



DOMESTIC VIOLENT EXTREMISM AND THE THREAT TO U.S. NATIONAL SECURITY

CONFERENCE REPORT



PRESENTED BY:

CENTER FOR ETHICS AND THE RULE OF LAW

THE ANNENBERG PUBLIC POLICY CENTER

PREPARED BY:

DR. ILYA RUDYAK

SENIOR FELLOW, CENTER FOR ETHICS AND THE RULE OF LAW

Conference Background

Since the September 11, 2001, terrorist attacks on the United States, government attention has been directed largely at threats to national security stemming from foreign violent extremism. But more recent incidents, such as the mass shootings in El Paso, Texas; Charleston, South Carolina; and Pittsburgh, Pennsylvania; the “Unite the Right” march in Charlottesville, Virginia; and the January 6 events at the U.S. Capitol, have brought renewed attention to the threats stemming from domestic violent extremism. According to Secretary of Homeland Security Alejandro Mayorkas, racially or ethnically motivated violent extremists and militia violent extremists currently pose one of the most critical threats to U.S. national security.

On September 28-30, 2022, the Center for Ethics and the Rule of Law (CERL), in partnership with the Annenberg Public Policy Center (APPC), hosted a conference titled [*Domestic Violent Extremism and the Threat to U.S. National Security*](#), which brought together leading scholars and practitioners in the fields of national security, law, ethics, psychology, and education to engage in interdisciplinary discussion and analysis of the threats posed by contemporary domestic violent extremism, and to examine new approaches for addressing the thorny legal and ethical dilemmas associated with responding to these threats.

The conference included two public events and seven closed workshop sessions. It began on September 28, 2022, with a public keynote by former U.S. Secretary of Homeland Security Jeh Charles Johnson entitled [*Is Violent Extremism a Threat to Democracy? Reflections on Current Challenges in U.S. National Security*](#). CERL Faculty Director Claire O. Finkelstein moderated the talk. The following day, conference participants attended four closed workshop sessions examining several topics, including the new challenges domestic violent extremism poses to U.S. national security; connections between domestic violent extremism and the spread of disinformation and conspiracy theories through social media, members of the government, the bar and the press; and novel ways of financing domestic violent extremism. The day culminated in a public keynote panel entitled [*Perspectives on Domestic Violent Extremism*](#) with Mr. Robert Kelner of Covington & Burling LLP, Professor Mary McCord of Georgetown University, and Mr. Oren Segal of the Anti-Defamation League. Professor Shawn Turner of Michigan State University

moderated. On September 30, 2022, participants attended three additional workshop sessions centering on questions such as: What should the role of the Intelligence Community be in detecting and surveilling domestic violent extremists? What are the strengths and shortcomings of extant law and the new national strategy for countering contemporary domestic violent extremism, as well as the ethical concerns they raise? Could promoting quality civics education, especially in communities particularly vulnerable to radicalization, aid in preventing domestic violent extremism?

This report provides a brief summary of the discussions among conference participants during the closed workshop sessions, which were held under Chatham House Rule.¹

Session 1: The New Threat of Domestic Violent Extremism

Moderator

Ilya Rudyak, Senior Fellow, Center for Ethics and the Rule of Law

Discussion Summary

Assessments by U.S. government agencies maintain that domestic violent extremism (DVE) poses an increased risk to the nation. Although DVE is hardly new to the U.S., its contemporary incarnation presents new challenges to U.S. national security. The sociological and technological changes that have reshaped the social and political landscape of the country over recent decades have also facilitated the spread of disinformation, amplified radical narratives, and provided effective tools for coordinating and financing violent action. This session centered on identifying the crucial aspects that make contemporary DVE different from past variations of this threat. Participants focused on the role of online platforms, the involvement of political actors, and the critical distinction between terrorism and different forms of extremism.

A unique aspect of contemporary DVE stressed by conference participants is the role online platforms play in connecting, recruiting, radicalizing, and financing violent extremists. While

¹ This report was prepared by Ilya Rudyak. Gratitude is due to Beatrice Wilson, Marcus Ellinas, David Glinbizzi, and Joe Dangtran for their excellent conference notes. A special gratitude is also due to David Joanson, Joe Dangtran, and Jennifer Cohen for their contributions in coordinating, drafting, and editing this report.

some participants noted that extremists' online activity has certain law enforcement benefits, as it enables better monitoring and policing, others stressed that these benefits are difficult to attain in practice due to extremists' exploitation of the moderation rules of major online platforms (e.g., Facebook or Twitter) and the relative ease with which they can migrate their activities to new platforms (e.g., Parler or Telegram). Participants also emphasized the role a growing number of prominent political figures play in embracing and encouraging extremists. Participants referred to former President Trump's call to the militia group Proud Boys to "stand back and stand by" during the 2020 presidential debates as an illustration of this broader phenomenon. Relatedly, some participants opined that such endorsements by politicians are further amplified (often uncritically) by modern media outlets that contribute to the mainstreaming of extremists' ideas and the public perceiving them as legitimate political views. This, in turn, makes efforts to counter them appear partisan and politically divisive, thus impeding effective response to violent extremism by the administration. In contrast, several participants stressed that violent extremists are more influenced by previous *acts* of violent extremism than by extremist ideology or words of politicians. These participants cautioned against dedicating outsized attention to the latter. Others noted that some violent extremist acts have been perpetrated by individuals struggling with mental health issues. Other participants still argued that focusing on the motivations of individual violent extremists may miss broader structural drivers of violent extremism such as the availability of firearms or economic disparities.

To conclude the session, participants also addressed the importance of distinguishing between terrorism and different forms of extremism. While terrorism is a particular tactic used to pursue political goals, extremism is a much broader term. As one participant underscored, this term can have at least three conceptually different meanings. Extremism can refer to: a) the (extreme) location of one's views on the spectrum of political views (e.g., extreme right-wing); b) the (extreme) intensity with which one's views are held (e.g., extreme centrist); or c) the (extreme) tactics one is willing to adopt to promote one's views (e.g., extreme, violent acts). Distinguishing among these three notions of extremism can be crucial for ethical, legal, and policy reasons, as measures that may be appropriate to apply to counter DVE—an example of extremism in the third sense—may be unacceptable, illegal, or unsuitable if applied to other forms of extremism.

Session 2: The New Threat of Domestic Violent Extremism

Moderator

Emily Kaufman, Investigative Researcher, Anti-Defamation League Center on Extremism

Discussion Summary

Social media has grown exponentially over the past two decades, becoming an increasingly popular arena for extremists to spread disinformation and advance their positions. Extremist groups use social media platforms to communicate, disseminate conspiracy theories, and radicalize potential sympathizers and recruits. The allure of social networks for these purposes is based, in part, on controversial characteristics of their proprietary algorithms, designed to promote the most polarizing and divisive content, including the very content extremist groups aspire and struggle to spread. At the same time, social media can be an invaluable resource for identifying extremists, refuting their propaganda, and de-radicalizing their targets. This session addressed the role social media can play in fomenting, facilitating, or frustrating DVE. Participants focused predominantly on the comparative merits of governmental and private sector regulation of media platforms, their legal liability according to Section 230 of the 1996 Communications Decency Act (Section 230), and questions relating to the limits and implications of content moderation.

Participants disagreed on whether social media platforms should be regulated by the government or the private sector. On the one hand, participants noted that federal legislation may be too blunt of an instrument for regulating the constantly evolving technological landscape of social media platforms. Participants were also concerned that legislators may not possess the technical expertise necessary for devising such regulation. On the other hand, participants stressed that tech companies are ultimately guided by commercial motivations and seek to protect proprietary interests, including their (arguably divisive) algorithms. These motivations and interests incentivize companies to minimize self-regulation efforts and disincentivize them from adopting effective policies to curtail extremist content—especially if such content increases user engagement that benefits the companies financially. Some participants noted that a potential solution to the regulation problem may lie in harnessing the relative strengths of the government and tech companies. The government is in a better position to act in the public interest. It should, therefore, determine the contours of the constraints to be imposed on tech companies and provide

definitions for inappropriate conduct, setting some minimal standards. Different tech companies, in turn, are better equipped to design appropriately nimble, nuanced, and potentially diverse policies to implement these standards within their operational environments.

Participants then considered more specific questions pertaining to Section 230 and content moderation. Some participants expressed concerns about Section 230's shielding of tech companies from liability for user-generated content, including hate speech. They also stressed that in other contexts, such as the dissemination of child pornography or incitement to imminent lawless action, legal restrictions on speech are justified—*notwithstanding* freedom of speech considerations. Yet participants have also noted that government ability to regulate tech companies, and specifically as it relates to their algorithms, is complicated by *Bernstein v. U.S. Dep't of State*,² which established, *inter alia*, that a computer code can constitute a constitutionally protected speech. Participants have also highlighted the legal uncertainty resulting from the circuit split on the constitutionality of state laws restricting tech companies' authority to moderate content, with Texas laws to that effect upheld by the 5th circuit,³ while Florida laws were declared by the 11th circuit as likely to be unconstitutional.⁴ Finally, participants also addressed the limits and implications of content moderation. Participants stressed that regulation should take into account that smaller tech companies may not be able to comply with robust content moderation rules. Additionally, participants discussed the implications of robust content moderation rules that essentially drive extremist actors away from mainstream media platforms. While such rules do curtail extremist messaging on these platforms, participants warned that they also encourage extremists to turn to alternative platforms that may be entirely unmoderated. The danger participants highlighted is that on these alternative platforms, the pace with which extremist ideas spread and radicalization occurs increases exponentially.

² *Bernstein*, 922 F. Supp. 1426.

³ *NetChoice, L.L.C. v. Paxton*, No. 21- 51178, 2022 WL 4285917, at 1-2 (5th Cir. Sept. 16, 2022)

⁴ *NetChoice, LLC v. Att'y Gen.*, 34 F.4 th 1196, 1231 (11th Cir. 2022)

Session 3: Sources of Disinformation – Members of the Government, the Bar, the Press, and Domestic Violent Extremism

Moderator

Claire O. Finkelstein, Algernon Biddle Professor of Law and Professor of Philosophy; Faculty Director, Center for Ethics and the Rule of Law

Discussion Summary

While social media is a new and prominent source of disinformation, traditional actors in the public sphere—including members of the government, the bar, and the press—might play a more critical role in spreading disinformation, lending credence to disinformation and conspiracy theories, and facilitating contemporary DVE. The recent growth of DVE correlates with officials at the highest levels of government encouraging—or acquiescing in—violent conduct by domestic extremists and with lawyers partaking in judicial proceedings intended to promote narratives that may incite or cover up violent conduct. The discussion revolved around the 65 cases brought by the Trump administration and the case brought by Texas to contest the results of the 2020 election (64 of the former cases were unsuccessful; the latter was denied by the Supreme Court for lack of standing). The central argument under consideration during the session was that these cases were fundamentally flawed and frivolous from the legal standpoint (as their high failure rate suggests). Yet lawyers were still willing to bring them on behalf of their clients, thereby providing a veneer of legal legitimacy to disinformation campaigns about the election’s results. The discussion focused on the responsibility of these lawyers and whether the judiciary (and bar associations) should be taking a more active role in sanctioning them.

Several participants argued that lawyers bringing such cases must be held accountable. Some stressed specific legal standards imposing accountability for frivolous arguments, most specifically Rule 11 of the Federal Rules of Civil Procedure (Rule 11). Others claimed that such arguments were, in fact, directly connected to, and provided legal justification for, January 6 events at the U.S. Capitol. One participant also highlighted a broader concern, arguing that a gross misuse of law, as evidenced in the aforementioned litigation-as-disinformation cases, can cause profound and long-term damage to the rule of law.

Other participants, however, expressed reservations. Some disputed different aspects of the central argument under consideration, suggesting that the extent of *additional* legitimacy that litigation aimed at disinformation derives from *lawyers'* involvement in it may be very limited; stressing that courts' involvement in sanctioning lawyers engaging in frivolous litigation is unlikely to reduce its disinformation value, as courts can determine frivolousness only after the litigation is submitted and made public; and noting that the institutional structure of bar associations makes them very unlikely to impose accountability on lawyers in this context. Others emphasized the fuzziness of the "frivolous" standard in Rule 11 and the difficulties lawyers face in ascertaining in advance whether a claim would be judged by the courts as frivolous. Other participants still raised concerns about the chilling effect of an aggressive stance against "frivolous" claims and reminded the group that many legal precedents we now hold dear are based on what, at the time, were non-conventional legal theories that could have been considered "frivolous."

Participants also considered the usefulness of relying on Rule 11's distinction between legal and factual contentions. Some noted that the aforementioned important considerations for preserving lawyers' ability to raise creative legal contentions do not extend to factual ones. Other participants stressed, in contrast, that sometimes the distinction between legal and factual contentions is blurry, and that whether certain factual contentions are true cannot be decided in advance; rather it is often *the* question to be determined in litigation through application of the structured and formal tools of the legal process. Finally, some participants highlighted the benefits of the judicial system adjudicating (rather than barring or deterring) litigation-as-disinformation cases containing questionable contentions, arguing that courts decisions in these cases can provide highly credible evidence against the disinformation these cases aimed to spread.

Session 4: Financing and Sponsoring Domestic Violent Extremism

Moderator

John M. Geiringer, Regulatory Section Leader, Barack Ferrazzano Financial Institutions Group

Discussion Summary

Violent extremists require financial resources to recruit members, coordinate logistics, and conduct operations. Domestic violent extremists finance their activities using both traditional financial institutions such as banks and charitable trusts, and more modern digital platforms such as crowdfunding sites and cryptocurrencies that obfuscate the origins of their funds. This session addressed both methods of DVE financing and ways to disrupt them. Participants focused predominantly on the banking industry and the implications of differences between its regulation in the foreign and domestic extremism context and considered a novel proposal for disrupting DVE financing through increased information-sharing between the government and financial institutions. Participants also discussed the unique difficulties pertaining to regulation of extremism financing through modern technologies.

The session started by briefly outlining the tools designed to curtail foreign extremism financing, including the Foreign Terrorist Organization (FTO) and Specially Designated Global Terrorist (SDGT) designations of organizations and individuals by the U.S. Departments of State and Treasury. It then surveyed the associated regulatory framework prohibiting the provision of financial services to entities so designated and imposing additional stringent requirements on the banking industry, including verifying that new clients are not on the FTO and SDGT lists during their onboarding and monitoring clients' financial activities to ensure regulatory compliance. The discussion centered on the lack of analogous designations and regulatory frameworks for DVE. While participants stressed the First Amendment arguments against making such designations domestically, they also recognized that the absence of these designations limits the role that banks and other financial institutions could play in curtailing DVE financing.

Participants then turned to discussing a novel proposal to disrupt DVE financing. In essence, the proposal advocates for establishing a public-private partnership through which the U.S. government will share information pertaining to DVE threats with the banking industry. While similar in some respects to the Financial Crimes Enforcement Network (FinCEN) operated by the U.S. government, the proposed public-private partnership will provide much more detailed information, and in time-sensitive situations, actionable intelligence, which will enable banks to better assess the risks associated with providing financial services to certain entities. Some participants stressed the benefits of this proposal, noting that it enables banks to make "risk-based"

business decisions concerning entities potentially linked to DVE without raising the same First Amendment concerns that an official designation of such entities as the domestic analogue of FTO or SDGT would. At the same time, since it is reasonable to assume that providing funds or other financial services to such entities entails an inherent risk, banks will be less likely to do so, and accordingly will disrupt DVE financing. Participants also discussed objections to this proposal, such as the governments' classification concerns and reluctance to provide information that may reveal the methods and means its agencies employ, as well as ways to address these objections through enhanced security measures (e.g., encryption) and modes of information sharing (e.g., geographic heat maps of suspicious activities). Notably some participants expressed serious concerns about private industry conducting risk assessments based on government-provided intelligence and using it as a basis to deny funding or financial services to private citizens.

Finally, participants turned to the question of extremism financing through modern technologies. Participants discussed different technologies used by contemporary domestic violent extremists, such as crowdfunding and cryptocurrencies (e.g., Patreon and Bitcoin). Participants agreed that these technologies present unique challenges for regulators and law enforcement authorities, because the legal framework applicable to them is substantially less robust in comparison to traditional financial industry. Moreover, as is the case with social media, platforms for online funding constantly proliferate and evolve, thus providing extremists with novel and creative means to obtain funds (e.g., soliciting donations in real time while live streaming), which are particularly difficult to regulate or disrupt.

Session 5: Detecting Domestic Violent Extremism – The Intelligence Community Challenge

Moderator

Patrick G. Eddington, Senior Fellow, Cato Institute

Discussion Summary

The 17 agencies comprising the U.S. Intelligence Community (IC) have a vast array of sophisticated and effective tools at their disposal. They also have the authority to use these tools for surveilling non-U.S. persons—including foreign violent extremists. In contrast, these agencies' authority to surveil U.S. persons is substantially limited by varied legal safeguards derived from

the U.S. Constitution, statutes, and executive orders (e.g., the Foreign Intelligence Surveillance Act and EO 12333). Abiding by these important safeguards poses a challenge for the IC even in the context of intelligence operations that focus exclusively on non-U.S. persons, because such operations may still affect U.S. persons. Abiding by these safeguards in the context of DVE, which requires intelligence operations to focus directly on U.S. persons, confronts the IC with even greater, arguably insurmountable, challenges. This session focused on these challenges and potential paths to address them. Participants discussed whether new legal authorities or collection efforts are needed to address the threat of DVE, examined various alternatives, including the creation of a new institution (whether within or outside of government) devoted to collecting and analyzing open-source intelligence on DVE, and explored the dangers of enhancing surveillance in the physical and online context.

The session started with a survey of examples from World War I to the present day, in which the U.S. government, in response to real and perceived threats, has adopted expansive security measures—including continuously increasing the number of its agencies and the amount of information they collect—that negatively affected the liberties of U.S. citizens. Participants used the example of the IC’s possession of crucial information before 9/11 along with its failure to “connect the dots” to demonstrate that the security benefits may not outweigh the costs to freedom. Participants considered whether new legal authorities or collection efforts are needed to address the threat of DVE. Most participants argued there is no such need. Some remarked that even the present number of IC agencies may be excessive and lead to inefficiency (though one participant noted that creating a new agency may lead to better intelligence outcomes, as it will increase constructive competition between agencies). Other participants stressed that the key problem for the IC is not an insufficient amount of information, but rather the budgetary and technical challenges in properly analyzing and synthesizing the *vast* amount of information the IC collects.

Participants then turned to discuss the topic of open-source intelligence and the proposal to create a new institution devoted to collecting and analyzing such intelligence in the context of DVE. Participants distinguished between open-source intelligence collection that is passive (monitoring and collecting information that already exists online) and active (engaging with people

online and eliciting new information), and noted that these two kinds of intelligence collection differ substantially with regard to their legal and ethical ramifications, the latter being more concerning. Participants also remarked that open-source intelligence collection may be challenging from a jurisdictional standpoint, as different jurisdictions have different laws regulating online activity generally, and privacy in particular. Further, participants noted that effective open-source intelligence collection is likely to necessitate cooperation and coordination with private sector entities that control much of the online infrastructure and the pertinent information. Lastly, participants highlighted a curious potential benefit of an agency dedicated to collecting open-source information, namely that its employees do not necessarily need a security clearance. Such agency could, therefore, recruit from a more diverse pool of qualified candidates who are unable to obtain security clearance, thereby attracting non-traditional talent to national security work.

Participants also explored the dangers of enhancing surveillance in the physical and online context. Much of the discussion revolved around the Federal Bureau of Investigation's (FBI) current practice of conducting certain basic investigative actions—"assessments"—without having factual predication (information) about possible criminal activity or national security threats. Participants discussed the various safeguards the FBI has in place to prevent abuse, yet disagreed on whether these safeguards are sufficient. Further, some participants noted more generally that internal safeguards may break down under the demands of the agency mission, and safeguards should be determined by Congress rather than by individual agencies. The discussion then pivoted to the online realm and centered around an analogy between collecting open-source information online, as it pertains to DVE activities, and having law enforcement officials "walk the beat." Arguably, just as there is no reasonable expectation of privacy when officials are patrolling public areas, there can be no reasonable expectation of privacy with regard to information available online. Some participants, however, observed that, as in the physical realm, broad authorities to "walk the [online] beat" may lead to abuses. And other participants pushed back on the analogy, arguing that having no reasonable expectations of privacy in a public space is entirely consistent with having such reasonable expectations in cyberspace.

Session 6: Preventing Domestic Violent Extremism – Strategic and Legal Landscape

Moderator

Jamil Jaffer, Founder and Executive Director, National Security Institute; Assistant Professor of Law, George Mason University

Discussion Summary

The Biden administration’s June 2021 release of the “National Strategy for Countering Domestic Terrorism” marked the first-ever comprehensive government response aimed at addressing DVE. This new national strategy signaled a shift in U.S. counter-terrorism policy away from foreign activity, refocusing federal resources on understanding, disrupting, and preventing DVE. This session evaluated this strategy and the strengths and shortcomings of extant law for countering contemporary DVE. The discussion focused predominantly on whether existing laws are adequate to address DVE and particularly the activities of private militias. Participants considered various proposals to change current law and debated whether they would be advisable and to what extent they could be squared with First Amendment protections. Finally, participants analyzed whether using the label “terrorism,” as it is commonly defined in political science, is useful in the DVE context.

The session started with a discussion on whether existing laws are adequate to address the problem of DVE generally. Participants noted that although the definition of domestic terrorism in the federal code parallels that of international terrorism, there is no domestic terrorism statute that applies to the most common kinds of domestic extremist acts such as mass shootings, or to other prevalent modes of committing such acts (e.g., using vehicles to drive into crowds). Some participants argued that this legal inconsistency leads to incongruous outcomes. For instance, acts that commonly would have been prosecuted under a terrorism statute, had they been committed by those affiliated with foreign extremist groups, can only be prosecuted under ordinary and often ill-fitting criminal statutes, if committed by those affiliated with domestic extremist groups. Similarly, the FBI’s ability to open investigations on actors affiliated with domestic extremist groups is comparatively limited. Moreover, even if domestic violent extremists are investigated and brought to justice, ordinary criminal prosecutions for such acts lack the distinctive punitive and expressive elements inherent to a prosecution for terrorism.

Participants moved on to discuss proposals to address these incongruities through legislation that would treat domestic violent extremism similarly to its foreign equivalent. This discussion also addressed specific legislative proposals pertaining to militia groups, aiming to criminalize, most specifically, the assumption of law enforcement authority and interruption of governmental or legal proceedings by members of these groups. Many participants, despite recognizing that such legislation may have instrumental value, expressed significant reservations. Some participants pointed out the fundamental tension between such legislation and First Amendment protections that would be conceptually difficult to resolve. Others emphasized the pragmatic danger that such legislation could be used to target and suppress dissent and criminalize disadvantaged groups voicing legitimate grievances against the government. Others still called attention to the counterproductive effects that the U.S. government anti-extremism efforts had on the Muslim community in the United States post-9/11, and that the British anti-extremism efforts had on the Irish community in the United Kingdom during the 1980s-90s, stressing that such efforts could both erode trust between law enforcement and law-abiding members of the “targeted” community and serve as a recruitment tool for extremists.

Finally, participants discussed whether using the label “terrorism,” as it is commonly defined in political science, is useful in the DVE context. Upon surveying the three commonly accepted elements of this definition—(1) non-state actor; (2) committing violence for a political purpose; (3) against a civilian target—participants highlighted ways in which this definition may break down in the domestic context. Some noted that breaking into the U.S. Capitol on January 6, for instance, may counterintuitively not be covered under this definition. First, if these acts were directed by the then-sitting president, then arguably they were committed by a state actor. Second, arguably these acts were committed not against a civilian but a governmental target. Other participants noted that using such a definition in legislation designed to counter extremism may also exclude violence perpetrated by extremist groups that are not politically motivated such as the Incels. Overall, conference participants were skeptical that the aforementioned definition of terrorism is particularly useful in the domestic context.

Session 7: Preempting Domestic Violent Extremism: Strengthening Civics Education

Moderator

Ted McConnell, Executive Director, Campaign for the Civic Mission of Schools

Discussion Summary

The 2021 Annenberg Public Policy Center’s annual civics survey found that over 40% percent of U.S. adults cannot correctly name all branches of government.⁵ With only nine states and the District of Columbia requiring one full year of teaching U.S. government or civics, the amount of time and resources dedicated to civics education in high schools across the country has declined considerably over the past decades. The resulting lack of civics knowledge may leave large swaths of the American public susceptible to the spread of disinformation and attempts to sway public affairs. Further, civics education is absent in the training of most military personnel; the DOD Common Military Training has no civics education requirement nor do the corresponding regulations for the Army, Navy, Marine Corps, or Air Force. The prevalence of erroneous claims about constitutional rights voiced by military personnel, including veterans who took part in January 6 events at the U.S. Capitol, raise further serious concerns. This session focused on three main themes, namely the connection between civics education and radicalization in children and young adults and means to address it; the aspects that civics education initiatives should include; and the ways civics education could be strengthened in the military community while balancing the risk of state-led civics education efforts becoming or being perceived as disinformation campaigns.

The session started by surveying the history of civics education in the United States and the decline in such educational programming, which could be tracked back to the 1957 launch of the Sputnik satellite by U.S.S.R., and the subsequent U.S. emphasis on enhancing education in science, technology, engineering and mathematics (STEM), which occurred at the “expense” of civics. The decline in civics education has continued to this day, and presently, the federal investment per student in STEM education exceeds federal investment in civics education by several orders of

⁵ For the Annenberg Public Policy Center’s 2022 civics survey, finding that over half of U.S. adults cannot correctly name all branches of government, see <https://www.annenbergpublicpolicycenter.org/americans-civics-knowledge-drops-on-first-amendment-and-branches-of-government>.

magnitude. Moreover, even the limited federal investment in civics education is not uniform, resulting in an opportunity gap, negatively affecting historically marginalized communities.

Participants then considered the connections between civics education and radicalization in children and young adults and means to address them. Some participants, for instance, criticized the U.K. model to address such radicalization, requiring teachers to report students suspected of being at risk of radicalization to state authorities. Participants stressed that reducing radicalization among at-risk population requires, in contrast, building communities of trust—in this case, among teachers, parents, students, and public officials. Moreover, participants mentioned that investment in civics education may be a valuable strategy for preventing and reducing radicalization, by enhancing students' understanding that they can make a difference in society without resorting to violent means and teaching them the tools to do so.

Participants also discussed the aspects that civics education initiatives should entail. Some participants emphasized the importance of not just civic knowledge, but also of civic skills and disposition. These include appreciating that one has the burden to provide grounds to others about one's convictions, being able to present such grounds, and acknowledging the authority of others to challenge them. A proficiency with moral ambidexterity (i.e., the ability to hold two conflicting moral positions in one's mind) is also necessary to fully grasp and successfully manage the complex value tradeoffs that democracy requires. Other participants stressed the importance of discrete practical skills, such as writing an effective letter to one's local representative, alongside life-long commitment to civic engagement. Others still maintained that teaching how to identify biased perspectives, misinformation, and disinformation is a necessary component of modern civics education, noting that older populations' deficiencies in digital literacy make them the most at-risk of being misinformed.

The discussion then turned to the ways civics education could be strengthened in the military community, while balancing the risk of state-led civics education efforts becoming or being perceived as disinformation campaigns. Participants noted the need to strengthen civics education in the military, *inter alia*, because DVE organizations target the military community (especially veterans), for recruitment. Participants discussed potential avenues for teaching civics in the military. Some suggested that an emphasis on critical thinking skills would be particularly

valuable in this context. Others noted that civics education in the military should be continuous and comprehensive and that mandating a few hours of military “training” on civics is unlikely to be sufficient. And others suggested that civics education in the military should revolve around the oath all U.S. servicemembers are required to take to “support and defend” the Constitution. Participants also discussed the risks associated with state-led civics education initiatives in the military, specifically that they would be perceived as an illegitimate indoctrination effort. While some participants argued that full transparency about these initiatives could assuage such concerns, others suggested to the contrary, that explicitly connecting civics education and preventing DVE in the military could create negative perceptions and prove counterproductive. Participants broadly agreed that strengthening civics education in the military would be valuable, but that such efforts should be initiated upon careful consideration of the concerns about how they might be perceived within the military as well as within the broader, sharply divided, national political environment.