, psychologists, community leaders) that meets weekly to review cases under assessment. During these meetings, the team continues to discuss and develop indirect and direct plans to move the individual off the pathway to violence. In cases in which the risk level is low, a detective will follow-up with the person of concern and a family member at 90 days after the assessment, at which time (if the team agrees), the case is dismissed. In moderate risk cases, the person of concern and a family member are interviewed monthly for one year, and the safety plan is assessed after each interview. In elevated risk cases, the individual and family member are interviewed by a detective bi-weekly, and the safety plan is assessed after each interview. Finally, in critical cases, the interviews and safety plan review occur weekly.

B. Building Resiliency in Service Members

The military's first line of defense against prohibited extremist activities is leadership and culture. The military, as a group characterized by clear values, rules of interaction and expectations, unambiguous membership criteria, cohesion, enduring qualities, shared goals, and common fate can be described as having *high entitativity*.[245] Such groups tend to reduce self-related uncertainty,[246] reducing the motivation to join other groups for this purpose. In this way, a developed identity as a soldier, sailor, airman, marine, or guardian makes a service member less vulnerable to radicalization, or more resilient to the influence of radicalization efforts.

---

[245] Donald T. Campbell, "Common Fate, Similarity, and Other Indices of the Status of Aggregates of Persons as Social Entities," *Behavioral Science* 3, no. 1 (1958): 14–25, https://doi.org/10.1002/bs.3830030103; D. L. Hamilton and S. J. Sherman, "Perceiving Persons and Groups," *Psychological Review* 103, no. 2 (1996): 336–355, https://doi.org/10.1037/0033-295X.103.2.336; B. Lickel, D. L. Hamilton, G. Wieczorkowska, A. Lewis, S. J. Sherman, and A. N. Uhles, "Varieties of Groups and the Perception of Group Entitativity," *Journal of Personality and Social Psychology* 78, no. 2 (2000): 223–246, https://doi.org/10.1037/0022-3514.78.2.223.

[246] J. Jetten, M. A. Hogg, and B.-A. Mullin, "In-Group Variability and Motivation to Reduce Subjective Uncertainty," *Group Dynamics: Theory, Research, and Practice* 4, no. 2 (2000): 184–198, https://doi.org/10.1037/1089-2699.4.2.184; Vincent Yzerbyt, Emanuele Castano, Jacques-Philippe Leyens, and Maria-Paola Paladino, "The Primacy of the Ingroup: The Interplay of Entitativity and Identification," *European Review of Social Psychology* 11, no. 1 (2000): 257-295, https://www.tandfonline.com/doi/abs/10.1080/14792772043000059; Cynthia L. Pickett and Marilynn B. Brewer, "Assimilation and Differentiation Needs as Motivational Determinants of Perceived In-Group and Out-Group Homogeneity," *Journal of Experimental Social Psychology* 37, no. 4 (July 2001): 341–348, https://doi.org/10.1006/jesp.2000.1469.

Each of the military services seeks to build a culture of excellence, including character, competence, and connectedness, and recognizes that this is a fundamental leadership responsibility. The process of building a culture of excellence starts with the inculcation of positive values through a process of training and education. Training and education in military core values is part of the process of becoming a soldier, sailor, airman, marine, or guardian. A Marine Corps leadership document explains, "Being a Marine is not a job or a particular occupational specialty. It is a calling. It is a state of mind."[247]

The services reinforce their codes of conduct with a set of "core values" that exemplify what it means to serve. The Army's core values are loyalty, duty, respect, selfless service, honor, integrity, and personal courage.[248] The core values of the Navy[249] and the Marine Corps[250] are honor, courage, and commitment. The Air Force's core values are Integrity, Service, and Excellence.[251] Military values can serve as a bulwark against radicalization by reducing self-related uncertainty and providing a basis for decision-making, a source of enduring aspiration, and a domain for self-categorization.

These military core values all include an element of treating others with dignity and respect that is at its heart inconsistent with the types of violent extremist and supremacist behaviors that constitute prohibited extremist activities. The Army core value of respect includes a pledge to "treat others with dignity and respect while expecting others to do the same." The Navy core value of commitment calls for showing "respect toward all people without regard to race, religion or gender" and treating each individual with human dignity. The Marine Corps core value of honor calls upon marines to "respect human dignity; and to have respect and concern for each other." The Air Force core value of respect directs airmen to "exhibit self-control and possess respect for the beliefs, authority and worth of others." One senior DOD official told the IDA team, "The most important weapon against intolerance is understanding and education."

The process of inculcating military core values through training and education begins with recruiting and continues until a service member returns to civilian life. Senior DOD officials told IDA that the military services are deliberate in their training of values, including lessons of civics and treating others with dignity and respect. "We don't do a good job of teaching civics in school anymore," one interviewee stated, so "the military has to make up for that deficiency in its own training. A positive mission—shared mission, shared identity, shared values—is a vital part of

---

[247] Marine Corps Warfighting Publication (MCWP) 6-10 (Formerly 6-11), *Leading Marines*, PCN 143 00129 00 (Washington, DC: Headquarters United States Marine Corps, January 23, 2019): 1-2, https://www.marines.mil/portals/1/Publications/MCWP%206-10.pdf?ver=2018-09-20-104415-507.

[248] "The Army Values," Army.mil Website, accessed June 16, 2022, https://www.army.mil/values/.

[249] "Our Core Values," Navy.mil Website, accessed June 16, 2022, https://www.navy.mil/About/Our-Core-Values/.

[250] "About the Marine Corps Values," Marines.mil Website, accessed June 16, 2022, https://www.hqmc.marines.mil/hrom/New-Employees/About-the-Marine-Corps/Values/.

[251] "Air Force Values and Corresponding Virtues," AF.mil Website, accessed June 16, 2022, http://www.usafa73.org/uploads/6/4/4/5/64457159/core_values_and_virtures.pdf.

building a cohesive force and weeding out individuals who do not belong." A second interviewee agreed, telling the IDA team, "When you focus on respect and positive values, and hit it hard from all parts of the force, at all levels of leadership, you'll get isolated incidents instead of systematic problems."[252]

The unique demands of military service require a comprehensive training and education process to transform civilian men and women into military professionals. For enlisted service members, the process begins with initial/basic training, or boot camp; for officers, it begins with schooling at one of the service academies, in the Reserve Officer Training Corps (ROTC), or in Officer Candidate School (OCS) or Officer Training School (OTS). These programs are only the beginning of a career-long continuum of professional military education (PME), both service-specific and joint, throughout which core values are reinforced. For example, an enlisted member of the Air Force would move from basic training to technical skills training.

This training is intended not only to help individuals develop new competencies, but also to instill a willingness to live by a set of core military values and establish a new identity as a service member. Not only is developing and cultivating a strong military identity necessary to maintain cohesion in military units and the Armed Forces as a whole, but it also helps maintain the trust of the American People, and it is critical to attracting and retaining the best in each new generation of Americans. Successful military indoctrination draws on the process of group identification to drive the internalization of military values and principles and achieve behaviors that can include the willingness to subordinate one's survival to both a military mission and the survival of others, and the readiness to ethically kill an enemy. Figure 23 shows a behavioral model of the military indoctrination process.[253]

---

[252] Unfortunately, not all values training is effective. Participants in discussion groups during IDA's site visits raised serious questions about the effectiveness of the training provided during the Department's day-long extremism stand-down. Most participants saw the stand-down training as ineffective, many felt that it was unbalanced, and a few felt inappropriately targeted by it. This reaction may be an indication that positive education on shared values may be more effective than negative training on prohibited practices.

[253] Dennis McGurk, Dave I. Cotting, Thomas Watson Britt, and Amy Adler, "Joining the Ranks: The Role of Indoctrination in Transforming Civilians to Service Members," volume 2, chap. 2 in *Military Life: The Psychology of Serving in Peace and Combat*, edited by Amy B. Adler, Carl A. Castro, and Thomas W. Britt (Westport, CT: Praeger Security International, 2005): 13–31, https://www.researchgate.net/publication/272745413_Joining_the_Ranks_The_Role_of_Indoctrination_in_transforming_Civilians_to_Service_Members. Praeger Security International, based on Robert S. Baron, "Arousal, Capacity, and Intense Indoctrination," *Personality and Social Psychology Review* 4, no. 3 (August 1, 2000): 238-254, https://journals.sagepub.com/doi/10.1207/S15327957PSPR0403_3. The model includes four stages:

1. Softening-up: Isolated from prior contacts, recruits are exposed to a variety of individual and group stressors that make salient the importance of the new group. By de-emphasizing the relevance of other social groups, the experience tends to eliminate/de-emphasize other group identities from the individual's sense of self. Further, intense physical demands and limited rest over an extended period of time, exhaust attention resources, causing the individual to be more vulnerable to persuasion.
2. Compliance: Recruits model what they believe is expected to avoid reprimands and any perceived punishment, both by military instructors and military peers. Familiarization with core values of the service member's branch of the military is initially performed for extrinsic reasons and is expected to generate superficial commitment.

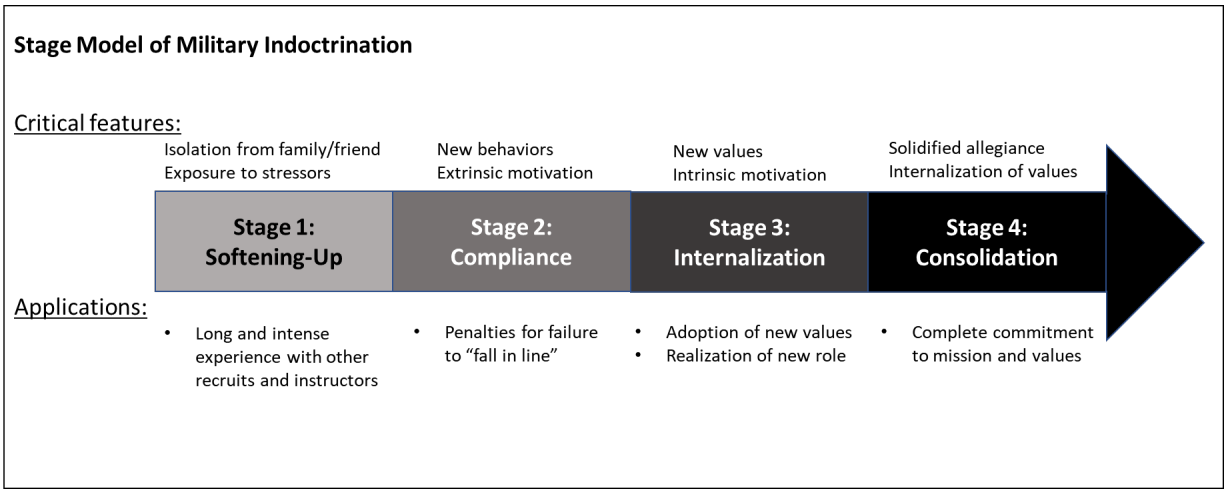


Figure 23. The Military Indoctrination Process

Indoctrination is not an irreversible process and self-related uncertainty does not evaporate once military identity takes on a central role in the service member's sense of self; lived experiences, in and out of uniform, affect military identity. Identification as a soldier, sailor, airman, marine, or guardian continuously develops throughout service, and internalization of related core values cannot be considered merely achieved, but always needs continued efforts to align thoughts and behaviors over time and broaden the applications of core values to all aspects of life.

Depending on experiences, personal challenges, and a variety of variables in the social environmental context faced while in uniform (e.g., unit cohesion, leadership), service members

---

Repeated and reinforced behaviors consistent with service core values increase likelihood of internalization of these values.

3. Internalization: This stage is characterized by an increasingly more active incorporation of military values in the individual sense of self. Increasing awareness and understanding of group norms and engagement in expected behaviors become critical for full-fledged inclusion in the unit; incrementally and reinforced by social confirmation, the recruit privately begins to accept and internalize the military belief system, its norms, and its values. In this stage, the military identity incrementally takes on central importance in the individual's sense of self; the recruit begins to sense what it will feel to be a soldier, sailor, airman, marine, or guardian. It is worth noting that different recruits may reach this stage at different times and paces; recruits who decided to join for mostly extrinsic reasons (i.e., financial rewards, family approval) may continue to go through the motions and pay relative lip service to military and unit demands, so as to avoid punishment by the instructors or military peers.
4. Consolidation: In this final stage, recruits solidify their military identity and actively integrate the associated values and norms with other pre-existing identities and beliefs. Recruits at this stage begin to categorize others as in-group and outgroup members, and newer recruits are commonly perceived as versions of their own past selves. In addition to affecting how recruits perceive outgroup members, in-group members are increasingly perceived through the lens of military excellence, core values, and norms. Behaviors that convey commitment to military excellence, core values, and norms become opportunity to gain in-group status. For recruits, it becomes increasingly less sufficient merely to identify as soldier, sailor, airman, marine, or guardian; qualities and behaviors of the prototypical (i.e., "true") soldier, sailor, airman, marine, guardian serve as guides for self-development.

may find themselves at odds with others, with military values, beliefs, and practices not perceived sufficient to maintain coherence and reduce self-related uncertainty. Military identity, as is the case for other identities, is subject to changes and shifts that fall into two types: short-term fluctuations in identity expression and long-term, more permanent, changes.

- Short-term identity changes are fluctuations in identity expression, as individuals choose to act on the basis of a repertoire of identities over time, including both military identities and other identities (e.g., spouse, parent, son, daughter, Muslim, Christian).[254]
- Long-term identity changes can take the form of adopting a new identity while abandoning an old one or altering the meaning and/or importance of an existing identity.[255]

In the case of radicalization by a service member, two types of identity threats may serve as catalysts to long-term identity change:[256] The service member may feel challenged in his/her claim to a military identity[257] or he/she may perceive a discrepancy between military values and the conduct of others in uniform (within unit or service). In either case, the service member could be expected to experience pronounced self-related uncertainty. For radicalization to occur, the service member would need to: a) feel wanted by an available extremist group; and b) perceive that the values of that group match the behaviors of its members.

Extremist groups, which tend to tolerate single absolutes of right and wrong, with values and behaviors tightly aligned into rigid and self-contained belief systems, characteristically have a very high entitativity,[258] making them attractive to individuals seeking to reduce self-related uncertainty. In addition, such groups tend to commonly exhibit group-centrism,[259] collective

---

[254] Penelope J. Oakes, "The Salience of Social Categories," Chap. 6 in *Rediscovering the Social Group: A Self Categorization Theory*, edited by John C. Turner, Michael A. Hogg, Penelope J. Oakes, Stephen D. Rieche, and Margaret S. Wetherell (Oxford, U.K.: Blackwell, 1987), 117-141, https://www.semanticscholar.org/paper/Rediscovering-the-social-group%3A-A-theory.-Turner-Hogg/469c5d279c5e0625f730f98dc07d2d8b875a2e82; Marilynn B. Brewer, "The Social Self: On Being the Same and Different at the Same Time," *Personality and Social Psychology Bulletin* 17, no. 5 (October 1, 1991): 475–82, https://doi.org/10.1177/0146167291175001; Marilynn B. Brewer, "The Role of Distinctiveness in Social Identity and Group Behaviour," in *Group Motivation: Social Psychological Perspectives* edited by Michael A. Hogg and Dominic D. Abrams (Hertfordshire, UK: Harvester Wheatsheaf, 1993): 1–16, https://psycnet.apa.org/record/1993-98846-001.

[255] Also described as "remooring." K. A. Ethier, and K. Deaux, "Negotiating Social Identity when Contexts Change: Maintaining Identification and Responding to Threat," *Journal of Personality and Social Psychology* 67, no. 2 (1994): 243–251, https://doi.org/10.1037/0022-3514.67.2.243.

[256] Glynis Marie Breakwell, *Coping with Threatened Identities* (North Yorkshire, UK: Methuen, January 1, 1986).

[257] Normative divergence (e.g., sub-standard performance), marginalization, exclusion, can all, alone or combined, contribute to challenging a service member claim to his/her military identity.

[258] Michael A. Hogg, "Uncertainty-Identity Theory," vol. 2 chap. 29 in *Handbook of Theories of Social Psychology*, edited by Paul A. M. Van Lange, Arie W. Kruglanski, and E. Tory Higgins (London, UK:SAGE Publications Ltd., 2012): 62–80, https://doi.org/10.4135/9781446249222.n29.

[259] A. W. Kruglanski, A. Pierro, L. Mannetti, and E. De Grada, "Groups as Epistemic Providers: Need for Closure and the Unfolding of Group-Centrism," *Psychological Review* 113, no. 1 (January 2006):84-100, doi: 10.1037/0033-295X.113.1.84.

narcissism,[260] and offer high status to individuals with military experience, which can be particularly appealing to service members with an uncertain sense of self. This vulnerability to radicalization can be accentuated further when service members perceive themselves to have been marginalized and have few other viable groups available with which they can identify to alleviate their self-related uncertainty. In such cases, these individuals may be inclined to exhibit the patterns of behaviors of lone wolves.

In this light, merely developing knowledge via *military value education*[261] and demanding compliance provides some level of resiliency but may not be sufficient to protect against identity changes. Fostering the integration of military values in an individual's self-concept, life-long and life-wide, requires *military value clarification*: A process that promotes awareness and understanding of principles, moral standards, and/or ethical qualities and their relationship to action and inaction with the objective of sustaining and solidifying the integration of military core values in the individual's self-concept. Furthermore, the value-alignment psychology literature suggests an approach that circumvents a common psychological barrier (myopic tendency in behavior choices) and shifts the interpretation (construal) of one's own behaviors as expressions of one's deeply held values. Last, much empirical evidence suggests that increasing the perceived value/utility of education is critical to *motivation to engage in* and *sustain learning*, and the *quality of learning*. In other words, increasing the perceived value/utility of military value education can be expected to improve subsequent military value clarification efforts.

Self-discrepancy is the perceived incongruence between different aspects of one's self-concept, particularly between one's ideal self, ought self, unwanted self, and actual self. Service members, based on idiosyncratic circumstances, can be expected at multiple points in time to experience some form of self-discrepancy related to their military identities. To reduce the psychological discomfort resulting from perceived inconsistencies in self-concept, service members are expected either to resolve the inconsistency directly (i.e., engage in behaviors that will reduce discrepancies) or to distance themselves from the discomfort related to their military identity by affirming other identities (or seeking other identities). Whereas the former is desirable (i.e., it motivates improvements and fosters excellence), the latter is not and can increase vulnerability to radicalism. To limit such vulnerability, *self-affirmation*[262] of one's military identity should be systematically infused in day-to-day military activities so as strengthen the integration of military values within one's self-concept and highlight the relevance of these values in life-long and life-wide pursuits.[263]

---

[260] Collective self-importance, grandiosity, arrogance, entitlement, unique status, exploitativeness.

[261] Instruction on principles, moral standards, and/or ethical qualities considered desirable in the military.

[262] Behaviors by which we express positive assertion of our values, attributes, and/or group identification. Of note, a constellation of out-of-uniform behaviors can also be understood as reflecting self-affirmation, including service paraphernalia, tattoos.

[263] In addition, juxtaposing actions and aims of common violent extremist with military core values may be used to highlight inconsistencies and exploit basic desires to avoid dissonance in self-concept.

C. Comprehensive Risk Assessment in the Department of Defense

1. Strategies to Address Other Forms of Violence

The Department has developed strategies to address multiple forms of violence, including suicide, domestic violence, sexual assault, and hate crimes, but the strategies for sexual assault and suicide prevention are most comprehensive and best-developed and serve as the best model for a response to violent extremism.

The Defense Suicide Prevention Office (DSPO), established in 2011, is tasked with using a collaborative approach to integrate a range of medical and non-medical resources to address suicide prevention, intervention, and postvention for the DOD. The Defense Strategy for Suicide Prevention (DSSP) provides a framework for the Department's suicide prevention and response efforts.[264] Two themes of the DSSP are particularly relevant to the prevention of extremism: (1) the need to build healthy and empowered individuals, families, and communities as a bulwark against destructive behavior; and (2) the importance of early detection and response. On the first point, the DSSP calls for "recognizing, reinforcing and promoting the protective factors associated with military life: belonging, membership, pride, camaraderie, loyalty, and responsibility."[265] On the second point, the DSSP points to the need to educate and engage leaders and peers at all levels, including personnel such a chaplains, trainers, military community service providers, and military health care providers in the suicide prevention effort.[266]

Sexual assault and harassment also remain a pervasive problem for the DOD, with estimates that one in four women and one in 16 men experience sexual harassment in the military.[267] In 2019, the Department released a Prevention Plan of Action 2019-2023 (PPoA) that leveraged scientific literature on sexual assault and sexual harassment prevention, the science of program implementation, and lessons learned to develop and establish expectations for a comprehensive prevention process, facilitated by a prevention system.[268] The PPoA emphasized the importance of early prevention through measures to address risk factors that make sexual assault more likely

---

[264] Under Secretary of Defense, *Department of Defense Strategy for Suicide Prevention* (Washington, DC: Department of Defense, December, 2015), https://www.dspo.mil/Portals/113/Documents/TAB%20B%20-%20DSSP_FINAL%20USD%20PR%20SIGNED.PDF. The objectives of the DSSP are carried out through the suicide prevention programs of the military components. DOD Instruction 6490.16, *Defense Suicide Prevention Program,* November 6, 2017 (Change 2 Effective September 11, 2020), https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/649016p.pdf?ver=2020-09-11-122632-850.

[265] Under Secretary of Defense, *Department of Defense Strategy for Suicide Prevention*, 10.

[266] Ibid., 6-7.

[267] Joie Acosta, Matthew Chinman, and Amy Shearer, *Countering Sexual Assault and Sexual Harassment in the U.S. Military: Lessons from RAND Research* (Santa Monica, CA: RAND Corporation, 2021), https://www.rand.org/pubs/research_reports/RRA1318-1.html.

[268] Office of the Under Secretary of Defense for Personnel and Readiness, *Prevention Plan of Action 2019-2023: The Department's Renewed Strategic Approach to Prevent Sexual Assault* (Washington, DC: Department of Defense, April 2019), https://www.sapr.mil/sites/default/files/PPoA_Final.pdf.

to occur and to enhance protective factors that provide a buffer against risk factors. To this end, the PPoA proposed a comprehensive approach, including activities to foster healthy environments and peer norms to build personal and interpersonal skills.[269] The PPoA also called for the development of a prevention workforce, supported by leadership, with "prevention-oriented knowledge and skills."[270]

In 2020, the Department sought to move beyond individualized response strategies for each type of problematic violent conduct by issuing an integrated policy on the prevention of all forms of self-directed harm and prohibited abuse or harm. DODI 6400.09[271] is based on the finding that various forms of self-directed and interpersonal violence (e.g., suicide, intimate partner violence, sexual harassment, and assault) share many risk and protective factors. The integration of prevention activities into a cohesive, cross-functional, and cross-organizational approach has the benefit of unifying efforts, avoiding redundancies, and possibly increasing effectiveness. In accordance with the DODI, military leaders at the command or installation level are required to implement data-informed prevention systems that identify and address common risk and protective factors for various forms of violent conduct. Primary prevention mechanisms are expected to promote healthy environments, address the needs of high-risk groups, and implement safety measures for high-risk locations (including social media and other virtual locations).

The comprehensive approach to addressing the various forms of self-directed and prohibited abuses or harms addressed in DODI 6400.09 appears to be consistent with best practices for risk assessment and response, as described in a previous section of this report. Unfortunately, the problem of radicalization, which shares some of the same risk and protective factors as other violent behaviors, appears to have been omitted from the policy. Given that radicalization has the potential to lead to violent action and that a primary focus of P/CVE programs is on preventing radicalization, it may be beneficial for the Department to expand DODI 6400.09 to include a focus on radicalization along with other types of abuses and harms. Such inclusion would be consistent with standards of the Association of Threat Assessment Professionals (ATAP) Certified Threat manager certification program,[272] which uses evidence-based practice to determine whether and to what extent an individual is moving toward violent action. Threat management focuses on the prevention of violence through interventions and strategies designed to disrupt the action from taking place.

Unfortunately, the Department's violence prevention effort appears to have been seriously under-resourced to date. As a result, leaders at command and installation levels have not had the

---

[269] Ibid., 6.

[270] Ibid., 10.

[271] Department of Defense, "DoD Policy on Integrated Primary Prevention of Self-Directed Harm and Prohibited Abuse or Harm," DODI 6400.09 (Washington, DC: Department of Defense, September 11, 2020), https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/640009p.pdf.

[272] See "Certified Threat Manager," Association of Threat Assessment Website, accessed June 16, 2022, https://www.atapworldwide.org/page/certificationexam.

resources to put together cross-disciplinary teams and may not have established processes needed to identify and address common risk factors and address the needs of high-risk groups.

In a 26 February 2021, memorandum addressing sexual harassment and sexual assault in the military, Secretary Austin established an Independent Review Commission (IRC) and directed the Secretaries of the Military Departments to assess compliance with sexual assault and sexual harassment policies and integrated violence prevention efforts.[273] The IRC found that the Department's commitment to preventing workplace violence is not "matched by the resources or capabilities of the current workforce."[274] The report stated:

> Leading in prevention requires more than a one-time awareness campaign or simple statements of support. In the same way that the military evaluates constantly shifting environments to develop winning combat strategies, DoD and the Services must conduct a comprehensive scan of its capabilities to determine the optimum full-time prevention workforce and invest the resources necessary to accomplish the mission.[275]

The report recommends that the Department develop a dedicated primary prevention workforce of full-time personnel with public health and behavioral social science expertise to carry out community-level prevention strategies.[276] This requirement was codified in section 549B of the National Defense Authorization Act for Fiscal Year 2022.[277] Although the Department's implementation strategy is not yet public, IDA understands that the Department plans to take significant steps and provide significant resources to implement the IRC recommendations.

2. Insider Threat Detection Program

At the same time, the Department is also working to build a broad threat assessment capability as a part of its insider threat program, managed by the DOD Insider Threat Management and Analysis Center (DITMAC). The objective of this program is to draw on a broad range of data sources, including data on behavioral problems, to get "to the left of boom" in the threat assessment

---

[273] Secretary of Defense, "Memorandum for Senior Pentagon Leadership, Commanders of the Combatant commands, and Defense Agency and DOD Field Activity Directors: Immediate Actions to Counter Sexual Assault and Harassment and the Establishment of a 90-Day Independent Review Commission on Sexual Assault in the Military" (memorandum, Washington, DC: Department of Defense, February 26, 2021), https://media.defense.gov/2021/Feb/26/2002590163/-1/-1/0/APPROVAL-OF-MEMO-DIRECTING-IMMEDIATE-ACTIONS-TO-COUNTER-SEXUAL-ASSAULT-AND-HARASSMENT.PDF.

[274] Independent Review Commission, *Hard Truths and the Duty to Change: Recommendations from the Independent Review Commission on Sexual Assault in the Military* (Washington, DC; Independent Review Commission, June 2021): 26, https://media.defense.gov/2021/Jul/02/2002755437/-1/-1/0/IRC-FULL-REPORT-FINAL-1923-7-1-21.PDF/IRC-FULL-REPORT-FINAL-1923-7-1-21.PDF.

[275] Ibid, 27.

[276] Ibid, recommendation 2.2, 34.

[277] National Defense Authorization Act for Fiscal Year 2022, Rules of Committee Print 117-21: Text of House Amendment to S. 1605, https://rules.house.gov/sites/democrats.rules.house.gov/files/BILLS-117S1605-RCP117-21.pdf.

process for destructive violent behaviors, including prohibited extremist activities. Like the primary prevention program, this program draws on best practices developed in threat detection programs developed by the NTAC and law enforcement authorities. Unfortunately, as described in Chapter 7.B.3 below, this program also appears to have been under-resourced to date.

Moreover, it does not appear that the incipient threat assessment system is linked to the primary prevention program carried out pursuant to DODI 6400.09. In IDA interviews, senior officials responsible for the primary prevention program ignored the DITMAC program, while officials responsible for the DITMAC program asserted that all reporting from both programs was supposed to come to them. Some of the separation between the two programs is natural: a program that is dedicated to counseling and treatment is naturally reluctant to be associated with insider threats and law enforcement as such associations could increase the reluctance of service members to seek help. Presumably for this reason, DODI 6400.09 specifically requires the separation of the two programs:

> The DoD will distinguish community-based primary prevention as outlined in this issuance from the assessment and mitigation of individual risk addressed through prevention, assistance, and response capabilities of the insider threat program. This will be done by maintaining separate entities, albeit potentially with the same functional participants, at the command or installation level that oversee prevention, assistance, and response capabilities and those that oversee integrated primary prevention.[278]

While this separation of functions is justified, a Department that finds it difficult to resource a single comprehensive risk identification and assessment program will surely find it impossible to resource two such programs. The Department will not be able to optimize its risk assessment capabilities without rationalizing the relationships between these two programs in an appropriate way.

D. Post-Service: Veterans Transition and Support Systems

Service members' tenure in uniform is often marked by change and transition. Service members experience many transitions throughout their time in uniform: from the psychological conditioning during basic training, to multiple duty stations, to field exercises, to deployment, and to educational programs of varying duration—all of which may require frequent relocations.[279] The transition out of the military poses a new range of challenges as the service member departs from a highly structured environment and faces the requirement to establish a post-military

[278] Department of Defense, "DoD Policy on Integrated Primary Prevention of Self-Directed Harm and Prohibited Abuse or Harm," DODI 6400.09 (Washington, DC: Department of Defense, September 11, 2020), https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/640009p.pdf?ver=2020-09-11-104936-223.

[279] Agatha Herman and Richard Yarwood, "From Services to Civilian: The Geographies of Veterans' Post-Military Lives," *Geoforum* 53 (May 2014): 43-44, doi: 10.1016/j.geoforum.2014.02.001.

identity.[280] Leaving the military, especially if not on a service member's own terms, can be one of the most challenging transitions for the individual.[281]

This transition may be particularly challenging for veterans with stronger military identities, health problems, and/or vocational challenges.[282] For many transitioning service members the very concept of self is "rooted in their military service," with their time in uniform informing "their self-image and self-esteem."[283] The stronger their military identity, the more difficult the post-military adjustment may be, at least in part due to their reticence to plan for their post-military life. For some individuals, the "commitment to the institution and to their identity as a valuable member to it made it difficult to fully engage in anticipatory socialization, envisioning a new identity, and planning for a new reality."[284]

After military service, individuals must find meaning through the formation of new connections in social groups. Fostering social connections of separated/retired service members with veterans' groups and other social groups can favorably affect post-transition adjustment, which in turn improves mental and physical health.[285] These interventions should focus on military and/or DOD values as they apply across both in-service and post-service contexts. Such a focus can help the individual sustain a healthy connection with his or her previous military identity. Focusing on values and connectedness, both during service and after separation/retirement, can help to strengthen resistance to radicalization.

---

[280] Many active-duty commitments are accompanied by a mandatory subsequent commitment in the reserve component, complicating the issue of when a service member actually returns to civilian life. It may also be worth noting that some reserve component members who return from deployment are eligible for veterans' benefits and may count as both reserve component members *and* veterans. As reserve component members, such veterans retain a military identity and continue to be subject to the UCMJ when in federal status. Accordingly, the issues and approaches applicable to reserve component members, discussed in Chapter 7.A.4., may be more relevant to such veterans than the issues and approaches in this discussion.

[281] Meredith Kleykamp, Sidra Montgomery, Alexis Pang, and Kristin Schrader, "Military Identity and Planning for the Transition out of the Military," *Military Psychology* 33, no. 6 (2021): 374, https://www.tandfonline.com/doi/full/10.1080/08995605.2021.1962176.

[282] Carl Andrew Castro, Sanela Dursun, Mary Beth MacLean, Raun Lazier, Matt Fossey, and David Pedlar, "Essential Components for a Successful Military-to-Civilian Transition," chap. 11 in *Military Veteran Reintegration: Approach, Management, and Assessment of Military Veterans Transitioning to Civilian Life*, edited by Carl Andrew Castro and Sanela Dursun (San Diego, CA: Elsevier Academic Press, 2019): 249, doi: 10.1016/B978-0-12-815312-3.00011-5.

[283] Meredith Kleykamp, Sidra Montgomery, Alexis Pang, and Kristin Schrader, "Military Identity and Planning for the Transition out of the Military," 384-385.

[284] Ibid.

[285] James Whitworth, Ben Smet, and Brian Anderson. "Reconceptualizing the U.S. Military's Transition Assistance Program: The Success in Transition Model," *Journal of Veterans Studies* 6, no. 1 (2020): 30, doi: http://doi.org/10.21061/jvs.v6i1.144.

Both the individual veteran and the community at large have a stake in promoting successful transitions to civilian life following military service.[286] Although a link between challenges in the transition process and vulnerability to adopting extremist behaviors has not been established, this phase of a veteran's life experience can be pivotal. As noted in a recent study on military transitions by members of the North Atlantic Treaty Organization (NATO) Human Factors and Medicine Research and Technology Group, newly separated veterans must "develop new social identities, finding meaning through memberships in social groups whose norms and values they adopt."[287] For this reason, "transition programs and processes should include a strong recognition of the contributions and sacrifice veterans have made through their military service and recognize the importance of acceptance in civilian social groups and the sense of belonging such memberships provide in life after service."[288]

Extremist organizations have been known to target veterans as they separate from service and transition to civilian life.[289] Former service members can be particularly vulnerable to extremist organizations that appear to offer a continuation of the camaraderie and shared identity and connectedness that individuals experienced while serving in uniform. For this reason, there are a number of ongoing DOD efforts to include information aimed at countering this vulnerability into the transition process at the conclusion of a service member's tenure.

The Transition Assistance Program (TAP) is a mandatory program that prepares separating service members "for their transition from active duty to civilian life."[290] This preparation includes individual self-assessments, transition counseling, employment assistance, and benefits information. The program can be augmented with two-day tracks at a commander's recommendation, including an employment track and a vocational track offered by the Department of Labor. Alternative tracks include an education track and an entrepreneurships track offered by the Small Business Administration. Because TAP is offered shortly before service members retire or separate, it also presents an opportunity for DOD to proactively inform veterans that extremist

---

[286] Truusa Tiia-Triin and Carl Andrew Castro, "Definition of a Veteran: The Military Viewed as a Culture," chap. 12 in *Military Veteran Reintegration: Approach, Management, and Assessment of Military Veterans Transitioning to Civilian Life*, edited by Carl Andrew Castro and Sanela Dursun (San Diego, CA: Elsevier Academic Press, 2019): 9, doi: 10.1016/B978-0-12-815312-3.00002-4.

[287] Carl Andrew Castro, "Essential Components for a Successful Military-to-Civilian Transition," chap. 11 in *Military Veteran Reintegration*, 250.

[288] Ibid.

[289] Seth Jones, Catrina Doxsee, Grace Hwang, and Jared Thompson, *The Military, Police, and the Rise of Terrorism in the United States*, 1.

[290] Office of the Under Secretary of Defense for Personnel and Readiness, *DoD Instruction1332.35: Transition Assistance Program (TAP) for Military Personnel*, (Washington, DC: Department of Defense, September 26, 2019): 4, https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/133235p.pdf?ver=2019-09-26-095932-007. Members of the Reserve Component (National Guard and Reserve) are eligible for TAP only if they have served for 180 days of continuous active duty. Program officials told IDA that a working group within DoD's TAP office is seeking commonalities between the TAP program and the needs of the Reserve Component.

groups may seek to recruit them. In 2021, the Secretary of Defense directed that "Service member transition checklists . . . include training on potential targeting of Service members by extremist groups".[291] According to DOD officials, a curriculum working group is continuing to update transition training to comply with this guidance.

During TAP, Service members receive information on benefits they may be eligible to receive through the VA and the Department of Labor. According to VA officials, engagement of the VA in the TAP process is fairly robust, and the VA is currently reviewing the potential for additional interactions during the transition process that could enhance its relationship with the veterans it serves. Currently, the relationship between a veteran and the VA tends to center on the delivery of medical care and other benefits, including educational programs such as the GI bill. The VA coordinates with DOD to ensure that veterans' health records are transmitted to VA clinicians via a warm handover to ensure continuity. This can include sharing with VA information from DOD systems, particularly if a service member's commander has recorded a concern. These warm handovers can result in a contact between the service member and a VA counselor, with follow-up meetings at the discretion of the individual.[292] In addition to this coordination with the VA, there is also a warm handover from the DOD to veterans' advisors in the Department of Labor, should a veteran request employment assistance.

Because transition programs are operated by the Military Departments, there is no single office that handles all transition issues, including the potential targeting of veterans by extremist groups. However, the DOD has established a TAP governance structure that promotes interagency collaboration among the VA, Department of Labor, and DOD. This structure includes a TAP Executive Council that can review issues that arise within the transition process and refer them to appropriate offices for resolution. For example, a health care issue would be referred to the Assistant Secretary of Defense (ASD) for Health Affairs. Within their respective transition assistance programs, each service conducts a self-assessment of each transitioning service member to match members with resources. In 2022, DOD's TAP office plans to institute an enterprise-level self-assessment that will be replace the service-level assessments. The TAP office is also seeking agreements with external agencies that will enable it to measure the long-term impact of DOD's efforts aimed at assisting the service member to veteran transition process.

At present, the transition process focuses predominantly on providing information on the resilience that is needed during transition, the job search process, and earned benefits such as the

---

[291] Secretary of Defense, "Memorandum for Senior Pentagon Leadership Commanders of the Combatant Commands Defense Agency and DOD Field Activity Directors: Immediate Actions to Counter Extremism in the Department and the Establishment of the Countering Extremism Working Group," memorandum, Washington, DC: Department of Defense, April 9, 2021, https://media.defense.gov/2021/Apr/09/2002617921/-1/-1/1/MEMORANDUM-IMMEDIATE-ACTIONS-TO-COUNTER-EXTREMISM-IN-THE-DEPARTMENT-AND-THE-ESTABLISHMENT-OF-THE-COUNTERING-EXTREMISM-WORKING-GROUP.PDF.

[292] The VA does not collect or process data on administrative or non-judicial punishment that a veteran may have received. This helps the VA maintain trust with the veterans it serves, which is of paramount importance in delivering care and other benefits.

GI Bill. Although the Department is currently endeavoring to adjust the program to address veterans' susceptibility to radicalization, efforts to date appear to focus largely on negative reinforcement: instructing departing service members on the dangers of recruitment by extremist groups. For example, the Marine Corps has added an extremism review to its pre-separation counseling program. This training includes a review of the oath of office, the continuing requirements that it entails, reporting requirements, and a mechanism the transitioning Marine can use if an extremist group reaches out or attempts recruitment.

Although these efforts could have some beneficial impact, they may also serve to increase veterans' awareness of such groups, which could have the unintended consequence of establishing new pathways toward radicalization for individuals with a proclivity in that direction. Additional measures, including a behavioral science-based survey of separating service members, could help inform radicalization prevention efforts. This type of survey could produce insights that would in turn lead to the development of new capabilities to increase resilience among veterans. For example, the survey might include questions regarding existing and desired social supports and social connectedness post-separation. The IDA team understands that DOD and VA are working together to develop such an approach.

More importantly, existing transition programs largely fail to address the crucial issue of military identity and a sense of belonging. After they separate or retire, veterans often retain their connection with the VA, but important limitations come into play. According to VA officials, the VA can engage only with those veterans who choose to enter its system and use its resources. To increase engagement, the VA typically reaches out to veterans upon separation or retirement, as well as at the six-month and one-year points. Within the subset of veterans with whom it is in contact, the VA can contribute to building awareness of how extremist organizations are targeting veterans and can help veterans build resilience against such recruitment through counseling and other benefits. A second line of effort within the VA is to engage with community partners who can augment its outreach to veterans, including Veterans Service Organizations (VSOs) and businesses that offer veterans discounts or training programs. Neither of these efforts are primarily oriented toward preventing extremism, and VA officials emphasized that these outreach efforts are aimed at helping veterans, not at influencing their thinking.

The DOD's Military OneSource program provides non-medical counseling, online training, and assistance with employment. Through this program, service members and dependents can access a variety of benefits while on active duty, during their pre-separation period, and within one year after separation or retirement. DOD TAP officials stated that Military OneSource is repeatedly introduced as a resource during the TAP process. Further, officials noted that if an individual expresses a desire for continuing connection to the military community—either to a TAP counselor or in their self-assessment—he or she can be referred to Military OneSource. Like VA benefits, counseling and other assistance offered by Military OneSource can be delivered only to those transitioning veterans who choose to take advantage of the program. Moreover, Military

OneSource is oriented toward providing assistance to those who need it, not toward providing connectedness or supporting self-identity.

Non-governmental sources of support designed to increase connectedness are also available to veterans. Private sector VSOs have long played a major role in welcoming veterans into local communities. In addition, informal networks of veterans can be helpful in the transition to civilian life. Veterans often maintain the bonds of friendship developed while serving in the same military unit or develop new relationships with other veterans in the community. More recently, ad hoc support networks have gained popularity as a way of serving veterans, both in-person and online. Due to their ad hoc nature, however, these networks may dissipate over time. For this reason, it may be helpful for the DOD or VA to consider sponsoring a more persistent network of former service members. The Department may also wish to convene representatives of VSOs and ad hoc support networks in order to maintain shared awareness of capabilities that comprise the public and private veterans support ecosystem, as well as to identify any significant gaps that may have developed in the ecosystem over time.

Perhaps the best example of a DOD program designed to maintain connectedness and service identity after transition to private life is the Marine for Life program.[293] According to officials in the Marine Corps transition office, the culture of the Marine Corps lends itself to building strong post-career networks. This program consists of four regional network coordinators who support 75 members of the Marine Corps Reserve in their local communities. These reserve members assist in making connections among veterans and their spouses from all services, currently-serving Marines, potential employers, educational institutions, and community organizations such as veterans support organizations. The Marine for Life program uses survey results from TAP to initiate contact if requested, and veterans can choose to reach out at any time. Interviewees reported that representatives hired by the program are drawn from former career Marines, many of whom are now entrepreneurs and executives. The representatives conduct regular networking meetings and employ social media to maintain contact with veterans. Although not its main role, the program can connect a veteran in need of assistance with community resource providers, including food pantries. The program aims to build community and encourage positive behaviors, which may have an indirect protective effect against engaging in extremist behaviors and activities among veterans.

The overall impact of Marine for Life is difficult to measure. Although all transitioning veterans are made aware of the program, participants ultimately self-select, and there are no statistics about the level of participation among veterans. Furthermore, once a connection is established between a veteran and a community resource or network, the Marine for Life representative may not be aware of the subsequent benefits the veteran derives. Much of the feedback from the field is incomplete because it reflects success stories of veterans who have

[293] "Marine for Life (M4L) Program/Expanded Transition Assistance," Marines.mil Website, accessed June 16, 2022, https://www.marines.mil/News/Messages/Messages-Display/Article/886845/marine-for-life-m4l-programexpanded-transition-assistance/.

connected with the program. Marine for Life and similar programs offered by the other services may not reach those most at risk for extremist behaviors. Typically, those who separate with less than honorable discharges do not associate with Marine for Life. These limitations on participation and measurement are inherent in the military's limited reach in the transition process and do not detract from the considerable benefits Marine for Life offers to veterans, including potential protective effects against involvement of veterans in extremist groups.

E. Findings and Recommendations

The access and ease of communication provided by the internet and online social networks come with a cost—the internet also serves as a catalyst and diffusion mechanism for disinformation, extremist content, and hate speech, all of which can play a role in radicalization. Social media platforms and search engine algorithms, which curate and proliferate content based on user preferences, amplify already existing beliefs through confirmation bias. Consumers of online information often lack the resources to fact-check each piece of the seemingly limitless information, viewpoints, and comments they encounter, including extremist propaganda. This overflow of online materials leads consumers to take cognitive shortcuts, whereby they navigate toward information that aligns with their beliefs and worldviews, which can perpetuate the spread of false information and in some cases can lead to radicalization. Research has identified improved cognitive and critical thinking skills that can mitigate the effects and spread of false information.

Recommendation 4: Work to actively counter false information campaigns by providing training and instruction on how to be a life-long and life-wide critical consumer of information, making sure that alternative viewpoints and more reliable sources of information are available to the force, and where possible, flagging fabricated information and foreign links to false information campaigns.

To implement this recommendation, the Department should consider the following options:

- The Secretary could direct the military services to systematically develop critical thinking skills in service members throughout the military training and education lifecycle. For example, such guidance could require:
  - The introduction of critical thinking skills during initial training and pre-commissioning and the reinforcement of critical thinking skills through interactive instruction and dialogue within military training venues;
  - The progressive development of critical thinking skills in professional military education and the inclusion of critical thinking in the selection of professional reading lists;
  - The promotion of critical thinking in the selection of commanders' call topics, interactive discussion templates, and other materials;

  - An emphasis on the importance of modeling critical thinking as a part of leadership development programs; and
  - The inclusion of critical thinking skills across civilian training, as appropriate.
- The training could also:
  - Provide instruction on the inclusion of metacognitive prompts (probing questions that cause reflection) or accuracy prompts (self-rating the accuracy of a headline or story) before sharing information via social media. Such prompts have been shown to increase resistance to believing (and subsequently sharing) false information;
  - Leverage public awareness products, such as have been released by the Cyber Security and Infrastructure Security Agency (CISA) of the U.S. Department of Homeland Security, to heighten awareness of misinformation and disinformation campaigns in the military community; and
  - Alert the military community to strategies employed by foreign entities to target service members and veterans with false information via social media and other websites (addressing tactics and mechanisms in use and educating service members and veterans on the risk of cyber threats, espionage, and manipulation, as well as indicators and warnings to raise awareness regarding such targeting).

The vulnerability of an individual to radicalization is driven by push, pull, and personal factors that change over time. Many of the same factors also drive other maladaptive behaviors such as suicide and other forms of violence. Comprehensive threat assessment is a proven approach to ensure that at-risk members of the community receive the care and support they need and protect against radicalization and other maladaptive behaviors.

Recommendation 5: Expand on comprehensive threat assessment teams established pursuant the Department's Primary Prevention Plan and on the threat assessment program established by DITMAC to identify at-risk behaviors, activities, and vulnerabilities at multiple levels (e.g., individual, inter-individual, group, culture/climate) that contribute to destructive behaviors, including violent extremist activities, in military populations.

The Department has already taken significant steps to implement a comprehensive threat assessment approach with regard to destructive behaviors other than prohibited extremist activities through the promulgation of DODI 6400.09 and the Primary Prevention Plan under development pursuant to the recommendations of the IRC, and with regard to prohibited extremist activities, through the DITMAC threat assessment program. However, these two programs do not appear to be well-coordinated and neither of the efforts has been fully resourced to date. Each military service has some form of threat assessment teams in place, but some are more successful and comprehensive than others.

To implement this recommendation fully, the Department should consider the following additional options:

- The Secretary could direct the DOD Components to develop a multi-phase approach to identify at-risk behaviors and formulate and enable/execute management strategies for individuals identified by commands as at-risk. These strategies could leverage the expertise of a wide-range of offices and individuals, including the Service Surgeons General, the offices of the Director of Force Resiliency, the Assistant Secretary of Defense for Health Affairs, the Under Secretary of Defense for Intelligence and Security (USD(I&S), the Service Military Criminal Investigative Organizations, Installation Management Commands, Judge Advocates General, chaplains, mental health professionals, and "buddies" and family members of at-risk individuals. Key phases of the approach could include:
  - Phase I: Identify at-risk individual and group behaviors, common pathways, and vulnerabilities that contribute to violence and other destructive behaviors in military populations. Refine and validate risk assessment tools and prevention models. This may include validating or refining existing models and risk assessment tools such as the START tool or creating entirely new tools specific to the military population.
  - Phase II: Leverage cutting edge research as well as best practices and lessons learned from the work of the NTAC, civilian law enforcement threat management teams, and the Army Command Ready and Resilient Councils (CR2C) to develop customized strength-based prevention and interventions modules that target specific at-risk behaviors and pathways, both throughout, and at specific stages of, military service careers. Utilize the military "buddy" and developmental systems to promote protective factors—including group identity/connection/belongingness, stress management and coping, unit support, identification of at-risk behaviors and reporting, and unit resilience to violent or destructive tendencies or radicalization.
- The Secretary could direct the expansion of DODI 6400.09 to cover individuals at risk for radicalization and take additional steps to ensure that primary prevention team efforts carried out pursuant to that instruction are better coordinated with threat assessment system managed by the DITMAC. Coordination steps could include:
  - Providing guidance to circumstances in which information developed by primary prevention teams is appropriate to report to the DITMAC threat assessment system;
  - Providing guidance to circumstances in which patient confidentiality and similar privileges may make it inappropriate to report such information to the DITMAC threat assessment system; and
  - Developing a process for resolving cases in which applicable protections appear to be in conflict with a clear need to report such information.

The content, execution, level of comprehensiveness, and participation of extremism stand-down training varied greatly across the Department. Individuals receiving the training had mixed,

often negative reactions. Some felt that the training requirement was sudden, unexpected, and unnecessary; others even felt targeted. Workplace training and education would be more effective to counter radicalization if it took advantage of existing cognitive structure in domains meaningful to the individual. For service members, military core values function effectively as a guide for greater self-insight/self-understanding, in-group cohesion, collective self-esteem, and intergroup comparison. For this reason, a focus on values offers an advantageous terrain from which to educate and train service members about the risks of radicalization, radicalization prevention, and the behaviors that build and sustain resistance to radicalization.

Recommendation 6: Expand on the military's current emphasis on education, training, and assessment on the core values and corresponding virtues of DOD and the Services (e.g., Loyalty, Duty, Honor, Mission) to build on core values as a barrier to radicalization in the force.

To implement this recommendation, the Department should consider the following options:

- The USD(P&R) could issue guidance directing to the military services to—
  - Reinforce core values through interactive instruction and dialogue during military training, the inclusion of core values in the selection of professional reading lists, and the promotion of core values in the selection of commanders' call topics, interactive discussion templates, and other materials. Because the focus on positive values needs to connect to service members' day-to-day experience, the interaction and instruction should be engaging and inspirational.
  - Develop an assessment concept that promotes a progressively deeper integration of core values into military professional development. Assessments could include:
    - Value-related knowledge and understanding (e.g., meaning of each value, what is expected of service members in reference to these values, understanding of how values are integrated in all aspects of military service);
    - Self-perceived development along these values (e.g., how service members perceive their own integration of military values into their self-concept, confidence in ability to positively influence others in accordance with military values); and
    - Behavioral intentions (e.g., intentions to act in accordance with military values and the professional military ethic, intentions to model and cultivate core values as part of leadership, and the military "buddy" system).
  - Emphasize positive messages about what to do, as opposed to negative messages about what not to do (prohibited practices) so as to emphasize individual *responsibility* and *action* (rather than passivity) in the cultivation of core DOD, military, and service values in individuals and units. Such positive messages could include the inspirational messages about American values ("why we fight") and

emphasize the importance of modeling military core values as a part of leadership training.

  - Ensure that the reinforcement of positive values falls under the purview of military leaders rather than being delegated to Equal Employment Opportunity (EEO) or other specialized organizations. Behavior (and attitude) change occurs at the unit level with group behaviors mirroring leader behaviors; thus, the reinforcement of positive values should begin with leadership and cascade throughout the chain of command.
  - Include deliberate uses of after-action reports (AARs) to connect military actions with military values so as to encourage awareness and understanding of values.
  - Include core DOD and service values across civilian training, as appropriate.

- The Secretary could direct the military services to promote inclusion, tolerance, and respect in the force by opening channels of communication through a series of "necessary conversations" along the lines set forth by the Chief of Naval Operations (CNO) in July 2020. As described in the Navy publication, such conversations would not be one-time occurrences, would be planned but open-ended, would take place in an environment that encourages sharing, and would be conducted pursuant to ground rules that ensure respect for a variety of perspectives.

Research shows that loss of military identity can be a problem in post-military adjustments. Military identity influences well-being during service through social connectedness and integration into military culture. After military service, individuals must find new meaning through the development of new connections in social groups. Fostering social connections of separated/retired service members with veterans groups and other social groups can make a significant positive impact on post-transition adjustment, which in turn improves mental and physical health. These interventions should focus on military and DOD values as they apply across in-service and post-service contexts, and help to sustain a healthy connection with previous military identity. Focusing on values and connectedness, both during service and after separation/retirement, can help to strengthen resistance to radicalization.

Recommendation 7: Through the expansion of best practices, such as the Marine for Life program, revitalize available opportunities and explore new venues to foster and cultivate stronger post-separation/retirement group identity (with integration of DOD and Military Service values) to provide social, personal, and professional connections and a sense of belongingness.

To implement this recommendation, the Department should consider the following options:

- The USD(P&R) could issue guidance directing the military services to:
  - Provide service members preparing to separate from the armed forces with education and training on the importance of transferring military values to civilian life;

  - Provide education and training to service members on the benefits, both personal and professional, of continuing to apply core military values to one's civilian community and in other non-military activities; and
  - Expand TAP programs to include speakers who are active in VSOs who can impart their story of continued service to their communities. Make such presentations available as a YouTube channel for elective post-TAP reinforcement.
  - Build a network, along the lines of the Marine for Life Program or the Yellow Ribbon Reintegration Program for the National Guard and Reserve, that is available to connect and support former service members if needed.
- The USD(P&R) could provide guidance to the military services on how to connect separating service members to networks of veterans and retirees to enable them to remain connected to the military community, with a view to promoting life-long and life-wide commitment to core military values. For example, such networks could conduct events recognizing individuals/groups for activities characterizing each specific DOD, military, and service value post-separation/retirement.
- The Under Secretary could work with Secretary of Veterans Affairs to expand access to Military OneSource tools, counseling, and referrals beyond the current one-year limit for veterans and retired service members.

7. Legal and Policy Mechanisms for Addressing Extremist Activities in the Military Community

A number of legal and policy regimes are potentially relevant to the Department's efforts to address extremist activities in the military community. Some of these legal and policy regimes are applicable only the service members, while others are applicable more broadly to service members, DOD civilians, and even defense contractors.

- First, there are positive approaches to inculcating military values through education and training. These start during the recruiting and onboarding processes, continue throughout a military career, and extend into post-service transition. The Department's training and education systems are addressed in Chapter 6.B of this report.
- Second, every service member is subject to military-unique administrative actions including verbal counseling, letters of counseling, admonition, or reprimand, adverse evaluation, bars to reenlistment, mandatory reclassification, and administrative elimination for misconduct or poor performance. Commander's authority and the disciplinary continuum are addressed in Section A.1., below.
- Third, service members and DOD civilians are subject to administrative approaches for the prevention of racial and sexual harassment through the Department's Equal Opportunity (EO) system and anti-harassment policies. The prevention of racial and sexual harassment is addressed in Section A.2., below.
- Fourth, service members are subject to the military justice system under the UCMJ with its criminal processes and sanctions. The UCMJ is addressed in Section A.3., below.
- Fifth, the Department has a series of screening processes designed to identify and address individuals with potentially problematic issues in their backgrounds. These processes, which include suitability determinations, security clearance decisions, and access authorizations, are applicable to service members, DOD civilians, and contractor employees. The Department's screening systems are addressed in Section B.2, below.
- Sixth, the insider programs, which are designed to assess threatening behaviors and activities in the military ranks and among DOD civilians and contractor employees. The Department's Insider Threat program is addressed in section B.3., below.
- Finally, the federal criminal justice system established in title 18 of the U.S. Code applies to all Americans whether or not they serve in the military, and therefore, applies to members of the Armed Forces before, during, and after their military service. Members of the military community are also subject to state criminal processes and

sanctions for crimes committed in state jurisdictions. The applicability of the criminal laws to extremist activities is addressed in section B.4 below.

These overlapping legal and policy regimes are shown in Figure 24.

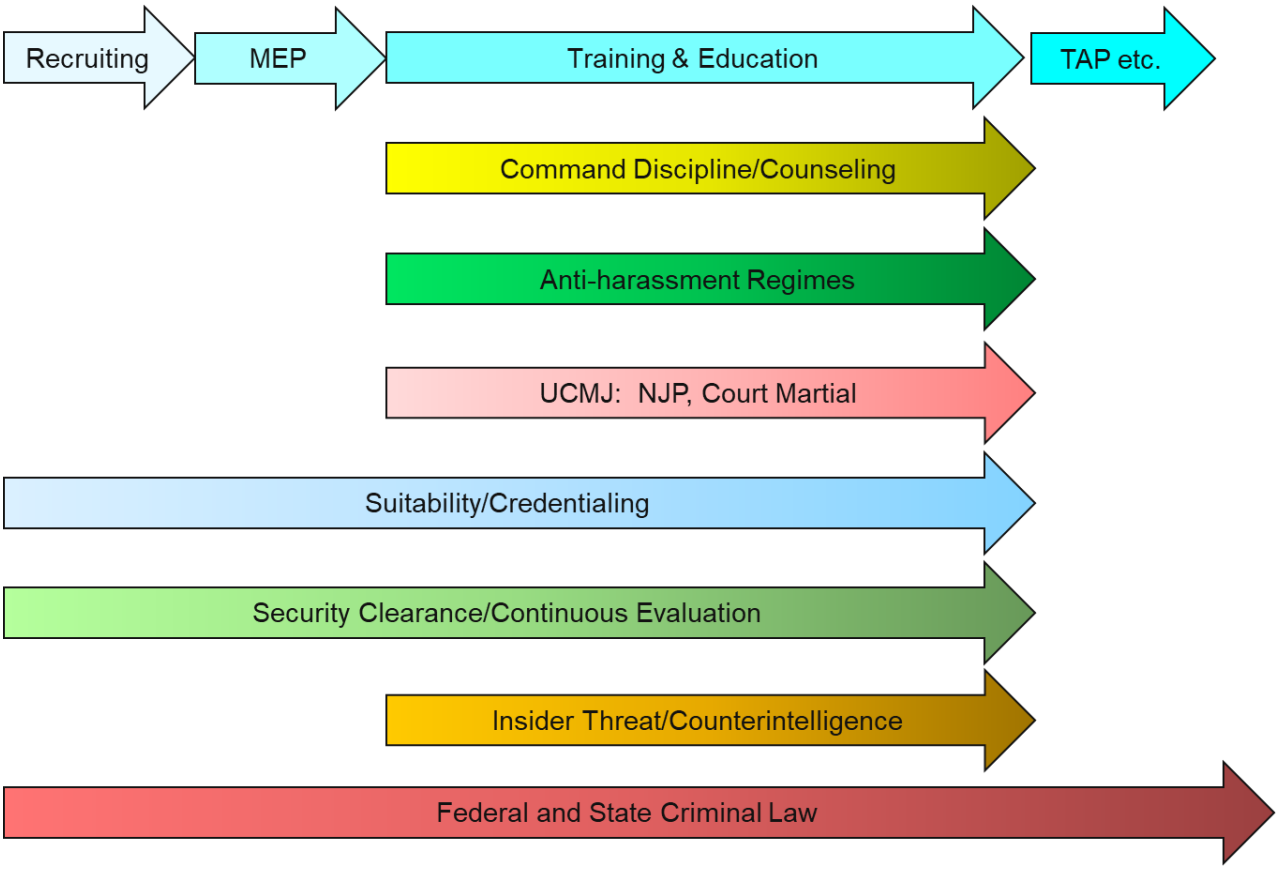


Figure 24. Legal and Policy Regimes for Addressing Potential Extremist Activities

A. Members of the Military

1. Command Authority and the Disciplinary Continuum

The military has a broad set of tools with which to push back against prohibited extremist behaviors and activities in its ranks. Unlike civilians, members of the Armed Forces are subject to teaching, training, supervision, and discipline in virtually every aspect of their lives, both on- and off-duty. As the Supreme Court explained in 1974, even the rights afforded by the First Amendment to the United States Constitution may be limited by the needs of military service:

> This Court has long recognized that the military is, by necessity, a specialized society separate from civilian society. . . The differences between the military and civilian communities result from the fact that 'it is the primary business of armies and navies to fight or be ready to fight wars should the occasion arise.' . . . [The Court has previously noted] that '[t]he military constitutes a specialized community

> governed by a separate discipline from that of the civilian,' . . . and that 'the rights of men in the armed forces must perforce be conditioned to meet certain overriding demands of discipline and duty . . ..'[294]

As noted above, some of these legal and policy regimes are applicable only to service members, while others are applicable to military, civilians, and DOD contractors alike. Because of the unique status of members of the Armed Forces, military-unique legal and policy regimes provide greater authority to regulate conduct. For this reason, DOD and each of the military services promulgate punitive regulations expressly prohibiting members of the military from engaging in certain extremist activities, even though many of those activities do not violate federal law. There are no counterpart regulations applicable to civilians. On the contrary, legal and policy regimes that are applicable both to members of the military and to civilians such as DOD employees and contractors do not reference extremism at all, but tend to refer instead to terrorism, sedition, and similar criminal activities. Military-unique disciplinary systems are discussed in this section; systems applicable to the broader range of military, civilians, and contractors are discussed in the next section.

The unique status of the Armed Forces affords the military services greater flexibility in the employment of disciplinary measures than is available in the civilian world. The criminal justice system under title 18 requires formal investigations and highly structured legal proceedings before subjecting an offender to sanctions. Even administrative sanctions applied to civilian employees or contractors under screening and security systems entail formal processes and specified sanctions. By contrast, military-unique disciplinary systems authorize a broad range of disciplinary measures ranging from feedback and verbal counseling; to informal and formal letters of counseling, admonition, or reprimand; to non-judicial punishment, to administrative separation; and criminal judicial processes and sanctions. The formality of procedures and the due process afforded the service member depend on the nature of the disciplinary measures to be applied.

Figure 25 is a chart supplied to the IDA team by the office of the Air Force Judge Advocate General (JAG), which shows one representation of this continuum of disciplinary approaches.

[294] Parker v. Levy, 417 U.S. 733 (Supreme Court. 1974).

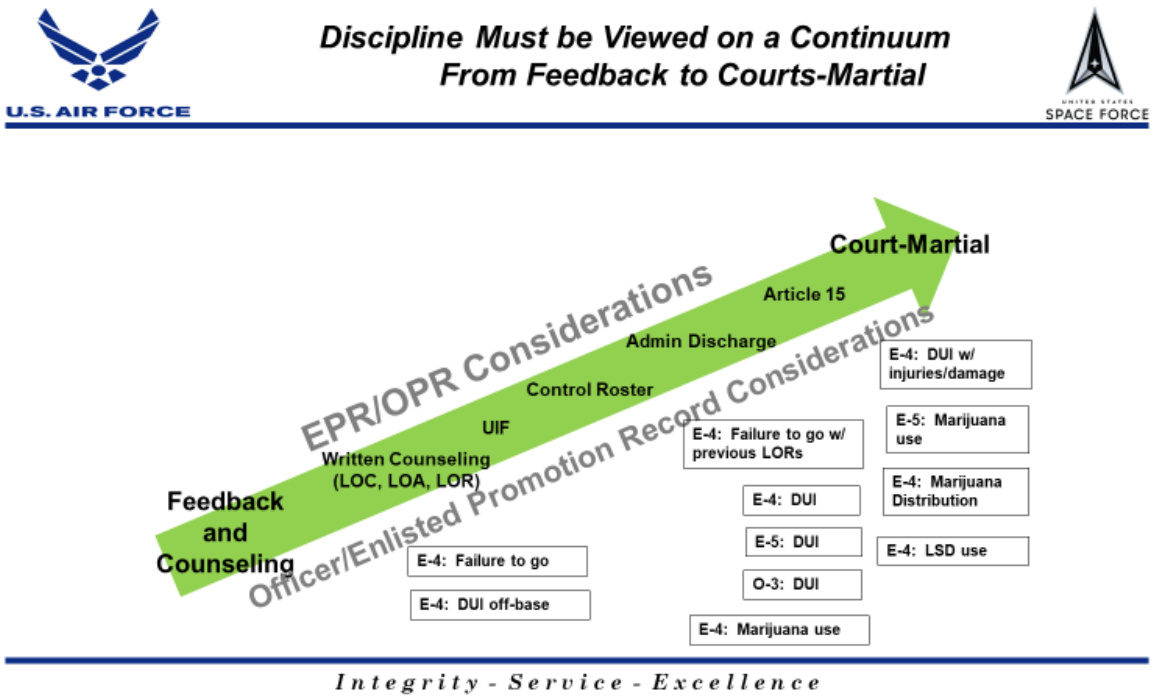


Figure 25. Continuum of Disciplinary Approaches within the Air Force and Space Force

Senior DOD officials interviewed by the IDA team placed a strong emphasis on the relevance of this disciplinary continuum to prohibited extremism and related offenses. Several interviewees pointed out that common push, pull, and personal factors—such as broken relationships, lack of connectedness, alienation, and isolation—are known to contribute to a wide range of destructive behaviors, including prohibited extremist activities, suicidal thoughts, abusive behaviors, and drug and alcohol abuse. If these problems can be identified early, interventions such as mentoring, training, and counseling are more likely to result in positive outcomes than immediate resort to the military justice system.

Moreover, prohibited extremist activities are closely associated with lesser forms of misconduct such as inappropriate use of language and symbols, and with elements of racism and misogyny that still appear to be widespread in American society. Although disciplinary actions are necessary in some cases, they could become counterproductive if they are overused and alienate a significant portion of the larger force. One interviewee told the IDA team that military leaders need to be alert to the impact of their actions on "the whole field, not just a few weeds."

Senior officials from all four military services[295] told IDA that there is no single "right" response to extremism and that understanding and education play at least as important a role in responding to inappropriate behaviors and activities as do disciplinary actions. An interviewee from one service told IDA that "[t]he reaction depends on the conduct. . . . Sometimes, people just

[295] IDA did not interview any officials in the Space Force, which was just being established at the time that the field work was conducted for this project.

come in from a bigoted or intolerant home situation and don't know any better. That can usually be addressed with mentoring." An interviewee from another service stated that the military takes in a broad segment of American society with diverse backgrounds and needs to "give them a chance," at least "up to a point:"

> We take in 40,000 people a year. People are people and they have their own backgrounds. The military is where many of them will interact with new people for the first time. We need to give them the space to grow and engage. The training and counseling with mentoring is important. That takes time, and we need to be able to work with people.[296]

An interviewee from a third military service agreed, noting that "some people come in [to the military] with dislike for other races or ethnicities." If this starts to become problematic, counseling may be necessary, but in other cases they can learn to work together and trust each other so that it does not impact the performance of the mission. An interviewee from a fourth military service stated that one can take service members "from different cultural perspectives and talk it through." "If you tell someone they're wrong, they'll push back," this official stated, "but if one service member tells another that their actions are hurtful, it can get them thinking." "That's how you want things to change. You don't just want them to comply, you want them to change because it's the right thing to do."

The revised DODI 1325.06 provides space for such "soft" approaches by directing commanders to intervene early to address actions that do not rise to the level of prohibited extremist activities but suggest the potential for future violations. The new DODI states:

> Commanders should remain alert for signs of future extremist activities. Commanders should intervene early, primarily through counseling, when observing such signs even though the signs may not rise to the level of active participation or threaten good order and discipline, but only suggest such potential. The goal of early intervention is to minimize the risk of future extremist activities. In these situations, commanders will educate the Service member regarding the potential adverse effects of their actions.[297]

This policy is consistent with the Department's objective of identifying potential problems before they lead to violent or divisive actions.

However, the new DODI does not provide significant guidance on the types of "signs of future extremist activities" for which commanders should be looking. The absence of guidance on this point is particularly problematic in light of the definitions of the terms "active participation" and "extremist activities," which in themselves appear to encompass a broad range of serious and less serious violations. In the course of IDA's site visits, a number of service members expressed the view that "intolerance of others' views," trying to force one's views on others, and not being

[296] Confidential Interview with IDA team.

[297] Confidential Interview with IDA team.

open to other points of views are building blocks of extremist behavior. Along these lines, behaviors that fall short of prohibited activities but still warrant a commander's attention could include the use of insensitive or offensive language, aggressive or harassing speech, and intolerance or disrespect for the views of others. Any of these behaviors could be a threat to good order and discipline, and if allowed to flourish unchecked, could grow into more violent or divisive actions.

2. Regimes for the Prevention of Racial and Sexual Harassment

The DOD maintains robust policies and programs to ensure equal opportunity, promote diversity in the DOD workforce, and prevent and respond to sexual harassment and assault. DOD Directive 1020.02E provides that all service members will be afforded equal opportunity "in an environment free from harassment, including sexual harassment, and unlawful discrimination on the basis of race, color, national origin, religion, sex (including gender identity), or sexual orientation."[298] Nested under this Directive, DOD Instruction 1350.02 establishes the Department's military equal opportunity program and DOD Instruction 1020.03 establishes procedures for the prevention of harassment on the basis of either race or sex.

DODI 1350.02 requires the Secretaries of the Military Departments to establish Military Equal Opportunity (MEO) programs to ensure that all service members are treated with dignity and respect. "Commanders and supervisors at all levels are held appropriately accountable for fostering a climate of inclusion within their respective organizations."[299] The Directive establishes detailed procedures for processing informal and formal MEO complaints; commanders are expected to hold offenders appropriately accountable when a complaint is substantiated.[300]

DODI 1020.03 establishes a goal of preventing harassing behavior that "is offensive to a reasonable person; unwelcome to the aggrieved party and creates conditions that interfere with work performance; or creates an intimidating, hostile, or offensive environment before it rises to the level of severe or pervasive."[301] Harassment is defined in DODI 1020.03 to include "offensive jokes, epithets, ridicule or mockery, insults or put-downs, displays of offensive objects or imagery, stereotyping, intimidating acts, veiled threats of violence, threatening or provoking remarks, racial or other slurs, derogatory remarks about a person's accent, or displays of racially offensive

---

[298] Department of Defense, "Diversity Management and Equal Opportunity in the DoD," DODD 1020.02E (Washington, DC: Department of Defense, June 1, 2018), https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/102002p.pdf.

[299] Department of Defense, "DoD Military Equal Opportunity Program," DODI 1350.02 (Washington, DC: Department of Defense, September 4, 2020), https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/135002p.pdf.

[300] Ibid, Section 4.

[301] Department of Defense, "Harassment Prevention and Response in the Armed Forces," DODI 1020.03 (Washington, DC: Department of Defense, December 29, 2020), https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/102003p.PDF?ver=DAAzonEUeFb8kUWRbT9Epw%3D%3D.

symbols."[302] Violations of this policy may subject an offender to the full range of adverse administrative actions, or to action under the Uniform Code of Military Justice.

IDA interviewees often had difficulty drawing a line between prohibited extremist activities and individual acts of harassment and unlawful discrimination prohibited by the Department's MEO and harassment policies. Depending on the motivation and circumstances, it would appear that "intimidating acts" and "veiled threats of violence" could constitute either unlawful harassment or prohibited extremist activities. Similarly, while the action of calling for widespread unlawful discrimination appears in principle to be distinct from engaging in individual acts of harassment, the difference is not always clear in practice. For example, several interviewees and participants in IDA site visits pointed to the display of Confederate flags, Swastikas, or nooses as examples of extremism. Such "displays of offensive objects or imagery" and "racially offensive symbols" clearly constitute individual acts of harassment, but they could also be interpreted as broad advocacy of illegal discrimination constituting a prohibited extremist activity. As an IDA interviewee commented:

> We have a lot of different people. I don't think the line between what is an offensive joke/statement and extremism is easy, but the person advocating and trying to get others to discriminate needs to be prevented.[303]

The overlapping nature of harassment, discrimination, and extremism offenses means that EO remedies are potentially available to address a wide range of conduct that borders on prohibited extremist activities without the need to demonstrate that the Department's extremism policy has been violated. Substantiated EO complaints are generally handled at the command level and through an administrative process. DODI 1350.02 establishes a hierarchy of informal complaints, which are to be addressed by a MEO professional and the complainant's chain of command through an informal resolution process, and formal complaints, which trigger formal investigations and potential adverse administrative, disciplinary, or other action under the Uniform Code. The instruction even provides for the consideration of anonymous complaints.[299] Consequently, all of these remedies are potentially available for activities based on unlawful discrimination that may also be prohibited extremist activities.

On the other hand, the overlap between harassment, discrimination, and extremism offenses may also make it difficult to track and quantify prohibited extremist activities in the Department. If too many EO cases are included in the count of prohibited extremist activities, the Department's extremism problem will be overstated; if too few cases are included, the problem will be understated. For this reason, the Department may want to consider providing additional guidance on factors to be considered in identifying which EO cases will be counted as prohibited extremist activities, and how the nature of prohibited extremist activities can be more accurately characterized to distinguish them from acts of discrimination or harassment. Factors that may

[302] Ibid, Section 3.1.

[303] Confidential Interview with IDA team.

weigh in favor of categorizing an EO violation as a prohibited extremist activity could include repeated actions, organized conduct, and efforts to persuade others to participate in "widespread" acts of discrimination or harassment.

3. Uniform Code of Military Justice

Members of the Armed Forces are subject to the UCMJ, which serves as a military parallel to the civilian criminal justice system.[304] The UCMJ can be enforced through non-judicial punishment imposed by a commanding officer[305] or through the formal court-martial process.[306] Non-judicial punishment can range from an admonition or reprimand to confinement or arrest for a period of up to 30 days, depending on the status of the service members subject to non-judicial punishment and the level of commander imposing the punishment. Conviction by a court-martial may result in punishments including reprimand, forfeiture of pay and allowances, fines, reduction in grade, confinement and restriction, hard labor, and punitive discharge.[307]

The UCMJ does not include a separate offense of "extremism." However, it includes a number of provisions under which the behaviors constituting prohibited extremist activities could be prosecuted. The following is a list of only a few of the crimes enumerated in the Uniform Code of Military Justice under which actions constituting prohibited extremist activities could be charged and prosecuted at court-martial:

- Article 88: Contempt toward Officials,
- Article 109: Destruction or Damage to Property,
- Article 115: Communication of Threats,
- Article 116: Riot of Breach of Peace,
- Article 117: Provoking Speeches or Gestures, or
- Article 128: Assault

Any violation of the prohibition on extremist activities in DODI 1325.06 could be prosecuted under Article 92 as a failure to obey a lawful order or regulation. Certain prohibited extremist activities could also be prosecuted under Article 80 (Attempts), Article 81 (Conspiracy), Article 82 (Soliciting Commission of Offenses), Article 133 (Conduct Unbecoming an Officer), or Article 134 (Prejudice to Good Order and Discipline).

---

[304] U.S. Congress, *United States Code: Uniform Code of Military Justice, 10 U.S.C. §§ 801-940*, December 20, 2019, https://jsc.defense.gov/Portals/99/Documents/UCMJ%20-%2020December2019.pdf?ver=2020-01-28-083235-930.

[305] Ibid, Article 15.

[306] Ibid, Subchapters IV and V.

[307] Joint Service Committee on Military Justice, *Manual for Courts-Martial*, 2016 ed. Marine Corps Publications Electronic Library, Rule 1003.

Senior military attorneys interviewed by the IDA team expressed confidence that the existing provisions of the UCMJ were sufficiently broad to provide a remedy for the more serious cases of prohibited extremist activities. The UCMJ authorizes command discipline and non-judicial punishment, so it can provide a remedy for less serious cases as well—but only if a clear definition allows the identification of such cases. One senior legal official told IDA, "When you cross the threshold of criminal behavior, that's been well-defined and crystal clear, and never has been confusing." What gets more difficult, this official stated, is "unacceptable behavior below the criminal threshold." "It's easy to define violence as criminal," a second official explained, but it is much harder with thoughts and words. A third official stated, "[t]here's a careful balance between good order and discipline and freedom of assembly and speech." For these reasons, actions such as counseling may be more appropriate, and more likely to induce future compliance with the DODI's proscriptions than would a trial by court-martial.

IDA interviewees almost uniformly opposed legislation to add a specific offense of "extremism" to the UCMJ. One senior military lawyer told the IDA team, "It's a bad idea," because an extremism offense "has potential political overtones." "We can punish conduct very well," he stated. "We don't need to categorize it that way." A second stated, "In reality, the word 'extremism' means nothing, which is why JAGs are hesitant to add an extremism article to the UCMJ." A third pointed out that "there are hundreds of crimes that someone could commit with extremist intent. It's impossible to capture all of them." A fourth noted that extremism would likely be more difficult to prosecute under a separate article than under existing law because of the requirement to prove motivation. "[N]o prosecutor wants to add an additional element [to a crime] that they have to prove [beyond a reasonable doubt]," he explained.[308]

On the other hand, IDA interviewees expressed support for the idea of making extremism an express "aggravating factor" in sentencing decisions under the UCMJ, similar to existing language addressing hate crimes. The UCMJ does not include a specific hate crimes offense similar to the Matthew Shepard and James Byrd, Jr., Hate Crimes Prevention Act of 2009.[309] In describing the categorization of evidence of "hate" as an aggravating factor to be considered in sentencing an accused service member, the Manual for Courts Martial provides:

> In addition, evidence in aggravation may include evidence that the accused intentionally selected any victim or any property as the object of the offense because of the actual or perceived race, color, religion, national origin, ethnicity, gender, disability, or sexual orientation of any person.[310]

---

[308] A single IDA interviewee expressed openness to the idea of a new UCMJ article establishing a separate extremism offense.

[309] Codified as 18 U.S.C. Section 249. A member of the military may be tried by court-martial for the commission of a federal crime, including a violation of the Hate Crimes Act.

[310] Joint Service Committee on Military Justice, *Manual for Courts-Martial*, 2019 ed., Marine Corps Publications Electronic Library, Rule 1001, II-141.

This language does not cover all prohibited extremist activities, but it would appear to provide the court-martial or military judge discretion to enhance the sentence of an accused convicted of the extremist activities described in clause (f) of the DOD definition—"Advocating widespread unlawful discrimination based on race, color, national origin, religion, sex (including pregnancy), gender identity, or sexual orientation."[311] DOD officials told IDA that in practice, the military courts are likely to accept evidence of violation of DODI 1325.06 as an aggravating factor, but there is no clear signal to this effect in the Manual for Courts-Martial itself.

Senior legal officials interviewed by the IDA team expressed support for the idea of using the aggravating factor approach to cover the full range of extremism offenses. One senior military lawyer told IDA, "I like that. You get them on the actual conduct, and then you increase punishment based on the other evidence." A second interviewee stated that "There are lots of violations of orders across the Department, and some cry out for greater punishment." The advantage of an enhanced sentencing provision would be that prosecutors could seek the greater punishment after achieving the conviction, rather than risking losing the conviction because of the need to prove the additional element of intent.

4. Applicability to Reserve Component: National Guard and Federal Reserve

Active and reserve components of the military face different challenges associated with extremist actions and behaviors. Although members of the reserve component (RC), including members of the National Guard and Reserve, have much in common with their active duty contemporaries, several interviewees pointed out that the National Guard primarily answers to the governors of their states via State Adjutants General when not serving in federal status.[312] As can be seen from the response to DOD's vaccine mandate, these governors may have a wide variety of views on acceptable and unacceptable behavior in the Armed Forces.[313]

Several senior DOD officials told the IDA team that the National Guard and Reserve might be more susceptible to penetration by violent extremists because members of the RC are embedded in their civilian communities and are likely to reflect the values and divisions in those communities. These officials also indicated that many members of the reserve elements, who generally participate in military activities for only one weekend each month and two weeks in the summer, especially more junior guardsmen, have far less "contact time" in which to absorb military culture

---

[311] Department of Defense, "Handling Protest, Extremist, and Criminal Gang Activities Among Members of the Armed Forces," DODI 1325.06, enclosure 3, paragraph 8.c(1)(f).

[312] The National Guard answers to the military chain of command when serving in federal "Title 10 status" and to State Governors and Adjutants General when serving in State "Title 32 status."

[313] E.g., "Governor Abbott Condemns U.S. Department of Defense's Vaccine Mandate and Refuses to Enforce it Against Texas National Guard," *Office of the Texas Governor*, December 16, 2021, https://gov.texas.gov/news/post/governor-abbott-condemns-u.s-department-of-defenses-vaccine-mandate-and-refuses-to-enforce-it-against-texas-national-guard.

and values, and that their activities are more difficult to monitor than those of active duty service members, who are required to be available for military duty on a "24-7" basis.

Senior national guard leaders interviewed by the IDA team acknowledged that a small number of guardsmen have been recruited into violent extremist groups or have participated in violent extremist activities including the attack on the Capitol. They also acknowledged that the Guard and Reserve reflect the values of the communities in which they live and work and that the actions of members of the RC may be difficult to observe when they act in their state and civilian capacities. One interviewee explained:

> In the Guard, you don't get up every day and serve with people that value Army values. You can hide a lot more. If you join a militia while at Fort Hood, you have a harder time hiding it since most of your time is accounted for. Not true for the National Guard.[314]

However, these leaders assessed that guard-related violent extremism is rare and disagreed that reserve elements are more susceptible to violent extremism than service members on active duty. They pointed out that members of the Guard and Reserve go through the same recruiting, screening, and training processes as their active counterparts, and that members of the RC are in the military because they share military values and "they just really want to be with us." They concluded that while the numbers are not large, even small numbers of violent extremists are a matter of great concern. Senior national guard leaders also shared views expressed by other DOD leaders that the definition of prohibited extremist activities remains unclear, that the use of the term "extremism" can be problematic, that there is strength in diversity of backgrounds and ideas, that a clearly-worded positive message based on military core values is the best response to violent extremism, and that the Department should exercise extreme care in monitoring the social media of service members.

In principle, the prohibitions on extremist activities in DODI 1325.06 are fully applicable to the Guard and Reserve. The general principle behind DODI 1325.06 is that it applies to service members at all times and in all capacities. The rationale for this approach is that a service member represents the Department regardless of whether they are in uniform or not. For example, if a guard member flies a Confederate flag while off duty, the conduct may still be attributable to that person as a member of the U.S. military. A senior DOD legal official told the IDA team that a commander's authority to enforce DOD rules in such a case would be tied to the need to maintain good order and discipline and the extent to which the service member's actions could be tied to his or her military service.

In practice, however, the Department will be challenged in its ability to enforce the federal requirements on individuals who are working on State duty or in civilian jobs (or at home in their communities). Members of the RC are not subject to the UCMJ unless they engage in prohibited conduct while in a federal status. Members of the National Guard in State status answer to the

[314] Confidential Interview with IDA team.

governor of their state via the State Adjutant General and are subject to their state Code of Military Justice. The Constitution allocates responsibility between the federal government/DOD (for forces in federal status) and the States (for regulating their own militias when in state status). Consequently, the Department could find it difficult to enforce the requirements of DODI 1325.06 with regard to Members of the National Guard without the support of the governor and the State Adjutant General. While DOD can require the State Guards to adhere to certain federal standards as a condition of eligibility for "federal recognition," the process of denying federal recognition for failure to apply federal rules on prohibited extremist conduct would be extremely difficult.

Moreover, the detection and prevention activities of the DOD primary prevention workforce and the internal threat assessment system will be challenged with regard to members of the Guard and Reserve. Unless an individual state elects to establish its own primary prevention workforce, the DOD primary prevention workforce is unlikely to reach non-active service members. Active duty units usually maintain daily contact with service members, while reserve units are normally limited to monthly unit training assemblies and periods of annual training. This difference between daily and monthly contact means that supervisors are likely to be far less familiar with the outside activities in which a guardsman or Reservist may be involved. Officials interviewed by the IDA team noted that problems associated with lack of contact can become particularly acute if a service member intentionally conceals involvement with extremist actions and behaviors. In cases in which problematic activity escapes the notice of an individual's chain of command, DOD may be reliant upon cooperation from local law enforcement to identify and report the behavior.

Finally, the Department may be challenged in its effort to mandate universal acceptance of and adherence to a singular definition and understanding of prohibited extremist activities when guard and reserve members are embedded in their communities and can be expected to reflect the values and divisions of those communities. One senior national guard official told IDA that "what is accepted as extremism in one location is not accepted in another." Another reported that the reaction to the DOD extremism stand-down varied greatly by community, saying that, "Some remote areas that are homogeneous . . . didn't see the point [of the stand-down], because it doesn't impact them. Other places . . . it was very impactful." Despite these difficulties of interpretation, assessment, and enforcement, the IDA review did not reveal any basis for establishing a different definition of prohibited extremist activities. Senior leaders interviewed by the IDA team argued strongly that it would not be appropriate to have one standard of conduct for the active duty force and another separate standard for the RC. The IDA team concluded that DODI 1325.06, like military core values, should apply equally for all components whether on duty or off duty.

5. Findings and Recommendations

The IDA team found that the multiple legal and policy regimes applicable to prohibited extremist activities provide the Department with a broad range of disciplinary options ranging from feedback and verbal counseling to informal and formal letters of counseling, admonition or reprimand; to non-judicial punishment, to administrative separation and criminal judicial

processes and sanctions. Multiple interviewees told the IDA team that racism and bias continue to be problems in the military, but only a handful of violent extremists have been identified in the military ranks. Push, pull, and personal factors for violent extremism appear to be similar to factors contributing to other negative behaviors, such as suicide, binge-drinking, drugs, and domestic abuse.

For these reasons, a carefully modulated range of responses is likely to influence behavior—and less likely to risk alienating the force—than an excessively punitive focus on extremist behaviors and activities. The IDA team recommends that the Department continue to take advantage of the full spectrum of disciplinary measures available to address prohibited extremist behaviors, resorting to criminal sanctions only when called for by the facts and circumstances of a particular case. Senior officials interviewed by the IDA team indicated that the military services are already taking a modulated approach to extremist behaviors and activities, avoiding the application of disproportionate disciplinary measures. However, a clear message from senior officials would be helpful to assure the Force that individual cases will continue to be judged on their merits and to ensure that the new policy is not construed either inside or outside the Department as changing that approach.

The IDA team also concluded that the establishment of a new criminal offense based on prohibited extremist activities would be counterproductive because: (1) a new provision would place an emphasis on criminal enforcement rather than on prevention; and (2) elements of intent likely to be included in the definition of such an offense would make it more difficult to prove the offense to the standard of reasonable doubt required to obtain a conviction. However, the IDA team is aware that in the absence of a specific extremism provision, the narrower grounds on which cases are prosecuted may not account for the full gravity of an offense that is committed to promote a political, religious, supremacist, or ideological agenda. In lieu of establishing a new criminal offense, IDA recommends that the Department take steps to amend the Manual for Courts-Martial to include an express reference to extremist motivation in the list of factors that may be considered aggravating in regard to sentencing decisions.

Neither of these recommendations can be implemented through a single action; rather, they will require a concerted effort over a period of time. Accordingly, the IDA team has developed a number of implementation options for the Department's consideration. These options are described for each recommendation below.

Recommendation 8: Unless more significant action is called for by the specific facts and circumstances of a particular case, seek rehabilitative and restorative interventions such as mentoring and counseling for activities that are not obviously violent or criminal.

To implement this recommendation, the Department should consider the following options:

- Department of Revised DODI 1325.06 appropriately directs Commanders to intervene early, primarily through counselling, to address actions that do not rise to the level of prohibited extremist activities but suggest the potential for future violations. The

USD(P&R) could supplement the revised DODI with guidance on types of conduct that do not rise to the level of prohibited extremist activities, or that merit counseling rather than punitive response. For example, such guidance could explain that, while each case must be assessed on the facts and circumstances:

- The aggressive, abusive, or disrespectful expression of political, ideological, or religious views is not in itself a prohibited extremist activity (although such may constitute discrimination or harassment) but could have the potential to disrupt good order and discipline and may merit early intervention through mentoring, counseling, or other feedback mechanisms.
- The expression of racist, sexist, or intolerant views is not in itself a prohibited extremist activity (although such may constitute discrimination or harassment). Where such expressions threaten to disrupt good order and discipline, they may merit early intervention through mentoring, counseling, or other feedback mechanisms.
- Discriminatory actions and harassing behaviors are prohibited by law and regulation, but absent advocacy of widespread discrimination or other specific facts and circumstances, most individual instances of discrimination or harassment would not, in themselves, rise to the level of prohibited extremist activity. In these cases, the MEO system and other tools may be more appropriate than the stronger punitive actions tied to active participation in prohibited extremist activities.
- Actions such as the display of inappropriate flags or paraphernalia and "liking" extremist websites are prohibited extremist activities but may not rise to a level that requires punitive action. Depending on the facts and circumstances of each individual case, it and may be possible to address these behaviors through mentoring and counseling.

Recommendation 9: Avoid making extremist activity a separate criminal offense under the UCMJ. Take action to modify the Manual for Courts-Martial to make evidence of prohibited extremist activity an aggravating factor in sentencing in a manner similar to Rule for Courts-Martial 1001(b)(4), which makes evidence of a hate crime an aggravating factor.

To implement this recommendation, the Department should consider the following options:

- The Secretary could recommend that the President amend the Manual for Courts-Martial to address this issue.
  - For example, the amendment could modify the sentence that currently reads: "In addition, evidence in aggravation may include evidence that the accused intentionally selected any victim or any property as the object of the offense because of the actual or perceived race, color, religion, national origin, ethnicity, gender, disability, or sexual orientation of any person" by adding language at the

end along the following lines: "or that the accused engaged in prohibited extremist activities such as the use of violent means to deprive individuals of lawful rights, to achieve goals that are political, religious, discriminatory, or ideological in nature, to alter or overthrow the government, or to disrupt military activities."

- The Secretary could direct the Service Judge Advocates General and the Staff Judge Advocate to the Commandant of the Marine Corps to develop standardized training materials for use by military judges charged to act on this change to the Manual.

B. The Military Community (including DOD Civilians and Contractor Employees)

1. Absence of a Prohibition on Extremist Behavior for DOD Civilians and Contractor Employees

Unlike members of the Armed Forces, who commit to obey lawful orders and are subject to military discipline throughout the period of their service, DOD civilian employees and defense contractors are bound only by the terms and conditions of their employment and are generally unregulated in their off-duty conduct. While workplace misconduct such as sexual or racial harassment is prohibited, the Department's enforcement tools as regards to civilian employees and contractors are more limited than for service members.

DOD civilians work under the government-wide civil service system, with strong procedural protections that cannot generally be waived or modified by the Department. DOD Directive 1440.1 establishes a civilian EEO program parallel to the MEO program established by DODI 1350.02, and DODI 1020.04 establishes a civilian anti-harassment policy parallel to the military policy established by DODI 1020.03. The civilian definition of prohibited harassment behaviors is nearly identical to the military definition.[315] Violations of the policy may be addressed through formal or informal administrative procedures,[316] through the federal EEO system,[317] or (in some circumstances) through the criminal justice system.[318] While these procedures address prohibited extremist activities that take place in the workplace and are based on race or gender, they do not reach advocacy or organization outside the workplace.

Contractor employees are subject to a contractor's internal human resources rules and to state and local employment laws. They may also be subject to DOD rules of conduct during working hours, especially if the place of performance is a DOD facility. Several IDA interviewees pointed out that the doctrine of "employment at will" makes it far easier to dismiss problematic employees

[315] Department of Defense, "Harassment Prevention and Responses for DoD Civilian Employees," DODI 1020.04 (Washington, DC: Department of Defense, June 30, 2020), Section 3.2.

[316] Ibid, Section 4.2 and 4.7.

[317] Ibid, Section 4.3.

[318] Ibid, Section 4.4.

in the private sector than in the federal government. While federal law affords government employees significant procedural rights before they may be disciplined or dismissed, a government contractor/private sector employer may generally dismiss an employee at any time, with the burden on the employee to take the matter to court or arbitration to demonstrate that the employer's action was unlawful or improper (for example, based on racial or sexual discrimination).

The Department can impose requirements on contractor employees through mandatory contract provisions (such as anti-drug requirements, whistleblower protections, human trafficking provisions). However, this has generally been done only in response to legislative requirements that directly relate to contract performance. Both civilian employees and contractors enjoy the full range of First Amendment rights without the limitations that may apply to members of the Armed Forces. A DOD contract provision that sought to restrict the rights of contractor employees to advocate for extremist causes (or associate with those who advocate for such causes) outside a of a DOD workplace would appear to limit First Amendment rights without any obvious nexus to contract performance and would be unlikely to survive legal scrutiny.

As a result, the toolset available to the Department to combat problematic extremist behaviors in its civilian and contractor workforces is substantially more constrained than the toolset applicable to service members. For civilian employees and contractors alike, there is no systematic recruiting process that can screen out individuals with potentially problematic backgrounds even before they are hired; there is no comprehensive education and training regime directed at instilling civic values; and there are no comprehensive regulations governing dissident and protest activities in the workforce. DOD-wide and service-specific regulations defining prohibited extremist activities do not apply to either civilians or contractors. Indeed, the application of regulations governing the speech and assembly activities of DOD civilians and contractor employees (at least on their own time) would likely conflict with protected First Amendment rights.

The legal and enforcement tools left to the Department fall into three major categories: (1) screening requirements for security clearances, suitability determinations, and access to DOD facilities and information systems; (2) insider threat assessments and counterintelligence investigations; and (3) prosecution for violations of the criminal laws of the United States or in some cases, the criminal laws of the state in which the federal workplace is located.

The DOD screening requirements do not currently identify participation in prohibited extremist activities as a basis for denial of a security clearance, a determination of unsuitability, or denial of access to facilities or information systems (although some extremist activities may violate other prohibitions). Rather, these screening requirements identify narrower categories of behavior, such as terrorism or efforts to overthrow the U.S. government, as a basis for denial. Because the Department has a strong interest in ensuring a relationship of trust and reliability when it grants employment and related privileges, it likely has the authority to make such privileges conditional on an employee or contractor's avoidance of conduct that clearly calls their trustworthiness and reliability into question, including most (if not all) prohibited extremist activities listed in DODI 1325.06. The contrast between military-only regulations (which directly address prohibited

extremist activities) and DOD- or government-wide regulations (which do not) is summarized in Figure 26.

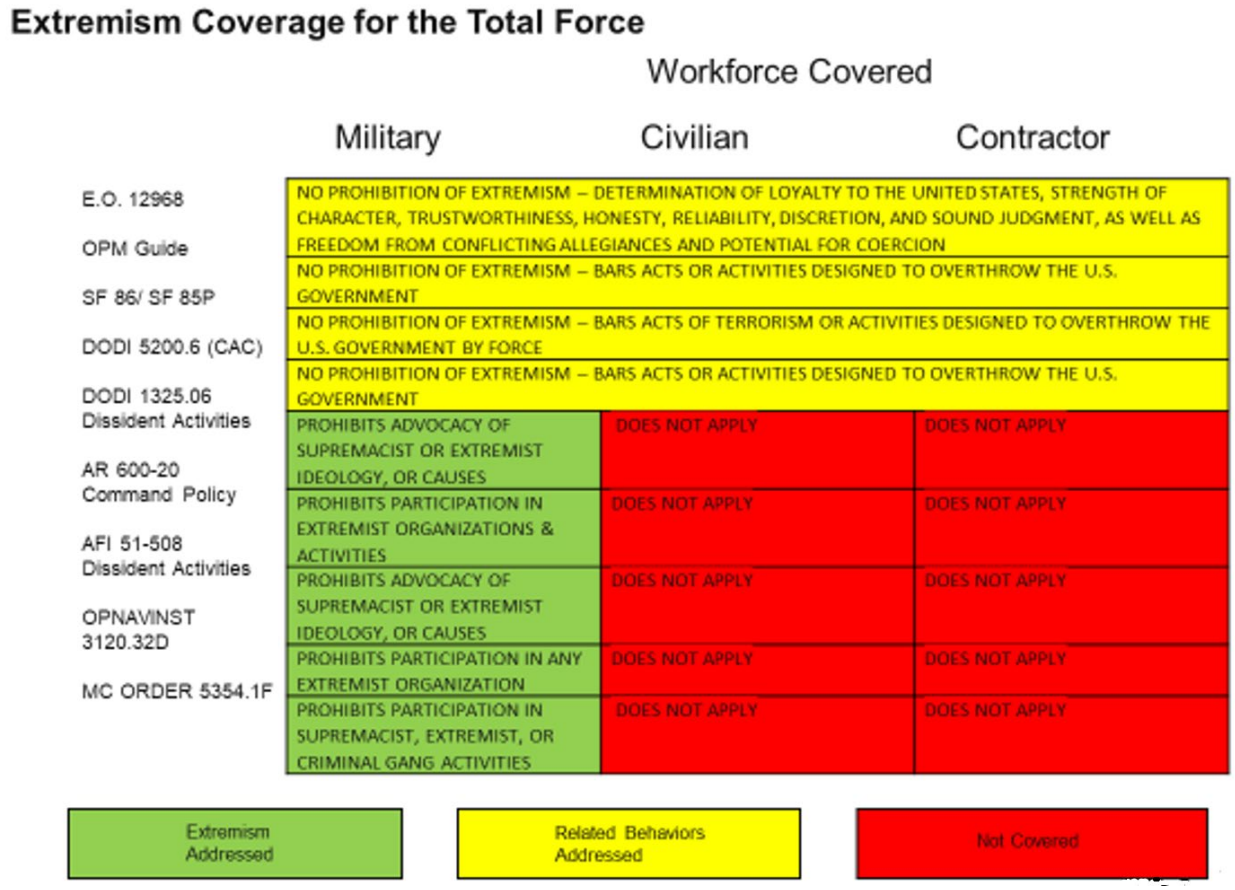


Figure 26. Coverage of Extremism in Military-Unique Regulations and in Regulations Applicable to Civilians

Criminal law enforcement tools applicable to the military community and the public are similarly narrow. Title 18 of the U.S. Code includes provisions addressing treason and sedition, provisions addressing hate crimes, and provisions addressing terrorism—but not provisions addressing violent extremist actions and other prohibited extremist activities listed in DODI 1325.06. While the Department of Justice (DOJ) and the FBI have significant investigative and enforcement tools that could be leveraged by the Department to help address prohibited extremist activities, there are serious limitations on the extent to which these tools can be used to address extremism without interfering with the First Amendment rights of American citizens.

The Department's insider threat programs are designed in principle to address the full range of extremist activities and precursor behaviors. As detailed below, however, these programs are still in an incipient stage and have not been as effective as intended due to a lack of consistent data streams and integration with other elements of the Department.

2. Suitability, Credentialing, Security Clearance, and Continuous Evaluation

DOD uses overlapping processes to ensure that its workforce is appropriately reliable to trust with classified information, important job responsibilities, and access to sensitive facilities and information systems.

- The security clearance process is designed to assess whether individuals are eligible to handle sensitive national security information. Roughly 3.6 million DOD service members, civilians, and contractor employees have security clearances.[319]
- The suitability and fitness process is designed to assess whether federal employees are fit for federal employment. The Department has roughly 800,000 civilian employees[320] who are required to undergo suitability determinations.
- The process for issuing DOD Common Access Cards (CAC) pursuant to HSPD-12[321] is designed to assess eligibility for access to federal property and information systems. The Department has issued millions of CAC cards to service members, civilian employees, contractors, family members, and others over the last two decades.[322]

The objectives of these three processes are closely related. The Defense Civilian Personnel Advisory Service (DCPAS) explains in a guide for employees:

> Suitability answers the question 'Would the person's employment in a covered position promote the efficiency and protect the integrity of the service?' Fitness answers the question 'Does the person have the required level of character and conduct necessary to perform work for or on behalf of a Federal Agency?' . . . Security answers the question 'Does the person have personal conduct or influences that could affect or potentially affect his or her trustworthiness?' . . . HSPD-12 . . . answers the question 'Does the person pose an unacceptable risk to life, safety or health to persons, assets or information?'[323]

---

[319] David Vergun, "All DOD Personnel Now Receive Continuous Security Vetting," *DOD News,* October 5, 2021, https://www.defense.gov/News/News-Stories/Article/Article/2800381/all-DoD-personnel-now-receive-continuous-security-vetting/#:~:text=The%20Defense%20Counterintelligence%20and%20Security,its%20current%20continuous%20vetting%20program.

[320] Congressional Research Service, *Defense Primer: Department of Defense Civilian Employees* (Washington, DC: Congressional Research Service, February 15, 2022), https://sgp.fas.org/crs/natsec/IF11510.pdf.

[321] "Homeland Security Presidential Directive 12: Policy for a Common Identification Standard for Federal Employees and Contractors," Department of Homeland Security Website, accessed June 16, 2022, https://www.dhs.gov/homeland-security-presidential-directive-12.

[322] Stephanie Ardiley, "History of the Common Access Card (CAC)," *Security Infowatch,* https://www.securityinfowatch.com/home/article/10653434/history-of-the-common-access-card-cac.

[323] Defense Civilian Personnel Advisory Service, *The Suitability Guide for Employees* (Washington, DC: Department of Defense, n.d.), 9, https://www.dcpas.osd.mil/sites/default/files/2021-04/Suitability_Guide_for_Employees.pdf.

a. The Security Clearance Process

The security clearance process is governed by Executive Order 12968, which states:

> [E]ligibility for access to classified information shall be granted only to employees who are United States citizens for whom an appropriate investigation has been completed and whose personal and professional history affirmatively indicates loyalty to the United states, strength of character, trustworthiness, honesty, reliability, discretion, and sound judgment, as well as freedom from conflicting allegiances and potential for coercion, and willingness and ability to abide by regulations governing the use, handling, and protection of classified information.[324]

Security Executive Agent Directive 4 (SEAD 4), issued by the Director of National Intelligence, establishes the National Security Adjudicative Guidelines, which are used to assess security clearance eligibility.[325] SEAD 4 establishes guidelines for 13 areas of assessment: Allegiance to the United States, Foreign Influence, Foreign Preference, Sexual Behavior, Personal Conduct, Financial Considerations, Alcohol Consumption, Drug Involvement and Substance Misuse, Psychological Conditions, Criminal Conduct, Handling Protected Information, Outside Activities, and Use of Information Technology. Of these, Guideline A on Allegiance to the United States and Guideline E on Personal Conduct come closest to addressing issues raised by prohibited extremist activities.

- Guideline A states that negative indictors of allegiance include "participation in or support for acts against the United States" and failure to adhere to the laws of the United States "if the violation of law is harmful to stated U.S. interests." This guideline expressly covers "involvement in, support of, training to commit, or advocacy of any act of sabotage, espionage, treason, terrorism, or sedition against the United States." It also addresses:

  > "association or sympathy with persons or organizations that advocate, threaten, or use force or violence, or use any other illegal or unconstitutional means, in an effort to:

1. "overthrow or influence the U.S. Government or any state or local government;
2. "prevent Federal, state or local government personnel from performing their official duties;
3. "gain retribution for perceived wrongs caused by the Federal, state, or local government; and

[324] White House Office of the Press Secretary, *Executive Order 12968: Access to Classified Information* (Washington, DC: White House Office of the Press Secretary, August 4, 1995).

[325] Office of the Director of National Intelligence, *Security Executive Agent Directive 4: National Security Adjudicative Guidelines* (n.p.: Office of the Director of National Intelligence, December 10, 2016), https://www.dni.gov/files/NCSC/documents/Regulations/SEAD-4-Adjudicative-Guidelines-U.pdf.

4. "prevent others from exercising their rights under the Constitution or laws of the United States or any state."

- While this provision addresses several categories of prohibited extremist activities, as defined in DODI 1325.06, it does not address all of them. For example, it does not address association with the full range of persons or organizations that advocate violence or the use of force "to achieve goals that are political, religious, discriminatory, or ideological in nature" or advocate (violent or nonviolent) "widespread unlawful discrimination based on race, color, national origin, religion, sex (including pregnancy), gender identity, or sexual orientation." Consequently, it is conceivable that a security clearance could be issued to an individual who has engaged in activities that would violate the DOD directive if engaged in by a service member.
- Guideline E states that "Conduct involving questionable judgment, lack of candor, dishonesty, or unwillingness to comply with rules and regulations can raise questions about an individual's reliability, trustworthiness, and ability to protect classified or sensitive information." The guideline further notes that considerations could include "any disruptive, violent, or other inappropriate behavior" and "association with persons involved in criminal activity." Although these factors could conceivably be used to disqualify an individual with a history of association with violent extremist groups, the Guideline includes no direction in this regard, leaving it open to question whether participation in prohibited extremist activities listed in DODI 1325.06 would be considered, for example, to be a sign of "questionable judgment.".

Each applicant for a security clearance is required to file an application form (generally the Standard Form 86 (SF86)). This form asks a series of questions about the applicant's background and activities and is one of the primary tools used by the federal government in the security clearance process to identify potential eligibility issues. The loyalty issues raised by Guideline A are addressed by Section 29 of the SF86, which poses a series of questions about an individual's associations. However, categories of associations covered by the questions in Section 29 are narrower than the categories covered by Guideline A (and hence, far narrower than the definition of prohibited extremist activities in DODI 1325.06). The form asks seven questions:

- Question 29.1 asks "Are you now or have you EVER been a member of an organization dedicated to terrorism, either with an awareness of the organization's dedication to that end, or with the specific intent to further such activities?" For the purpose of this question, "terrorism is defined as any criminal acts that involve violence or are dangerous to human life and appear to be intended to intimidate or coerce a civilian population to influence the policy of a government by intimidation or coercion, or to affect the conduct of a government by mass destruction, assassination or kidnapping."
  - Although Guideline A covers "association or sympathy with" groups that "advocate or threaten" the use of force, this question addresses only membership in an

organization that commits specific violent criminal acts. Although Guideline A covers the use of violent or illegal means to influence government policy, this question addresses only efforts to influence government policy by intimidating or coercing a civilian population, mass destruction, assassination, or kidnapping. As a result, broad areas of extremist activities covered by Guideline A are not addressed at all by question 29.1.

- Question 29.2 asks "Have you EVER knowingly engaged in any acts of terrorism?" and Question 29.3 asks "Have you EVER advocated any acts of terrorism or activities designed to overthrow the U.S. government by force?"
  - These questions are subject to the same limited definition of terrorism as Question 29.1, and cover only personal acts of terrorism or advocacy—a category much narrower than the associational activities addressed by Guideline A and DODI 1325.06.
- Question 29.4 asks "Have you EVER been a member of an organization dedicated to the use of violence or force to overthrow the United States government, and which engaged in activities to that end with an awareness of the organization's dedication to that end or with the specific intent to further such activities?"
  - This question addresses only membership, not "association or sympathy with" an organization; it requires that the organization be "dedicated to" (rather than merely advocating) the use of force or violence to overthrow the government; and it addresses only organizations seeking the overthrow of the U.S. government—in contrast to Guideline A and DODI 1325.06, both of which address unlawful efforts to overthrow state or local governments.
- Question 29.5 asks "Have you EVER been a member of an organization that advocates or practices omission of acts of force or violence to discourage others from exercising their rights under the U.S. Constitution or any state of the United States with the specific intent to further such action?"
  - This question is narrower than comparable constructions in Guideline A and DODI 1325.06, in that requires both membership and "specific intent" to merit a positive answer.
- Question 29.6 asks "Have you EVER knowingly engaged in activities designed to overthrow the U.S. Government by force?"
  - Like several previous questions, this question addresses only personal activities, not associations or advocacy, and omits efforts to overthrow state or local governments.
- Question 29.7 asks "Have you EVER associated with anyone involved in activities to further terrorism?"

– This is the sole question on the list that addresses associational activities. However, it is limited by the narrow definition of terrorism (described above), which requires specific violent criminal acts intended to intimidate or coerce a civilian population. This excludes a much broader category of violent and illegal activities, as well as advocacy activities, all of which are covered by Guideline A and DODI 1325.06.

Senior DOD officials with expertise in this area were generally opposed to the idea of a separate guideline for extremism, believing that guidelines on allegiance and personal conduct should be broad enough to cover prohibited extremist activities. With this caveat, they expressed the strong view that the SF86 questions need to be rewritten, expressed concern that some of the language in SEAD 4 may be too narrow, and suggested that additional guidance on how extremism fits within the existing guidelines would be helpful. The IDA team was told anecdotally that officials are aware of only a single individual who has ever been screened out of a security clearance as a result of question 29—presumably on the basis of information indicating that a false answer had been provided. Several interviewees expressed frustration with the burdensome and time-consuming interagency process required to accomplish any modification to government-wide security clearance eligibility forms and standards.

b. The Suitability Process

The suitability process for federal employees is governed by Office of Personnel Management (OPM) regulations codified in the Code of Federal Regulations.[326] The purpose of this process is to make "determinations based on a person's character or conduct that may have an impact on the integrity or efficiency of the service."[327] The OPM regulations authorize the consideration of eight factors, which are the exclusive basis for finding a person unsuitable for federal employment:

1. "Misconduct or negligence in employment;
2. "Criminal or dishonest conduct;
3. "Material, intentional false statements . . . ;
4. "Refusal to furnish testimony . . . ;
5. "Alcohol abuse . . . ;
6. "Illegal use of narcotics, drugs, or other controlled substances . . . ;
7. "Knowing and willful engagement in acts or activities designed to overthrow the U.S. Government by force; and

[326] Office of Personnel Management, *Code of Federal Regulations*, Title 5, Chapter 1, Part 731 (n.p.: Office of Personnel Management, 2012), https://www.ecfr.gov/current/title-5/chapter-I.

[327] Ibid, Title 5, Chapter 1, Part 731.101.

8. "Any statutory or regulatory bar which prevents lawful employment . . ."[328]

Short of a criminal conviction, the only one of these factors that addresses any category of prohibited extremist activities is number (7), which covers only a narrow category of activities designed to overthrow the U.S. government by force. This factor does not address active and associational activities designed to illegally deprive individuals of their constitutional rights; to overthrow state and local governments; to achieve political, religious, discriminatory goals by unlawful force or violence; to encourage DOD personnel to disobey lawful orders; or to advocate widespread unlawful discrimination. The Standard Form SF85,[329] OPM's suitability questionnaire for non-sensitive positions, does not include even the inadequate questions about violent terrorist activities included in the SF86. As a result, the Department currently appears to lack both the knowledge and the authority that would be needed to screen out applicants for employment on the basis of such conduct.

c. The Homeland Security Presidential Directive 12 (HSPD-12) Process

The HSPD-12 process governing the issuance of federal Personal Identity Verification cards is applied to DOD Common Access Cards (CAC) by DODI 5200.46. The purpose of this process is to establish eligibility to access federally-controlled facilities and information systems. DODI 5200.46 includes six "Basic Adjudicative Standards" and seven "Supplemental Adjudicative Standards."[330] Of these, only one Basic Standard and One Supplemental Standard address any category of prohibited extremism.

- Basic Adjudicative Standard 1[331] states: "A CAC will not be issued to a person if the individual is known to be or reasonably suspected of being a terrorist." Disqualifying conditions under this standard include "evidence that the individual has knowingly and willfully been involved with reportable domestic or international terrorist contacts or foreign intelligence entities, counterintelligence activities, indicators, or other behaviors . . .."

[328] Ibid, Title 5, Chapter 1, Part 731.102.

[329] Office of Personnel Management, *Standard Form 85: Questionnaire for Non-Sensitive Positions* (n.p.: Office of Personnel Management, December 2013), https://www.opm.gov/forms/pdf_fill/sf85.pdf.

[330] Department of Defense, "DoD Investigative and Adjudicative Guidance for Issuing the Common Access Card (CAC)," DODI 5200.46 (Washington, DC: Department of Defense, November 2, 2020), https://www.cac.mil/Portals/53/Documents/520046p%20DoDI%20DoD%20Investigative%20and%20Adjudicative%20Guidance%20for%20Issuing%20the%20Common%20Access%20Card.pdf?ver=2020-05-01-092718-907.

[331] The other basic standards address inability to authenticate identity, fraudulent identity information, unauthorized use of classified or sensitive documents, improper use of identity credentials, and misuse of federal information systems.

- Supplemental Adjudicative Standard 7[332] states: "A CAC will not be issued to a person if the individual has knowingly and willfully engaged in acts or activities designed to overthrow the U.S. government by force." Disqualifying conditions under this standard may include:
  - "Illegal involvement in, support of, training to commit, or advocacy of any act of sabotage, espionage, treason or sedition against the United States of America;"
  - "Association or agreement with persons who attempt to or commit" any such acts; and
  - "Association or agreement with persons or organizations that advocate, threaten, or use force or violence, or use any other illegal or unconstitutional means in an effort to overthrow or influence the U.S. Government."

These standards authorize the Department to reject CAC applications by individuals who engage in terrorist activities or have knowing contact with terrorists, and individuals who seek to overthrow the U.S. government. Like the federal government's suitability standards, however, they do not address applications by individuals who engage in active or associational activities designed to illegally deprive individuals of their constitutional rights; who seek to overthrow state and local governments; who engage in actions or activities to achieve political, religious, discriminatory goals by unlawful force or violence; who encourage DOD personnel to disobey lawful orders; or who advocate widespread unlawful discrimination. Consequently, DOD regulations do not currently authorize the denial of a CAC card to civilian employees, contractors, or applicants for employment who have engaged in most forms of prohibited extremist activities.

The IDA team is aware that at least two military services have reinforced the questions on the SF86 and the SF85 by directing their military recruiters to ask supplemental questions about prohibited extremist activities. Since 2011, all marine recruits have been asked to sign a statement of understanding regarding the Marine Corps policy on extremism. Recruits are required to acknowledge a policy that states:

> Marines are prohibited from participation in criminal gangs, extremist organizations and activities. Extremist organizations and activities are ones that advocate racial, gender, or ethnic hatred or intolerance; advocate, create, or engage in illegal discrimination based on race, color, sex, religion, or national origin; advocate the use of or use force or violence or unlawful means to deprive individuals of their rights under the United States Constitution or the laws of the

[332] The other supplemental standards address misconduct or negligence in employment, criminal or dishonest conduct, fraudulent statements in connection with employment, alcohol abuse, drug use, and statutory or regulatory bars on employment.

United States or any State; or advocate or seek to overthrow the Government of the United States, or any State by unlawful means.[333]

Similarly, in April 2021, the Air Force began asking all new recruits: "Have you ever had or currently have any association with an extremist/hate organization or gang?"[334] The IDA team was not able to identify questions or statements developed by the other military services for the purpose of identifying potential extremist conduct among new recruits.

The December 2021 report of the Secretary's Combating Extremist Activities Working Group (CEAWG) directed the Secretaries of the Military Departments to "update and standardize accession screening questionnaires to solicit specific information about current or previous extremist activity."[335] This recommendation was implemented by a memorandum from the Department's Director of Accession Policy, which directs that all military recruits be asked at least the following questions:

1. Has the applicant ever participated, either in person or via electronic communications, in an act of treason, terrorism, or sedition against the United States, regardless of whether the action resulted in a citation, arrest, or conviction?
2. Has the applicant ever associated with, either in person or via electronic communications, persons who are attempting to commit or who are committing an act of treason, terrorism, or sedition against the United States?
3. Has the applicant ever associated with, either in person or via electronic communications, persons or organizations that advocate, threaten, or use force or violence, or use any other illegal or unconstitutional means in an effort to:
    a. Overthrow or influence the U.S. Government or any state or local government?
    b. Prevent federal, state, or local government personnel from performing their official duties?
    c. Gain retribution for perceived wrongs caused by the federal, state, or local government?
    d. Prevent others from exercising their rights under the Constitution or laws of the United State or of any state?
4. Has the applicant, either in person or via electronic communications, ever advocated for the denial of civil rights based on the supremacy of one race, color, religion, national

[333] Marine Corps Recruiting Command, "Participation in Gangs, Extremist Organizations or Activities," MCRCO 1100.1 (Quantico, VA: United States Marine Corps, November 9, 2011), 3-107, https://www.yumpu.com/en/document/read/40514012/mcrco-11001-headquarters-marine-corps.

[334] Department of the Air Force, AFRS/RSO Accessions Standards NOTAM 21-09, April 23, 2021 (document provided by the Office of the Air Force Judge Advocate General).

[335] Department of Defense, *Report on Countering Extremist Activity Within the Department of Defense*.

origin, sexual orientation, gender, gender identity or disability over another race, color, religion, national origin, sexual orientation, gender, gender identity or disability?

5. Has the applicant, either in person or via electronic communications, ever committed or conspired to commit a crime motivated by bias against race, color, religion, national origin, sexual orientation, gender, gender identity, or disability?"

As shown in Figure 27, these questions parallel the issues raised in the revised DODI 1325.06, SEAD 4, and the SF86, but do not match any of them. Green boxes indicate areas that are covered by the various regulations, directives, and questionnaires; brown boxes indicate gaps.

DODI 1325.06	SEAD 4 (GUIDELINE A)	SF86	RECRUITING QUESTIONS
Advocating or engaging in unlawful force, unlawful violence, or other illegal means to deprive individuals of their rights under the United States Constitution or the laws of the United States . . .	Prevent others from exercising their rights under the Constitution or laws of the United State or of any state	Have you EVER been a member of an organization that advocates or practices commission of acts of force or violence to discourage others from exercising their rights . . .	Prevent others from exercising their rights under the Constitution or laws of the United State or of any state
Advocating or engaging in unlawful force or violence to achieve goals that are political, religious, discriminatory, or ideological in nature			
Advocating, engaging in, or supporting terrorism, within the United States or abroad		Are you now or have you EVER been a member of an organization dedicated to terrorism . . .	An act of treason, terrorism or sedition against the United States
Advocating, engaging in, or supporting the overthrow of the government of the United States . . .	Overthrow or influence the U.S. Government or any state or local government	Have you EVER been a member of an organization dedicated to the use of violence or force to overthrow the United States government . . .	Overthrow or influence the U.S. Government or any state or local government
Advocating or encouraging military, civilian, or contractor personnel . . . to violate the laws of the United States . . . or to disobey lawful orders or regulations, for the purpose of disrupting military activities			

DODI 1325.06	SEAD 4 (GUIDELINE A)	SF86	RECRUITING QUESTIONS
Advocating widespread unlawful discrimination based on race, color, national origin, religion, sex (including pregnancy), gender identity, or sexual orientation			Advocated for the denial of civil rights based on the supremacy of one race, color, religion, national origin, sexual orientation, gender, gender identity or disability over another race, color, religion, national origin, sexual orientation, gender, gender identity or disability
	Prevent Federal, state, or local government personnel from performing their official duties		Prevent Federal, state, or local government personnel from performing their official duties
	Gain retribution for perceived wrongs caused by the Federal, state, or local government		Gain retribution for perceived wrongs caused by the Federal, state, or local government
			Committed or conspired to commit a crime motivated by bias against race, color, religion, national origin, sexual orientation, gender, gender identity, or disability

Figure 27. Comparative Coverage of DoDI 1325.06, SEAD 4, SF86, and Standard Recruiting Questions.

As a result, the revised question could perpetuate the Department's inconsistent approach to defining prohibited extremist activities. More importantly, the revised questionnaire applies only to military recruits, not to civilian employees or contractors. As a result, the Department remains at risk of unknowingly permitting persons who may have engaged in violent extremist conduct to enter and encumber privileged positions as civilian employees or contractors in the military community.

3. Insider Threat Program

DOD Directive 5205.16 establishes an insider threat program for the Department to "prevent, deter, detect, and mitigate" threats from "espionage, terrorism, unauthorized disclosure of national security information, or through the loss or degradation of departmental resources or capabilities."[336] The program is managed by the office of the USD(I&S).

[336] Department of Defense, "The DoD Insider Threat Program," DODD 5205.16 (Washington, DC: Department of Defense, August 28, 2017), https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/520516p.pdf?ver=2019-04-03-141607-017.

Although DODD 5205.16 does not specifically refer to prohibited extremist activities, officials responsible for the program told IDA that the threat assessment system now covers the full range of problematic behaviors, including prohibited extremist activities, workplace violence, and even suicidal behavior. The insider threat program covers anyone with a DOD identification card that provides access to military installations, including CACs, and military retiree and dependent identification cards. Therefore, the insider threat program applies broadly to virtually any person with a DOD connection. A DOD official told IDA: "If you work on base at a McDonalds, you are in the program."

The insider threat program is authorized to "gather, integrate, review, assess, and respond to information derived from [counterintelligence], security, cybersecurity, civilian and military personnel management, workplace violence, [anti-terrorism] risk management, [law enforcement], the monitoring of user activity on DOD information networks, and other sources as necessary and appropriate to identify, mitigate, and counter insider threats."[337] The program evaluates risks of individuals who are demonstrating behaviors that could be indicative of insider risk; coordinates appropriate actions to ensure support and mitigation of risk; and assesses the effectiveness of those mitigation actions.

The insider threat program is not a law enforcement program, but no element of the Department may utilize investigative tools unless it complies with constitutional standards requiring probable cause. Insider threat programs are able to overcome this limitation, to some extent, by requiring consent to monitoring as a condition for access to government systems and government information.

Individual users of classified networks and other official government networks must consent to monitoring of their online behavior before being granted access. IDA understands that communications on classified networks are regularly monitored using key words and other discovery mechanisms, but systems for comprehensive and continuous monitoring of individuals using unclassified DOD networks are not currently in place, although there has been discussion in the Department of the possibility of such a program.

Monitoring communications that are not conducted on government networks is more problematic. Applicants for security clearances and for employment are required to authorize investigators to access any "publicly available social media information" regarding their activities.[338] Even where authorities exist for monitoring computer network and online activities, the Department has been hampered by technological limitations and concerns about excessively

[337] Ibid.

[338] U.S. Office of Personnel Management, *Questionnaire for Public Trust Positions*, SF 85P (n.p.: U.S. Office of Personnel Management, revised December 2017), https://www.opm.gov/forms/pdf_fill/sf85p.pdf; U.S. Office of Personnel Management, *Questionnaire for National Security Positions*, SF 86 (n.p.: U.S. Office of Personnel Management, revised November 2016), https://www.opm.gov/forms/pdf_fill/sf86.pdf.

intrusive methods and has not yet been able to make effective use of this authority outside of government systems.

Senior officials informed the IDA team that individuals can be added to the insider threat program if they are reported by others, or through internal systems or tip lines. A neighbor could call a government tip line if they know that the individual in question is a government worker, for example. Members of the DOD community and public can also report on suspicious behavior using tip lines, but these cases have generally been difficult to verify. The perception of research participants regarding the value of tip lines was varied. Some individuals felt that a specific reporting requirement for extremism would make the tip lines more helpful. Others felt that specific definitions could be counterproductive. Multiple individuals interviewed expressed the perception that tip lines are used as "weapons" or for "complaints" instead of providing useful information. Overall, there have been very few cases of extremism being reported internally through tip lines, but this could be because there are few cases of extremism.

Officials also informed the team that individuals can be flagged as "risky" during their security clearance adjudication process. If an individual is adjudicated with certain condition codes, they can be added to the insider threat program. An interview participant explained that there is no "extremism" condition code, but an individual with a risk of extremist behavior could be identified through the condition code of "criminal or personal conduct or allegiance to the United States."

Insider threat officials can also refer cases to investigative agencies, which can access further information about potential security risks upon a determination of probable cause, triggering access to information that is not publicly available, including information that is behind privacy filters or on the dark web. Counterintelligence investigations can employ these additional investigative methods once they have been expressly authorized to do so. Even in regard to counterintelligence investigations, however, there was a perception that there exist certain measures that unnecessarily prevent the use of reasonable internet searching. One individual interviewed expressed that the more capable their organization becomes at acquiring information, the more they feel they are stopped from legitimate investigative methods.

The Department is now working to build a broader threat assessment capability that will enable it to identify and mitigate insider risks at an early stage. The DITMAC, which was established in the wake of the Navy Yard shooting in 2013, sits at the top of the organizational pyramid responsible for the new program. DOD policy requires the components to have risk prevention programs in place, and to feed data on risks to the DITMAC. However, the original recommendation to field broad threat assessment teams at the installation level was deemed too expensive and has not been implemented to date.

As a result, the planned insider threat detection system is still in its incipient stages. Installations are required to have insider threat coordinators and to report threat data to DITMAC, but there has been no systematic assessment of compliance with this requirement. The Department

has not yet developed specific data requirements and reporting criteria. The Information Technology (IT) systems needed to support comprehensive reporting are not in place, so data is reported to DITMAC (when it is reported) in manual spreadsheets. "It's the lack of integrated systems through the Department," one official told IDA. He added:

> It is broken. It doesn't alert, it doesn't work well with data, and it doesn't work with our partners. You could say that the IT system is the way we need to do this right. We need a mandate to do it, and a system to do it.[339]

Insider threat officials told IDA that it was their intent to draw on personnel data, including data on behavioral problems, to get "to the left of boom" in the threat assessment process. "We have psychologists and threat assessors," one official stated. "We are more rooted in threat assessment than security." As discussed in Chapter 6.C above, however, it does not appear that the incipient threat assessment system is linked to the an integrated policy on the prevention of self-directed harm and prohibited abuse or harm overseen by the USD(P&R).[340] In the absence of a clear set of definitions and thresholds, which have not yet been developed, members of the military community might be deterred from seeking counseling and other beneficial assistance if this action might result in an insider threat report.

By design, the insider threat program screens for escalating behavior. A senior research participant informed the IDA team that the insider threat program uses standard behavioral science assessments such as Terrorist Radicalization Assessment Protocol-18 (TRAP-18) [341] and Workplace Assessment of Violent Risk (WAVR-21). [342] Another research participant highlighted that insider threat policies could help detect individuals who could benefit from intervention before their behavior escalates.

The insider threat program is currently seeking to update training to address the risk of violent extremism and other forms of workplace violence and problematic behaviors. The problem is that insider threat training is fractured in the Department, with different installations and organizations responsible for developing their own security awareness training. Moreover, as discussed below, it appears that this program has limited connectivity with a separate prevention program for workplace violence and problematic behaviors under the purview of the USD(P&R). As a result, it has been difficult to ensure that a problem like violent extremism is consistently addressed

---

[339] Confidential Interview with IDA team.

[340] Secretary of Defense, "Memorandum for Senior Pentagon Leadership, Commanders of the Combatant Commands, and Defense Agency and DoD Field Activity Directors. DoD Actions to Address Findings and Recommendations of the 2021 On-Site Installation Evaluations," memorandum (Washington, DC. Department of Defense, March 30, 2022), https://media.defense.gov/2022/Mar/31/2002967351/-1/-1/1/DOD-ACTIONS-TO-ADDRESS-FINDINGS-AND-RECOMMENDATIONS-OF-THE-2021-ON-SITE-INSTALLATION-EVALUATION.PDF.

[341] "TRAP-18 Manual & Code Sheets Annual User License," Global Institute of Forensic Research Inc. Website, accessed June 16, 2022, https://gifrinc.com/trap-18-manual/.

[342] "The WAVR-21 Threat Assessment App," WAVR-21 Website, accessed June 16, 2022, https://www.wavr21.com/.

throughout the Department. The insider threat program hopes to ensure greater consistency by developing educational learning objectives (ELOs) and technical learning objectives (TLOs) that could be required for all insider threat training.

4. Criminal Code

Neither extremism nor violent extremism is a prohibited act under federal criminal code (Title 18 of the U.S. Code).[343] International terrorism is prohibited under 18 U.S.C. section 2332b, but domestic terrorism—although defined in law (18 U.S.C. section 2331(5))—is not a criminal offense. The U.S. Code includes offenses for treason,[344] seditious conspiracy,[345] and advocating the overthrow of the government.[346] It contains offenses for the use of weapons of mass destruction,[347] bombings of government facilities,[348] and acts of nuclear terrorism, [349] but it contains no offense for acts intended to influence government policy through the use or threat of force, to intimidate or coerce a civilian population, or to influence the policy of a government by intimidation or coercion, unless these acts cross international boundaries.

Law review articles have been written proposing that this "gap" be closed through the enactment of a domestic terrorism offense,[350] but no legislative action has been taken. As a result, domestic terrorists and members of violent extremist groups are generally investigated or prosecuted by law enforcement authorities only when they commit other offenses, such as fraud, assault, or trespassing. Law enforcement officials interviewed by the IDA team reported that the number one charge for which domestic violent extremists are arrested is felony possession of illegally modified firearms. "We have to get creative in going after them," IDA was told.

The reason for this gap is straightforward: The First Amendment to the U.S. Constitution protects the rights of free speech and assembly. Extremism, violent extremism, and terrorism are all defined, at least in part, by their political and ideological motivation, which gives them a significant speech component. Even advocacy of violence, unless it takes the form of incitement to immediate action, may be protected under the First Amendment.

---

[343] IDA is not aware of any state laws that make domestic terrorism or violent extremism a crime. As explained below it would be difficult for a state to enact such a law consistent with First Amendment requirements.

[344] 18 U.S.C. Section 2381, https://www.law.cornell.edu/uscode/text/18.

[345] Ibid, Section 2384.

[346] Ibid, Section 2385.

[347] Ibid, Section 2332a.

[348] Ibid, Section 2332f.

[349] Ibid, Section 2332i.

[350] Mary McCord, *Filling the Gap in our Terrorism Statutes* (Washington, DC: The George Washington University Program on Extremism, August 2019), https://extremism.gwu.edu/sites/g/files/zaxdzs2191/f/Filling%20The%20Gap%20in%20Our%20Terrorism%20Statutes.pdf.

The DOJ and the FBI categorize domestic violent extremists into specific "subthreats" (see Table 6): radically or ethnically-motivated violent extremists; anti-government or anti-authority violent extremists (including anarchists, militia groups, and "sovereign citizen" groups); animal or environmental rights extremists; and abortion extremists. The FBI even has a domestic terrorism/hate crime fusion cell. Law enforcement agencies receive numerous tips about extremist groups and the activities in which they are engaged.

However, law enforcement does not have the authority to investigate domestic violent extremist groups, or to investigate individuals for being members of violent extremist groups. For example, unlike foreign terrorist organizations, the DOJ does not have a mechanism to designate domestic entities as terrorist organizations. Evidence of a specific crime by a specific individual is required before an investigation can be initiated.[351] Domestic extremist groups may look like international terrorist groups and even have similar objectives, but absent indicia of a crime, they cannot be investigated or prosecuted in the same ways.

The DOJ and the FBI have partners in the military criminal investigative organizations and maintain a strong relationship with DOD. This relationship is memorialized in a two-way Memorandum of Understanding between DOD and DOJ. DOJ can refer cases involving members of the military to DOD for investigation and prosecution under the UCMJ, and DOD can request assistance from the greater resources and expertise of the civilian federal law enforcement agencies in investigating crimes DOD has identified. Although the federal law enforcement agencies have great investigative and prosecutorial resources, however, they can only investigate federal crimes, which are far narrower in scope than the prohibited extremist activities listed in DODI 1325.06. Consequently, their jurisdiction to pursue extremism-related cases remains far more limited than that of the DOD.

5. Interagency Cooperation and Coordination

Several federal agencies play central roles in countering extremist behaviors within the military community. As indicated above, the FBI and DOJ are important partners in the investigation and prosecution of violent extremists. DHS and the Department of Veterans Affairs (VA) are key players in the prevention and mitigation of potential prohibited extremist activities by individuals with current or past DOD affiliations. Continued interagency cooperation is essential to marshal the resources, knowledge, and situational awareness needed to effectively address prohibited extremist behaviors in the military community.

Resources available to the Department from external agencies include information sharing about extremist threats, training on warning signs of extremism, tips on specific individuals under

[351] National Public Radio (NPR), "Why the Government Can't Bring Terrorism Charges in Charlottesville," *NPR*, August 14, 2017, https://www.cpr.org/2017/08/14/why-the-government-cant-bring-terrorism-charges-in-charlottesville/.

investigation, and mitigation efforts with regard to individuals whom the Department can no longer reach.

- DOJ provides assistance to DOD in the form of investigative tools in ongoing criminal investigations, training for military lawyers and judges on how to effectively leverage those tools, and advice on potentially relevant legal statutes. DOJ takes the lead in prosecuting complex terrorism cases in federal court and assists military lawyers in prosecuting similar cases pursuant to the UCMJ.
- The FBI also shares investigative resources and techniques, often through military operations support teams and other direct relationships, with counterparts in military criminal investigative organizations. Through these channels, the FBI notifies the Department when a person of interest has a service affiliation. The FBI also shares information on potential threats with DOD counterintelligence authorities and personnel security organizations. In addition, the FBI provides threat briefings to military leaders on potential extremist activities and provides information to the military recruiting commands on extremist symbology and tattoos.
- DHS has developed a number of preventative approaches to CVE that could be useful to DOD (see Figure 22). For example, DHS has developed a comprehensive threat assessment approach that builds relationships with local law enforcement, community organizations, and the public to spot warning signs of violent extremism and build up effective reporting mechanisms. DHS is also conducting research into pathways to extremism and evidence-based practices to respond to extremism, as well as to the challenges posed by false information. DHS has shared this research with DOD and has connected DOD personnel research organizations with relevant resources.
- The VA focuses on providing assistance to veterans, not assessing threats. Consequently, the VA does not generally seek to address extremist behaviors, except by fostering a productive sense of community amongst veterans and providing counseling and other resources that may help build resistance to extremist recruiting. DOD makes some effort to notify VA of transitioning veterans who might need help, but better awareness and linkage to VA resources could improve the Department's ability to combat potential extremism across the military community.

Notwithstanding these resources, non-DOD agencies face significant constraints in their counter-extremism efforts when compared with DOD. Unlike DOD, these agencies do not benefit from Supreme Court case law that recognizes the special nature of military service. Unlike the Armed Forces, they cannot issue orders that define proper speech or conduct. They do not have the authority to unilaterally sanction individuals whose improper conduct falls short of criminal behavior. They must fully comply with constitutional requirements regarding freedom of speech and association that strictly limit the monitoring or regulation of political activities of U.S. citizens. As a DOJ official told the IDA team, an individual's public exhortations for death to all members

of a specific ethnic group would not, in itself, be a sufficient basis for DOJ to open an investigation against such persons; in contrast, DOD has access to a range of possible interventions to address similar behavior by a member of the military.

Investigative agencies operate within these constraints by focusing on specific threats posed by individuals rather than on their ideology, and by using non-extremism-specific criminal statutes, such as gun violations or money laundering statutes, to prosecute potential extremists before they commit an act of violence. Non-investigative agencies focus on community-building partnerships that aim to mitigate concerns before they rise to the level of criminal behavior.

One best practice, as described elsewhere in this report, is a comprehensive threat assessment approach that brings together a diverse team of stakeholders—including law enforcement, mental health professionals, domestic violence prevention organizations, school counselors, and local business security—to share information on individuals of concern. The goal of this approach is to help individuals, rather than punishing them. Early intervention is seen by advocates as forestalling problems before they get worse. DOD can potentially benefit not only from continued partnership with outside agencies in implementing these practices, but also from pursuing similar activities on its own.

6. Findings and Recommendations

The IDA team found that the Department has fewer legal tools to address extremist activities in its civilian and contractor workforces than the military workforce. The First Amendment rights of civilians and contractors are not limited by the demands of military service, so the Department's ability to directly regulate conduct are limited. For the same reason, the criminal law provisions of title 18, U.S. Code do not generally reach beyond activities that are unlawful without regard to political, ideological, or religious motivation. As a result, the most effective legal tools available to the Department to reach the broader military community are screening mechanisms designed to ensure the loyalty and reliability of individuals who serve in positions of trust and confidence or have access to classified materials or federal facilities and information systems.

The Department's processes for awarding security clearances, assessing suitability, and granting access to facilities and information systems are generally pointed at longstanding threats such as foreign influence and threats arising out of the Global War on Terrorism. The Department's insider threat programs have a broader focus, but have yet to establish a flow of information sufficient to support their ambitious intent. As a result, these processes do not appear to be effective at screening for prohibited extremist behaviors and activities. In many cases, the existing standards and training materials applicable to these processes do not even specifically identify such behaviors and activities as a potential problem. Where they do so, the standards and questions that they use appear to be inconsistent with each other and incomplete in their coverage.

For these reasons, IDA recommends that the Department take steps to:

- Update and standardize security and suitability questions asked of military and civilian employees, recruits for military service, and applicants for civilian positions, to directly address concerns about loyalty and reliability due to involvement in prohibited extremist activities;
- Develop guidance for security clearances, access and suitability determinations, explaining how active participation in prohibited extremist activities will be considered in these processes pursuant to existing criteria; and
- Update insider threat training and related materials to provide definitions and examples of prohibited extremist activities and to expressly encourage early reporting of potential problems.

The implementation of these recommendations cannot be accomplished through a single action but will require a concerted effort over a period of time. While IDA is not in a position to design a comprehensive course of action for each recommendation, the IDA team has developed a number of implementation options for the Department's consideration. These options are described below.

Recommendation 10: Update security and suitability questions asked of military and civilian employees, contractor employees, and applicants for employment, to incorporate the standard questions now asked of military recruits about participation in extremist activities, and expand those questions to address the full range of extremist activities prohibited by revised DODI 1325.06. [352]

To implement this recommendation with regard to civilians, contractors, and currently serving military personnel, the Department should consider the following option:

- The USD(P&R) could work with the USD(I&S), the Director of Washington Headquarters Services, and other appropriate officials to extend the use of the standard questions to all applications for DOD suitability determinations, security clearances, and access to facilities.
    - In addition, the Department could consider additional steps with regard to the military accessions process. For example:
- The USD(P&R) could expand the current set of five standardized questions identified in the 24 December 2021 memorandum to more fully reflect the definition of prohibited

[352] A working group of the Department of Homeland Security has made a similar recommendation for the workforce of that Department. U. S. Department of Homeland Security Office of the Chief Security Officer, *Report to the Secretary of Homeland Security Domestic Violent Extremism Internal Review: Observations, Findings, and Recommendations* (Washington, DC: Department of Homeland Security, March 11, 2022), Recommendation 8.1, 13, https://www.dhs.gov/sites/default/files/2022-03/Report%20to%20the%20Secretary%20of%20Homeland%20Security%20Domestic%20Violent%20Extremism%20Internal%20Review%20Observations%2C%20Findings%2C%20and%20Recommendations.pdf.

extremist activities in DODI 1325.06. For example, the Under Secretary could modify Question 3 of the standard questions by adding the following:

  - "v. achieve goals that are political, religious, discriminatory, or ideological in nature?"

Recommendation 11: Develop guidance on security clearances and access and suitability determinations, explaining how active participation in prohibited extremist activities will be considered pursuant to existing criteria.

To implement this recommendation, the Department should consider the following options:

- The USD(P&R) could work with the Director of the Office of Personnel Management to revise the criteria in 5 C.F.R. section 731 for making suitability determinations for federal employment to provide that active participation in prohibited extremist activities, as defined in DODI 1325.06, is a basis for determining that an individual is not suitable for Federal employment. The new language could be added to the existing provision regarding knowing and willful engagement in acts of activities designed to overthrow the U.S. Government by force.
  - Language along the following lines could be considered for insertion into 5 C.F.R. section 731.202(b), which lists factors that may be considered as a basis for an unsuitability determination:
  - "(8) Advocating or engaging in unlawful force or violence to achieve goals that are political, religious, discriminatory or ideological in nature; and"
- The USD(P&R) could work with the Director of the Office of Personnel Management to revise the Final Credentialing Standards for Issuing Personal Identity Verification (PIV) Cards under HSPD-12 to prohibit the issuance of a PIV Card to an individual who actively participates in violent extremist activities, as defined in DODI 1325.06. The new language could be added to the existing provision regarding individuals who are known to be or reasonably suspected of being terrorists.
  - Language along the following lines could be considered for insertion into the list of Supplemental Credentialing Standards in the OPM Memorandum:
  - "7. The individual has actively participated in advocating or engaging in unlawful force or violence to achieve goals that are political, religious, discriminatory or ideological in nature."
- The USD(I&S) could work with the Director of National Intelligence to revise Security Executive Agent Directive 4 to align *Guideline A: Allegiance to the United States,* more closely with the definition of prohibited extremist activities, as defined in DODI 1325.06. The existing provision regarding association or sympathy with persons or organizations that advocate, threaten, or use force or violence, or use other illegal or

unconstitutional means for specified purposes could be modified to achieve this objective.

  - Language along the following lines could be considered for insertion on the list of "specified purposes" in Paragraph 4(c) of Guideline A:
  - "(5) achieve goals that are political, religious, discriminatory, or ideological in nature."

Recommendation 12: Update insider threat training and related materials to provide definitions and examples of prohibited extremist activities and to expressly encourage early reporting of potential problems.

  - The Secretary's 20 December 2021, memorandum on Countering Extremist Activities directs the implementation of a similar recommendation by the CEAWG to develop a comprehensive training and education program addressing these issues as a part of the Department's Insider Threat program. Because these materials had not yet been developed at the time the IDA team competed its field work for this report, IDA is not in a position to assess the sufficiency of these training and education materials.
  - To further implement this recommendation, the Department should consider the following additional option:

- The USD(I&S) could work with the FBI and DHS to ensure that the Department is in a position to incorporate the latest information on prohibited extremist activities, groups, symbols, and recruitment trends into insider threat training materials on an ongoing basis.

This page is intentionally blank

8. Data and Technology Aspects of DOD Efforts to Counter Extremist Behaviors and Activities

A. DOD Data Systems

DOD maintains various information systems that can directly or indirectly track aspects of prohibited extremist activities and behaviors. DOD is now required by statute to track and report to Congress on the prevalence of these activities in the Armed Forces. Even before this requirement was established, DOD had already begun to make significant strides to establish mechanisms for systematically tracking prohibited extremist activities. However, these data tracking efforts have yet to be standardized throughout DOD in accordance with the statutory requirement. This section summarizes the statutory requirement, existing data tracking capabilities and practices, and areas for potential improvement.

1. Section 554 Data Tracking Requirements

On 1 January 2021, Congress passed the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (Pub. L. 116-283). Section 554 of this law, "Inspector General Oversight of Diversity and Inclusion in Department of Defense; Supremacist, Extremist, or Criminal Gang Activity in the Armed Forces," created a new DOD Deputy Inspector General (DIG) to oversee programs relating to diversity and inclusion and to prevent or mitigate "supremacist, extremist, and criminal gang activity" committed by members of the Armed Forces. Monitoring and gauging the effectiveness of "policies, programs, systems, and processes in preventing and responding to supremacist, extremist, and criminal gang activity" within the Armed Forces is a key responsibility of this position.

Section 554(b) calls for the "establishment of standard policies, processes, tracking mechanisms, and reporting requirements for supremacist, extremist, and criminal gang activities" within the Armed Forces. This requires standardizing data collection throughout DOD on these activities and reporting annually to Congress on their frequency. Section 554(b) requires the development of standard "policies, processes, and mechanisms" to ensure that the Inspector General receives information on all allegations of these prohibited activities and "can document and track" each through its ultimate outcome. The DIG is required to identify "total number of investigations and inquiries;" the number of individuals who were "subject to action" (including court-martial, other criminal prosecution, non-judicial punishment, or administrative action); the number who "engaged in prohibited activity" and "were not subject to action;" and the number of referrals to a civilian law enforcement agency.

The DOD Office of the Inspector General (DOD OIG) published a one-time report to Congress in June 2021, as required by Section 554(a)(4)(A), proposing the establishment of a new Diversity and Inclusion and Extremism in the Military (DIEM) Component, with responsibility for "strategic planning, coordination with military department IG Offices and other stakeholders, policy and program development, data management, and communications" in this domain.[353] The report noted three challenges that would need to be remedied before the DIEM component could be successfully established.

- The first challenge is that the appointment of the DIG by the Secretary of Defense, rather than by the Inspector General, could compromise the independence of the DOD OIG under the Inspector General Act of 1978, as amended. This problem was temporarily addressed by having the Secretary of Defense delegate appointment authority to the Inspector General. Congress then resolved the issue by realigning appointment authority in section 549K of the National Defense Authorization Act for Fiscal Year 2022.[354]
- A second challenge is that the Secretary of Defense had not yet issued DOD-wide procedures for meeting the Section 554 requirements.
- The last challenge—and the most difficult to overcome—is the "the absence or lack of interoperability of systems within the DOD to capture and track required information at command and local law enforcement organizations."[355] The DOD OIG suggested that its own system, the Defense Case Activity Tracking System-Enterprise (D-CATSe), would be an appropriate system to track referrals of prohibited activities. However, the DOD OIG would "require additional resources to accelerate deployment of the case-management system" to other entities within the DOD that have a responsibility for tracking prohibited activities.[356] In addition to system upgrades to facilitate tracking, Department-wide guidance would be needed to ensure the proper use of the system.

[353] DoD OIG, *The Department of Defense Office of Inspector General's Report to Congress Pursuant to Section 554 of the Fiscal Year 2021 National Defense Authorization Act* (Washington, DC: DoD OIG, June 10, 2021), 5, https://www.oversight.gov/sites/default/files/oig-reports/DoD/Department-Defense-Office-Inspector-General%E2%80%99s-Report-Congress-Pursuant-Section-554-Fiscal-Year-2021.pdf. Data management would include DoD hotline and information systems to keep track of cases as required in Section 554.

[354] National Authorization Act for Fiscal Year 2022, Rules Committee Print 117-21, Text of House Amendment to S. 1605, December 7, 2021, https://rules.house.gov/sites/democrats.rules.house.gov/files/BILLS-117S1605-RCP117-21.pdf.

[355] Ibid, 11.

[356] Ibid, 12.

The DOD OIG published its first annual report on prohibited activated within the Armed Forces on 1 December 2021.[357] The report noted many shortcomings in the Department's data collection systems and processes. For example:

- "We found that data collection across the Military Departments is inconsistent."[358]
- "The Military Departments reported issues with compiling and validating their data and, in some cases, the reported numbers were conflicting."[359]
- "We did not independently verify the reliability of the data from each Department."[360]
- The Secretary of Defense "has not yet established or implemented standard policies to report and track prohibited activities, including supremacist and extremist activity."[361]

The DOD OIG reported that the "Military Departments generally submitted their data using the standardized terminology" used by the FBI and DHS "to describe acts of domestic terrorism."[362] Although this may be a useful construct for categorizing different types of violent extremism, section 554(b) explicitly requires the reporting of any "activity prohibited under" DODI 1325.06 or any successor instruction. To the extent that the prohibited activities specified under DODI 1325.06 do not align with the FBI and DHS definitions and terminology for domestic terrorism the current approach could lead to under-reporting. The report concluded that a consistent definition of prohibited activity is crucial for the tracking and reporting of extremism, as is required in Section 554:

> Until the DoD establishes DoD-wide policy for tracking and reporting allegations of prohibited activities, the DoD will continue to have inconsistent tracking of disciplinary actions for participation in extremist organizations and activities; problems identifying and collecting data from multiple, decentralized systems; and difficulty validating the accuracy of the data.[363]

As described in Chapter 4.B.3 above, the Department has developed a new definition, but has yet to apply it consistently throughout. The data systems of the military departments reflect this continued inconsistency.

---

[357] DoD OIG, *Department of Defense Progress on Implementing Fiscal Year 2021 NDAA Section 554 Requirements Involving Prohibited Activities of Covered Armed Forces* (Washington, DC: DoD OIG, December 1, 2021), https://media.defense.gov/2021/Dec/02/2002902153/-1/-1/1/DODIG-2022-042.PDF.

[358] Ibid, 4.

[359] Ibid, 6.

[360] Ibid.

[361] Ibid, 4.

[362] Ibid, 5. For the FBI and DHS terminology, see National Defense Authorization Act for Fiscal Year 2020 Pub. L. 116-92, "Domestic Terrorism: Definitions, Terminology, and Methodology," November 2020, https://www.fbi.gov/file-repository/fbi-dhs-domestic-terrorism-definitions-terminology-methodology.pdf/view.

[363] Ibid, 9.

Notwithstanding inconsistencies in data collection and tracking practices, to be compliant with the Section 554(b) requirement, the DOD OIG collected information from each of the Military Departments on the numbers of allegations and substantiated cases between 1 January and 30 September 2021. The DOD IG reported that the vast majority of allegations identified to the DOD OIG (96%) were investigated. Fewer than one-third of allegations (31%) were substantiated. In cases where the allegation was substantiated, the Military Departments consistently took some form of official action. Specifically, the report notes that:

> The Military Departments reported a total of 294 allegations, 281 investigations and inquiries, 92 instances where action was taken, zero [substantiated] instances where no action was taken, and 83 referrals to civilian law enforcement agencies . . .. The Military Departments also reported incidents of criminal gang activity involving military members [and those incidents are included in these numbers].[364]

Over the next year, the DOD OIG plans to continue evaluating the "extent to which the DoD and the military services have implemented policy and procedures that prohibit active advocacy and active participation related to prohibited activities as required by DoD Instruction 1325.06."[365]

2. DOD Data Collection Systems and Extremism Flags

Each of the military services maintains multiple data systems for tracking instances of criminal, prohibited, or other wrongful behavior. Prominent and well-developed systems reside in criminal investigative, military justice, and equal opportunity organizations. Precise rules for the types of incidents to be tracked and the processes for them vary from one organization to another. In recent years, many of these organizations have made changes to their case-management systems to begin to explicitly flag cases involving some form of prohibited extremist activity. This is typically done by incorporating a checkbox or radio button that can be marked as information about the case being entered into the system.

Although marking a checkbox or radio button is a relatively simple step, it can greatly facilitate data tracking of prohibited extremist activities. Otherwise, the information can easily be buried within the vast amounts of data in a case-management system, requiring patience and ingenuity to identify the relative handful of cases that may describe some element of a prohibited extremist activity. In the absence of a flagging system, keyword searches can be useful, at least for case files that have been digitized. However, the chosen keywords need to appear somewhere within the case, so the set of keywords needs to be sufficiently broad to capture the right cases. Conversely, the presence of a keyword within a case does not necessarily indicate that the case involves a prohibited extremist activity, and sorting through the cases that may populate in a search can be costly and time consuming.

---

[364] Ibid, 5–6.

[365] Ibid, 9.

Multiple events over the last few years have heightened public awareness of various forms of extremism and have been an impetus for more systematic tracking of military involvement in prohibited extremist activities. Such events include the 2017 Unite the Right rally in Charlottesville and the violent protests and looting in the summer of 2020. These were later coupled with the Section 554(b) tracking requirement, passed on 1 January 2021, and tracking of the U.S. Capitol events on 6 January 2021.

Beginning in 2018, the Marine Corps Equal Opportunity system—the Discrimination and Sexual Harassment (DASH) Reporting system—was the first to incorporate an explicit flag for tracking extremism.[366] The NCIS followed suit in April 2019, with the Army Criminal Investigation Division (Army CID) and the Army military justice systems also incorporating flags into their systems in 2019. The Navy and Marine Corps military justice system added a flag in March 2021; the Air Force military justice system also added a flag in 2021. The Air Force Office of Special Investigations (OSI) is in the process of transitioning to a new case-management system and was unable to make changes to its legacy system but anticipates having some kind of flagging system for cases involving prohibited extremist activities in its new system.

This movement toward tracking of cases of prohibited extremist activities began before the Section 554(b) requirement was enacted. However, a key element of that requirement that has not yet been addressed in these data tracking processes is standardization. Section 554(b) calls for "standard policies, processes, tracking mechanisms." At present, there are nuances and differences across systems. This begins with how these flags for tracking prohibited extremist behaviors are labeled. Examples from different systems include:

- "Dissident and Protest Activity" (in the Marine Corps Equal Opportunity system, DASH)
- "Extremism and Hate Groups" (in the Air Force Automated Military Justice Analysis and Management System (AMJAMS))
- "Case involves an allegation of supremacist, extremist, or criminal gang activity" (in the Navy & Marine Corps military justice system, Wolverine)

Differences also extend to what types of activities are flagged and which ones are not. Part of this is due to the historic inconsistency in DOD definitions of prohibited extremist activities, as documented in earlier sections of this paper. The December 2021 update to DODI 1325.06 should provide some clarification. However, further clarity will likely be needed on some points.

For instance, some organizations are flagging the use of racist, sexist, anti-Semitic, or other discriminatory language in the workplace as prohibited extremist activity. While certainly inappropriate, such language, by itself may not reach the threshold for prohibited extremist activities under either the new or old version of DODI 1325.06. If flagging systems fail to

[366] The DASH system is administered within the Opportunity, Diversity, and Inclusion Branch (MPE) of the Office of the Deputy Commandant of the Marine Corps for Manpower and Reserve Affairs.

accurately reflect the definitions of prohibited extremist activities in DODI 1325.06, reporting has the potential to misrepresent the magnitude and severity of such activities in the DOD.

Identifying the full range of information required for Section 554(b) can necessitate pulling information from both a Military Department's criminal investigative organization and military justice organization. Although these organizations routinely work together, their systems are not necessarily aligned to pass information from one system to another. This can require information to be independently entered into each system, including information related to prohibited extremist activities.

The Army policy on "Extremist organizations and activities" was significantly updated and expanded in July 2020 to provide improved guidance and add a new reporting requirement. The new regulation provides that "Commanders will notify the supporting counterintelligence organization in cases where they know or suspect that Soldiers are engaging in the activities" defined within the policy (p. 32).[367] The effect of this Army policy is that all prohibited extremist activities, whether criminal or non-criminal, must be reported to the Army CID. Although non-criminal cases may be referred back to commanders,[368] CID is designated as the centralized location for tracking all cases. In the absence of this requirement, a non-criminal case might not be reported outside of the local command and could not be incorporated into the Department's tracking systems.

In addition, the Army recently implemented a data feed between its criminal investigative system, the Army Law Enforcement Reporting and Tracking System (ALERTS), and its military justice system (Military Justice Online (MJO)). Although not all information passes (or needs to pass) between systems, the connection enables visibility within MJO into such things as commanders' actions taken in response to cases in ALERTS.[369] To the extent that systems are able to connect across organizations, this can facilitate better end-to-end tracking of individual cases.[370]

The Marine Corps uses its Equal Opportunity system, DASH, as a central repository for tracking harassment, bullying, discrimination, and hazing. Since 2018, DASH also tracks

---

[367] Department of the Army, "Army Command Policy," Army Regulation 600-20 (Washington, DC: Department of the Army, November 2014), 32, http://milreg.com/File.aspx?id=321#:~:text=This%20regulation%20prescribes%20the%20policies,Program%20(formerly%20the%20Army%20Sexual.

[368] Criminal investigative organizations are quick to note that there must be a criminal component to a case for them to remain involved. A criminal investigative organization can conduct an initial investigation if there is a suspected criminal component (under, for instance, Force Protection or Counter Terrorism authority if there is a belief that a crime has been or may soon be committed). However, if no criminal conduct is found, the case is referred back to the command.

[369] Such as through DA Form 4833, "Commander's Report of Disciplinary or Administrative Action."

[370] One Military Department reported that the process of identifying cases of prohibited extremist activity for the 2021 Section 554(b) data call involved pulling cases from both the criminal investigative organization and the military justice organization. Some cases were more easily identified as relevant cases in one system or the other, and it took a combined look at both systems to pull together a complete set of relevant cases.

"dissident and protest activities," which includes prohibited extremist activities. Once a report of a dissident or protest activity is made, it is logged in DASH and tracked from cradle to grave. This includes noting whether an allegation has been substantiated or not, and any subsequent actions. If the case goes to court-martial or counseling, it is noted. Other actions are likewise tracked in DASH, such as if a case is appealed or if the person is administratively separated. DASH is administered as a tracking system: it is a place to document commanders' actions, together with any legal and court actions. DASH is also integrated with the Marine Corps' personnel system. A key benefit of maintaining DASH outside of the law enforcement sphere is that it can capture both criminal and non-criminal cases and track each throughout the entirety of the case. Law enforcement organizations can investigate suspected crimes, but their authorities are limited when there is not a criminal component to a case.

Table 10 provides a summary of several DOD Criminal Investigative, Military Justice, and Equal Opportunity Systems as they pertain to tracking prohibited extremist activities. Six of the seven systems listed have incorporated some kind of flag for tracking cases involving prohibited extremist activities. Three of the systems (including the one that does not have a flag) are scheduled to be replaced in the near future.[371] This is significant because these systems are either dated or limited in their overall capabilities—such as in the types of data they can track, the ease of updating or changing features of the system, or their ability to connect with other systems.

Table 10. Summary of DOD Criminal Investigative, Military Justice, and Equal Opportunity Systems

Organization	System	Overview
Marine Corps Opportunity, Diversity, and Inclusion Branch	DASH	• Tracks all violations of MCO 5354.1F: Marine Corps Prohibited Activities and Conduct (PAC) Prevention and Response Policy, which includes instances of harassment, extremist activity, hazing, bullying, and sexual assault • Multiple flags for different PAC violations. Commanders make final decision about checking one or more flags • 2018: Added flag to track "Dissident and protest activities"
Army Criminal Investigative Division	ALERTS	• Tracks all criminal cases and non-criminal Serious Incident Reports • 2019: Added flag for tracking cases involving extremism • July 2020: Implemented a new policy requiring commanders to report suspected extremist activity, either criminal or non-criminal, to Army CID

[371] For example, information about the new system for the Air Force Office of Special Investigation is available from Brading, Thomas, "OSI Modernizing Case Management Platform," *OSI Public Affairs*, February 25, 2022, https://www.osi.af.mil/News/Article-Display/Article/2947008/osi-modernizing-case-management-platform/.

Army Judge Advocate General (JAG)	MJO	• Tracks all incidents that result in formal action (e.g., letters of reprimand, Articles15, courts-martial), but not cases resulting in informal actions, such as counseling • Late 2019: Added a yes/no checkbox to track cases involving extremism • 2021: Began receiving direct data feeds form ALERTS
Naval Criminal Investigative Services	CLEOC	• Tracks a variety of law enforcement related cases • April 2019: Added flag in April 2019 to track cases involving extremism
Navy & Marine Corps JAG	Wolverine (replacing with NCORS in 2022)	• March 2021: Added mandatory yes/no field to mark if "Case involves an allegation of supremacist, extremist, or criminal gang activity." Users are trained to revisit this field as new information arises • 2022: Replacement system, NCORS, will have similar field
Air Force JAG	AMJAMS (replacing with DCMS in 2022)	• Tracks all Air Force military justice cases • 2021: Added special identifier to track cases involving "Extremism and Hate Groups"
Air Force Office of Special Investigations	I2MS (replacing with ORION in 2022)	• Tracks variety of Air Force law enforcement related cases • Legacy system with no flag for tracking cases involving extremism; anticipates capability in new system ORION

Full names of systems are as follows: AMJAMS – Automated Military Justice Analysis and Management System; CLEOC – Consolidated Law Enforcement Operations Center; DCMS – Disciplinary Case Management System; I2MS – Investigative Incident Management System; JAG – Judge Advocate General MJO – Military Justice Online; NCORS – Naval Court-Martial Reporting System; ORION – OSI Records, Investigation, and Operations Network.

Even with the capability to flag cases involving prohibited extremist activities, the process of flagging cases can still be prone to error. Users can forget to flag cases or may flag cases incorrectly. Most systems allow users to update a flag as new information about a case is identified. This allows a case to be flagged later in an investigation if a prohibited extremist activity is not clear or apparent when a case is opened. Likewise, if a case is mistakenly flagged and is determined not to involve prohibited extremist activity, most systems allow the user to remove the flag. System users are typically trained on how to enter information, and systems sometimes include user instructions. For example, the Department of the Navy's military justice system (Wolverine) includes the following instructions: "Personnel shall answer 'Yes' if the investigation or prosecution of the case ever involved an allegation of supremacist, extremist, or criminal gang activity, as defined in DOD 1325.06. Otherwise, personnel shall answer 'No.'" Wolverine likewise requires users to affirmatively answer "Yes" or "No." It is a required field.

Since the reliability of these flags is based on the reliability of the data entry process, steps that make it easy to remember to flag cases are beneficial. Such steps could require a "Yes" or "No" answer like in Wolverine. If an investigation goes on for a period of time (or reaches a

significant milestone), a subsequent system prompt requiring the user to provide another affirmative response based on the updated information about the case might be helpful.

At present, keyword searches are still used in a few systems to identify relevant cases.[372] That practice could continue as a quality control check (at least in the near term) to help ensure that the proper set of cases is being flagged.[373] However, system prompts and proper training on when to flag cases could decrease user error and help improve the data entry process.

3. Findings and Recommendations

Formal tracking of prohibited extremist activities within DOD systems has improved in recent years. Beginning in 2018, various criminal investigative, military justice, and equal opportunity systems incorporated explicit mechanisms (such as checkboxes or radio buttons) for flagging cases involving prohibited extremist activities. Without such flags, the process of identifying cases involving prohibited extremist activities relies on keyword queries and ad hoc searches. These searches can be time intensive and costly.

Explicitly flagging cases has improved tracking considerably. However, there remains a lack of standardization. The determination to flag a case as involving prohibited extremist behavior is subjective, and the lack of clear definitional guidance leads to inconsistencies in the types of activities that are being tracked within and across organizations. The lack of a clear DOD definition of prohibited extremist activities—especially prior to the 20 December 2021 update to DODI 1325.06—has contributed to these variations. Even with the update, ambiguities persist and further guidance is needed to standardize practices for identifying cases of prohibited extremist activities.

Section 554(b) requires standard mechanisms for tracking supremacist, extremist, and criminal gang activity across the Armed Forces. The Office for the USD(P&R) is in the process of coordinating a new policy with the relevant DOD stakeholders to improve standardization. However, even once a new policy is in place, it will likely be a major effort to implement it. It may be a year or more before the Section 554(b) reporting requirements can be met with a higher level of standardization.

Our recommendations are geared toward enhancing the reliability and consistency of data tracking processes to enable greater standardization for meeting the Section 554(b) reporting requirements across organizations and over time.

---

[372] Search terms may include such things as “extremis*,” “racis*,” “organization,” names of known extremism groups, or various other relevant terms.

[373] Reviewing the cases identified by a keyword search is still a manual process. If used as a quality control check, it may be appropriate only to review a sample of the cases identified by a keyword search. If cases are stored in different parts of a system, the search would need to include each relevant portion of the system.

Recommendation 13: Continue the improvement of mechanisms for tracking cases of prohibited extremist activities in relevant DOD systems to ensure they are adequate to meet section 554(b), FY2021 (National Defense Authorization Act) NDAA, reporting requirements.

DOD has already made significant strides in establishing mechanisms for tracking cases of prohibited extremist activities. The DOD OIG's report to Congress on 1 December 2021 (DODIG-2022-042) would have been considerably harder to put together just a few years earlier absent investments that had already been made in capabilities and processes for tracking prohibited extremist activities. However, there remain several improvements that could be made to ensure the adequacy of these tracking mechanisms, including the following implementation options:

- System owners should consider making the flag for marking whether a case involves prohibited activities (as defined in DODI 1325.06) a mandatory field that must be filled out during the process of entering a case. Some systems already take this approach (e.g., the Navy and Marine Corps JAG system, Wolverine, which has a yes/no field that must be marked one way or the other). If the field is not mandatory (e.g., the system has only a yes field or a yes/no field, but does not require an affirmative "yes" or "no" response), system owners should consider implementing other changes to help ensure that the field is marked, such as having automatic alerts that remind the user to mark it or preclude progress through the data entry process until the field is marked.
- System owners could ensure that the flag can be marked and revisited throughout the life-cycle of a case. Most systems with flags allow users to mark a flag as information is discovered during an investigation. As cases reach major milestones or prepare to close, system owners could direct users to ensure that the case has been appropriately marked. This could be done through training or through automatic alerts within the system.
- System owners of organizations that routinely work together (e.g., a service's criminal investigative organization and military justice organization) could identify workflows so that information about DODI 1325.06 violations is appropriately shared once both organizations are involved in a case. For instance, if a criminal investigative organization flags a case as a DODI 1325.06 violation in its system, that information should be transferred to the military justice system, ideally in an automated manner.
- Each military department secretary could issue a policy requiring that all allegations of prohibited activities be reported to a single organization. For example, the Army adopted a policy that commanders must report all suspected extremist activity, either criminal or non-criminal, to Army CID. Consolidating reports of allegations in a single organization per service, where possible, has the potential to improve tracking. Criminal investigative organizations typically focus on criminal activity and need specific direction to cover non-criminal cases that violate DOD policies, such as DODI 1325.06.

Recommendation 14: Ensure that the military departments use consistent definitions and criteria for flagging cases of prohibited extremist activities.

IDA understands that this recommendation will be partially implemented by the USD(P&R) draft policy memorandum to the secretaries of the military departments, USD(I&S), and the DOD IG that is currently in coordination. The memorandum is expected to require the military department secretaries to submit draft policies describing how they will meet the requirements of Section 554(b) of the FY21 NDAA, to OUSD(P&R) for review.

To more fully meet this recommendation, the OUSD(P&R) review will need to ensure consistency across the service's policies in their definitions and criteria for flagging cases of prohibited extremist activities. To this end, the Department should consider the following options:

- Even if each service's policy has consistent definition and criteria for flagging cases of prohibited extremist activities, there may be inconsistencies in how those definitions and criteria are implemented in practice. To support consistency in implementation, the USD(P&R) could issue guidance requiring that the service policies include a short set of standardized questions that could be used in the data entry process to assess whether a given incident is a prohibited extremist activity.
  - The questions would focus on the definition of prohibited extremist activities in DODI 1325.06 (December 2021). The standardized accession screening questionnaire issued by OUSD(P&R) in December 2021 could be used as a model, but the questions would need to be tailored to classifying incidents (rather than assessing whether an individual ever previously engaged in one of these behaviors).
  - To be effective, the set of questions would have to be short and not overburden the system. However, it would be appropriate for systems to impose a standardized set of follow-up questions in the event that the incident is classified as a prohibited extremist activity. Any standardized follow-up questions would seek to flag information that may be desired for reporting and querying.
  - Given that the types of organizations tracking incidents vary in their scope and authority (e.g., equal opportunity, criminal investigation, military justice), some questions might need to be tailored to the type of organization. However, there would be uniformity across organizations to the extent possible.
  - The set of questions could consist of something like the following:
    - Is the accused associated with a known criminal gang?
    - Did the accused engage in or support terrorism?
    - Did the accused seek to overthrow the government of the United States (or any subdivision thereof), commit any act of sedition, or encourage anybody else to do the same?
    - Did the accused advocate widespread unlawful discrimination on the basis of race, color, national origin, religion, sex, gender identity, or sexual orientation?

- Are the accused's actions associated with any known extremist group? (If yes, answer the questions below)

  Did the accused attend meetings, activities, rallies, and/or demonstrations with the intent to support an extremist group or activity?

  Did the accused display or distribute literature, paraphernalia, or symbols that support extremist activities, either in person or online?

  Did the accused advocate for or engage in unlawful force or violence in support of extremist activities?

  Did the accused knowingly take any other action in support of, or engage in, extremist activities?

Recommendation 15: Ensure flagging capabilities can differentiate between substantiated cases and non-substantiated allegations. For substantiated cases, consider common coding criteria for indicating the severity or nature of the misconduct.

To implement this recommendation, the Department should consider the following options:

- The USD(P&R) could issue guidance to those conducting reviews of the draft service policies, directing that each DOD system for flagging cases of prohibited extremist behaviors and activities contain a separate field or fields reflecting the status of investigative and prosecutorial activities. The Under Secretary could establish consistent categories for reporting status that, at a minimum, differentiate between substantiated and unsubstantiated allegations.
- The Under Secretary could include, in standardized questions used for flagging such cases, standardized questions to identify the status of a case in accordance with the guidance. Such questions could also be used to enable consistent coding to indicate the severity and nature of the misconduct.

Recommendation 16: Implement quality control checks (automated to the extent possible) for ensuring that cases are being flagged appropriately.

To implement this recommendation, the Department should consider the following options:

- The USD(P&R) could issue guidance directing that:
  - Owners of the various systems should establish procedures for checking for false positives and false negatives.
    - False Positives: If the number of incidents flagged is sufficiently small, this may entail an independent check of the flagged cases to ensure that they have been flagged correctly. If there is a higher number of incidents, a sample of the cases may be checked. The process of checking for false positives should include a recording procedure for tracking which cases were checked and any false positives identified.

- False Negatives: Checking for false negatives may entail conducting system-wide searches for keywords related to prohibited extremist activities to look for cases that were accidentally not flagged. This process should be automated to the extent possible (e.g., maintaining a Structured Query Language (SQL) query that can run periodically).

– System owners should submit information on their procedures for checking for false positives and false negatives to the DOD IG, together with information on the number of false positives and false negatives identified. This process should be automated to the extent possible (e.g., standardized output that can be generated each time a SQL query is run checking for false negatives, and standardized outputs from false positive checks).

– System owners would not necessarily have to coordinate to determine a single model of implementation, but they could be encouraged to do so.

B. Non-Government Systems for Tracking Extremism

In addition to the various databases hosted and maintained by the military or federal government for tracking prohibited extremist behaviors, several nongovernmental organizations either investigate terrorism and extremism directly or host databases where information about extremists can be found and investigated. We discuss several of these databases and summarize potential connections to tracking prohibited extremist behaviors among those with military affiliations. IDA utilized information from these databases for the purpose of this study; information collected in the databases will be vital to future studies and to the Department's efforts to monitor and understand prohibited extremist activities in its ranks.

1. Databases Maintained by the National Consortium for the Study of Terrorism and Reponses to Terrorism (START)

The National Consortium for the Study of Terrorism and Reponses to Terrorism, a DHS consortium of more than 50 institutions headquartered at the University of Maryland, maintains several databases relevant to the study of violent extremist activities.

a. Profiles of Individual Radicalization in the United States (PIRUS)

The PIRUS database includes information on 2,226 de-identified individuals who were radicalized "to the point of violent or nonviolent ideologically motivated criminal activity, or ideologically motivated association with a foreign or domestic extremist organization" in the United States from 1948 to 2018.[374] The data consist of 112 variables describing the subject's

[374] START also maintains and curates more recent data, but the publicly released database is only updated through 2018. (Gary LaFree, Michael Jensen, Sheehan Kane, et al., *Profiles on Radicalization in the United States*

demographics, details, and outcomes of their planned attacks (if any), and information regarding the method of radicalization. In 2021, START began to add information documenting the military background of subjects in the database, including active duty, veteran, and deployment status; separation information; diagnoses of post-traumatic stress disorder, if any; and more. The database is available for free download for academic research and non-commercial purposes.

All PIRUS data is from open sources, so there is a risk that the data disproportionately capture individuals associated with extremist ideologies that are the focus of current media attention. In addition, individuals currently serving in the Armed Forces are likely to be identified only if their military links are reported in the press or in publicly-available information from the military justice system.[375] The database includes substantially more information on recent cases than on cases from earlier years (especially before the 1990s), for which fewer documents are available. The START website explains:

> Achieving a comprehensive dataset of all individuals who meet the database's inclusion criteria remains implausible for several reasons. Such a hypothetical database would encompass an unwieldy population of interest, face an extreme shortage of similar, reliable sources of data from which to draw upon, and would require a massive investment in resources.[376]

b. Global Terrorism Database (GTD)

The Global Terrorism Database (GTD) contains information about terrorist attacks across the world since 1970.[377] A substantial update in 1997 added many new variables, and more recent entries (since 2012) contain information for approximately 120 variables. Incidents are marked with personal information on up to three perpetrators, including their group affiliation, if any, as well as intended targets. Since 2012, researchers have used automation to find and review sources, which has increased the number of identifiable incidents, but renders any comparison of the number of incidents between pre- and post-2012 statistically invalid.[378]

The GTD uses the following definition of a terrorist attack: "The threatened or actual use of illegal force and violence by a non-state actor to attain a political, economic, religious, or social

---

(PIRUS) (College Park, MD: National Consortium for the Study of Terrorism and Responses to Terrorism (START), 2018), https://www.start.umd.edu/data-tools/profiles-individual-radicalization-united-states-pirus.

[375] Ibid.

[376] Ibid.

[377] Gary LaFree and Laura Dugan, "Introducing the Global Terrorism Database," *Terrorism and Political Violence* 19 (April 4, 2007): 181-204, http://ccjs.umd.edu/sites/ccjs.umd.edu/files/pubs/FTPV_A_224594.pdf.

[378] Michael Jensen, *Discussion Point: The Benefits and Drawbacks of Methodological Advancements in Data Collection and Coding: Insights from the Global Terrorism Database (GTD)* (College Park, MD: National Consortium for the Study of Terrorism and Responses to Terrorism (START), 2013, https://www.start.umd.edu/publication/discussion-point-benefits-and-drawbacks-methodological-advancements-data-collection-and.

goal through fear, coercion, or intimidation."[379] Any included act must be intentional, involve violence or a threat of violence, and be committed by sub-national actors. Additionally, the acts must meet at least two of the following criteria:

- The act is aimed at attaining a political, economic, religious, or social goal.
- There is evidence of an intention to coerce, intimidate, or convey some other message to a larger audience (or audiences) than the immediate victims.
- The action takes place outside the context of legitimate warfare activities. [380]

The GTD data can be filtered according to these different inclusion criteria.

c. Profiles of Perpetrators of Terrorism in the United States (PPT-US)

The Profiles of Perpetrators of Terrorism in the United States (PPT-US) database contains information on organizations, rather than individuals, involved in terrorist activities from 1970 to 2016. According to the database description, "data included for each organization includes information on its terrorist attacks, its history and base of operations, its ideology and goals, its engagement in political and criminal activities (other than terrorism), its alliances, its network and structure, and its financial resources," as well as information about the reliability of sources used.[381]

d. The Terrorism and Extremist Violence in the United States (TEVUS) Database

The Terrorism and Extremist Violence in the United States (TEVUS) Database integrates four open-source data sets to facilitate more robust and sophisticated analyses of the behaviors, operations, and activities of violent extremists within the United States from 1970 to 2015. Of the four databases, two of them (PPT-US and GTD) are START-owned and available for download. The other two are owned by other organizations: the American Terrorism Study (ATS) by the Terrorism Research Center at the University of Arkansas, and the U.S. Extremist Crime Database (ECDB) by researchers at John Jay College of Criminal Justice, Michigan State University, Seattle University, and Indiana University.

- The ATS reports on FBI "domestic security/terrorism investigations" with information about perpetrators and events from 1980 to 2002.[382]

---

[379] National Consortium for the Study of Terrorism and Responses to Terrorism (START), *Global Terrorism Database Codebook: Methodology, Inclusion Criteria, and Variables* (College Park, MD: National Consortium for the Study of Terrorism and Responses to Terrorism (START), August 2021).

[380] Ibid, 12.

[381] Erin Miller and Kathleen Smarick, *Profiles of Perpetrators of Terrorism in the United States* (College Park, MD: START, July 2014), https://www.start.umd.edu/pubs/START_ProfilesofPerpetratorsofTerrorismintheUS_ResearchHighlight_July2014.pdf.

[382] Brent L. Smith, and Kelly R. Damphousse, "American Terrorism Study, 1980-2002," (n.p.: Inter-University Consortium for Political and Social Research, July 30, 2007), https://doi.org/10.3886/ICPSR04639.v1.

- The ECDB includes individuals who committed a violent or financial crime from 1990 to 2018, with at least one perpetrator of the crime "subscrib[ing] to an extremist belief system." These belief systems are limited to the far-right, Al-Qaeda or a group inspired by Al-Qaeda, or extreme commitments to animal/environmental rights.[383]

ATS and ECDB are not available for download. The full TEVUS dataset feeds into an interactive online portal to better aid analyst analysis. The portal includes information on "over 3440 terrorist incidents, 2530 pre-incident activities, and 260 extremist crimes in the United States and identifies relationships between these events and individuals (3559), groups (422), and court cases (451)."[384] There are also multiple reports that have been written based on TEVUS data, although none are currently focused on the connection between military service and extremist violence.

2. Other Non-Government Database

a. The Armed Conflict Location & Event Data Project (ACLED)

The Armed Conflict Location & Event Data Project (ACLED) is a non-profit organization that tracks politically important events, including political violence, protests, and some nonviolent expression, in close to real-time.[385] The database is available for download by anyone who creates a profile on the site. The full ACLED database is global, but there is also a specific collection effort for information about the United States. The collection process started as a pilot project in 2019, then was continued in 2020 as part of the *US Crisis Monitor* initiative with Princeton University. Data is now added by ACLED's research team alone, using more than 2800 verified sources, in partnerships with other groups such as MilitaWatch, Live Universal Awareness Map, and The Network Contagion Research Institute.[386]

The data in ACLED is made up of events with details about up to two types of perpetrators and their group affiliation. Events are also marked with the time they occurred and location, as well as a narrative description of the specific details. Events are one of six types: battles, explosions/remote violence, violence against civilians, protests, riots, or nonviolent strategic

---

[383] Joshua Freilich, Stephen Chermak, Roberta Belli, Jeff Gruenewald, and William Parkin, "Introducing the United States Extremist Crime Database (ECDB)," *Terrorism and Political Violence* 26 (November 20, 2013): 372-384, http://www.tandfon-line.com/doi/full/10.1080/09546553.2012.713229?mobileUi=0.

[384] "Terrorism and Extremist Violence in the United States Database (TEVUS)," National Consortium for the Study of Terrorism and Responses to Terrorism Website, accessed June 16, 2022, https://www.start.umd.edu/research-projects/terrorism-and-extremist-violence-united-states-tevus-database.

[385] Clionadh Raleigh, Andrew Linke, Håvard Hegre, and Joakim Karlsen, "Introducing ACLED: An Armed Conflict Location and Event Dataset: Special Data Feature," *Journal of Peace Research* 47, no. 5 (September 28, 2010): 651–660, doi: 10.1177/0022343310378914.

[386] "FAQs: ACLED US Coverage," Armed Conflict Location & Even Data Project Website, accessed June 16, 2022, https://acleddata.com/acleddatanew/wp-content/uploads/2021/12/ACLED_US-Coverage-FAQs_v4_December-2021.pdf.

developments. These events are then broken into sub-event categories, which are defined in detail in a codebook.[387] No personally identifiable information is included, which means that even in a "lone wolf" situation, the actor is marked as "Sole Perpetrator ([Nationality])" instead of by name. The main advantage of ACLED over other databases discussed here is the nearly real-time updates.

b. The Anti-Defamation League's (ADL) Hate, Extremism, Anti-Semitism, and Terrorism (H.E.A.T.) Map

Like the data from ACLED, the Anti-Defamation League's (ADL) Hate, Extremism, Anti-Semitism, and Terrorism (H.E.A.T.) map focuses on events instead of perpetrators. The database contains information on the date, location, ideology, and type of H.E.A.T. event, with a narrative description of the details. Sometimes this written description contains information about the name of the perpetrator or perpetrators, together with other details important to the story. The events can be anti-Semitic incidents, extremist murders, terrorist plots and attacks, extremist/police shootouts, white supremacist events, or white supremacist propaganda. The database allows for the identification of locational trends over time.[388]

c. Center for Strategic and International Studies (CSIS) Terrorism Investigation

In April 2021, the CSIS TNT published a brief regarding terrorism in the United States.[389] Data consisted of 980 terrorist incidents in the United States that spanned the period between January 1994 and 31 January 2021. The researchers used data from a number of publicly available databases and news sources, including:

- The ACLED (2020–2021);
- The ADL H.E.A.T. map (2002–2021);
- Jane's Terrorism and Insurgency Events (2009–2021);
- START GTD (1994–2017); and
- Press releases and reports from the FBI and DOJ. [390]

---

[387] "Armed Conflict Location & Event Data Project (ACLED) Codebook," Armed Conflict Location & Event Data Project Website, accessed June 16, 2022, 8-18, https://acleddata.com/acleddatanew/wp-content/uploads/2021/11/ACLED_Codebook_v1_January-2021.pdf.

[388] "ADL H.E.A.T. Map (Hate, Extremism, Antisemitism, Terrorism)," Anti-Defamation League Website, accessed June 16, 2022, https://www.adl.org/resources/tools-to-track-hate/heat-map.

[389] Jones, Doxsee, Hwang, Thompson, *The Military, Police, and the Rise of Terrorism in the United States*.

[390] Seth Jones, Catrina Doxsee, Grace Hwang, and Jared Thompson, *Methodology and Codebook. The Military, Police, and the Rise of Terrorism in the United States* (Washington, DC: Center for Strategic & International Studies (CSIS), April 12, 2021), https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/210412_Jones_Methodology.pdf?mG2pmLJmpc4OAKQdPDm8n.9cWaDW8Pj4.

3. Social Media Databases

Several databases developed by non-government entities could be useful to identify and track extremist threats.

a. University of North Carolina at Charlotte's (UNC-C) Gab Data Leak Database

Gab is a largely text-based social media network that brands itself as the "free speech social network." Because of its near-total lack of moderation, it is a haven for ultra-conservative and alt-right-wing discourse. Some right-leaning Americans view Facebook and Twitter as unfairly censoring their views, and many had joined Parler, another "free speech social network," which allowed for extreme ideas to be posted without removal. However, Parler was deplatformed following the U.S. Capitol events of 6 January 2021, removing it from app stores and Amazon Web Services. This change led to a significant increase in traffic on Gab.[391]

In 2019, researchers from the University of North Carolina at Charlotte (UNC-C) released a database of "37,012,061 posts (with additional edit histories), 24,551,804 comments, and 819,957 user profiles web-scraped from Gab between August 2016 and December 2018."[392] Unlike some other scraped data from Gab, the UNC-C dataset is also indexed with information about friend groups, edits on posts, and comments. UNC-C researchers state that the dataset represents all publicly available data on the website at the time. The dataset is publicly available for download with no restrictions on use. This data could be used to investigate extreme language as it is used on a site without censorship, which could be used to inform DOD social media policies around extremism.

b. Pushshift

Pushshift is a data collection platform with code available on Github, which collects data from both Reddit and Telegram.

- Pushshift ingests data from Reddit posts and comments on a monthly basis and maintains an Application Programming Interface (API) for easy searching of the data. The data is publicly available for download; each month is split into two zipped files, one with data from comments and the other with data from original posts. Extensive

[391] Jazmin Goodwin, "Gab: Everything you Need to Know about the Fast-Growing, Controversial Social Network," *CNN*, January 17, 2021, https://www.cnn.com/2021/01/17/tech/what-is-gab-explainer/index.html; Jack Nicas and Davey Alba, "How Parler, a Chosen App of Trump Fans, Became a Test of Free Speech," *The New York Times*, updated February 15, 2021, https://www.nytimes.com/2021/01/10/technology/parler-app-trump-free-speech.html.

[392] Gabriel Fair and Ryan Wesslen, "Data for Shouting into the Void: A Database of the Alternative Social Media Platform Gab," paper presented at the Proceedings of the Thirteenth International AAAI Conference on Web and Social Media, Munich, Germany, June 11-14, 2019, https://ojs.aaai.org/index.php/ICWSM/article/view/3258/3126.

documentation is available on Github,[393] the Pushshift website,[394] and a published paper describing the dataset and API.[395] The API hosts two endpoints, one for searching submissions and the other for searching comments. Because older data is archived, the API can be used to search subreddits that have since been banned. This feature is particularly relevant as Reddit banned approximately 2,000 subreddits in June of 2020 for violating their guidelines regarding hate speech.[396]

  - API users can filter their searches to specific keywords and phrases, using the 'subreddit' parameter to confine their searches to specific subreddits. In this manner, military-themed subreddits[397] such as r/military, r/army, r/navy, and r/MilitaryMemes could be searched for extremist keywords, while known political and extremist subreddits could be searched for any evidence of military affiliation.

- Telegram is a messaging service that features public channels where users can interact and share information on various topics. Pushshift has compiled a dataset of Telegram messages from publicly available right-wing and cryptocurrency channels and makes them available for download at no cost to the user.[398] However, unlike in the case of Reddit, Pushshift does not maintain an API that can be used to search the existing data. Any analysis would require direct manipulation of the 51.9GB (gigabyte) file.

C. Social Media Screening

1. Legal and Technical Issues

Discussions with DOD personnel during interviews and site visits for this study revealed significant discomfort with the idea that the Department would monitor the social media postings

[393] "Pushshift Reddit API Documentation," Github Website, accessed June 16, 2022, https://github.com/pushshift/api.

[394] "Full List of Pushshift Reddit Specific Parameters," Pushshift.io Website, accessed June 16, 2022, https://pushshift.io/api-parameters/.

[395] Jason Baumgartner, Savvas Zannettou, Brian Keegan, Megan Squire, Jeremy Blackburn, "The Pushshift Reddit Dataset" (paper presented at Proceedings of the Thirteenth International AAAI Conference on Web and Social Media, Munich, Germany, June 11-14, 2019, Munich, Germany), 830–839, https://ojs.aaai.org/index.php/ICWSM/article/view/7347/7201.

[396] Bobby Allyn, "Reddit Bans The_Donald, Forum Of Nearly 800,000 Trump Fans, Over Abusive Posts," *NPR*, June 29, 2020, https://www.npr.org/2020/06/29/884819923/reddit-bans-the_donald-forum-of-nearly-800-000-trump-fans-over-abusive-posts.

[397] For a more comprehensive list, see https://www.reddit.com/r/Military/comments/js9132/lets_make_a_directory_of_all_the_military/ (last accessed April 29, 2022).

[398] Jason Baumgartner, Savvas Zannettou, Megan Squire, and Jeremy Blackburn, "The Pushshift Telegram Dataset," (paper presented in Proceedings of the Thirteenth International AAAI Conference on Web and Social Media, Munich, Germany, June 11-14, 2019, 840–847, https://ojs.aaai.org/index.php/ICWSM/article/view/7348/7202; Jason Baumgartner, Savvas Zannettou, Megan Squire, and Jeremy Blackburn, "The Pushshift Telegram Dataset," Database.

of service members or employees on an ongoing basis. Some expressed confusion as to what types of online behavior would be considered inappropriate—with one individual asking whether posting pro-gun or pro-Second Amendment material online would be a prohibited extremist activity. In general, service members did not have a good idea of the extent to which their media profiles are or are not being tracked and monitored but understood that anything posted online may not remain private and can have negative repercussions.

The question of how to incorporate social media and other online internet content into initial and continuing personnel screening processes is one with which DOD and the larger federal government have wrestled with for some time. In the past, when an adverse incident garnered significant public attention and there existed readily accessible online information demonstrating that the alleged offender had exhibited signs of potentially risky behaviors, DOD has been forced to explain why it was not aware of the information (or did not act on information of which it was aware). On the other hand, DOD is bound by Fourth Amendment proscriptions against unreasonable search and seizure, as well as by-laws, such as the Privacy Act of 1974 (5 U.S.C. 552a), that constrain DOD's ability to access personal information about service members and others. DOD's surveillance capacity is limited by design in accordance with the Constitutional objective of protecting citizens from intrusive observation by their government.

Standards for employment in government positions, together with requirements for accessing sensitive facilities, information, or networks, provide DOD with broader authority to "intrude" into the personal lives of service members and employees, however, people must make a deliberate choice to pursue employment with DOD. Most arrive at an understanding that any offer of employment is conditioned on an applicant's consent to the Department's access to certain details about the applicant's private life and activities. However, DOD's legal authority to investigate and monitor its personnel must be balanced by an ethical commitment to the responsible use of that authority.

If DOD surveillance of its own personnel reaches an overly uncomfortable level, DOD risks losing critical talent. Over-surveillance can erode trust, suppress diversity of thought and background, create disunity, and lead individuals to distance themselves from the organization. Conversely, under-surveillance risks security breaches, attacks, and vulnerability to a variety of other threats. Thus, balance is needed. DOD needs sufficient latitude to protect itself and the Nation against insider threats and individuals who exhibit risky behaviors. At the same time, DOD needs to exemplify the core American values it is bound to protect. To achieve an appropriate balance, the Department must continue to exercise judicious restraint on the surveillance authority that it does have.

In addition to striking an appropriate legal and ethical balance, monitoring online information for any sizeable fraction of the DOD workforce would require a high level of technical ingenuity. Monitoring online information at any scale requires a large degree of automation across multiple

tasks.[399] This includes automating processes for searching for information about designated individuals, verifying that the information is indeed about the individual in question, ascertaining that a piece of information can be collected lawfully, and determining whether a piece of information demonstrates that the individual may pose an unacceptable risk. These tasks are further complicated by the broad range of formats for online information (e.g., text, pictures, video), platform specific information formats (e.g., likes, friends, posts, tweets), and the sheer number and breadth of online sites. Content can also be difficult to assess in an automated fashion due to the complexity of cultural nuances that can be combined in a single short post such as in a meme.

Even if all of these tasks were automated to a high level of accuracy, there remains the question of how easily computer search algorithms could be fooled by malicious actors who seek not only to avoid detection, but sometimes even to impersonate or defame single individuals or groups of individuals. Appropriate screening procedures thus need to adjudicate not only whether the information refers to the individual in question, but whether the information faithfully represents the individual in question.[400]

Within DOD, there are different use cases for monitoring on-line information.

Personnel security background investigations and continuous evaluation are vetting processes for determining whether individuals can be trusted with sensitive government information. Individuals under investigation must provide information about various aspects of their lives; the investigation supplements this information with third-party documents and interviews with co-workers, neighbors, and others. In addition, individuals subject to a background investigation must authorize government investigators to access other types of information, including online information, or forfeit the opportunity to hold a security clearance and, in some cases, a position of employment with DOD. Because these investigations already exist and provide authority to access online data, they provide a natural forum in which to incorporate social media screening. DOD is moving in that direction but must address both technical issues and questions about reasonable levels of intrusiveness before determining how far to go and how to get there.

---

[399] In recent years, DOD has significantly improved its security background investigation process to reduce a significant backlog that had developed and shorten the average time to completion of a investigation. After making these process improvements, there is some hesitation among senior leaders about adding steps that would significantly lengthen investigation times. In addition to the scale of the defense workforce and the breath of potential online information that may need to be evaluated, a large degree of automation is also needed to incorporate this vetting within an already lengthy and costly investigation process.

[400] In one example, a fraudulent individual created a fake Facebook profile for a California high school teacher. The fraudulent individual then began to harass several of the teachers' students through the fake Facebook profile. Only when a complaint was filed against the teacher did the teacher become aware of the fake profile. See Andrée Rose, Howard Timm, Corrie Pogson, et al., *Developing a Cybervetting Strategy for Law Enforcement* (International Association of Chiefs of Police and PERSEREC, December 2010), 17, https://www.theiacp.org/sites/default/files/2018-08/CybervettingReport-2.pdf.

Senior officials interviewed by the IDA team indicated that the Department has similar authority to access online information in connection with insider threat assessments. This authority extends beyond individuals who hold or are applying for a security clearance and applies to all individuals who have access to government facilities or information systems.

Access is achieved in part through User Activity Monitoring of government information systems. In the process of logging on to a DOD computer or restricted-access DOD information system, the user consents to monitoring. The consent banner informs users that "communications using, or data stored on, this [Information System] are not private, are subject to routine monitoring, interception, and search, and may be disclosed for any [U.S. Government] authorized purpose," and that the government may "at any time … inspect and seize data stored" on the information system. User Activity Monitoring is geared toward information security and insider threat concerns and monitoring prioritizes information systems containing more sensitive data. At present, User Activity Monitoring may be initiated as a result of the user typing a trigger word or engaging in behavioral activities that merit further evaluation.

It would be possible to expand User Activity Monitoring to address unclassified DOD computer systems, and DOD anticipates developing capabilities in that regard. However, it would be a technical challenge to monitor every DOD user's online activities and systematically flag a broad range of potentially inappropriate communications or activities. Some government employees are likely to find such monitoring excessively intrusive. Moreover, the benefit of comprehensive monitoring of government computer systems for behaviors unrelated to information security is unclear. Some monitoring may be appropriate to establish a credible deterrent against misuse of government systems, but most nefarious actors who wish to engage in violent extremism are likely to avoid the use of government systems that are subject to monitoring in carrying out their activities.

It is also conceivable that the Department could develop a system specifically designed to monitor the online activities of service members for compliance with DODI 1325.06 even when such activities are not conducted on DOD computer systems. The revised Instruction specifically prohibits "engaging in electronic and cyber activities regarding extremist activities, or groups that support extremist activities—including posting, liking, sharing, re-tweeting, or otherwise distributing content—when such action is taken with the intent to promote or otherwise endorse extremist activities." DODI 1325.06 also provides the guidance that "military personnel are responsible for the content they publish on all personal and public Internet domains, including social media sites, blogs, websites, and applications." The DODI does not state how these requirements will be enforced, and service members have not been asked to waive privacy protections for such a purpose. Accordingly, the Department's ability to enforce restrictions on online conduct are likely limited to reports by others and outputs from existing monitoring systems with independent legal justifications (such as personal security investigations and User Activity Monitoring).

This section focuses primarily on the use case of incorporating social media screening into the security background investigation because that appears to be the direction in which the Department is most likely to move at this time. We briefly describe the constraints under which DOD is allowed to conduct social media screening, summarize some of the groundwork DOD has laid thus far to operationalize this type of screening, and outline a few of the many challenges that remain.

a. Scope of Legal Authorization

Security Executive Agent Directive 5 (SEAD 5), issued by the DNI on 12 May 2016, authorizes federal agencies to collect, use, and retain "publicly available social media information during the conduct of personnel security background investigations and adjudications."[401] SEAD 5 sets several parameters for how publicly available social media information can be used. The information must "pertain to the adjudicative guidelines." That is, SEAD 5 is not an unrestricted license to collect a broad swath of online information on individuals. Any information collected must be relevant to the investigation. The information must also use a "period of coverage" that is "consistent with the scope of the investigation." For example, a five-year investigation window cannot use publicly available social media information from ten years ago. Information must be "intentionally" collected about the "covered individual under investigation" (information on others "will not be investigated" or retained unless it presents a national security or criminal concern).

To emphasize that only publicly available social media information may be used in an investigation, SEAD 5 expressly shelters individuals under investigation from providing passwords, logging into a private account, or otherwise disclosing non-publicly available social media information. Investigators may not take steps to "bypass privacy controls," such as by making use of third-party connections or attempting to "friend" or "follow" the individual under investigation.

SF86, the application form used for security background investigations, was updated shortly after the issuance of SEAD 5 to address the use of publicly available social media in the investigative process.[402] By signing the "Authorization for Release of Information" in the SF86, individuals explicitly authorize the use of publicly available social media information in the investigation process. This authorization incorporates verbatim the definition of publicly available social media information from SEAD 5 in its entirety:[403]

---

[401] See the full text of SEAD 5 at Office of Director of National Intelligence, *Security Executive Agent Directive 5: Collection, Use, and Retention of Publicly Available Social Media Information in Personnel Security Background Investigations and Adjudications* (n.p.: Office of Director of National Intelligence, May 12, 2016), https://www.odni.gov/files/NCSC/documents/Regulations/SEAD_5.pdf.

[402] See the November 2016 revision, U.S. Office of Personnel Management, *Questionnaire for National Security Positions.* SF 86.

[403] The verbatim definition from SEAD 5 begins with "any electronic" and continues through the end of the first sentence of the block quote.

> **I Understand** that, for these purposes, publicly available social media information includes any electronic social media information that has been published or broadcast for public consumption, is available on request to the public, is accessible on-line to the public, is available to the public by subscription or purchase, or is otherwise lawfully accessible to the public. I further understand that this authorization does not require me to provide passwords; log into a private account; or take any action that would disclose non-publicly available social media information.[404]

The definition of publicly available social media information is quite broad, especially with the inclusion of the clause "available to the public by subscription or purchase." This can extend well beyond a typical internet search for information about an individual. User activity online is monitored extensively by third parties (through cookies and other tracking devices), and this information can be sold for advertising and other purposes. Data privacy laws are continuing to evolve. The trend in recent years has been toward more individual choice in opting out of data tracking and the sale of personal information, but at present, individuals throughout much of the U.S. have a limited ability either to determine what online user activity about them might be subject to sale or to prevent it from being sold.[405] An expansive interpretation of "available to the public for subscription or purchase" potentially could incorporate any online data that can be bought and sold. As an extreme example, data enabling, hyper-targeted, online advertisements could be subscribed to or purchased, so the information could be incorporated into the security background investigation process. The fact that information is technically "available to the public for subscription or purchase" may not match the spirit of limiting the investigation to publicly available information.

On the other hand, the SEAD 5 definition of "social media" (which is separate from its definition of "publicly available social media information") is relatively narrow. Social media is defined as:

> Websites, applications, and web-based tools that allow the creation and exchange of user generated content. Through social media, people or groups can engage in dialogue, interact, and create, organize, edit, comment on, combine, and share content.

---

[404] November 2016 revision, U.S. Office of Personnel Management, Questionnaire for National Security Positions. SF 86.

[405] Data privacy laws tend to be stricter in Europe than in the U.S. However, in recent years, a handful of states have adopted restrictions on how online personal information can be used, shared, or sold by businesses and data brokers. For instance, the California Consumer Privacy Act of 2018 (Cal. Civ. Code 1798.100 et seq.), accords California consumers a "right to know about the personal information a business collects about them and how it is used and shared," together with rights to "delete personal information collected from them" and to "opt-out of the sale of their personal information" (https://oag.ca.gov/privacy/ccpa). See "State Laws Related to Digital Privacy," *National Conference of State Legislatures*, June 7, 2022, https://www.ncsl.org/research/telecommunications-and-information-technology/state-laws-related-to-internet-privacy.aspx.

This definition emphasizes user generated content that is interactive. A lot of user activity that is tracked online is not logged or created for human-to-human dialogue, sharing, or interaction (e.g., user activity tracked by website cookies). Such data is arguably off-limits for social media screening. Even if the data is "available to the public by subscription or purchase," it could be off-limits because it lacks an interactive element that would qualify it as social media by this definition. Before DOD could implement a comprehensive program for monitoring social media, it would have to address the relationship between the definitions of "social media" and "publicly available social media information" and specify rules for the types of data that can or cannot be accessed.

b. Increasing Privacy Protections

With the increase in public awareness and concern about online privacy, privacy laws have become more strict and social media platforms have limited the amount of data readily accessible from their systems. In the years leading up to the 2016 release of SEAD 5, many social media platforms maintained fairly loose terms of service and the culture surrounding the use of available privacy protections, such as limiting posts to a pre-determined set of followers (e.g., allowing only "friends" or even "friends of friends" to view posts), was not particularly strong. APIs used as official portals for connecting to specific platforms and accessing large quantities of data likewise had few restrictions.

However, in the wake of negative incidents of social media information harvesting (such as the Cambridge Analytica data scandal in which Facebook profiles were used for political purposes without the knowledge of users), social media platforms have implemented stricter privacy protections for their sites and APIs. Default user settings have changed in many cases to further enable privacy. Users may have to opt-into making their posts publicly available, rather than deferring (whether or not intentionally) to public posting by default.[406] Some platforms are auditing the use of their APIs to limit inappropriate usage.[407] Web-scraping is limited or not permitted by the terms of service of many platforms, with security measures built in to limit and detect potential web-scraping efforts. As a result, without express user permission, it is increasingly more difficult to secure legal and proper access to data on many platforms. The social media platforms from which data can be broadly gathered tend to be those that operate with a high-level of anonymity for individual users (such as the Reddit and Telegram data described earlier). The sphere of publicly available social media information that is not anonymous is shrinking.

Users can dynamically change their privacy settings. Depending on the platform, information once marked public may be changed to private, or vice versa. This can further complicate the

[406] Facebook, for instance, made this change in 2014. See Ellis Hamburger, "Facebook Increases Privacy on all New Posts by Default," *The Verge*, May 22, 2014, https://www.theverge.com/2014/5/22/5739744/facebook-changes-default-privacy-of-posts-from-public-to-friends.

[407] For example, in addition to having a pre-approval process for use cases of its API, Twitter began auditing high-volume users of its API in 2019. See Josh Constine, "Twitter Cracks Down on API Abuse, will Charge B2B Devs," *Tech Crunch*, March 19 2019, https://techcrunch.com/2019/03/19/twitter-developer-review/.

process of determining whether information is public or private and increases the burden for accurate and careful documentation. At a deeper level is the legal question as to whether an individual intended to communicate the information publicly or privately. The Supreme Court ruled in Katz v. U.S., 389 U.S. 347 (1967) that "what a person knowingly exposes to the public, even in his own home or office is not a subject of Fourth Amendment protections." However, "what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected." As social media platforms and individuals increase the level of their privacy protections, the extent to which DOD is able to access online information is likely to decrease.

c. Identity Resolution

Determining whether publicly available social media information is associated with a given individual can be a complex task. An internet browser search for a common name can turn up information on scores of distinct individuals, none of whom may be the person intended. The security background investigation process has the benefit of soliciting a wide array of personal identifiers from the applicant through the SF86.[408] Among other things, this includes the individual's full name, former names or aliases, current and former addresses, current and former employers, schools attended, date and place of birth, phone number, email address, height and weight, hair color and eye color, and information about family members (extending even to details such as the place and date of birth of an individual's mother- and father-in-law). These various identifiers provide context that can be used to identify whether or not information from an online source is associated with the individual under investigation. Even still, it may be difficult to positively associate online information with a given individual. There may be multiple individuals with the same name who also share additional attributes, such as attendance at the same school, or residence in the same city.

If information does appear to be associated with a given individual, there is the further step determining whether the information faithfully represents the individual. An internet search may result in second- or third-hand information about the individual that may or may not be accurate. There is also the risk that someone else is impersonating an individual online and linking them maliciously to online spurious, derogatory information. The Department could likely address many of these issues by using certain information obtained through initial online screening systems as a trigger for additional and more thorough investigation. Since SEAD 5 authority is limited to the "covered individual under investigation," any online search must be targeted toward a specific person, and the identity resolution process needs to resolve that any information collected

[408] See U.S. Office of Personnel Management, *Questionnaire for National Security Positions*, SF 86.

positively matches that person. This rules out broad, open-ended searches of online material that may happen to be associated with a person who has a connection to the Department.[409]

d. Information Relevant for Adjudication

Of all the publicly available social media information that may exist about an individual, only a small fraction is likely to be relevant to the adjudication of a background investigation. Security clearance investigations address the trustworthiness of an individual from a holistic perspective and address areas of potential risk, such as undue foreign influence or connections, alcohol and substance abuse, financial instability, significant mental health concerns, illegal behavior, and association with unlawful causes.[410]

Social media screening requires the ability to identify potential issues in each of these categories. Some of these are easier to detect than others. For example:

- If an individual maintains a public-facing profile that publicly lists associates (e.g., "friends" on a platform), then the listing could be a source for identifying foreign connections. However, the strength of those foreign connections may not be apparent.[411]
- A single publicly available post using machine-readable text that directly reveals inappropriate behavior may be discernable by automated processes. However, if the information is spread in pieces across multiple posts, or if the information is in a more complex electronic format (e.g., combining words with images), it will be harder to detect.

Because of the number of individuals associated with the Department, any screening system for online information will necessarily require a high degree of automation. Some automated processes are still in their infancy and may not be able to detect signals that would be discernable by a human. If an individual knowingly engages in questionable behavior online, there is a strong likelihood that the individual will attempt to obfuscate the behavior. Any level of obfuscation

---

[409] However, the American public may not be comfortable with a system in which DOD screens postings by a wide segment of the public in an effort to determine whether or not the posters have DOD connections, even if data on non-DOD persons is not retained.

[410] As noted earlier in this report, Section 29 of the SF86 ("Association Record") calls out some, but not all, aspects of extremist activities prohibited by the DOD. However, this is a poor screening proxy for the full set of prohibited activities enumerated in DODI 1325.06. The standardized screening questions about current or previous extremist activity issued by the Department's Director of Accession policy are more closely tied to DODI 1325.06. However, those questions apply only to military accessions, whereas the SF86 screening process applies to all those seeking (or continuing to hold) a security clearance.

[411] The SF86 solicits information on foreign nationals with whom the individual (or spouse, domestic partner, or cohabitant) is "bound by affection, influence, common interests, and/or obligation" (see U.S. Office of Personnel Management, *Questionnaire for National Security Positions*, SF 86, 60). Not all connections that exist on a social media profile necessarily rise to the threshold of being "bound" together in this way.

raises the complexity of identifying inappropriate behavior through an automated screening process.

e. Redacting Information

SEAD 5 states that "information inadvertently collected relating to other individuals (i.e., individuals who are not the subject of the background investigation) will not be retained unless that information is relevant to a security determination of the covered individual." Accordingly, any social media screening process must be combined with a reticulated automated process for redacting and deleting information about other individuals from online information captured and collected in furtherance of a "covered individual's" background investigation. The more standardized a piece of information is, the easier it is to develop an algorithm for redacting content not authorized for collection. For instance, Google Street View obscures license plates and faces from images, and legal documents may redact signatures, names, or other salient identifying information. These are more targeted redaction exercises. Depending on the breadth of the social media platforms and websites screened, however, the wide variety of formats for social media information can present a significant technical redaction challenge. Names, handles or usernames, email addresses, images, videos, textual descriptions, and a variety of other potential identifying information can appear in any number of formats. Testing and ongoing monitoring will be necessary to ensure compliance with the content collection proscriptions set forth in SEAD 5 as part of any social media screening process.

f. Establishing Appropriate Business Processes

Implementing a process for incorporating publicly available online information into a screening process is far from trivial. In addition to assessing legal boundaries and authorities, the process of identifying viable business rules for conducting the online searches and evaluating the content is essential. Business rules must comport with applicable authorities and, from a technical and practical standpoint, must be susceptible of implementation. There must likewise be a process for ensuring that any business rules are being followed. When DOD contracts for support in conducting screening of online information, there must be adequate transparency for DOD to audit the process on an ongoing basis to ascertain that the contractors are indeed following business rules. Even if vendors rely on proprietary software and algorithms, the need for transparent audits is paramount.

Business rules need to be tested to determine whether they are adequate to identify types of posts appropriate for background screening and information collection. This can be done by developing a library of online entries that have been determined to include information that would properly be flagged in the context of an investigation, and if so, the category of issue raised by that information. Business rules can then be independently applied to the library of online entries to determine if the rules would result in similar categorization in each case. In this manner, business rules can be assessed in an iterative process to ensure that they result in both consistent

categorization of content and in a categorization satisfactory to subject matter experts. IDA interviewees indicated that the Department has conducted assessments of potential business rules for the screening of online information.

g. Testing and Audit Requirements

Once business rules have been established, they must be tested to assess how well they can be implemented by automated technologies. A library of entries used in evaluating business rules can be used as a benchmark against which the performance of an automated technology is assessed. However, to be used as a representative benchmark, the library of entries needs to be adequately large and varied, with the goal of representing the myriad of potential issues and non-issues that may arise in publicly available social media content. It is not clear that a sufficient library of pre-assessed entries exists at present, and as the Department moves forward in implementation efforts, this may be an area that merits investment. The Department may likewise seek to ensure that a sufficient number of entries related to prohibited extremist activities are included in the library of cases used to assess the performance of automated technologies.

The above tests focus on evaluating the content of online entries. However, the full end-to-end process for incorporating publicly available social media into the background investigation process needs to be assessed. This includes examining:

- The quantity and types of identifying information that would routinely be used in online searches,
- The scope of online information that can be appropriately searched,
- The steps that need to be taken for identity resolution and ensuring that the information accurately represents the individual in question,
- Sufficient documentation of potentially ephemeral online information,
- Content analysis,
- Redaction of information about individuals not subject to investigation,
- Report generation capturing documentation and content analysis for relevant online information,
- Further investigative steps based on discovered information,
- Opportunities for the individual being investigated to refute or provide clarifying information about the content, and
- Incorporation of the content into final adjudication of the clearance decision and any potential appeals.

This is a complex process to conduct and assess. Conducting and assessing the various steps requires the input and coordination of multiple entities, including various elements of the Defense

Counterintelligence and Security Agency (such as the Vetting Risk Operations Center and the DOD Consolidated Adjudications Facility), as well as any organization performing the automated content search and analysis.

Since 2009, the Defense Personnel and Security Research Center (PERSEREC) has conducted research to examine how publicly available electronic information could be incorporated into security background investigations and other employment decisions. Early work by PERSEREC focused on examining case law and engaging with subject matter experts to identify viable guidelines for conducting online vetting for national security positions and law enforcement.[412] Some of the concepts that PERSEREC touched on in this early work are reflected in the policy guidelines established in SEAD 5.

IDA interviewees indicated that the Department has conducted testing on a very limited scale to examine how aspects of this end-to-end process might work in practice. This is a valuable exercise. However, the efficacy of such an exercise is based almost exclusively on a contractor's capabilities to conduct many of the steps for collecting and analyzing pertinent content. The Department has solicited multiple contractors to demonstrate their capabilities in this regard. Moreover, "to provide independent testing and evaluation of approaches to collecting relevant data for background investigations," the Department has partnered with the Applied Research Laboratory for Intelligence and Security (ARLIS), a University Affiliated Research Center sponsored by the USD(I&S).[413]

Assessments to date indicate that scalability remains a significant challenge. Technologies for automating individual processes are improving over time, but the pipeline as a whole does not appear to have reached the level of automated capability needed to ensure that the process can operate at scale while complying with DOD's authorities and practices.

2. Findings and Recommendations

Recommendation 17: Expand on the guidance regarding extremist activities on the internet in revised DODI 1325.06 to establish clear expectations for online behavior and social media activities for those who are affiliated with DOD.

To implement this recommendation, the Department should consider the following option:

- The USD(P&R) could supplement the updates to DODI 1325.06 with an information campaign that quickly and clearly articulates expectations for online behavior. An

[412] See, for example, Andrée Rose, Howard Timm, Corrie Pogson, et al., *Developing a Cybervetting Strategy for Law Enforcement: Special Report* (Alexandria, VA: International Association of Chiefs of Police and PERSEREC, December 2010), https://www.theiacp.org/sites/default/files/2018-08/CybervettingReport-2.pdf. The majority of PERSEREC's reports are published with the "For Official Use Only" (FOUO) designation (predating the current "Controlled Unclassified Information" (CUI) designation). Our overview herein touches only on high-level concepts, and only from portions of PERSEREC Management Reports that do not carry an FOUO caveat.

[413] Department of Defense, *Report on Countering Extremist Activity Within the Department of Defense*, 15.

information campaign could balance positive messaging of acceptable behavior with messaging on prohibited behavior.

  - Acceptable behavior: An information campaign could highlight the need to reflect military values and decorum (e.g., respect, dignity, honor, discipline) in all online behavior and activities.
  - Prohibited behavior: To eliminate confusion about the types of online activities that may be subject to disciplinary action, an information campaign could provide a quick, easily understood concept of what is prohibited online. For example:

    > "*Don't 'Like' treason, terrorism, sedition, or efforts to deny civil rights, prevent government personnel from performing official duties, or prevent others from exercising legal rights*."

- The Secretary could require the military services to update their policies on the use of social media specifically to address prohibited extremist activities in a manner consistent with DODI 1325.06. Such policies include DODI 8170.01 ("Online Information Management and Electronic Messaging"); Air Force Handbook, Chapter 14E ("Electronic Communications and the Internet"); Army ALARACT 061/2019 ("Professionalization of Online Conduct"); the U.S. Navy Social Media Handbook; and the U.S. Marine Corps 2021 Social Media Handbook.

Recommendation 18: Exercise caution in fielding systems and technologies for automated screening activities, such as systems implementing SEAD 5 through monitoring of social media information or user activity monitoring.

Caution is warranted due to technological limitations and because of the strong likelihood of adverse reactions among members of the military community driven by perceptions of excessive ("big brother"-like) surveillance. For instance, although SEAD 5 provides a broad definition of "publicly available social media information," it may be prudent to consider both strategic restraint in the amount of information actually monitored and to establish well-defined, transparent triggers that will prompt more intensive investigation.

To implement this recommendation, the Department should consider the following options:

- The USD(I&S) could implement clear guidelines on the use of publicly available electronic information in screening for security clearances and, with a view to managing expectations, make a high-level overview of these guidelines publicly accessible.
- USD(I&S) could take steps to ensure that screening algorithms and investigative activities follow its guidelines for the use of publicly available electronic information. For instance, USD(I&S) could direct the periodic assessment, via an independent audit, of screening algorithms for compliance with established rules, and require that the practices of investigative offices likewise be periodically audited.

- USD(I&S) could consider structuring screening guidelines around the principles of sampling and triggers for deeper investigations. Large portions (or samples) of the eligible population may be subject to an initial screening for any readily apparent prohibited online activities. Deeper investigations would be undertaken only when prompted by well-defined and transparent triggers. Small numbers of the eligible population could additionally be sampled at random for deeper investigation as a quality assurance measure.
- USD(I&S) could ensure that the viability of the screening systems and technologies are rigorously tested and that the systems' limitations are well understood and investigated. Tests should be done both prior to launching a new technology and periodically on technologies that have been launched. Testing could take a variety of forms, including:
  - Identity resolution tests: A variety of tests can be implemented to assess the efficacy of identity resolution processes. For instance, standardized test data sets can be used to examine algorithmic performance on common identity resolution tasks. Red teaming can assess how satisfactorily a technology performed in identifying attempts by others to impersonate or defame an individual subject to a background investigation.
  - Legal, moral, and ethical tests: The Joint Artificial Intelligence Center could provide guidance on steps that a particular technology would need to take to satisfy the DOD AI Ethics Principles. This guidance should be coupled with a (preferably independent) review of the data used in the algorithms and any potential limitations or biases they may have; algorithmic performance metrics across various demographic groups (race, religion, gender, etc.); privacy measures; corrective actions that may need to be taken to minimize differential outcomes across populations; implementation guidance for responsibly using the algorithmic outputs and ensuring that those using the outputs understand their proper use and limitations; and safeguards to identify and mitigate unintended consequences.
  - Operational tests: Prior to a broad rollout of a technology, it should be subject to rigorous operational testing over a period of time sufficient to understand how the technology will perform in practice and to identify and mitigate potential limitations. These tests should maintain metrics on the reliability and validity of the technology.

9. Conclusions and Recommendations

IDA's review found no evidence that the number of violent extremists in the military is disproportionate to the number of violent extremists in the United States as a whole. Extremism in the veterans' community has seen peaks and valleys over recent decades, and currently appears to be on the increase. Racism and sexism continue to be problems in the military, but only a handful of violent extremists have been identified in the military ranks. Of course, even a single incident of violent extremism can have significant negative repercussions for DOD, the military community, and the Nation itself. For this reason, the Department can no more tolerate advocacy of violent extremism in the ranks than it can tolerate racism, sexism, and discrimination.

At the same time, the Department must not overreact and draw too large of a target. The U.S. military draws on the strengths of the American public and appropriately reflects the full range of political, ideological, and religious backgrounds that shape American society today. As Americans, service members have every right to their own opinions, including opinions that may appear extreme or even distasteful to others. Diversity of views, like diversity of race, gender, and ethnicity, is both a necessity and an asset for the Department, providing an aggregation of strengths, perspectives, and capabilities that transcend individual contributions.

For this reason, IDA recommends a carefully-modulated response to extremist activities in the Department and in the military community. Consistent with the newly-revised definitions in DODI 1325.06, extremist activities should be prohibited only when they become inconsistent with military core values—values such as duty, loyalty, respect, honor, courage, commitment, discipline and teamwork—that are designed to build a united, disciplined, and effective fighting force. Even in cases in which the policy is violated, the Department should keep in mind that most violators are not enemies, but Americans who volunteered to serve their country.

IDA found that pathways to violent extremism often include some of the same push, pull, and personal factors as pathways to other negative behaviors, including suicide, binge-drinking, and drug abuse. Just as the Department's response to these negative behaviors has balanced support and understanding with more punitive measures, so too should its response to violations of prohibitions on extremist activities. Simply put, a carefully modulated range of responses is likely to be more successful—and less likely to risk alienating the force—than an excessively punitive focus on extremist behaviors and activities.

Consistent with these principles, the IDA team makes 18 recommendations, as follows:

Recommendation 1: Build on the new definition of prohibited extremist activities in DODI 1325.06 to ensure that prohibited extremist behaviors and activities are consistently defined throughout the Department.

Recommendation 2: Consistently link prohibitions on extremist behaviors and activities to a broader context, emphasizing the need to bridge differences and continue to build a united, disciplined fighting force comprising individuals with diverse backgrounds and opinions.

Recommendation 3: Clarify the line between individual offenses of prejudice/harassment/bullying and cases of prohibited extremist behavior. Not all misconduct is extremist and reporting individual incidents as prohibited extremism may give a distorted picture of the role and influence of extremist groups in the Department.

Recommendation 4: Work to actively counter false information campaigns by providing training and instruction on how to be a life-long and life-wide critical consumer of information, making sure that alternative viewpoints and more reliable sources of information are available to the force, and where possible flagging fabricated information and foreign links to false information campaigns.

Recommendation 5: Expand on comprehensive threat assessment teams established pursuant to the Department's Primary Prevention Plan and on the threat assessment program established by DITMAC to identify at-risk behaviors, activities, and vulnerabilities at multiple levels (e.g., individual, inter-individual, group, culture/climate) that contribute to destructive behaviors, including violent extremist activities, in military populations.

Recommendation 6: Expand on the military's current emphasis on education, training, and assessment on the core values and corresponding virtues of DOD and the services (e.g., Loyalty, Duty, Honor, Mission) to build on core values as a barrier to radicalization in the force.

Recommendation 7: Through the expansion of best practices, such as the Marine for Life program, revitalize available opportunities and explore new venues to foster and cultivate stronger post-separation/retirement group identity (with integration of DOD and military service values) to provide social, personal, and professional connections and a sense of belongingness.

Recommendation 8: Unless more significant action is called for by the specific facts and circumstances of a particular case, seek rehabilitative and restorative interventions such as mentoring and counseling for activities that are not violent or criminal.

Recommendation 9: Avoid making extremist activity a separate criminal offense under the UCMJ. Take action to modify the Manual for Courts-Martial to make evidence of prohibited extremist activity an aggravating factor in sentencing in a manner similar to Rule for Courts-Martial 1001(b)(4), which makes evidence of a hate crime an aggravating factor.

Recommendation 10: Update security and suitability questions asked of military and civilian employees, contractor employees, and applicants for employment to incorporate the standard questions now asked of military recruits about participation in extremist activities, and expand

those questions to address the full range of extremist activities prohibited by revised DODI 1325.06.

Recommendation 11: Develop guidance on security clearances and access and suitability determinations, explaining how active participation in prohibited extremist activities will be considered pursuant to existing criteria.

Recommendation 12: Update insider threat training and related materials to provide definitions and examples of prohibited extremist activities and to expressly encourage early reporting of potential problems.

Recommendation 13: Continue the improvement of mechanisms for tracking cases of prohibited extremist activities in relevant DOD systems to ensure they are adequate to meet section 554(b), FY2021 NDAA, reporting requirements.

Recommendation 14: Ensure that the Military Departments use consistent definitions and criteria for flagging cases of prohibited extremist activities.

Recommendation 15: Ensure flagging capabilities can differentiate between substantiated cases and non-substantiated allegations. For substantiated cases, consider common coding criteria for indicating the severity or nature of the misconduct.

Recommendation 16: Implement quality control check (automated to the extent possible) for ensuring that cases are being flagged appropriately.

Recommendation 17: Expand on the guidance regarding extremist activities on the internet in revised DODI 1325.06 to establish clear expectations for online behavior and social media activities for those who are affiliated with DOD.

Recommendation 18: Exercise caution in fielding systems and technologies for automated screening activities, such as systems implementing SEAD 5 through monitoring of social media information or user activity monitoring.

No set of actions can completely eradicate prohibited extremist activities from the force because the military will always reflect American society as a whole with all of its imperfections. By implementing the IDA recommendations, however, the Department should be able to make continued progress in its effort to ensure that core military values prevail over fringe beliefs, and violent extremism is not able to undermine the effectiveness of the U.S. Armed Forces or their place in American society.

This page is intentionally blank.

Appendix A.
Illustrations

Figures

Tables

Appendix B.
References

Abendroth, Johanna, and Tobias Richter. "How to understand what you don't believe: Metacognitive training prevents belief-biases in multiple text comprehension." *Learning and Instruction* 71 (February 2021): 1-16. https://www.sciencedirect.com/science/article/pii/S095947521930739X.

Acosta, Joie, Matthew Chinman, and Amy Shearer. *Countering Sexual Assault and Sexual Harassment in the U.S. Military: Lessons from RAND Research*. Santa Monica, CA: RAND Corporation, 2021. https://www.rand.org/pubs/research_reports/RRA1318-1.html.

AF.mil Website. "Air Force Values and Corresponding Virtues." Accessed June 16, 2022. http://www.usafa73.org/uploads/6/4/4/5/64457159/core_values_and_virtures.pdf

Allyn, Bobby. "Reddit Bans The_Donald, Forum Of Nearly 800,000 Trump Fans, Over Abusive Posts." *NPR*, June 29, 2020. https://www.npr.org/2020/06/29/884819923/reddit-bans-the_donald-forum-of-nearly-800-000-trump-fans-over-abusive-posts.

Altier, Mary Beth, Emma Leonard Boyle, and John G. Horgan. "Returning to the Fight: An Empirical Analysis of Terrorist Reengagement and Recidivism." Terrorsim and Political Violence 18 (November 18, 2019): 1-25. https://www.tandfonline.com/doi/full/10.1080/09546553.2019.1679781.

Aly, Anne, Elisabeth Taylor, and Saul Karnovsky. "Moral Disengagement and Building Resilience to Violent Extremism: An Education Intervention." *Studies in Conflict & Terrorism* 37, no. 4 (March 11, 2014): 369-385. doi: 10.1080/1057610X.2014.879379.

Anti-Defamation League Website. "ADL H.E.A.T. Map (Hate, Extremism, Antisemitism, Terrorism)." Accessed June 16, 2022. https://www.adl.org/resources/tools-to-track-hate/heat-map.

Armed Conflict Location & Event Data Project Website. "Armed Conflict Location & Event Data Project (ACLED) Codebook." Accessed June 16, 2022. https://acleddata.com/acleddatanew/wp-content/uploads/2021/11/ACLED_Codebook_v1_January-2021.pdf.

Ardiley, Stephanie. "History of the Common Access Card (CAC)." *Security Infowatch*. https://www.securityinfowatch.com/home/article/10653434/history-of-the-common-access-card-cac.

Armed Conflict Location & Event Data Project Website. "FAQs: ACLED US Coverage." Accessed June 16, 2022. https://acleddata.com/acleddatanew/wp-content/uploads/2021/12/ACLED_US-Coverage-FAQs_v4_December-2021.pdf.

Army.mil Website. "The Army Values." Accessed June 16, 2022. https://www.army.mil/values/.

Association of Threat Assessment Website. "Certified Threat Manager." Accessed June 16, 2022. https://www.atapworldwide.org/page/certificationexam.

Badger, T.A. “Soldier Punished for Racial Incident at Army Base.” *The Associated Press*, April 6, 1993. https://apnews.com/article/84b02b8c599f783fce1185f851d13c72.

Bago, Bence, David Rand, and Gordon Pennycook. “Fake News, Fast and Slow: Deliberation Reduces Belief in False (but not true) News Headlines.” *Journal of Experimental Psychology: General* 149, (January 9, 2020): 1608-1613. https://doi.org/10.1037/xge0000729.

Banas, John A., and Stephen A. Rains. “A Meta-Analysis of Research on Inoculation Theory.” *Communication Monographs* 77, no. 3 (September 22, 2010): 281-311. https://doi.org/10.1080/03637751003758193.

Baron, Robert S. “Arousal, Capacity, and Intense Indoctrination.” *Personality and Social Psychology Review* 4, no. 3 (August 1, 2000): 238-254. https://journals.sagepub.com/doi/10.1207/S15327957PSPR0403_3.

Bartlett, Jamie, and Carl Miller. The Power of Unreason: *Conspiracy Theories, Extremism and Counterterrorism*. London: Demos, August 2010.

Bartlett, Jamie, Jonathan Birdwell, and Michael King. *The Edge of Violence: A Radical Approach to Extremism*. London, UK: Demos, 2010.

Bastick, Zach. “Would you Notice if Fake News Changed your Behavior? An Experiment on the Unconscious Effects of Disinformation.” *Computers in Human Behavior* 116, no. 106633 (March 2021). https://doi.org/10.1016/j.chb.2020.106633.

Baumgartner, Jason, Savvas Zannettou, Brian Keegan, Megan Squire, and Jeremy Blackburn. “The Pushshift Reddit Dataset.” Paper presented at the Proceedings of the Thirteenth International AAAI Conference on Web and Social Media, Munich, Germany, June 11-14, 2019, 830–839. https://ojs.aaai.org/index.php/ICWSM/article/view/7347/7201.

Baumgartner, Jason, Savvas Zannettou, Megan Squire, and Jeremy Blackburn. “The Pushshift Telegram Dataset.” Paper presented at the Proceedings of the Fourteenth International AAAI Conference on Web and Social Media, 840–847, June 11-14, 2019. https://ojs.aaai.org/index.php/ICWSM/article/view/7348/7202.

Baumgartner, Jason, Savvas Zannettou, Megan Squire, and Jeremy Blackburn. “The Pushshift Telegram Dataset.” Database.

Blue Star Families. *2020 Military Family Lifestyle Survey Comprehensive Report: Finding 1*. Encintas, CA: Blue Star Families, Syracuse University, 2020. https://bluestarfam.org/wp-content/uploads/2021/03/BSF_MFLS_CompReport_FINDING_1.pdf.

Borch, Fred L. “The Largest Murder Trial in the History of the United States: The Houston Riots Courts-Martial of 1917.” *The Army Lawyer* (March 2012): 28-30.

Borum, Randy. *Psychology of Terrorism*. Tampa, FL: University of South Florida, 2004.

Borum, Randy. “Radicalization in Violent Extremism I: A Review of Social Science Theories.” Journal of Strategic Security 4, no. 4, (Winter 2011): 7-36. https://www.jstor.org/stable/26463910?seq=1.

Boyd-MacMillan, Eolene M. “Increasing Cognitive Complexity and Collaboration Across Communities: Being Muslim Being Scottish.” *Journal of Strategic Security* 9, no. 4 (Winter 2016): 79-110. 10.5038/1944-0472.9.4.1563.

Bradbury, Roger, Terry Bossomaier, and David Kernot. "Predicting the Emergence of Self-Radicalization Through Social Media: A Complex Systems Approach." Pages 379-389 in *Terrorists' Use of the Internet*, edited by Maura Conway, Lee Jarvis, Orla Lehane, Stuart Macdonald, and Lella Nouri. IOS Press, 2017. doi:10.3233/978-1-61499-765-8-379.

Breakwell, Glynis Marie. *Coping with Threatened Identities*. North Yorkshire, UK: Methuen, January 1, 1986.

Brewer, Marilynn B. "The Social Self: On Being the Same and Different at the Same Time," *Personality and Social Psychology Bulletin* 17, no. 5 (October 1, 1991): 475-82, https://doi.org/10.1177/0146167291175001.

Brewer, Marilynn B. "The Role of Distinctiveness in Social Identity and Group Behaviour." In *Group Motivation: Social Psychological Perspectives* edited by Michael A. Hogg and Dominic D. Abrams. Hertfordshire, UK: Harvester Wheatsheaf, 1993: 1-16, https://psycnet.apa.org/record/1993-98846-001.

Brading, Thomas. "OSI Modernizing Case Management Platform." *OSI Public Affairs*, February 25, 2022. https://www.osi.af.mil/News/Article-Display/Article/2947008/osi-modernizing-case-management-platform/.

Branigin, William, and Dana Priest. "3 White Soldiers Held in Slaying of Black Couple." *The Washington Post*, December 9, 1995. https://www.washingtonpost.com/archive/politics/1995/12/09/3-white-soldiers-held-in-slaying-of-black-couple/1f11ca9f-9fe2-4e28-a637-a635007deeaf/.

Butler, Nick. "The Charleston Riot of 1919." *Charleston County Public Library*, May 10, 2019. https://www.ccpl.org/charleston-time-machine/charleston-riot-1919#_edn3.

Byman, Daniel L. "How to Hunt a Lone Wolf: Countering Terrorists who Act on their Own." *Brookings*, February 14, 2017. https://www.brookings.edu/opinions/how-to-hunt-a-lone-wolf-countering-terrorists-who-act-on-their-own/.

Campbell, Donald T. "Common Fate, Similarity, and Other Indices of the Status of Aggregates of Persons as Social Entities." *Behavioral Science* 3, No. 1 (1958): 14-25. https://doi.org/10.1002/bs.3830030103.

Cancian, Mark. "A Year After January 6, DoD's Vague Extremism Definition Could set up New Problems." *Breaking Defense*, January 6, 2022. https://breakingdefense.com/2022/01/a-year-after-jan-6-dods-vague-extremism-definition-could-set-up-new-problems/.

Castro, Carl Andrew, Sanela Dursun, Mary Beth MacLean, Raun Lazier, Matt Fossey, and David Pedlar. "Essential Components for a Successful Military-to-Civilian Transition." Chap. 11 in *Military Veteran Reintegration: Approach, Management, and Assessment of Military Veterans Transitioning to Civilian Life*, edited by Carl Andrew Castro and Sanela Sursun. San Diego, CA: Elsevier Academic Press, 2019. 245-251. doi: 10.1016/B978-0-12-815312-3.00011-5.

Chermak, Steven, Joshua Freilich, and Michael Suttmoeller. "The Organizational Dynamics of Far-Right Hate Groups in the United States: Comparing Violent to Nonviolent Organizations." *Studies in Conflict and Terrorism* 36, no. 3 (February 14, 2013): 193-218. https://www.tandfonline.com/doi/full/10.1080/1057610X.2013.755912.

Cherney, Adrian, and Jason Hartley. "Community Engagement to Tackle Terrorism and Violent Extremism: Challenges, Tensions, and Pitfalls." *Policing and Society* 27, no. 7 (October 5, 2015): 750-763. https://www.tandfonline.com/doi/full/10.1080/10439463.2015.1089871.

Cherney, Adrian, Idhamsyah Putra, Vici Putera, Fajar Erikha, and Muhammad Faisal Magrie. "The Push and Pull of Radicalization and Extremist Disengagement: The Application of Criminological Theory to Indonesian and Australian Cases of Radicalization." *Journal of Criminology* 54, no. 4 (July 30, 2021): 407-424. doi:10.1177/26338076211034893.

Chiodo, John J. "The Zoot Suit Riots: Exploring Social Issues in American History." *Social Studies* 104, no.1 (2013): 1-14. doi:10.1080/00377996.2011.642421.

Civil Air Patrol Website. "Cadet FAQs," "Do cadets have to join the military?" Accessed June 16, 2022. https://www.gocivilairpatrol.com/join/youth-in-cadet-program/cadet-faqs.

Civil Air Patrol Website. "Youth." Accessed June 16, 2022. https://www.gocivilairpatrol.com/join/youth-in-cadet-program.

Clifford, Bennett and Jon Lewis. *"This is the Aftermath:" Assessing Domestic Violent Extremism One Year After the Capitol Siege*. Washington, DC: Program on Extremism at The George Washington University, January 2022. https://extremism.gwu.edu/sites/g/files/zaxdzs2191/f/This%20is%the%20Aftermath.pdf.

Compton, Josh, Ben Jackson, and James A. Dimmock. "Persuading others to avoid persuasion: Inoculation theory and resistant health attitudes." *Frontiers in Psychology* 122, no. 7 (February 9, 2016). https://psycnet.apa.org/record/2016-19527-001.

Congressional Research Service. *Defense Primer: Department of Defense Civilian Employees*. Washington, DC: Congressional Research Service, February 15, 2022. https://sgp.fas.org/crs/natsec/IF11510.pdf.

Constine, Josh. "Twitter Cracks Down on API Abuse, will Charge B2B Devs." *Tech Crunch*, March 19, 2019. https://techcrunch.com/2019/03/19/twitter-developer-review/.

Crenshaw, Martha. Explaining Terrorism: Causes, Processes and Consequences. New York, NY: Routledge, November 2010.

Dalgaard-Nielsen, Anja, and Patrick Schack. "Community Resilience to Militant Islamism: Who and What?: An Explorative Study of Resilience in Three Danish Communities." *Democracy and Security* 12, no. 4 (October 13, 2016): 309-327. https://www.tandfonline.com/doi/full/10.1080/17419166.2016.1236691.

Defense Civilian Personnel Advisory Service. *The Suitability Guide for Employees*. Washington, DC: Department of Defense, n.d. 9. https://www.dcpas.osd.mil/sites/default/files/2021-04/Suitability_Guide_for_Employees.pdf.

Secretary of Defense. "Memorandum for Senior Pentagon Leadership, Commanders of the Combatant Commands and Defense Agency and DoD Field Activity Directors: DoD Actions to Address Findings and Recommendations of the 2021 On-Site Installation Evaluations." Memorandum. Washington, DC: DOD, March 30, 2022. https://media.defense.gov/2022/Mar/31/2002967351/-1/-1/1/DOD-ACTIONS-TO-ADDRESS-FINDINGS-AND-RECOMMENDATIONS-OF-THE-2021-ON-SITE-INSTALLATION-EVALUATION.PDF.

Department of the Air Force. AFRS/RSO Accessions Standards NOTAM 21-09, April 23, 2021 (document provided by the Office of the Air Force Judge Advocate General).

Department of the Army, "Army Command Policy," Army Regulation 600-20 (Washington, DC: Department of the Army, November 2014), 32, http://milreg.com/File.aspx?id=321#:~:text=This%20regulation%20prescribes%20the%20policies,Program%20(formerly%20the%20Army%20Sexual.

Department of Defense. "Diversity Management and Equal Opportunity in the DoD." DODD 1020.02E. Washington, DC: Department of Defense, June 1, 2018. https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/102002p.pdf.

Department of Defense. "The DoD Insider Threat Program." DODD 5205.16. Washington, DC: Department of Defense, August 28, 2017. https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/520516p.pdf?ver=2019-04-03-141607-017.

Department of Defense. "Harassment Prevention and Response in the Armed Forces." DODI 1020.03. Washington, DC: Department of Defense, December 29, 2020. https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/102003p.PDF?ver=DAAzonEUeFb8kUWRbT9Epw%3D%3D.

Department of Defense. "Harassment Prevention and Responses for DoD Civilian Employees." DODI 1020.04. Washington, DC: Department of Defense, June 30, 2020. https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/102004p.pdf.

Department of Defense. *Report on Countering Extremist Activity Within the Department of Defense*. Washington, DC: Department of Defense, December 2021. https://media.defense.gov/2021/Dec/20/2002912573/-1/-1/0/REPORT-ON-COUNTERING-EXTREMIST-ACTIVITY-WITHIN-THE-DEPARTMENT-OF-DEFENSE.PDF.

Department of Defense. "Handling Protest, Extremist, and Criminal Gang Activities Among Members of the Armed Forces." DODI 1325.06. Washington, DC: Department of Defense, December 20, 2021. https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/132506p.PDF.

Department of Defense, Office of Inspector General. *The Department of Defense Office of Inspector General's Report to Congress Pursuant to Section 554 of the Fiscal Year 2021 National Defense Authorization Act*. Washington, DC: Department of Defense Office of Inspector General, June 10, 2021. https://www.oversight.gov/sites/default/files/oig-reports/DoD/Department-Defense-Office-Inspector-General%E2%80%99s-Report-Congress-Pursuant-Section-554-Fiscal-Year-2021.pdf.

Department of Defense, Office of Inspector General. *Department of Defense Progress on Implementing Fiscal Year 2021 NDAA Section 554 Requirements Involving Prohibited Activities of Covered Armed Forces*. Washington, DC: Department of Defense Office of Inspector General, December 1, 2021. https://media.defense.gov/2021/Dec/02/2002902153/-1/-1/1/DODIG-2022-042.PDF.

Department of Defense. "DoD Military Equal Opportunity Program." DODI 1350.02. Washington, DC: Department of Defense, September 4, 2020. https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/135002p.pdf.

Department of Defense. "DoD Investigative and Adjudicative Guidance for Issuing the Common Access Card (CAC)." DODI 5200.46. Washington, DC: Department of Defense, November 2, 2020. https://www.cac.mil/Portals/53/Documents/520046p%20DoDI%20DoD%20Investigative%20and%20Adjudicative%20Guidance%20for%20Issuing%20the%20Common%20Access%20Card.pdf?ver=2020-05-01-092718-907.

Department of Defense. "DoD Policy on Integrated Primary Prevention of Self-Directed Harm and Prohibited Abuse or Harm." DODI 6400.09. Washington, DC: Department of Defense, September 11, 2020. https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/640009p.pdf.

Department of Defense Website. "Suicide Prevention." Accessed June 16, 2022. https://dod.defense.gov/News/Special-Reports/0916_suicideprevention/.

Under Secretary of Defense. *Department of Defense Strategy for Suicide Prevention*. Washington, DC: Department of Defense, December 2015. https://www.dspo.mil/Portals/113/Documents/TAB%20B%20-%20DSSP_FINAL%20USD%20PR%20SIGNED.PDF.

Department of Homeland Security. *Strategic Framework for Countering Terrorism and Targeted Violence*. Washington, DC: Department of Homeland Security, September 2019. https://www.hsdl.org/?abstract&did=829572.

Department of Homeland Security Website. "Center for Prevention Programs Partnerships." Accessed June 16, 2022. https://www.dhs.gov/CP3.

Department of Homeland Security Website. "Homeland Security Presidential Directive 12: Policy for a Common Identification Standard for Federal Employees and Contractors." Accessed June 16, 2022. https://www.dhs.gov/homeland-security-presidential-directive-12.

Department of Homeland Security. "Center for Prevention Programs and Partnerships." Last updated May 17, 2022. https://www.dhs.gov/CP3.

Director of National Intelligence. *US Violent Extremist Mobilization Indicators*. Washington, DC: Director of National Intelligence, 2021. https://www.dni.gov/files/NCTC/documents/news_documents/Mobilization_Indicators_Booklet_2021.pdf.

Douglas, Karen, Joseph Uscinski, Robbie Sutton, Aleksandra Cichocka, Turkay Nefes, Chee Ang, and Farzin Deravi. "Understanding Conspiracy Theories." *Political Psychology* 40, Suppl. 1 (February 2019): 1-33. doi: 10.1111/pops.12568.

Douglas, Karen, Jan-Willem van Prooijen, and Robbie Sutton. "Is the Label 'Conspiracy Theory' a Cause or a Consequence of Disbelief in Alternative Narratives?" *British Journal of Psychology* 00 (December 17, 2021): 1-16. doi: 10.1111/bjop.12548.

Douglas, Kevin, Stephen Hart, Christopher Webster, Henrik Belfrage, Laura Guy, and Catherine Wilson. "Historical-Clinical-Risk Management-20, Version 3 (HCR-20V3): Development and Overview." International Journal of Forensic Mental Health 13 (May 19, 2014): 903-108. doi: 10.1080/14999013.2014.906519.

Dzhekova, Rositsa, Mila Mancheva, Nadya Stoynova, and Dia Anagnostou. *Monitoring Radicalization: A Framework for Risk Indicators*. Sofia, Bulgaria: Center for the Study of Democracy, February 2017.

Easson, Joseph, and Alex Schmid. "250+ Academic, Governmental and Intergovernmental Defitions of Terrorism." In *The Routledge Handbook of Terrorism Research*, edited by Alex Schmid, 99-200. New York City, NY: Routledge, 2011. https://www.routledge.com/The-Routledge-Handbook-of-Terrorism-Research/Schmid/p/book/9780415520997.

Ecker, Ullrich, Stephan Lewandowsky, John Cook, Philipp Schmid, Lisa Fazio, Nadia Brashier, Panayiota Kendeou, et al. "The Psychological Drivers of Misinformation Belief and its Resistance to Correction." *Nature Reviews Psychology* 1 (January 12, 2022): 13-29. https://www.nature.com/articles/s44159-021-00006-y.

Ellis, Mark. "J. Edgar Hoover and the "Red Summer" of 1919." *Journal of American Studies* 28, no. 1 (April 1994): 39-59. https://history.msu.edu/files/2010/04/Mark-Ellis.pdf.

Eslick, Andrea, Lisa Fazio, and Elizabeth Marsh. "Ironic Effects of Drawing Attention to Story Errors." *Memory* 19, no. 2 (February 2, 2011): 184-191. doi: 10.1080/09658211.2010.543908.

Ethier, K. A., and K. Deaux. "Negotiating Social Identity when Contexts Change: Maintaining Identification and Responding to Threat." *Journal of Personality and Social Psychology* 67, no. 2 (1994): 243-251. https://doi.org/10.1037/0022-3514.67.2.243.

Executive Office of the President. *Strategic Implementation Plan for Empowering Local Partners to Prevent Violent Extremism in the United States*. Washington, DC: Executive Office of the President, December 2011. https://obamawhitehouse.archives.gov/sites/default/files/sip-final.pdf.

Fair, Gabriel, and Ryan Wesslen. "Data for Shouting into the Void: A Database of the Alternative Social Media Platform Gab. Paper presented at the Proceedings of the Thirteenth Annual International AAAI Conference on Web and Social Media, Munich, Germany, June 11-14, 2019. https://ojs.aaai.org/index.php/ICWSM/article/view/3258/3126.

FBI.gov Website. "Oklahoma City Bombing." Accessed June 16, 2022. https://www.fbi.gov/history/famous-cases/oklahoma-city-bombing.

Fazio, Lisa. "Pausing to Consider why a Headline is True or False can Help Reduce the Sharing of False News." *Harvard Kennedy School Misinformation Review*, February 10, 2010. https://doi.org/10.37016/mr-2020-009.

Federal Bureau of Investigation Behavioral Threat Assessment Center. *Lone Offender: A Study of Lone Offender Terrorism in the United States (1972-2015)*. Washington, DC: U.S. Department of Justice, Federal Bureau of Investigation, Behavioral Analysis Unit, National Center for the Analysis of Violent Crime, November 13, 2019. https://www.fbi.gov/file-repository/lone-offender-terrorism-report-111319.pdf/view.

Federal Bureau of Investigation (FBI) and Department of Homeland Security (DHS). *Strategic Intelligence Assessment and Data on Domestic Terrorism*. Washington, DC: FBI and DHS, May 2021. https://www.fbi.gov/file-repository/fbi-dhs-domestic-terrorism-strategic-report.pdf/view.

Federal Bureau of Investigation. *News*. Retrieved from FBI Behavioral Threat Assessment Center Releases Lone Offender Terrorism Report, November 13, 2019. https://www.fbi.gov/news/pressrel/press-releases/fbi-behavioral-threat-assessment-center-releases-lone-offender-terrorism-report.

Freilich, Joshua, Stephen Chermak, Roberta Belli, Jeff Gruenewald, and William Parkin. "Introducing the United States Extremist Crime Database (ECDB)." *Terrorism and Political Violence* 26 (November 20, 2013): 372-384. https://www.tandfonline.com/doi/full/10.1080/09546553.2012.713229.

Gill, Paul, and Emily Corner. "Lone-Actor Terrorist Target Choice." *Behavioral Sciences & the Law* 34 (November 20, 2016): 693-705. https://onlinelibrary.wiley.com/doi/10.1002/bsl.2268.

Github Website. "Pushsift Reddit API Documentation." Accessed June 16, 2022. https://github.com/pushshift/api.

Global Institute of Forensic Research Inc. Website. "TRAP-18 Manual & Code Sheets Annual User License." Accessed June 16, 2022. https://gifrinc.com/trap-18-manual/.

Goodman, Gerald F. "Black and White in Vietnam." *The New York Times*, July 18, 2017. https://www.nytimes.com/2017/07/18/opinion/racism-vietnam-war.html.

Goodwin, Jazmin. "Gab: Everything you need to know about the fast-growing, controversial social network." *CNN*, January 17, 2021. https://www.cnn.com/2021/01/17/tech/what-is-gab-explainer/index.html.

Government Accountability Office (GAO). *Countering Violent Extremism: Actions Needed to Define Strategy and Assess Progress of Federal Efforts*. Washington, DC: GAO, April 6, 2017. https://www.gao.gov/assets/gao-17-300.pdf.

"Governor Abbott Condemns U.S. Department of Defense's Vaccine Mandate and Refuses to Enforce it Against Texas National Guard." *Office of the Texas Governor*, December 16, 2021. https://gov.texas.gov/news/post/governor-abbott-condemns-u.s-department-of-defenses-vaccine-mandate-and-refuses-to-enforce-it-against-texas-national-guard.

Greifeneder, Rainer, Mariela Jaffé, Eryn Newman, and Norbert Schwartz. *The Psychology of Fake News: Accepting, Sharing, and Correcting Misinformation*. New York City, NY: Routledge, 2021.

Griffin, Ronald C. "A Black Perspective of the Military." *Negro History Bulletin* 36, no. 6 (October 1973): 133-136. https://www.jstor.org/stable/44175572?seq=1.

Guess, Andrew, Michael Lerner, Benjamin Lyons, Jacob Montgomery, Brendan Nyhan, Jason Reifler, and Neelanjan Sircar. "A Digital Media Literacy Intervention Increases Discernment between Mainstream and False News in the United States and India," *Proceedings from the National Academies of Sciences* 117, no. 27 (June 22, 2020): 15536-15545. https://www.pnas.org/doi/10.1073/pnas.1920498117.

Guhl, Jakob, and Jacob Davey. *A Safe Space to Hate: White Supremacist Mobilisation on Telegram*. London, UK: Institute for Strategic Dialogue, June 26, 2020. https://www.isdglobal.org/isd-publications/a-safe-space-to-hate-white-supremacist-mobilisation-on-telegram/.

Guy, Laura, Ira Packer, and William Warnken. "Assessing Risk of Violence Using Structured Professional Judgment Guidelines." *Journal of Forensic Psychology Practice* 12 (May 24, 2012): 270-283. 10.1080/15228932.2012.674471.

Hafez, Mohammed. “Radicalization in the Persian Gulf: Assessing the potential of Islamist militancy in Saudi Arabia and Yemen.” *Dynamics of Asymmetric Conflict* 1, no. 1 (July 28, 2008): 6-24. https://www.tandfonline.com/doi/full/10.1080/17467580802034000.

Hamburger, Ellis. “Facebook Increases Privacy on all New Posts by Default.” *The Verge*, May 22, 2014. https://www.theverge.com/2014/5/22/5739744/facebook-changes-default-privacy-of-posts-from-public-to-friends.

Hamilton, D.L., and S. J. Sherman. “Perceiving Persons and Groups.” *Psychological Review* 103, no. 2 (1996): 336-355. https://doi.org/10.1037/0033-295X.103.2.336.

Harden, Blaine. “Sailors Wearing Sheets Create Racial Incident Aboard Aircraft Carrier.” *The Washington Post*, September 6, 1979. https://www.washingtonpost.com/archive/local/1979/09/06/sailors-wearing-sheets-create-racial-incident-aboard-aircraft-carrier/cbc97c28-ff49-4221-9fbb-ffd1977905f7/.

Haynes, Robert V. “The Houston Mutiny and Riot of 1917.” *The Southwestern Historical Quarterly* 76, no. 4 (April 1973): 418-439. http://www.jstor.org/stable/30238208.

Hegghammer, Thomas. “Should I Stay or Should I Go? Explaining Variation in Western Jihadists' Choice between Domestic and Foreign Fighting.” *American Political Science Review* 107 no. 1 (January 28, 2013): 1-15. https://doi.org/10.1017/S0003055412000615.

Helmus, Leslie, and David Thornton. “Stability and Predictive and Incremental Accuracy of the Individual Items of Static-99r and Static 2002r in Predicting Sexual Recidivism: A Meta-Analysis.” *Criminal Justice and Behavior* 42 (February 12, 2015): 917-973. doi: 10.1177/0093854814568891.

Hemmingway, Theodore. “Prelude to Change: Black Carolinians in the War Years, 1914-1920.” *The Journal of Negro History* 65, no. 3 (Summer 1980): 223. https://www.journals.uchicago.edu/doi/10.2307/2717096.

Herman, Agatha, and Richard Yarwood. “From Services to Civilian: The Geographies of Veterans Post-Military Lives.” *Geoforum* 53 (May 2014): 41-50. doi: 10.1016/j.geoforum.2014.02.001.

History.com Editors. “Army Major Kills 13 People in Fort Hood Shooting Spree.” *History.com*, last updated April 8, 2022. https://www.history.com/this-day-in-history/army-major-kills-13-people-in-fort-hood-shooting-spree.

History.com Editors. “Olympic Park Bomber Eric Rudolph Agrees to Plead Guilty.” *History.com*, last updated April 8, 2022. https://www.history.com/this-day-in-history/olympic-park-bomber-eric-rudolph-agrees-to-plead-guilty.

Hogg, Michael A., “Uncertainty-Identity Theory.” Vol. chap. 29 in *Handbook of Theories of Social Psychology*, edited by Paul A. M. Van Lange, Arie W, Jruglanski, and E. Tory Higgins. London, UK: SAGE Publications Ltd., 2012: 62-80. https://doi.org/10.4135/9781446249222.n29.

Holles, Everett R. “Marines in Klan Openly Abused Blacks at Pendleton, Panel Hears.” *The New York Times*, January 9, 1977. https://www.nytimes.com/1977/01/09/archives/marines-in-klan-openly-abused-blacks-at-pendleton-panel-hears.html?searchResultPosition=1.

Hollewell, Georgia, and Nicholas Longpré. "Radicalization in the Social Media Era: Understanding the Relationship between Self-Radicalization and the Internet." *International Journal of Offender Therapy and Comparative Criminology* 66, no. 8 (June 30, 2021). doi:10.1177/0306624X211028771.

Hughes, Brian, and Cynthia Miller-Idriss. "Uniting for Total Collapse: The January 6 Boost to Accelerationism." *CTC Sentinel* 14, no. 4 (April/May 2021): 12-17. https://ctc.usma.edu/uniting-for-total-collapse-the-january-6-boost-to-accelerationism/.

Huguet, Alice, Jennifer Kavanagh, Garrett Baker, and Marjory Blumenthal. *Exploring Media Literacy Education as a Tool for Mitigating Truth Decay*. Santa Monica, CA: RAND Corporation, 2019. https://www.rand.org/pubs/research_reports/RR3050.html.

Independent Review Commission. *Hard Truths and the Duty to Change: Recommendations from the Independent Review Commission on Sexual Assault in the Military*. Washington, DC: Independent Review Commission, June 2021. https://media.defense.gov/2021/Jul/02/2002755437/-1/-1/0/IRC-FULL-REPORT-FINAL-1923-7-1-21.PDF/IRC-FULL-REPORT-FINAL-1923-7-1-21.PDF.

Institute for Strategic Dialogue. *Accelerationism: An Overview of Extremist Narratives about the Need for Societal Collapse to Preserve the White Race*. London, UK: Institute for Strategic Dialogue, 2021. https://www.isdglobal.org/wp-content/uploads/2021/09/Accelerationism-External-May-2021.pdf.

James, Laura. "Army Unveils Memorial to a Black Soldier Lynched on Military Base 80 Years Ago." *CNN*, August 4, 2021. https://www.cnn.com/2021/08/03/us/felix-hall-soldier-lynched-memorial-fort-benning/index.html.

Jensen, Michael. *Discussion Point: The Benefits and Drawbacks of Methodological Advancements in Data Collection and Coding: Insights from the Global Terrorism Database (GTD)*. College Park, MD: National Consortium for the Study of Terrorism and Responses to Terrorism (START), 2013. https://www.start.umd.edu/publication/discussion-point-benefits-and-drawbacks-methodological-advancements-data-collection-and.

Jensen, Michael, Anita Seate, and Patrick James. "Radicalization to Violence: A Pathway Approach to Studying Extremism." Terrorism and Political Violence 32, no. 5 (April 9, 2018): 1067-1090. https://www.tandfonline.com/doi/full/10.1080/09546553.2018.1442330.

Jensen, Michael, Elizabeth Yates, and Sheehan Kane. *Extremism in the Ranks and After*. College Park, MD: National Consortium for the Study of Terrorism and Responses to Terrorism (START), July 2021. https://www.start.umd.edu/news/start-releases-new-data-extremism-among-us-service-members-and-veterans.

Jensen, Michael, Elizabeth Yates, and Sheehan Kane. *Extremism in the Ranks and After*. College Park, MD: National Consortium for the Study of Terrorism and Responses to Terrorism (START), December 2021. https://www.start.umd.edu/publication/extremism-ranks-and-after.

Jensen, Michael, Elizabeth Yates, and Sheehan Kane. *Radicalization in the Ranks: An Assessment of the Scope and Nature of Criminal Extremism in the United States Military*. College Park, MD: National Consortium for the Study of Terrorism and Responses to

Terrorism (START), April 2022. https://www.start.umd.edu/publication/radicalization-ranks.

Jerit, Jennnifer, and Yangzi Zhao, Y. "Political Misinformation." *Annual Review of Political Science* 23 (May 2020): 77-94. 10.1146/annurev-polisci-050718-032814.

Jettin, J., M.A.Hogg, and B.-A. Mullin. "In-Group Variability and Motivation to Reduce Subjective Uncertainty," *Group Dynamics: Theory, Research, and Practice* 4, no. 2 (2000): 184-198. https://doi.org/10.1037/1089-2699.4.2.184.

Joint Service Committee on Military Justice. *Manual for Courts-Martial*. 2016 ed. Marine Corps Publications Electronic Library.

Joint Service Committee on Military Justice. *Manual for Courts-Martial*. 2019 ed. Marine Corps Publications Electronic Library.

Jones, Seth, Catrina Doxsee, Grace Hwang, and Jared Thompson. *Methodology and Codebook. The Military, Police, and the Rise of Terrorism in the United States*. Washington, DC: Center for Strategic & International Studies (CSIS), April 12, 2021. https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/210412_Jones_Methodology.pdf?mG2pmLJmpc4OAKQdPDm8n.9cWaDW8Pj4.

Jones, Seth, Catrina Doxsee, Grace Hwang, and Jared Thompson. *The Military, Police, and the Rise of Terrorism in the United States*. Washington, DC: Center for Strategic & International Studies (CSIS), April 12, 2021. https://www.csis.org/analysis/military-police-and-rise-terrorism-united-states.

Kaplan, Shawn. "A Typology of Terrorism." *Review Journal of Political Philosophy* 6, no. 1 (2008): 1-38. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1460938.

Klausen, Jytte, Tyler Morrill, and Rosanne Liberetti. "The Terrorist Age-Crime Curve: An Analysis of American Islamist Terrorist Offenders and Age-Specific Propensity for Participation in Violent and Nonviolent Incidents." Social Science Quarterly 97, no. 1 (February 26, 2016): 19-32. https://onlinelibrary.wiley.com/doi/10.1111/ssqu.12249.

Klein, Kristen, and Arie Kruglanski. "Commitment and Extremism: A Goal Systemic Analysis." *Journal of Social Issues* 69, no. 3 (September 9, 2013): 419-435. https://spssi.onlinelibrary.wiley.com/doi/abs/10.1111/josi.12022.

Kleykamp, Meredith, Sidra Montgomery, Alexis Pang, and Kristin Schrader. "Military Identity and Planning for the Transition out of the Military." *Military Psychology* 33, no. 6 (2021): 372-391. https://www.tandfonline.com/doi/full/10.1080/08995605.2021.1962176.

Kraig, Beth. "The Unquiet Death of Guglielmo Olivotto." *Peace and Change* 30, no. 3 (July 2005): 295-328. doi:10.1111/j.1468-0130.2005.00322.

Kruglanski, Arie, Katarzyna Jasko, David Webber, Marina Chernikova, and Erica Molinario. "The Making of Violent Extremists." *Review of General Psychology* 22, no. 1 (March 1, 2018): 107-120. https://journals.sagepub.com/doi/10.1037/gpr0000144.

Kruglanski, Arie, Michele Gelfand, Jocelyn Belanger, Anna Sheveland, Malkanthi Hetiaranchchi, and Rohan Gunaratna. "The Psychology of Radicalization and Deradicalization: How Significance Quest Impacts Violent Extremism." Political

Psychology 35, no. 1 (February 2014), 69-93. https://onlinelibrary.wiley.com/doi/10.1111/pops.12163.

Kruglanski, A. W., A. Pierro, L. Mannetti, and E. De Grada. "Groups as Epistemic Providers: Need for Closure and the Unfolding of Group-Centrism," *Psychological Review* 113, no. 1 (January 2006): 84-100. doi: 10.1037/0033-295X.113.1.84.

Krugler, David F. "1919: Defending Black Lives." *Washington History* 32, no. ½ (Fall 2020): 27-30. https://www.jstor.org/stable/26947511?seq=1.

Krugler, David F. "A Mob in Uniform: Soldiers and Civillians in Washington's Red Summer, 1919." *Washington History* 21 (2009): 48-77. https://www.jstor.org/stable/25704908?pq-origsite=360link?pq-origsite=360link.

Lacassagne, Doris, Jeremy Béna, and Olivier Corneille. "Is Earth a Perfect Square? Repetition Increases the Perceived Truth of Highly Implausible Statements." Cognition 223 (June 2022). https://www.sciencedirect.com/science/article/pii/S0010027722000403.

LaFree, Gary, and Laura Dugan. "Introducing the Global Terrorism Database." Terrorism and Political Violence 19 (April 4, 2007): 181–204. http://ccjs.umd.edu/sites/ccjs.umd.edu/files/pubs/FTPV_A_224594.pdf.

LaFree, Gary, and Anina Schwarzenbach. "Micro and Macro-Level Risk Factors for Extremism and Terrorism: Toward a Criminology of Extremist Violence," *Monatsschrift für Kriminologie und Strafrechtsreform* 104, no. 3 (August 18, 2021): 184-202. https://www.degruyter.com/document/doi/10.1515/mks-2021-0127/html?lang=en.

LaFree, Gary, Bo Jiang, and Lauren Porter. "Prison and Violent Political Extremism in the United States. *Journal of Quantitative Criminology* 36, no. 3 (April 16, 2019): 1-26. https://link.springer.com/article/10.1007/s10940-019-09412-1.

LaFree, Gary, Michael Jensen, Patrick James, and Aaron Safer-Lichtenstein. "Correlates of Violent Political Extremism in the United States." Criminology 56, no. 2 (February 2, 2018): 233-268. https://onlinelibrary.wiley.com/doi/abs/10.1111/1745-9125.12169.

LaFree, Gary, Michael Jensen, Sheehan Kane, et al. *Profiles of Individual Radicalization in the United States (PIRUS)*. College Park, MD: National Consortium for the Study of Terrorism and Responses to Terrorism (START), 2018. https://www.start.umd.edu/data-tools/profiles-individual-radicalization-united-states-pirus.

LaFree, Gary, and Laura Dugan. "Introducing the Global Terrorism Database." *Terrorism and Political Violence* 19, no. 2 (July 2007): 181-204. https://ccjs.umd.edu/sites/ccjs.umd.edu/files/pubs/FTPV_A_224594.pdf.

Laqueur, Walter. *The Age of Terrorism*. New York City, NY: Little Brown and Company, 1987.

Lee, Dave. "Instagram now asks Bullies: 'Are you Sure?'" *BBC News*, July 8, 2019. www.bbc.com: https://www.bbc.com/news/technology-48916828?

Lee, E. "Hate Perspective on Terror: Domestic and International." Chap. 2 Vol. 3 in *The Psychology of Hate Crimes as Domestic Terrorism: U.S. and Global Issues*, edited by Edward Dunbar, Amalio Blanco, and Desirée A. Crèvecoeur-MacPhail. Santa Barbara, CA: Praeger, November 2016.

Lepre, George. *Fragging: Why U.S. Soldiers Assaulted Their Officers in Vietnam*. Lubbock, TX: Texas Tech University, 2011.

Levinsson, Anna, Diana Miconi, Zhiyin Li, Rochelle L. Frounfelker, and Cécile Rousseau. "Conspiracy Theories, Psychological Distress, and Symapthy for Violent Radicalization in Young Adults During the COVID-19 Pandemic: A Cross-Sectional Study." *International Journal of Environmental Research and Public Health* 18, no. 15 (July 24, 2021):7846-7858. doi:10.3390/ijerph18157846.

Lewandowsky, Stephan, Ullrich K. H. Ecker, Colleen. M. Seifert, Norbert Schwarz, and John Cook. "Misinformation and its Correction: Continued Influence and Successful Debiasing." *Psychological Science in the Public Interest* 13, no. 3 (September 17, 2012): 106-131. doi:10.1177/1529100612451018.

Lickel, B., D. L. Hamilton, G. Wieczorkowska, A. Lewis, S. J. Sherman, and A. N. Uhles. "Varieties of Groups and the Perception of Group Entitativity," *Journal of Personality and Social Psychology* 78, no. 2 (2000): 223-246. https://doi.org/10.1037/0022-3514.78.2.223.

Liht, Jose, and Sara Savage. "Preventing Violent Extremism Through Value Complexity: Being Muslim Being British." *Journal of Strategic Security* 6 no. 4 (2013): 44-66. doi:10.5038/1944-0472.6.4.3.

Logan, Caroline, and Monica Lloyd. "Violent Extremism: A Comparison of Approaches to Assessing and Managing Risk." *Legal and Criminological Psychology* 24, no. 1 (August 29, 2018): 141-161. doi:10.1111/lcrp.12140.

Lösel, Friedrich, Sonja King, Doris Bender, and Irina Jugl. "Protective Factors Against Extremism and Violent Radicalization: A Systematic Review of Research." International Journal of Developmental Science 12, no. 1-2 (2018): 89-102. https://content.iospress.com/articles/international-journal-of-developmental-science/dev170241.

Marine Corps Recruiting Command. "Participation in Gangs, Extremist Organizations or Activities." MCRCO 1100.1. Quantico, VA: United States Marine Corps, November 9, 2011. 3-107. https://www.yumpu.com/en/document/read/40514012/mcrco-11001-headquarters-marine-corps.

Marine Corps Warfighting Publication (MCWP) 6-10 (Formerly 6-11). *Leading Marines*, PCN 143 001290 00. Washington, DC: Headquarters United States Marine Corps, January 23, 2019. 1-2. https://www.marines.mil/portals/1/Publications/MCWP%206-10.pdf?ver=2018-09-20-104415-507.

Marines.mil Website. "About the Marine Corps Values." Accessed June 16, 2022. https://www.hqmc.marines.mil/hrom/New-Employees/About-the-Marine-Corps/Values/.

Marines.mil Website. "Marine for Life (M4L) Program/Expanded Transition Assistance." Accessed June 16, 2022. https://www.marines.mil/News/Messages/Messages-Display/Article/886845/marine-for-life-m4l-programexpanded-transition-assistance/.

Marshall, Jack. "Gallup's Institutional Trust Poll." *Ethics Alarms*, July 18, 2021. https://ethicsalarms.com/2021/07/18/gallups-institutional-trust-poll/.

Martin, Jonathan. "U.S. Army Overturns Convictions of Ft. Lawton Soldiers Court-Martialed in 1994 After Riot, Lynching." *Seattle Times*, October 26, 2007. https://www.seattletimes.com/seattle-news/us-army-overturns-convictions-of-fort-lawton-soldiers-court-martialed-in-1944-after-riot-lynching/.

Marwick, Alice, and Rebecca Lewis. *Media Manipulation and Disinformation Online*. New York City, NY: Data & Society, May 2017. http://www.chinhnghia.com/DataAndSociety_MediaManipulationAndDisinformationOnline.pdf.

Mastroe, Caitlin, and Susan Szmania. *Surveying CVE Metrics in Prevention, Disengagement and Deradicalization Programs*. College Park, MD: START, March 2016. https://www.start.umd.edu/pubs/START_SurveyingCVEMetrics_March2016.pdf.

McCauley, Clark, and Sophia Moskalenko. "Understanding Political Radicalization: The Two-Pyramids Model." *American Psychologist* 72 no. 3 (April 2017): 205-216. doi:10.1037/amp0000062.

McCord, Mary. *Filling the Gap in our Terrorism Statutes*. Washington, DC: The George Washington University Program on Extremism, August 2019. https://extremism.gwu.edu/sites/g/files/zaxdzs2191/f/Filling%20The%20Gap%20in%20Our%20Terrorism%20Statutes.pdf.

McCormik, Gordon H. "Terrorist Decision Making." *Annual Review of Political Science* 6 (June 2003): 473-507. doi:10.1146/annurev.polisci.6.121901.085601.

McGuire, W. J., and D. Papageorgis. (1961). "The Relative Efficacy of Various Types of Prior Belief-Defense in Producing Immunity Against Persuasion." *The Journal of Abnormal and Social Psychology* 62, no. 2 (March 1961): 327-337. doi:10.1037/h0042026.

McGurk, Dennis, Dave I. Cotting, Thomas Watson Britt, and Amy Alder. "Joinging the Ranks: The Role of Indoctrination in Transforming Civilians to Service Members." Volume 2, chap. 2 in *Military Life: The Psychology of Serving in Peace and Combat*, edited by Amy B. Alder, Carl A. Castro, and Thomas W. Britt. Westport, CT: Praeger Security International, 2005. 13-31. https://www.researchgate.net/publication/272745413_Joining_the_Ranks_The_Role_of_Indoctrination_in_transforming_Civilians_to_Service_Members.

Meloy, J. R., Karoline Roshdi, Justine Glaz-Ocik, and Jens Hoffmann. "Investigating the Individual Terrorist in Europe." *Journal of Threat Assessment Management* 2, no. 3-4 (September 2015): 140-152. doi:10.1037/tam0000036.

Miller, Erin, and Kathleen Smarick. *Profiles of Perpetrators of Terrorism in the United States*. College Park, MD: START, July 2014. https://www.start.umd.edu/pubs/START_ProfilesofPerpetratorsofTerrorismintheUS_ResearchHighlight_July2014.pdf.

Miller, Erin, and Kathleen Smarick, "Profiles of Perpetrators of Terrorism in the United States," *Harvard Dataverse, V7*. doi: https://doi.org/10.7910/DVN/IO1RYI.

Miller, Gregory D. "Blurred Lines: The New 'Domestic' Terrorism." Perspectives on Terrorism 13, no. 3 (June 2019): 63-75. https://www.researchgate.net/publication/333676937_Blurred_Lines_The_New_Domestic_Terrorism.

Miller, Joyce. "REsilience, Violent Extremism, and Religious Education." British Journal of Religious Education 35, no. 2 (November 23, 2012): 188-200. doi:10.1080/01416200.2012.740444.

Milton, Daniel, and Andrew Mines. *"This is War:" Examining Military Experience Among the Capitol Hill Siege Participants*. Washington, DC: Program on Extremism at George Washington University, Combatting Terrorism Center at West Point, April 12, 2021. https://ctc.usma.edu/this-is-war-examining-military-experience-among-the-capitol-hill-siege-participants/.

Mosleh, Mohsen, Gordon Pennycook, Antonio A. Arechar, and David G. Rand. "Cognitive Reflection Correlates with Behavior on Twitter." *Nature Communications* 12 (February 10, 2021): 921. doi:10.1038/s41467-020-20043-0.

National Authorization Act for Fiscal Year 2022, Rules Committee Print 117-21, Text of House Amendment to S. 1605, December 7, 2021, https://rules.house.gov/sites/democrats.rules.house.gov/files/BILLS-117S1605-RCP117-21.pdf.

National Consortium for the Study of Terrorism and Responses to Terrorism. "Terrorism and Extremist Violence in the United States Database (TEVUS)." Accessed June 17, 2022. https://www.start.umd.edu/research-projects/terrorism-and-extremist-violence-united-states-tevus-database.

National Consortium for the Study of Terrorism and Responses to Terrorism. *Global Terrorism Database: Codebook: Methodology, Inclusion Criteria, and Variables*. College Park, MD: University of Maryland, August 2021. https://www.start.umd.edu/gtd/downloads/Codebook.pdf.

National Consortium for the Study of Terrorism and Responses to Terrorism Website. "PIRUS – Frequently Asked Questions, Is the PIRUS dataset a *representative* sample of individuals radicalized in the United States?" Accessed June 16, 2022, https://www.start.umd.edu/pirus-frequently-asked-questions#q12.

National Consortium for the Study of Terrorism and Responses to Terrorism (START) Website. "PIRUS – Frequently Asked Questions, What is PIRUS?" Accessed June 16, 2022. https://www.start.umd.edu/pirus-frequently-asked-questions#q12.

National Counterterrorism Center, Department of Justice, Department of Homeland Security. *Domestic Terrorism Conference Report*. n.p.: January 2020. https://www.dni.gov/files/2020-01-02-DT_Conference_Report.pdf.

National Defense Authorization Act for Fiscal Year 2020 Pub. L. 116-92. "Domestic Terrorism: Definitions, Terminology, and Methodology." November 2020. https://www.fbi.gov/file-repository/fbi-dhs-domestic-terrorism-definitions-terminology-methodology.pdf/view.

National Defense Authorization Act for Fiscal Year 2022. Rules of Committee Print 117-21: Text of House Amendment to S. 1605. https://rules.house.gov/sites/democrats.rules.house.gov/files/BILLS-117S1605-RCP117-21.pdf.

National Public Radio (NPR). "Why the Government Can't Bring Terrorism Charges in Charlottesville." *NPR*, August 14, 2017. https://www.cpr.org/2017/08/14/why-the-government-cant-bring-terrorism-charges-in-charlottesville/.

National Threat Assessment Center. *Enhancing School Safety Using a Threat Assessment Model: An Operational Guide for Preventing Targeted School Violence*. Washington, DC: U.S. Department of Homeland Security, United States Secret Service, National Threat Assessment Center, July 2018. https://www.cisa.gov/sites/default/files/publications/18_0711_USSS_NTAC-Enhancing-School-Safety-Guide.pdf.

Navy.mil Website. "Our Core Values." Accessed June 16, 2022. https://www.navy.mil/About/Our-Core-Values/.

Alathari, Lina, Diana Drysdale, Steven Driscoll, Ashley Blair, David Mauldin, Arna Carlock, Jeffrey McGary, et al. *Averting Targeted School Violence: A U.S. Secret Service Analysis of Plots Against Schools*. Washington, DC: U.S. Department of Homeland Security, United States Secret Service, National Threat Assessment Center, March 2021. https://www.secretservice.gov/sites/default/files/reports/2021-03/USSS%20Averting%20Targeted%20School%20Violence.2021.03.pdf.

Newhouse, Alex. "The Threat is the Network: The Multi-Node Structure of Neo-Fascist Accelerationsim." *CTC Sentinel* 14, no. 5 (June 2021): 17-25. https://ctc.usma.edu/wp-content/uploads/2021/05/CTC-SENTINEL-052021.pdf.

Neumann, Peter R. (2013). "The Trouble with Radicalization." *Internal Affairs* 89, no.4 (July 2013): 873-893. doi:10.1111/1468-2346.12049.

Nicas, Jack, and Davey Alba. "How Parler, a Chosen App of Trump Fans, Became a Test of Free Speech." *The New York Times*, updated February 15, 2021. https://www.nytimes.com/2021/01/10/technology/parler-app-trump-free-speech.html.

Oaks, Penelope J. "The Salience of Social Categories." Chap. 6 in Rediscovering the Social Group: A Self-Categorization Theory. Edited by John C. Turner, Michael A Hogg, Penelope J. Oakes, Stephen D. Rieche, and Margaret S. Wetherell. Oxford, UK: Blackwell, 1987. 117-141. https://www.semanticscholar.org/paper/Rediscovering-the-social-group%3A-A-theory.-Turner-Hogg/469c5d279c5e0625f730f98dc07d2d8b875a2e82.

Office of the Director of National Intelligence. *Security Executive Agent Directive 4: National Security Adjudicative Guidelines*. n.p.: Office of the Director of National Intelligence, December 10, 2016. https://www.dni.gov/files/NCSC/documents/Regulations/SEAD-4-Adjudicative-Guidelines-U.pdf.

Office of the Director of National Intelligence. *Security Executive Agent Directive 5: Collection, Use, and Retention of Publicly Available Social Media Information in Personnel Security Background Investigations and Adjudications*. n.p. Office of the Director of National Intelligence, May 12, 2016. https://www.odni.gov/files/NCSC/documents/Regulations/SEAD_5.pdf.

Office of the Under Secretary of Defense for Personnel and Readiness. *Prevention Plan of Action 2019-2023: The Department's Renewed Strategic Approach to Prevent Sexual Assault*. Washington, DC: Department of Defense, April 2019. https://www.sapr.mil/sites/default/files/PPoA_Final.pdf.

Office of Personnel Management. *Standard Form 85: Questionnaire for Non-Sensitive Positions*. n.p.: Office of Personnel Management, December 2013. https://www.opm.gov/forms/pdf_fill/sf85.pdf.

Office of Personnel Management. Code of Federal Regulations, Title 5, Chapter 1. n.p.: Office of Personnel Management, 2012. https://www.ecfr.gov/current/title-5/chapter-I.

Office of the Under Secretary of Defense for Personnel and Readiness. *DoD Instruction 1332.35: Transition Assistance Program (TAP) for Military Personnel*. Washington, DC: Department of Defense, September 26, 2019. https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/133235p.pdf?ver=2019-09-26-095932-007.

Ortbals, Candice D., and Lori Poloni-Staudinger. Gender and Political Violence: Women Changing the Politics of Terrorism. Cham, Switzerland: Springer, 2018.

Ou, Adrienne. "Hearts and Minds: A Comparison of the Counter-Radicalization Strategies in Britain and the United States." *Cornell International Affairs Review* 9, no. 2 (2016): 1-3. http://www.inquiriesjournal.com/articles/1413/hearts-and-minds-a-comparison-of-counter-radicalization-strategies-in-britain-and-the-united-states.

Pagán, Eduardo Obregón. "Los Angeles Geopolitics and the Zoot Suit Riot, 1943." *Social Science History* 24, no. 1 (April 200): 223-256. https://www.cambridge.org/core/journals/social-science-history/article/abs/los-angeles-geopolitics-and-the-zoot-suit-riot-1943/88C78F0516856B0B8157585685882E06.

Parker, Jade. "Accerlationism in America: Threat Perceptions." *Global Network on Extremism & Technology*, February 4, 2020. https://gnet-research.org/2020/02/04/accelerationism-in-america-threat-perceptions/.

Parker V. Levy. 417 U.S. 733 (Supreme Court. 1974).

Pennycook, Gordon, and David G. Rand. "Fighting Misinformation on Social Media Using Crowdsourced Judgments of News Source Quality." *Proceedings from the National Academies of Sciences of the United States of America* 116, no. 7 (January 28, 2019): 2521-2526. doi:10.1073/pnas.1806781116.

Pennycook, Gordon, and David G. Rand. (2019). "Lazy, Not Biased: Susceptibility to Partisan Fake News is Better Explained by Lack of Reasoning Than by Motivated Reasoning." *Cognition* 188 (July 2019): 39-50. doi:10.1016/j.cognition.2018.06.011.

Pennycook, Gordon, James Allen Cheyne, Paul Seli, Derek J. Koehler, and Jonathan A. Fugelsang. "Analytic Cognitive Style Predicts Religious and Paranormal Belief." *Cognition* 123, no. 3 (June 2012): 335-346. doi:10.1016/j.cognition.2012.03.003.

Perliger, Arie. "CARR Policy Insight Series: Deciphering the Second Wave of the American Militia Movement." *Centre for Analysis of the Radical Right*, January 7, 2021. https://www.radicalrightanalysis.com/2021/01/07/carr-policy-insight-series-deciphering-the-second-wave-of-the-american-militia-movement/.

Pfau, Michael, David Park, R. Lance Holbert, and Jaeho Cho. (2001). "The Effects of Party-and PAC Sponsored Issue Advertising and the Potential of Inoculation to Combat its Impact on the Democratic Process." *American Behavioral Scientist* 44, no. 12 (August 2001): 2379-2397. https://www.researchgate.net/publication/247751775_The_Effects_of_Party_and_PAC-Sponsored_Issue_Advertising_and_the_Potential_of_Inoculation_to_Combat_its_Impact_on_the_Democratic_Process.

Philipps, Dave. “White Supremacism in the U.S. Military, Explained.” *The New York Times*, February 27, 2019. https://www.nytimes.com/2019/02/27/us/military-white-nationalists-extremists.html.

Pickett, Cynthia L., and Marilynn B. Brewer. “Assimilation and Differentiation Needs as Motivational Determinants of Perceived In-Group and Out-Group Homogeneity.” *Journal of Experimental Social Psychology* 37, no. 4 (July 2001): 341-348. https://doi.org/10.1006/jesp.2000.1469

Poppe, Katharine. *Nidal Hasan: A Case Study in Lone-Actor Terrorism.* Washington, DC: George Washington University, Program on Extremism, October 2018. https://extremism.gwu.edu/sites/g/files/zaxdzs2191/f/Nidal%20Hasan.pdf.

Pressman, D. Elaine, and John Flockton. “Calibrating Risk for Violent Political Extremists and Terrorists: The VERA 2 Structured Assessment.” *British Journal of Forensic Practice* 14, no. 4 (November 16, 2012): 237-251. doi:10.1108/14636641211283057.

Pushshift.io Website. “Full List of Pushshift Reddit Specific Parameters.” Accessed June 16, 2022. https://pushshift.io/api-parameters/.

Pyrooz, David C., Gary LaFree, Scott H. Decker, and Patrick A. James. "Cut from the Same Cloth? Comparing Gangs and Violent Political Extremists." Justice Quarterly, 35, no. 1 (May 18, 2017): 1-32. https://www.tandfonline.com/doi/full/10.1080/07418825.2017.1311357.

Quartermaine, Angela. “Discussing Terrorism: A Pupil-Inspired Guide to UK Counterterrorism Policy Implementation in Religious Education Classrooms in England.” *British Journal of Religious Education* 38, no. 1 (September 5, 2014): 13-29. doi:10.1080/01416200.2014.953911.

Clionadh Raleigh, Andrew Linke, Håvard Hegre, and Joakim Karlsen. "Introducing ACLED: An Armed Conflict Location and Event Dataset: Special Data Feature." Journal of Peace Research 47, no. 5 (September 28, 2010): 651–660. doi: 10.1177/0022343310378914.

Rapp, David N., Scott R. Hinze, Kristine Kohlhepp, and Rachel A. Ryskin. “Reducing Reliance on Inaccurate Information.” *Memory & Cognition* 42 (June 13, 2013): 11-26. doi:10.3758/s13421-013-0339-0.

Reichenbach, Sarah Chaney. “CVE and Constitutionality in the Twin Cities: How Countering Violent Extremism Threatens the Equal Protection Rights of American Muslims in Minneapolis-St. Paul.” *American University Law Review* 69 no. 6 (2020): 1989-2046. https://digitalcommons.wcl.american.edu/cgi/viewcontent.cgi?article=2222&context=aulr.

Richter, Tobias, and David N. Rapp. “Comprehension and Validation of Text Information: Introduction to the Special Issue.” *Discourse Processes* 51, no. 1-2 (January 9, 2014): 1-6. doi: 10.1080/0163853X.2013.855533.

Roof, Dylann. *The Last Rhodesian: The Manifesto's of Dylann Roof*. n.p.: Create Space Independent Publishing Platform, October 5, 2017.

Rose, Andrée, Howard Timm, Corrie Pogson, Jose Gonzalez, Edward Appel, and Nancy Kolb. *Developing a Cybervetting Strategy for Law Enforcement*. Alexandria, VA: International

Association of Chiefs of Police and PERSEREC, December 2010. https://www.theiacp.org/sites/default/files/2018-08/CybervettingReport-2.pdf.

Rottweiler, Bettina, and Paul Gill. "Conspiracy Beliefs and Violent Extremist Intentions: The Contingent Effects of Self-Efficacy, Self Control, and Law-Related Morality." Terrorism and Political Violence (October 20, 2020): 1-20. https://www.tandfonline.com/doi/full/10.1080/09546553.2020.1803288.

Rousis, Gregory J., F. Dan Richard, and Dong-Yuan Debbie Wang. "The Truth is out There: The Prevalence of Conspiracy Theory Use by Radical Violent Extremist Organizations." *Terrorism and Political Violence* (November 19, 2020): 1-19. doi:10.1080/09546553.2020.1835654.

Roychowdhury, Ashimesh, and Gwen Adshead. "Violence Risk Assessment as a Medical Intervention: Ethical Tensions." *Psychiatric Bulletin* 38, no. 2 (April 2014): 75-82. doi:10.1192/pb.bp.113.043315.

RTI International. *Countering Violent Extremism: The Application of Risk Assessment Tools in the Criminal Justice and Rehabilitation Process*. Research Triangle Park, NC: RTI International, February 2018. https://www.dhs.gov/sites/default/files/publications/OPSR_TP_CVE-Application-Risk-Assessment-Tools-Criminal-Rehab-Process_2018Feb-508.pdf.

Sacco, Lisa N. Sifting Domestic Terrorism from Hate Crime and Homegrown Violent Extremism. Washington, DC: Congressional Research Service, January 15, 2021. https://www.everycrsreport.com/files/2021-01-15_IN10299_572203b7de901830d66301cbd676c81a3cab67b9.pdf.

Sageman, Marc. *Understanding Terror Networks*. Philadelphia, PA: University of Pennsylvania Press, May 14, 2004.

Salovich, Nikita A., and David N. Rapp. "Misinformed and Unaware? Metacognition and the Influence of Inaccurate Information." *Journal of Experimental Psychology: Learning, Memory, and Cognition* 47, no. 4 (April 2021): 608-624. doi:10.1037/xlm0000977.

Sampson, Robert J. and Dawn Jeglum Bartusch. "Legal Cynicism and (Subcultural?) Tolerance of Deviance: The Neighborhood Context of Racial Differences." *Law & Society Review* 32, no. 4 (1998): 777-804. https://doi.org/10.2307/827739.

Sarma, Kiran M. "Risk Assessment and the Prevention of Radicalization from Nonviolence into Terrorism." *American Psychologist* 72 no. 3 (April 2017): 278-288. doi:10.1037/amp0000121.

Schmid, Alex. "Terrorism-The Definitional Problem." *Case Western Reserve Journal of International Law* 36, no. 2 (2004): 375-419. https://scholarlycommons.law.case.edu/jil/vol36/iss2/8/.

Schmid, Alex. "The Definition of Terrorism," in *The Routledge Handbook on Terrorism Research*, edited by Alex Schmid. New York City, NY: Routledge, 2011.

Schmidt, William E. "Soldiers Said to Attend Klan-Related Activities." *The New York Times*, April 15, 1986. https://www.nytimes.com/1986/04/15/us/soldiers-said-to-attend-klan-related-activities.html.

Schuler, Edgar A. “Race Riots During and After the First World War.” *Negro History Bulletin* 7, no. 7 (April 1944): 155-156, 158-160, 166. https://www.jstor.org/stable/44212138?seq=1.

Scruton, Roger. The Palgrave Macmillan Dictionary of Political Thought (3rd ed.). New York City, NY: Palgrave Macmillan, February 7, 2007.

Secretary of Defense. “Memorandum for Senior Pentagon Leadership Commanders of the Combatant Commands Defense Agency and DOD Field Activity Directors: Immediate Actions to Counter Extremism in the Department and the Establishment of the Countering Extremism Working Group.” Memorandum. Washington, DC: Department of Defense, April 9, 2021. https://media.defense.gov/2021/Apr/09/2002617921/-1/-1/1/MEMORANDUM-IMMEDIATE-ACTIONS-TO-COUNTER-EXTREMISM-IN-THE-DEPARTMENT-AND-THE-ESTABLISHMENT-OF-THE-COUNTERING-EXTREMISM-WORKING-GROUP.PDF.

Secretary of Defense. “Memorandum for Senior Pentagon Leadership Defense Agency and DOD Field Agency Activity Directors: Stand-Down to Address Extremism in the Ranks.” Memorandum. Washington, DC: Department of Defense, February 5, 2021. https://media.defense.gov/2021/Feb/05/2002577485/-1/-1/0/STAND-DOWN-TO-ADDRESS-EXTREMISM-IN-THE-RANKS.PDF.

Secretary of Defense, “Memorandum for Senior Pentagon Leadership, Commanders of the Combatant commands, and Defense Agency and DOD Field Activity Directors: Immediate Actions to Counter Sexual Assault and Harassment and the Establishment of a 90-Day Independent Review Commission on Sexual Assault in the Military” (memorandum, Washington, DC: Department of Defense, February 26, 2021), https://media.defense.gov/2021/Feb/26/2002590163/-1/-1/0/APPROVAL-OF-MEMO-DIRECTING-IMMEDIATE-ACTIONS-TO-COUNTER-SEXUAL-ASSAULT-AND-HARASSMENT.PDF.

Sherwood, John Darrell. *Black Sailor, White Navy: Racial Unrest in the Fleet During the Vietnam Era.* New York City, NY: New York University Press, November 2007.

Singer, Murray. “Challenges in Processes of Validation and Comprehension.” *Discourse Processes* 56, no. 5-6 (April 19. 2019): 1-19. doi:10.1080/0163853X.2019.1598167.

Sinnar, Shirin. “Separate and Unequal: The Law of “Domestic” and “International” Terrorism.” *Michigan Law Review* 117, no. 7 (May 2019): 1333-1404. doi:10.36644/mlr.117.7.separate.

Smith, Allison G. *Risk Factors and Indicators Associated with Radicalization to Terrorism in the United States: What Research Sponsored by the National Institutes of Justice Tells Us*. Washington, DC: National Institute of Justice, June 2018. https://www.ojp.gov/pdffiles1/nij/251789.pdf.

Smith, Brent L., and Kelly R. Damphousse. “American Terrorism Study, 1980-2002.” Inter-University Consortium for Political and Social Research, July 30, 2007. https://doi.org/10.3886/ICPSR04639.v1.

Snow, Shawn. “Marine with Alleged Neo-Nazi Connections Booted from the Marine Corps.” *Marine Corps Times*, August 1, 2018. https://www.marinecorpstimes.com/news/your-marine-corps/2018/08/01/marine-with-alleged-neo-nazi-connections-booted-from-the-marine-corps/.

Sotlar, Andrej. "Some Problems with a Definition and Perception of Extremism within a Society." In Policing in Central and Eastern Europe, edited by Gorazd Meško, M. Pagon, & B. Dobovšek. Ljubljana, Slovenia: Faculty of Criminal Justice, University of Maribor, December 2004. https://www.ojp.gov/pdffiles1/nij/Mesko/208033.pdf.

"State Laws Related to Digital Privacy." National Conference of State Legislatures, June 7, 2022. https://www.ncsl.org/research/telecommunications-and-information-technology/state-laws-related-to-internet-privacy.aspx.

Stephens, William, Sieckelinck, Stijn, and Hans Boutellier. "Preventing Violent Extremism: A Review of the Literature." *Studies in Conflict & Terrorism* 44, no, 4 (January 2, 2019): 346-361. doi:10.1080/1057610X.2018.1543144.

Sullaway, Megan. "Hate Crime, Violent Extremism, Domestic Terrorism—Distinctions without Difference?" *In The Psychology of Hate Crimes as Domestic Terrorism: U.S. and Global Issues*, edited by A. B.-M. Edward Dunbar. Santa Barbara, CA: Praeger, 2017. https://psycnet.apa.org/record/2016-51715-003.

Swami, Viren, Martin Voracek, Stefan Stieger, Ulrich S. Tran, and Adrian Furnham. "Analytic Thinking Reduces Belief in Conspiracy Theories." *Cognition* 133, no. 3 (December 2014): 572-585. doi:10.1016/j.cognition.2014.08.006.

Terry, Wallace. "Bringing the War Home." *The Black Scholar* 2, no. 3 (November 1970): 6-18. http://www.jstor.org/stable/41202864.

The Associated Press. "Soldier Convicted in Deadly Attack on His Camp." *The New York Times*, April 22, 2005. https://www.nytimes.com/2005/04/22/us/soldier-convicted-in-deadly-attack-on-his-camp.html.

The United States Army Judge Advocate General's (JAG) Corps Website. Accessed February 8, 2022. https://www.jagcnet.army.mil/ACCALibrary/rss/opinions.

Thompson, A.C., and Ali Winston. "U.S. Marine to be Imprisoned Over Involvement with Hate Groups." *Frontline*, June 20, 2018. https://www.pbs.org/wgbh/frontline/article/u-s-marine-to-be-imprisoned-over-involvement-with-hate-groups/.

Tiia-Triin, Truusa, and Carl Andrew Castro. "Definition of a Veteran: The Military Viewed as a Culture." Chap. 12 in *Military Veteran Reintegration: Approach, Management, and Assessment of Military Veterans Transitioning to Civilian Life*. Edited by Carl Andrew Castro and Sanela Dursun. San Diego, CA: Elsevier Academic Press, 2019): 5-19. doi: 10.1016/B978-0-12-815312-3.00002-4.

Trip, Simona, Carmen Hortensia Bora, Mihai Marian, Angelica Halmajan, and Marius Ioan Drugas. "Psychological Mechanisms Involved in Radicalization and Extremism: A Rational Emotive Behavioral Conceptualization." *Frontiers in Psychology* 10 (March 6, 2019): 1-8. doi:10.3389/fpsyg.2019.00437.

Truman, Harry S. "Executive Order 9981: Desegregation of the Armed Forces (1948)." *National Archives Milestone Documents*. https://www.archives.gov/milestone-documents/executive-order-9981.

Tuman, Joseph S. *Communicating Terror: The Rhetorical Dimensions of Terrorism* (2nd ed.). Thousand Oaks, CA: Sage Publications, Inc., 2010. doi: https://dx.doi.org/10.4135/9781452275161.

U.S. Congress. *United States Code: Uniform Code of Military Justice, 10 U.S.C. §§ 801-940*. December 20, 2019. https://jsc.defense.gov/Portals/99/Documents/UCMJ%20-%2020December2019.pdf?ver=2020-01-28-083235-930.

U.S. Navy Judge Advocate General's Corps Website. "NMCCA Decisions (Court Opinions)." Accessed February 8, 2022. https://www.jag.navy.mil/courts/opinion_archive.htm.

United States Air Force Court of Criminal Appeals Website. "AFCCA Opinions." Accessed February 8, 2022. https://afcca.law.af.mil/opinions_cnm_2021.html.

United States Court of Appeals for the Armed Forces Website. "Opinions." Accessed February 8, 2022. https://www.armfor.uscourts.gov/opinions.htm.

United States Secret Service Website. "National Threat Assessment Center." Accessed June 16, 2022. https://www.secretservice.gov/protection/ntac.

U.S. Department of Homeland Security Office of the Chief Security Officer. *Report to the Secretary of Homeland Security Domestic Violent Extremism Internal Review: Observations, Findings, and Recommendations*. Washington, DC: Department of Homeland Security, March 11, 2022. https://www.dhs.gov/sites/default/files/2022-03/Report%20to%20the%20Secretary%20of%20Homeland%20Security%20Domestic%20Violent%20Extremism%20Internal%20Review%20Observations%2C%20Findings%2C%20and%20Recommendations.pdf.

U.S. Office of Personnel Management. *Questionnaire for Public Trust Positions*. SF 85P. n.p.: U.S. Office of Personnel Management, revised December 2017. https://www.opm.gov/forms/pdf_fill/sf85p.pdf.

U.S. Office of Personnel Management. *Questionnaire for National Security Positions. SF 86*. n.p.: U.S. Office of Personnel Management, revised November 2016. https://www.opm.gov/forms/pdf_fill/sf86.pdf.

Van der Linden, Sander, and Jon Roozenbeek. "Psychological Innoculation Against Fake News." Chap. 9 in The Psychology of Fake News, edited by Eryn Newman, Mariella Jaffé, Norbert Schwarz, and Rainer Greifeneder. New York City, NY: Routledge, 2020. https://www.taylorfrancis.com/chapters/oa-edit/10.4324/9780429295379-11/psychological-inoculation-fake-news-sander-van-der-linden-jon-roozenbeek.

Van Hiel, Alain, Emma Onraet, Dries H. Bostyn, Jonas Stadeus, Tessa Haesevoets, Jasper Van Assche, and Arne Roets. "A Meta-Analytic Integration of Research on the Relationship Between Right-Wing Ideological Attitudes and Aggressive Tendencies." *European Review of Social Psychology* 31, no. 1 (December 2020): 183-221. doi: 10.1080/10463283.2020.1778324.

Vegetti, Federico, and Levente Littvay. "Belief in Conspiracy Theories and Attitudes Towards Political Violence." *Italian Political Science Review* 52, no. 1 (May 10, 2021): 18-32. doi:10.1017/iop.2021.17.

Venhuizen, Harm. "US Soldier Arrested for Planning Attacks on NYC 9/11 Memorial and Troops Overseas." *ArmyTimes*, January 19, 2021. https://www.armytimes.com/news/your-army/2021/01/19/us-soldier-arrested-in-plot-to-blow-up-nyc-911-memorial/.

Vergani, Matteo, Muhammad Iqbal, Ekin Ilbahar, and Greg Barton. "The Three Ps of Radicalization: Push, Pull and Personal. A Systematic Scoping Review of the Scientific Evidence about Radicalization into Violent Extremism." *Studies in Conflict & Terrorism* 43, no. 10 (2020): 854-885. doi:10.1080/1057610X.2018.1505686.

Vergun, David. "All DOD Personnel Now Receive Continuous Security Vetting." *DOD News*, October 5, 2021. https://www.defense.gov/News/News-Stories/Article/Article/2800381/all-DoD-personnel-now-receive-continuous-security-vetting/#:~:text=The%20Defense%20Counterintelligence%20and%20Security,its%20current%20continuous%20vetting%20program.

Vespa, Jonathan E. *Those Who Served: America's Veterans from World War II to the War on Terror: American Community Survey Report*. Washington, DC: U.S. Census Bureau, Department of Commerce, June 2020. https://www.census.gov/content/dam/Census/library/publications/2020/demo/acs-43.pdf.

Vidino, Lorenzo. Countering Radicalization in America. Washington, DC: United States Institute for Peace, 2010. https://www.usip.org/sites/default/files/resources/SR262%20-%20Countering_Radicalization_in_America.pdf.

Wallace, Terry. "Bringing the War Home." *The Black Scholar* 2, no. 3 (November 1970): 6-18. https://www.jstor.org/stable/41202864.

WAVR-21 Website. "The WAVR-21 Threat Assessment App." Accessed June 16, 2022. https://www.wavr21.com/.

Weisman, Jonathan, and Annie Karni. "McConnell Denounces R.N.C. Censure of Jan. 6 Panel Members." *New York Times*, February 8, 2022. https://www.nytimes.com/2022/02/08/us/politics/republicans-censure-mcconnell.html.

Westheider, James E. *Fighting on Two Fronts: African Americans and the Vietnam War.* New York City, NY: NYU Press, 1997.

White House Office of the Press Secretary. *Executive Order 12968: Access to Classified Information*. Washington, DC: White House Office of the Press Secretary, August 4, 1995.

Whitworth, James, Ben Smet, and Brian Anderson. "Reconceptualizing the U.S. Military's Transition Assistance Program: The success in Transition Model." *Journal of Veterans Studies* 6, no. 1 (2020): 25-35. doi: http://doi.org/10.21061/jvs.v6i1.144.

Williams, John A. "The Long Hot Summers of Yesteryear." *The History Teacher* 1, no. 3 (March 1968): 9-23. http://users.clas.ufl.edu/davidson/HistArch/Week%2014/williams%201968.pdf.

Wolfowicz, Michael, Yael Litmanovitz, David Weisburd, and Badi Hasisi. "Cognitive and Behavioral Radicalization: A Systematic Review of the Putative Risk and Protective Factors." *Campbell Systematic Reviews* 16, no. 3 (September 9, 2020): e1102. doi:10.1002/cl2.1102.

Yaccino, Steven, Michael Schwirtz, and Marc Santora. “Gunman Kills 6 at a Sikh Temple near Milwaukee.” *The New York Times*. https://www.nytimes.com/2012/08/06/us/shooting-reported-at-temple-in-wisconsin.html.

Yzerbyt, Vincent, Emanuele Castano, Jacques-Philippe Leyens, and Maria-Paola Paladino. “The Primacy of the Ingroup: The Interplay of Entitativity and Identification,” *European Review of Social Psychology* 11, no. 1 (2000): 257-295, https://www.tandfonline.com/doi/abs/10.1080/14792772043000059.

Zannettou, Savvas, Michael Sirivianos, Jeremy Blackburn, and Nicolas Kourtellis. "The Web of False Information: Rumors, Fake News, Hoaxes, Clickbait, and Various Other Shenanigans." Journal of Data and Information Quality 11, no. 3 (September 2019): 1-37. doi:10.1145/3309699.

Appendix C.
Abbreviations

AAR	After-Action Reports
ADL	Anti-Defamation League
ACLED	Armed Conflict Location & Event Data Project
ALERTS	Army Law Enforcement Reporting and Tracking System
AMJAMS	Automated Military Justice Analysis and Management System
API	Application Programming Interface
ARLIS	Applied Research Laboratory for Intelligence and Security
Army CID	Army Criminal Investigation Division
Army JAG	Army Judge Advocate General
ASD	Assistant Secretary of Defense
ATAP	Association of Threat Assessment Professionals
ATS	American Terrorism Study
BAU	Behavioral Analysis Unit
BTAC	Behavioral Threat Assessment Center
CEAWG	Countering Extremist Activity Working Group
FBI	Federal Bureau of Investigation
CAC	Common Access Card
CEAWG	Combating Extremist Activities Working Group
CISA	Cyber Security and Infrastructure Security Agency
CLEOC	Consolidated Law Enforcement Operations Center
CNO	Chief of Naval Operations
CP3	Center for Prevention Programs and Partnerships
CR2C	Command Ready and Resilient Councils
CSIS	Center for Strategic & International Studies
CVE	Countering Violent Extremism
DASH	Discrimination and Sexual Harassment
DCMS	Disciplinary Case Management System

DCPAS	Defense Civilian Personnel Advisory Service
DHS	Department of Homeland Security
DIEM	Diversity and Inclusion and Extremism in the Military
DIG	Deputy Inspector General
DITMAC	DOD Insider Threat Management and Analysis Center
DNI	Director of National Intelligence
DOD	Department of Defense
DODI	Department of Defense Instruction
DOD IG	Inspector General of the Department of Defense
DOD OIG	Department of Defense Office of the Inspector General
DOJ	Department of Justice
D&T	Data and Technology
DSPO	Defense Suicide Prevention Office
DSSP	Defense Strategy for Suicide Prevention
D-CATSe	Defense Case Activity Tracking System-Enterprise
ECDB	Extremist Crime Database
EEO	Equal Employment Opportunity
ELO	Educational Learning Objective
EO	Equal Opportunity
FBI	Federal Bureau of Investigations
FY 2020 NDAA	Fiscal Year 2020 National Defense Authorization Act
GAO	Government Accountability Office
GB	Gigabyte
GTD	Global Terrorism Database
H.E.A.T.	Hate, Extremism, Anti-Semitism, and Terrorism
HSPD-12	Homeland Security Presidential Directive 12
HVE	Homegrown Violent Extremism
I2MS	Investigative Incident Management System
IDA	Institute for Defense Analyses
IRC	Independent Review Commission
IT	Information Technology
JAG	Judge Advocate General
LEIA	Law Enforcement and Intelligence Agencies
L&P	Law and Policy
MCIO	Military Criminal Investigative Organization
MCO	Marine Corps Order

MEO	Military Equal Opportunity
MJO	Military Justice Online
NATO	North Atlantic Treaty Organization
NCAVAC	National Center for the Analysis of Violent Crime
NCIS	Naval Criminal Investigative Service
NCORS	Naval Court-Martial Reporting System
NDAA	National Defense Authorization Act
NIJ	National Institute of Justice
NTAC	National Threat Assessment Center
OCS	Officer Candidate School
OPM	Office of Personnel Management
ORION	Office of Special Investigations Records, Investigation, and Operations Network
OSD	Office of the Secretary of Defense
OSI	Office of Special Investigations
OTC	Officer Training School
PAC	Prohibited Activities and Conduct
PERSEREC	Personnel and Security Research Center
PIRUS	Profiles of Individual Radicalization in the United States
PIV	Personal Identity Verification
PME	Professional Military Education
POW	Prisoner of War
PPoA	Prevention Plan of Action
PPT-US	Profiles of Perpetrators of Terrorism in the United States
P/CVE	Preventing and Countering Violent Extremism
P/TMS	Pinellas County Sheriff's Threat Management Section
RC	Reserve Component
ROCTAC	Rochester Threat Advisory Committee
ROTC	Reserve Officer Training Corps
SBS	Social and Behavioral Sciences
SEAD 4	Security Executive Agent Directive 4
SEAD 5	Security Executive Agent Directive 5
SF86	Standard Form 86
SIP	Strategic Implementation Plan
SJP	Structured Professional Judgement
SLTT	State, Local, Tribal, and Territorial

SQL	Structured Query Language
START	Study of Terrorism and Responses to Terrorism
TAP	Transition Assistance Program
TEVUS	Terrorism and Extremist Violence in the United States
TLO	Technical Learning Objective
TNT	Transnational Threats Project
TRAP-18	Terrorist Radicalization Assessment Protocol-18
UCMJ	Uniform Code of Military Justice
UNC-C	University of North Carolina at Charlotte
USD(I&S)	Under Secretary of Defense for Intelligence and Security
USD(P&R)	Under Secretary of Defense for Personnel and Readiness
USSS	United States Secret Service
VA	Veterans Affairs
VSO	Veterans Service Organizations
WAVR-21	Workplace Assessment of Violent Risk

Appendix D.
Methodology for Review of Published Court Martial Opinions

To determine the prevalence of prohibited extremist activities appearing in court-martial opinions, we first collected all publicly available opinions that were published between 1 January 2011 and 31 December 2021 and posted by a service's Court of Criminal Appeals on its website in a machine-readable format.[414] We also included the opinions published by the U.S. Court of Appeals for the Armed Forces during the same timeframe.[415] Table D-1 shows the total number of published opinions for each Court, as well as the number and percentage of opinions posted in a machine-readable format.[416] Only machine-readable opinions were included in the analysis. In some cases, multiple opinions were published for the same case; duplicates are included in the counts here but were removed from further analysis.

Each opinion was scanned for instances of the following words: "extremism/extremist," "discriminate/discrimination," "racism/racist," "gang," "supremacy/supremacism/supremacist," "terror/terrorist/terrorism," "sedition," and "dissident."[417] 78 opinions contained at least one of these words;[418] each was manually reviewed to verify that the case represented an instance of

[414] 2011 was the earliest date for which comprehensive collections of court-martial opinions could be obtained from each of the Courts of Criminal Appeals. Opinions were readily accessible for some courts for earlier dates, but we chose to maintain a common timeframe for all services in this analysis.

[415] We accessed court-martial opinions from the following websites:
Army: "ACCA Opinions," The United States Army Judge Advocate General's (JAG) Corps Website, accessed February 8, 2022, https://www.jagcnet.army.mil/ACCALibrary/rss/opinions;

Navy-Marine Corps: "NMCCA Decisions (Court Opinions)," U.S. Navy Judge Advocate General's Corps Website, accessed February 8, 2022, https://www.jag.navy.mil/courts/opinion_archive.htm;

Air Force: "AFCCA Opinions," United States Air Force Court of Criminal Appeals Website, accessed February 8, 2022, https://afcca.law.af.mil/opinions_cnm_2021.html;

U.S. Court of Appeals for the Armed Forces: "Opinions," United States Court of Appeals for the Armed Forces Website, accessed February 8, 2022, https://www.armfor.uscourts.gov/opinions.htm.

[416] Machine readable here refers to files which are saved in a format that enables the text of the document to be parsed (such as a PDF file with selectable text or a Microsoft Word document). This excludes files that are saved as images, where the text would first need to be extracted from the image by optical character recognition or another similar process.

[417] Although DODI 1325.06 also concerns prohibited protest activity, a preliminary search for "protest" returned 113 cases, the majority of which were descriptions of sexual assault. Therefore, "protest" and its derivatives were excluded from further searches.

[418] The keyword, "terror/terrorism/terrorist" appeared in 34 opinions; "gang" appeared in 32 opinions; "racism/racist" and "extremism/extremist" each appeared in 10 opinions; "discriminate/discrimination" and

prohibited extremist activities, a hate crime, or other related behavior. Cases were counted as incidents of prohibited extremist activities if the actions involved appeared to meet one of the criteria defined in DODI 1325.06:

- Using force or violence to deprive others of their rights under the law;
- Using force or violence to achieve political, religious, discriminatory, or ideological goals;
- Committing acts of terrorism or supporting terrorism in any way;
- Using force or violence to overthrow the government or supporting such actions;
- Violating laws or orders in order to disrupt military activities (or encouraging others in the defense community to do so);
- Advocating widespread unlawful discrimination on the basis of race, color, national origin, religion, sex, gender identity, or sexual orientation;
- Participating in or otherwise supporting a criminal gang.

Table D-1. Number and Percent of Court-Martial Opinions that are Machine-Readable.

Court of Appeals	Total Opinions	Machine-readable Opinions	Percent Machine-readable
Air Force	2632	2554	97%
Army	1942	1511	78%
Navy/Marine Corps	1353	1353	100%
Armed Forces	388	385	99%
Total	**6315**	**5803**	**92%**

"supremacy/supremacist" each appeared in 8 opinions; and "dissident" and "sedition" each appeared in 1 opinion.

Appendix E.
Law Enforcement Participation in Incidents of Violent Extremism

Like members of the military, law enforcement officers are often targeted by extremist groups because of their specialized training and experience. Some groups, such as the Oath Keepers, are known to recruit current and former military and law enforcement members deliberately. Law enforcement involvement in extremist activities raises concerns similar to those raised by prohibited extremist activities in the military, as these law enforcement officers have training in the use of force and official roles that could place them in the position to misuse such force in ways that could cause significant harm.

Numerous media articles have included anecdotes about members of law enforcement engaging in violence or otherwise showing support for established extremist groups, typically those with far-right or anti-government ideologies. Fewer studies have attempted to quantify the scope of this involvement; however, both the CSIS and the ADL have compiled data regarding law enforcement involvement in terrorist plots and support for known extremist groups, respectively.

The CSIS dataset consists of 980 terrorist acts that were plotted or carried out in the United States between January 1, 1994, and January 31, 2021. Actions were included only if they involved the use or threat of violence to fulfill political or ideological goals and cause a widespread psychological impact. Therefore, many instances of hate speech, hate crimes, and unlawful discrimination were excluded from the dataset. With respect to law enforcement, the dataset includes a binary flag to indicate whether the perpetrator is a law enforcement officer. For cases coded as "yes," another data field indicates whether the individual is a current or former member.

CSIS identified six terrorist incidents involving current or former law enforcement officers as perpetrators. Although CSIS data span 25 years, from 1994 to 2021, all of the identified incidents occurred since 2017. Three of the incidents involved current members of law enforcement; one was the 6 January 2021 Capitol riots, while the other two occurred in the three months preceding the riots. The other three incidents involved former officers: two occurred in 2017, and the third in October 2020. Although these incidents represent less than 1% of all incidents listed in the dataset, the fact that all of the incidents involving current and former law enforcement officers took place in the last five years of the 25-year period studied suggests that the overall rate of law enforcement involvement in extremist activity has increased in recent years.

The Anti-Defamation League used publicly available media reports and social media posts, together with internal documents from ADL's Center on Extremism, to compile a list of 76 incidents of extremism involving law enforcement from 2010 to 2021. 73 of the incidents involved unique individuals; the remaining three were instances in which one of the previously identified officers was hired by a new agency after the officer's connections to extremist groups were revealed. The dataset considered all branches of law enforcement, including corrections officers; however, approximately 80% of the identified individuals worked in local law enforcement. The data include information about the individual's actions, as well as the final action taken against the officer (such as suspension, termination, or reassignment), if that information was publicly available.

Cases were included in the ADL dataset only if they could be verified by photographs or extensive media reporting. Furthermore, this dataset only considers instances in which a currently employed member of law enforcement expressed support for or was clearly associated with a known extremist group. Unlike the CSIS dataset, a case included in the ADL set did not need to involve violence or the threat of violence in order to be considered. However, the ADL criteria exclude any act committed by a lone actor, as well as many instances of discriminatory or bigoted speech or actions.

The ADL identified 73 unique incidents since 2010 in which a law enforcement officer acted in support of an established extremist group. The majority of the cases involved anti-government or white supremacist groups, such as the Three Percenters, the Oath Keepers, Neo-Nazi movements, and the January 6 Capitol riots. However, a smaller fraction of incidents involved other groups and ideologies, such as QAnon and Black nationalist movements. The incidents documented vary in severity. The majority involved nonviolent expressions of support for extremist groups, such as social media posts, bumper stickers on personal vehicles, or collecting Nazi memorabilia. Notably, a number of cases involved officers who displayed extremist patches, symbols, or tattoos while in uniform. A small number of cases involved violence or threatened violence; for example, in April 2015, three individuals with associations to the KKK were convicted of plotting to murder a black inmate in a Florida prison.

The ADL found that 42% of the identified individuals were fired or otherwise removed from their law enforcement departments. Three of these individuals were later hired by another department. Another 40% of the officers continued to serve after their investigations were concluded. The final outcomes of the remaining cases are unknown.

Overall, these two studies demonstrate that relatively few law enforcement officers are involved in terrorist and extremist activities. However, the data collection is limited by the availability of publicly available documents. It is impossible to obtain an accurate count of the number of incidents that are revealed and handled internally without media coverage. Additionally, the data do not consider the full spectrum of discrimination, racism, and other bigoted actions that still cause harm to the communities that these officers are sworn to protect.

As is the case with military service members, relatively few law enforcement officers have a demonstrable connection to terrorist or extremist activities and groups. However, even a handful of such cases can lead to widespread harm (particularly among vulnerable communities) and erode public trust in law enforcement. Additionally, the ADL's observations about final outcomes demonstrate that many departments do not have established and transparent guidelines regarding prohibited activities and consequences. Moving forward, law enforcement entities may benefit from implementing some of the recommendations suggested elsewhere in this report.

This page is intentionally blank.

Appendix F.
Further Details on Ages and Demographics for Individuals Charged in Connection with the January 6th Events

Table F-1. Estimates Counts of Individuals Charged for the 6 January 2021 Events by Age and Gender

Age Range	Number Charged	Estimated Counts for Unknown Ages	Estimated Male Charges	Estimated Female Charges
18 to 19	9	1.0	8.7	1.3
20 to 29	135	15.4	130.9	19.4
30 to 39	189	21.5	183.3	27.2
40 to 49	141	16.1	136.8	20.3
50 to 59	115	13.1	111.5	16.6
60 to 69	35	4.0	33.9	5.0
70 to 79	7	0.8	6.8	1.0
80	1	0.1	1.0	0.1
Unknown	**72**			
Total	**704**	**72**	**613**	**91**

Notes: Based on the 704 individuals with federal charges that were publicly available as of 1 January 2022, as cited in Clifford and Lewis (2022, p. 12–13). The 72 individuals with unknown ages are assumed to have the same age distribution as the 632 individuals with known ages. The age distribution for the 613 (87%) males and the 91 (13%) females who were charged is assumed to be the same as the 632 individuals with known ages.

This page is intentionally blank.

Appendix G.
DOD Policy Documents Used to Track Frequency of Terms

Table G-1. DOD Policy Documents Used to Track Frequency Terms

Full Citation	Short Title
Lloyd Austin, SECDEF, "Immediate Actions to Counter Extremism in the Department and the Establishment of the Countering Extremism Working Group," Memorandum for Senior Pentagon Leadership, Commanders of the Combatant Commands, Defense Agency and DoD Field Activity Directors, April 9, 2021.	SECDEF Stand Down Order
Report to Armed Services Committees on Screening Individuals Who Seek to Enlist in the Armed Forces	Report to Armed Services Committees on Screening Individuals Who Seek to Enlist in the Armed Forces
Christopher Miller, Acting SECDEF, "Actions to Improve Racial and Ethnic Diversity and Inclusion in the U.S. Military," Memorandum for Senior Pentagon Leadership (See Distribution), Commanders of the Combatant Commands, Defense Agency and DoD Field Activity Directors, December 17, 2020	SECDEF Actions to Improve Diversity and Inclusion Memo
The Department of Defense Office of the Inspector General's Report to Congress Pursuant to Section 554 of the Fiscal Year 2021 National Defense Authorization Act, June 10, 2021	DoDIG Report to Congress on 2021 NDAA Section 554
The Joint Chiefs of Staff, "Memorandum for the Joint Force," undated 2021.	2021 JCS Memo to the Joint Force
USMC MCRCO, "Statement of Understanding: Marine Corps Policy Concerning Tattoos, Branding, and Ornamentation"	USMC Policy Concerning Tattoos, Branding, and Ornamentation
USMC MCRCO, "MCRC Enlisted Tattoo Screening Form"	USMC Tattoo Screening Form
USMC MCRCO, "Questionable Conduct, or Aberrant Behavior Screening Form"	USMC Questionable Conduct, or Aberrant Behavior Screening Form
USMC G-3, "Marine Corps Recruiting Command Order 1100.1," November 9, 2011	USMC Recruiting Command Order 1100.1
Army Regulation 600-20, 24 July 2020, Section 4-12	AR 600-20
AR 195-2: Criminal Investigation Activities	AR 195-2

Air Force Instruction 51-508, 12 October 2018, Section 3.4 Prohibited Activities.	AFI 51-508
Air Force Instruction 51-508: Political Activities, Free Speech and Freedom of Assembly of Air Force Personnel. Chapter 2 defines political activities.	AFI 51-508
Air Force Recruiting Service Extremist, Hate Organization or Gang Questions	Air Force Recruiting Service Extremist, Hate Organization or Gang Questions
NOTAM 21-09: Applicant Suitability Check - Association with an Extremist/Hate Organization or Gang	NOTAM 21-09
US Air Force, "Progressive Discipline" Briefing.	USAF "Progressive Discipline"
Air Force Instruction 1-1: Air Force Culture, Chapter 2	AFI 1-1
PERSEREC, Leveraging FBI Resources to Enhance Military Accessions Screening and Personnel Security Vetting.	PERSEREC on Leveraging FBI Resources to Enhance Screening
Defense Personnel and Security Research Center, Defense Manpower Data Center, *Adjudicative Desk Reference: Assisting Security Clearance Adjudicators, Investigators, and Security Managers in Implementing the U.S. Government Personnel Security Program*, Version 4 (Washington, DC: OSD, 2014).	Adjudicative Desk Reference: Assisting Security Clearance Adjudicators, Investigators, and Security Managers in Implementing the U.S. Government Personnel Security Program, Version 4
Navy Personnel Command (NAVPERSOM), MILPERSMAN 1910-160: Separation by Reason of Supremacist or Extremist Conduct	MILPERSMAN 1910-160
Department of the Navy, Navy General Regulations	USN General Regulations
USMCRC, MCRC 1100 1.A EPM	MCRC 1100.1A EPM
James Clapper, "Security Executive Agent Directive (SEAD) 5: Collection, Use, and Retention of Publicly Available Social Media Information in Personnel Security Background Investigations and Adjudications," Version 5.4, May 5, 2016	SEAD 5
"Political Activities by Members of Armed Forces," DoD Directive 1344.10, February 19, 2008	DoDD 1344.10
"USN Screen to Discover Training," United States Navy	USN Screen to Discover
"Initial Screening Checklist" in *U.S. Marine Corps Opportunities Book*.	USMC Opportunities Book Initial Screening Checklist
"Navy Organization and Standards," OPNAVINST 3120.32D,	Navy Organization and Standards
Under Secretary of Defense for Personnel and Readiness (OSD(P&R)), "Qualification Standards for Enlistment, Appointment, and Induction," DoDI 1302.46, October 26, 2018.	DoDI 1302.14
Office of Personnel Management, Standard Form 85P, December 2017.	SF85P

• Under Secretary of Defense for Intelligence (USD(I)), "The DoD Insider Threat Program," DoDD 5205.16, September 30, 2014, Incorporating Change 2, August 28, 2017	DoDD 5205.16

This page is intentionally blank.

Appendix H.
Keywords Used for Analysis of Policy Documents

The following table contains all subcategories and keywords used in the search. An asterisk in a keyword indicates that any character will produce a match. For example, the keyword "extremis*" would produce matches for "extremist," "extremism," and "extremists," but not "extreme." When two keywords are separated by a space, they must be present exactly as written. For example, the keyword "far left" would not produce a match for the phrase "he left and went far away." Finally, in the case of two words separated by a +, both words must be present in the same sentence (in any order) to produce a match. For example, the phrase "violat* + UCMJ" would produce matches for "violate the UCMJ," "violation under the UCMJ," or "UCMJ violation."

Table H-1. Policy Analysis Keywords

Category	Subcategory	Keywords
State of Mind	Knowing or willful	knowing, willful, intend*, intent
Nature of Participation	Protest or demonstrate	rally, rallies, demonstrat*, protest*
Nature of Participation	Associate or sympathize with	Associate*, sympathize, involv*
Nature of Participation	Have tattoos/ body markings	tattoo
Nature of Participation	Be a member of	member*
Nature of Participation	Support or advocate for	Support, advocat*, encourag*, help, assist, abet
Nature of Participation	Actively participate	participat\w*
Nature of Participation	Support or advocate for	proselytiz*, preach
Nature of Participation	Fundraise	fundrais\w*, raise funds, raise money, raise capital, increase funds, increase money, increase capital
Nature of Participation	Recruit	recruit*, train, increase + member*, increase + ranks, increase + size, increase + organization, increase + group, increase + cell, grow + member*, grow + ranks, grow + size, grow +

		organization, grow + group, grow + cell, expand + member*, expand + ranks, expand + size, expand + organization, expand + group, expand + cell, add + member*, add + ranks, add + size, add + organization, add + group, add + cell, build + member*, build + ranks, build + size, build + organization, build + group, build + cell
Type of Group	Groups with ideological goals	ideolog*, political goal, religious goal, right wing, left wing, far right, far left, alt right, leftist, supremac*
Type of Group	Lone actors	lone wolf, lone actor
Type of Group	Extremist organizations	extremis\w*
Type of Group	Criminal gangs	gang, organized crim*, criminal
Type of Group	Terrorist organizations	terror* group, terror* organization, terror* gang, terror* cell
Desired Outcomes	Prevent others from exercising rights	prevent + right
Desired Outcomes	Prevent others from exercising rights	prevent + privilege\w*
Desired Outcomes	Prevent others from exercising rights	prevent + activit\w*
Desired Outcomes	Prevent others from exercising rights	prevent + program\w*
Desired Outcomes	Prevent others from exercising rights	obstruct + right
Desired Outcomes	Prevent others from exercising rights	obstruct + privilege\w*
Desired Outcomes	Prevent others from exercising rights	obstruct + activit\w*
Desired Outcomes	Prevent others from exercising rights	obstruct + program\w*
Desired Outcomes	Prevent others from exercising rights	interfer\w* + right

Desired Outcomes	Prevent others from exercising rights	interfer\w* + privilege\w*
Desired Outcomes	Prevent others from exercising rights	interfer\w* + activit\w*
Desired Outcomes	Prevent others from exercising rights	interfer\w* + program\w*
Desired Outcomes	Prevent others from exercising rights	imped\w* + right
Desired Outcomes	Prevent others from exercising rights	imped\w* + privilege\w*
Desired Outcomes	Prevent others from exercising rights	imped\w* + activit\w*
Desired Outcomes	Prevent others from exercising rights	imped\w* + program\w*
Desired Outcomes	Prevent others from exercising rights	discriminat\w*
Desired Outcomes	Affect conduct of government	affect + government
Desired Outcomes	Affect conduct of government	affect + policy
Desired Outcomes	Affect conduct of government	influence + government
Desired Outcomes	Affect conduct of government	influence + policy
Desired Outcomes	Affect conduct of government	impact + government
Desired Outcomes	Affect conduct of government	impact + policy
Desired Outcomes	Affect conduct of government	sway + government
Desired Outcomes	Affect conduct of government	sway + policy

Desired Outcomes	Affect conduct of government	pressure + government
Desired Outcomes	Affect conduct of government	pressure + policy
Nonviolent Criminal Activity	Unlawfully discriminate	discriminat\w* + race
Nonviolent Criminal Activity	Unlawfully discriminate	discriminat\w* + color
Nonviolent Criminal Activity	Unlawfully discriminate	discriminat\w* + gender
Nonviolent Criminal Activity	Unlawfully discriminate	discriminat\w* + religion
Nonviolent Criminal Activity	Unlawfully discriminate	discriminat\w* + national + origin
Nonviolent Criminal Activity	Intimidate or coerce	intimidat\w*
Nonviolent Criminal Activity	Intimidate or coerce	coerc\w*
Nonviolent Criminal Activity	Violate a law (nonviolent)	criminal
Nonviolent Criminal Activity	Violate a law (nonviolent)	crime
Violent or Criminal Activity	Endanger human life	danger
Violent or Criminal Activity	Engage in unlawful violence	violen\w*
Violent or Criminal Activity	Engage in unlawful violence	force
Violent or Criminal Activity	Assassinate or kidnap	assassinat\w*
Violent or Criminal Activity	Assassinate or kidnap	kidnap\w*
Violent or Criminal Activity	Engage in mass destruction	destruction
Violent or Criminal Activity	Commit acts of subversion	sabotage
Violent or Criminal Activity	Commit acts of subversion	espionage
Violent or Criminal Activity	Commit acts of subversion	treason

Violent or Criminal Activity	Commit acts of subversion	sedition
Violent or Criminal Activity	Commit acts of subversion	overthrow + government
Violent or Criminal Activity	Engage in terrorism	terror\w*
Intervention	Bar from enlistment	unsuitab\w*
Intervention	Bar from enlistment	unfit + serv\w*
Intervention	Bar from enlistment	disqualif\w* + enlist\w*
Intervention	Bar from enlistment	ineligib\w* + enlist\w*
Intervention	Bar from enlistment	not qualified + enlist\w*
Intervention	Bar from enlistment	not eligible + enlist\w*
Intervention	Bar from enlistment	not suitable
Intervention	Bar from enlistment	bar + enlist\w*
Intervention	Bar from enlistment	prevent\w* + enlist\w*
Intervention	Deny security clearance	deny + clearance
Intervention	Deny security clearance	denial + clearance
Intervention	Deny security clearance	eligib\w* + classif\w*
Intervention	Deny security clearance	adjudicat\w*
Intervention	Revoke security clearance	revok\w* + clearance
Intervention	Revoke security clearance	continu\w* + eligib\w*
Intervention	Discipline under UCMJ	disciplin\w* + UCMJ
Intervention	Discipline under UCMJ	disciplin\w* + uniform code
Intervention	Discipline under UCMJ	disciplin\w* + article

Intervention	Discipline under UCMJ	action + UCMJ
Intervention	Discipline under UCMJ	action + uniform code
Intervention	Discipline under UCMJ	action + article
Intervention	Discipline under UCMJ	punish + UCMJ
Intervention	Discipline under UCMJ	punish + uniform code
Intervention	Discipline under UCMJ	punish + article
Intervention	Discipline under UCMJ	violat\w* + UCMJ
Intervention	Discipline under UCMJ	violat\w* + article
Intervention	Discipline under UCMJ	violat\w* + uniform code
Intervention	Screen recruits	screen
Intervention	Mandate counseling	counsel\w*
Intervention	Refer to commanders	commander\w*
Intervention	Refer to commanders	site\w* + off-limit\w*
Intervention	Refer to commanders	place\w* + off-limit\w*
Intervention	Refer to commanders	establishment\w* + off-limit\w*
Intervention	Refer to commanders	location\w* + off-limit\w*
Intervention	Refer to commanders	site\w* + prohibit\w*
Intervention	Refer to commanders	place\w* + prohibit\w*
Intervention	Refer to commanders	establishment\w* + prohibit\w*
Intervention	Refer to commanders	location\w* + prohibit\w*
Intervention	Refer to commanders	command\w* + interven\w*

REPORT DOCUMENTATION PAGE	Form Approved OMB No. 0704-0188

1. REPORT DATE (DD-MM-YY)	2. REPORT TYPE	3. DATES COVERED (From – To)
XX-12-2023	Final	June 2021 - June 2022

4. TITLE AND SUBTITLE

Prohibited Extremist Activities in the Department of Defense

5a. CONTRACT NO.

HQ0034-19-D-0001

5b. GRANT NO.

5c. PROGRAM ELEMENT NO(S).

6. AUTHOR(S)

Peter K. Levine, Joseph F. Adams, Amy A. Alrich, Rachel G. Augustine, Margaret D.M. Barber, Sujeeta B. Bhatt, Kathleen M. Conley, Dave I. Cotting, Alan B. Gelder, Jeffery M. Jaworski, Mark F. Kaye, Carrington A. Metts, Neil V. Mithal, Matthew J. Reed

5d. PROJECT NO.

5e. TASK NO.

BE-6-5006

5f. WORK UNIT NO.

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Institute for Defense Analyses
4850 Mark Center Drive
Alexandria, VA 22311-1882

8. PERFORMING ORGANIZATION REPORT NO.

IDA Paper P-33076
Log: H 22-000175

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

OUSD(P&R)
1400 Defense Pentagon,
Arlington, VA 22202

10. SPONSOR'S / MONITOR'S ACRONYM(S)

OUSD(P&R)

11. SPONSOR'S / MONITOR'S REPORT NO(S).

12. DISTRIBUTION / AVAILABILITY STATEMENT

Approved for public release; distribution unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

The objective of the IDA study is to gain greater fidelity on the scope and nature of extremist ideologies and behaviors in the Department, identify the sources of such ideologies and behavior, assess their impact, and develop strategies for preventing, countering, and neutralizing that impact.

15. SUBJECT TERMS

Extremism, violent extremism, homegrown violent extremism, domestic terrorism, radicalization, supremacism, racially or ethnically motivated extremism, anti-government or anti-authority extremism, insider threats, hate crimes, risk assessment and mitigation, military justice, social media, misinformation, disinformation

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NO. OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Aaron Radtke
U	U	U	U	264	19b. TELEPHONE NUMBER (Include Area Code) (703) 695-6949

This page is intentionally blank.