

COUNTERING VIOLENT EXTREMISM IN THE UNITED STATES

CLAIRE ATWOOD AND SARAH JACOB

Abstract

As the post-9/11 threat landscape has evolved, the United States has struggled to adapt its prevention and risk mitigation efforts accordingly. One such effort, countering violent extremism (CVE), captures the mixed success of the federal government's efforts to prevent and protect against the threat of violent extremism. The reality of modern radicalization is fluid and complex, rendering CVE efforts ineffective at best and counterproductive at worst. This study examines the effectiveness of CVE efforts within the United States in light of the current threat environment, similar lines of efforts by the United Kingdom, and comprehensive research by field experts. It concludes that CVE efforts are constrained by ambiguity and tenuous relationships with key communities. Ultimately, this study recommends a holistic approach to countering violent extremism that begins with clearly defining the threat and culminates in a whole-of-society approach grounded in accessible research, strengthened community engagement, and balanced adjudication of offenders.

Introduction

In September 2014, President Barack Obama stood before the United Nations and demanded an escalation in global efforts to counter violent extremism (CVE): “It is time for a new compact among the civilized peoples of this world to eradicate war at its most fundamental source, and that is the corruption of young minds by violent ideology” (White House/Office of the Press Secretary, 2014, para. 30). Although the imperative was lauded internationally, it was a demand for a solution to a nebulous problem. Despite many policy efforts and trillions of dollars that have been poured into extinguishing violent extremism, the increasing potency and reach of terrorist groups has left United States law enforcement and intelligence officers scrambling for a cohesive strategy. The pursuit of such a strategy has spawned inadequate policies that this study seeks to address. This study aims to define the issue, examine the current and future threat environments, explore current United States and United Kingdom CVE policies, evaluate policy issues, and provide policy recommendations to address identified gaps and vulnerabilities.

Definition

It is difficult to define what it means to “counter violent extremism” because there is not yet an agreed-upon definition of “violent extremism.” Generally, countering violent extremism (CVE) refers to the “soft” side of counterterrorism strategies (Frazer & Nunlist, 2015). This soft approach is characterized by a focus on the ideological, political, and social drivers that push an individual to radicalization. Radicalization is a fluid, nonlinear, and highly individualized process (Holmer, 2013). It is thought to be predicated upon a dynamic set of drivers, which can include structural conditions, psychological and emotional characteristics, the influence of group dynamics, and the allure of social messaging. However, these diverse factors are not predictive of radicalization and only provide a rudimentary understanding of the extremist psyche.

Background

Although the United States can trace the formal genesis of CVE efforts to 2014, initiatives to counter violent extremism began over a decade earlier. The aftermath of the terrorist attacks on September 11, 2001, fostered a paradigm shift towards prevention. The attacks highlighted the evolving nature of warfare and terrorism, particularly the rise of decentralized actors, self-radicalized small groups, and lone wolves (Holmer, 2013). It also highlighted the inadequacy and damaging effects of Cold War era counterterrorism tactics. Governments began to realize that the

pursuit and apprehension of terrorists had to be addressed in conjunction with countering recruitment efforts. As early as December 2001, the Organization for Security and Cooperation in Europe (OSCE) demanded that global terrorism be countered not only with military and intelligence means, but also by identifying and eradicating its root causes (Frazer & Nunlist, 2015).

Current Situation and Future Threats

Violent extremism is constantly changing in its form and methods. It is characterized by a broad range of actor profiles, motivating drivers, and manifestations. Violent extremists may commit violence in alignment with a cause, in reaction to a policy shift, or as a result of a myriad of other factors. While there is a concerning lack of a definitive equation for violence, there are identified triggers within the current threat environment that decision makers and their auxiliaries ought to consider. Overall, governments should expect growing competition among terrorist networks, infrequent and less sophisticated attacks, and a diverse array of recruits. In alignment with this future state, CVE efforts must anticipate new technologies, infrastructure, and innovation within the area of violent extremism (“The Future,” 2016).

The widespread accessibility to and use of social media platforms has been a primary influence on the methods of violent extremism today. Extremists now have the ability to identify and directly recruit vulnerable individuals across the globe. Although YouTube, Twitter, and Facebook have been heavily touted as breeding grounds for recruitment, extremists are increasingly turning to platforms that provide greater anonymity and encryption capabilities, such as WhatsApp and Telegram. They have also experimented with lesser-known platforms such as Friendica, Diaspora, KIK, WICKR, and VKontakte (“The future,” 2016). Although it is expected that terrorists will continue to rely heavily on higher-profile platforms, these niche platforms are less porous and may gain sizeable memberships, posing a security vulnerability for governments that do not focus resources towards monitoring these platforms.

Social media can also enable extremist groups, particularly in their efforts to recruit Muslim youth. As noted by Scott Atran, Muslim millennials throughout the world are suffering from a profound identity crisis (Green & Proctor, 2016). The resulting ennui is exploited heavily by terrorist recruiters. Atran elaborated, “Joining a violent extremist movement is, for many, an aspirational social act—an opportunity to gain power, prestige, and status; to address the abuses suffered by their coreligionists; or to participate in a utopian effort to remake the world” (as cited in Green & Proctor, 2016, p. 16). It should be noted, however, that terrorist groups have recognized the current Western focus on youth preservation and have

thus begun to diversify their recruitment pool. They have increasingly reached out to women, as well as older and younger generations. Women in particular are assuming high-profile roles as supporters, mobilizers, and members of terrorist groups, and should be monitored as a key feature of the future landscape (“The future,” 2016).

Furthermore, it is expected that the military campaign against ISIS in Syria and Iraq and improved intelligence and law enforcement efforts aimed at foreign fighters will prompt more concerted efforts towards homegrown extremism (“The future,” 2016). This will continue the trend of attacks perpetrated by lone actors or small groups against individuals and soft targets. The appeal of these attacks lies in their low-cost, high-benefit framework. The weapons are usually less sophisticated and are easy to acquire. Little training is required to use them. Due to the lack of a planning and coordination trail, such attacks are harder to anticipate and potentially more lethal.

In order to properly evaluate and critique current U.S. CVE policies, it is important to examine both domestic and international efforts. This study examines both U.S. and U.K. CVE policies. This is primarily due to the U.K.’s tragic history of mass attacks and continuing struggle against violent extremists. Additionally, the U.K. shares a number of political and ideological characteristics with the U.S., making it an effective case study. This provides greater insight into gaps and vulnerabilities inherent to U.S. policy, as well as the broader applicability of lessons learned and best practices.

Lines of Effort in the United States

In 2011, the Obama White House issued its “National Strategy for Empowering Local Partners to Prevent Violent Extremism in the United States.” The document marked the first formal national strategy to supplement law enforcement counterterrorism tactics with auxiliary prevention measures. Prior to the Strategy’s release, law enforcement efforts had largely been localized with little interoperability. These efforts were reactive in nature, including surveillance, investigations, and prosecutions (Patel & Koushik, 2017). A string of global attacks shed light on domestic vulnerabilities, primarily the lack of a concerted and coordinated offensive CVE strategy.

The resultant National Strategy has three prongs. First, identifying vulnerable and at-risk individuals. Such individuals, often young people, tend to have exhibited signs of alienation and to have adopted “radical” ideas. Second, funding and facilitating programs that mitigate the socioeconomic factors that are thought to contribute to radicalization. This includes the provision of health, education, and social services to vulnerable communities. Third, developing and promoting counterpropaganda. Historically, this has also included monitoring and suppressing

messages that encourage extremism and pressuring social media platforms to remove extremist content and promote counter-messages (Patel & Koushik, 2017). In 2014, the Department of Justice (DOJ) piloted this multifaceted strategy in Boston, Los Angeles, Minneapolis, and Montgomery County, Maryland. Additionally, the Federal Bureau of Investigation (FBI) launched concomitant initiatives. The Department of Homeland Security (DHS) established the Office of Community Partnerships (OCP), which distributes \$10 million in Congressionally-appropriated grant funding to police departments, academic institutions, and non-profit groups (Patel & Koushik, 2017).

In October 2016, the White House released the “Strategic Implementation Plan for Empowering Local Partners to Prevent Violent Extremism in the United States.” The plan provides an updated actionable arm to the National Strategy that had been released five years earlier. It outlines a multi-tiered approach to CVE, with delineated efforts at the federal, local, and individual levels. The federal government’s role in CVE efforts is to act as “a convener, facilitator, and conduit for relevant information” (Executive Office of the President, 2016, p. 3). Local efforts aim to build resilient communities through local youth engagement, internet safety education, community service, and other community-led local initiatives. In order to maximize effectiveness and interoperability, these initiatives are to be integrated into existing programs and public safety strategies. At the individual level, CVE efforts focus on identifying behavioral indicators and reporting any suspicious behaviors.

As stated, the National Strategy had identified three priority action areas: (1) enhancing engagement with and support to local communities, (2) building government and law enforcement expertise for preventing violent extremism, and (3) countering violent extremist propaganda while promoting American ideals (Executive Office of the President, 2016). The new Strategic Implementation Plan delineates four lines of effort that correspond to these priority action areas. These include Research and Analysis, Engagement and Technical Assistance, Interventions, and Communications and Digital Strategy (Executive Office of the President, 2016). The CVE Task Force, which is comprised of DHS, DOJ, FBI, NCTC and other federal departments and agencies, is tasked with managing these efforts. These federal entities are also responsible for “funding research, disseminating best practices, issuing grants, and building partnerships with non-government stakeholders” (Executive Office of the President, 2016, p. 3).

Research and Analysis

The research component of domestic CVE efforts is primarily tasked to DHS and DOJ. The plan harnesses the resources of federally-funded research and development centers (FFRDCs), academic partners, government analysts, and private-sector program implementers

to build expertise on topics such as recruitment narratives and tactics, radicalization to violence, the role of the Internet in the radicalization process, youth radicalization and recruitment, behaviors commonly undertaken during mobilization to violence, and what motivates individuals to travel to conflict zones and join violent extremist groups. (Executive Office of the President, 2016, p. 5)

There are three tasks outlined within Research and Analysis. The first is to map existing CVE-relevant research and analysis, identify gaps, and coordinate future projects. As part of this task, the CVE Task Force and Department of State jointly conduct CVE research with foreign partners through bilateral research and development agreements. The second task is to increase stakeholder access to research and feedback. This includes synthesizing and sharing research findings with stakeholders, increasing the applicability of CVE research and analysis, and ensuring that research products inform CVE training. The third task is to establish evaluation methods for CVE programs. This effort builds on previous assessments conducted by DHS, DOJ, and USAID to develop benchmarks that measure program effectiveness.

Engagement and Technical Assistance

Engagement and Technical Assistance focuses on building community outreach and engagement programs to foster information sharing and coordination between local communities and the federal government. Prior engagement efforts have included local “roundtable” discussions featuring officials with special expertise to address the unique challenges facing a jurisdiction. In addition to these prior efforts, the CVE Task Force now coordinates regional CVE engagements to provide training and technical assistance. This assistance includes sponsoring regional support staff to provide CVE-specific expertise to local community authorities, providing customized trainings and presentations (i.e., Community Awareness Briefings and Community Resilience Exercises), and stewarding direct government grants and funding assistance (Executive Office of the President, 2016).

Interventions

The fourth line of effort, Interventions, is perhaps the most controversial. Designed to identify alternative pathways for individuals who are progressing towards violent extremism, intervention approaches are multidisciplinary and are applied on a case-by-case basis (Executive Office of the President, 2016). For instance, a mentally-ill individual who has progressed to virulent expressions of extremist thought on social media would benefit from a rehabilitation program, whereas a teenager who has only recently begun their foray into extremism would

benefit from a disengagement plan. The first step of intervention is identifying the candidate. This is to be accomplished by disseminating resources and training to American citizens to educate them on the signs of radicalization. The second step is developing local intervention models, which are supported by multidisciplinary teams of mental health professionals, local law enforcement officials, and non-government representatives (Executive Office of the President, 2016). The Strategic Implementation Plan ultimately aims to enable local officials to develop and maintain these teams independently of the federal government.

Communications and Digital Strategy

Digital communication is a primary and powerful recruitment tool in the violent extremist's arsenal. The rapidly shifting digital environment and broad accessibility of platforms also makes it particularly challenging for the federal government to address. Instead of focusing resources on identifying and shutting down potentially dangerous actors and social media accounts, the Strategic Implementation Plan adopts a counter-narrative approach. To this end, the CVE Task Force seeks to develop a new online platform, including a public website to provide and adapt resources to local and individual contexts. This platform will centralize and streamline "access to: training; research, analysis, and lessons learned; financial resources and grant information; networks and communities of interest; and intervention resources" (Executive Office of the President, 2016, p. 13). Additionally, the Task Force will develop a social media strategy that promotes American ideals and provides a counter-narrative to extremist recruitment.

Lines of Effort in the United Kingdom

The concept of CVE entered European political thought following the 2004 Madrid and 2005 London attacks. The attacks spurred widespread fears concerning homegrown Islamist terrorism and, as with the U.S., shed light on gaps and vulnerabilities within European security and counterterrorism approaches. The first precursor to an established "CVE" program was the *Prevent* initiative, which ran from 2005 to 2011 (Frazer & Nunlist, 2015). The project focused on developing local projects to hinder jihadist radicalization. The program was rooted in the European Union's four-pillar counterterrorism framework: prevent, protect, pursue, and respond (Frazer & Nunlist, 2015). This complemented the United Nations' call in 2006 for a "holistic" approach to global anti-terrorism initiatives that would consider the socioeconomic factors of radicalization. Although the program was eventually shut down, its fundamental idea continues to frame U.K. CVE policies. This fundamental idea is the same idea that characterizes U.S. policy: that the

terrorist profile, however ill-defined and spectral, can be identified and mitigated by community-led approaches (Cottee, 2015).

This community-centric approach was mandated by the U.K.'s 2015 Counterterrorism and Security Act. The Act frames violent extremism as an illness of sorts; an ideological contagion to which vulnerable individuals helplessly fall prey (Cottee, 2015). This mentality removes any vestige of responsibility from the person and lays it entirely on his upbringing, education, and society. "Early intervention" has been the primary approach to coping with vulnerable individuals. The Act obligates community partners, such as teachers, social workers, and "credible community organizations," to monitor their charges for vulnerability indicators (Cottee, 2015, para. 6). Once identified, these individuals are processed through the British government's radicalization referral program. There were 796 referrals during the summer of 2015 alone, which aligns with the rapid ascension of ISIS in 2014 (Cottee, 2015).

Like the U.S., the U.K. has also adopted a counter-narrative strategy. In 2011, the Home Office and a secretive government department called the RICU (Research, Information, and Communications Unit) began developing a grassroots network of Muslim voices to provide counter-narratives to British Muslim youth. These counter-narratives are disseminated through multimedia campaigns that target specific groups of internet users "chosen on the basis of their demographics, the websites they visit, the social media accounts they 'follow,' and the search terms they use" (Hayes & Qureshi, 2016, para. 6). These multimedia campaigns are provided with technical and financial assistance from the government and selected PR firms. Some of these campaigns contain headlines such as "Open Your Eyes: ISIS Lies," "The Truth About ISIS," and "Making a Stand" (Hayes & Qureshi, 2016, para. 6). This counter-narrative program was covert until it was discovered in 2016, with Parliament being entirely unaware of its existence.

In its development of a CVE strategy, the U.K. also pioneered the censorship of "terrorist content" with the establishment of the first Counter-Terrorism Internet Referral Unit (CTIRU) in 2010 (Hayes & Qureshi, 2016). The CTIRU was modeled after the Child Exploitation and Online Protection Agency, which censors child pornography. It provides a central point of contact for law enforcement and intelligence officers seeking to block web pages or close social media accounts. CTIRU refers these requests to accommodating internet service providers, search engines, and content platforms who can elect to block or take down the content. These ad hoc public-private partnerships between CTIRU and Silicon Valley have resulted in the take-down of over 120,000 pieces of unlawful terrorist-related online content (Hayes & Qureshi, 2016).

Policy Issues

Ambiguity of Terms and Focus

CVE programs suffer from a lack of clear terms and goals. Even before considering the subject's particular ambiguities, policymakers and law enforcement officials have difficulty distinguishing CVE actions and goals from counterterrorism actions and goals (Challgren, Kenyon, Kervick, Scudder, Walters, & Whitehead, 2016). There is no international consensus on what can be defined as "violent extremism" (Anyadike, 2016). Even once actors settle on a working definition, the scale and complexity of the problem fluctuates greatly among different communities (McKenzie, 2016). The process of violent radicalization has limited universal indicators, thus reducing the probable success of any catch-all strategic response (Challgren et al., 2016). CVE actors, particularly law enforcement, have assumed that there are particular behaviors and backgrounds that radicalized persons will share in common. However, these factors are often extremely broad and subjective. This will likely result in a large number of false positives, which can potentially have lasting ramifications (Patel & Koushik, 2017).

Inconclusive Knowledge Base

An underlying assumption of CVE programs is that the process of radicalization is defined by a predictable framework. This framework is supposedly characterized by static signposts, or "red flags," that law enforcement officials, peers, teachers, and family can identify (Patel & Koushik, 2017). However, this assumption is fundamentally flawed and disputed by established research. Empirical studies, including those funded by the U.S. government, have concluded that the path of radicalization is fluid and adaptable to the subject (Patel & Koushik, 2017). By forcing radicalization into preset parameters, the government has effectively ignored those aspects of radicalization that arguably require the greatest amount of study and resources. This includes studying homegrown terrorists who have no history of mental illness or religious affiliation—two "reliable" drivers ascribed to extremist behaviors (Patel & Koushik, 2017).

Stigmatization and Distrust

The Trump administration is seeking to focus U.S. CVE efforts explicitly and almost exclusively on Muslim communities. This effort results in the stigmatization of Muslim communities as inherently suspect (Patel & Koushik, 2017). Such a narrowly focused CVE strategy could undermine efforts to incentivize the very communities that the government is reliant on for assistance (Rosand, 2017a). Muslim community members are essential partners in preventing radicalization and recruitment to violence. They are unlikely to partner with government actors if

they feel that law enforcement is conducting ideological policing and surveillance. Critical responses to the FBI program “Don’t Be a Puppet: Pull Back the Curtain on Violent Extremism” exemplify the fermenting division and distrust. The program is an interactive website that teaches teens how to recognize violent extremism messaging. Critics question why the FBI is in charge as opposed to an NGO or the Department of Education. They predict a chilling effect in schools and immigrant communities (Rosand, 2017a). Damaged relationships between law enforcement and Muslim communities will undermine the mutual goal of preventing terrorism. If Muslim community members feel pressure to restrict discourse and debate, terrorist narratives will be driven underground and thus be harder to combat (Patel & Koushik, 2017). Community-level programs have begun to recognize and adjust based on these concerns. Rather than using the term “CVE” for fear of community backlash, local programs are increasingly using labels like “building community resilience” or “preventing targeted violence” (Rosand, 2017a, para. 5).

Confused and Constrained Actors

CVE efforts in the United States also suffer from a lack of coordination and defined roles. Multiple federal agencies are involved in CVE on the national level. They are expected not only to work with one another but also to work with state and local law enforcement, NGOs, and community leaders. Partners are easily confused, and there is no clear division of labor (Rosand, 2017a). This can lead to duplication of efforts or, even worse, gaps in coverage. The federal government has yet to fully develop measures to handle young persons who are sympathetic to extremist causes. For example, federal law enforcement is currently limited to arresting and prosecuting young people suspected of supporting the Islamic State who do not yet pose a security threat (Rosand, 2017a). Government funding for CVE efforts is also limited to short-term, tactical efforts (Rosand, 2016).

Ethical Issues

Undermined Relationships

When used by the government, CVE soft tools risk becoming a system of soft surveillance, to the detriment of crucial social compacts. Even when not run by government actors, many CVE programs closely cooperate with law enforcement officials without safeguards to prevent the exchange of confidential information (Patel & Koushik, 2017). Through CVE programs, law enforcement receives reporting from community members traditionally bound by confidentiality—counselors, doctors, social workers, etc. As community members become aware of these connections, they may withhold information that they believe will be reported to the police. This undermines relationships and limits effective service.

The American Federation of Teachers, the country's second largest teachers' union, warned that any CVE program verging on "ideological profiling and surveillance" will have "a chilling effect on our schools and immigrant communities, jeopardizing children's sense of safety and well-being and threatening the security and sense of trust of entire communities" (Patel & Koushik, 2017, p. 17).

Abuse of Ambiguities

Conceptual clarity is crucial as the government further explores the purpose and desired effects of CVE strategies and policies. As indicated in the earlier section on ambiguous terms and focus, there is no clear definition of who constitutes an "extremist." This term's ambiguity could allow actors to impose their personal or political agendas (Hadra, 2016). CVE officials must carefully avoid misusing or abusing the term "extremist." Additionally, politicians should be cautious in labeling programs as "CVE," as misinterpreted intentions or crossed boundaries could further destabilize vulnerable communities (Hadra, 2016). Overly broad interpretations of CVE will likely exacerbate feelings of stigmatization or marginalization in suspect communities, thus heightening community-level tensions (Rosand, 2016).

Blurred Lines

The government's CVE efforts obscure the intentions and roles of community members and suspected radicalized persons. As CVE strategy seeks to prevent religiously-motivated or ideologically-motivated violence, it risks flagging innocuous activity as pre-terrorism and suppressing religious speech (Patel & Koushik, 2017). There is a temptation to equate protest, rebellion, and unfamiliar religious beliefs with "violent extremism" (Anyadike, 2016). Even with obvious radical movements, federal actors may apply broad assumptions to distinct movements without first disaggregating them. As law enforcement works with key community members, it also risks transforming CVE programs into intelligence collection operations. Community members may be pressed to serve as conduits for the personal information of individuals who are not even suspected of involvement in terrorism (Patel & Koushik, 2017). These community members should not be placed in a position where they feel forced to choose between neighbor and country.

Recommendations

Recommendation 1: "Whole of Society" Partnerships

Following Canada's lead, the United States should take a "whole of society" approach to CVE efforts. Commenting on Canada's new CVE coordination body, Prime Minister Justin Trudeau explained its purpose as providing "national leadership, coordination, and support to prevent the radicalization of young people"

(Rosand, 2017b, para. 10). The body's explicit purpose indicates the government's effort to attract broad-based community and non-law enforcement support. As the United States continues to adjust its CVE efforts under the Trump administration, it must emphasize diversity of governmental and nongovernmental stakeholders and the formation of durable, trust-based partnerships (Rosand, 2016). Governmental CVE efforts cannot be viewed as exclusively serving a security agenda. Government officials should partner with local communities, strengthening relationships to build trust between all levels of government and society. As initiatives emerge at the local and state levels, the federal government should encourage the creation of a range of reinforcing networks outside the law enforcement sphere (Rosand, 2017a). Throughout this process, CVE actors should consult experts from other fields including development programming, conflict and peacebuilding, communications campaigns, counterterrorism, and public health campaigns for lessons learned (Glazzard & Rosand, 2017). The utilization of such wide-ranging expertise acknowledges the complexity and many remaining unknowns of CVE.

Recommendation 2: Community Engagement

America's CVE strategy must move from a state-centric approach to a community-centric approach. Programs must be framed by community concerns rather than by the concerns of donors, national authorities, and international organizations (Rosand, 2016). They should be locally owned when possible and should always be responsive to local demands. When communities request federal assistance, it should come without bureaucratic or political strings attached (Rosand, 2017a). Specific agency participation should be transparent and clearly articulated. As efforts focus on the local level, CVE actors must acknowledge and learn from failed programs. Pilot programs in Boston, Los Angeles, and Minneapolis were widely criticized by Muslim communities for their lack of cultural and communal understanding. American Muslim leaders explained that most eventual attackers were radicalized in small, cloistered groups rather than in open, social settings (McKenzie, 2016). As government actors collaborate with Muslim communities, outreach efforts should be centered on community concerns without an explicit counterterrorism framework. For local governments who oppose the Trump administration but want to participate in CVE efforts, they should be encouraged to develop their own initiatives that can attract resources and other support from local businesses, leaders, and nonprofits (Rosand, 2017a).

Recommendation 3: Accessible Research

Federal government agencies should encourage and participate in expanded cross-disciplinary research on CVE. As new programs move past the implementation stage, actors should be transparent about CVE successes and failures. Knowledge

gained from pilot projects should be used both to expand what works and to contribute to the shared evidence base (Glazzard & Rosand, 2017). As evidence is compiled, the government should remain open to funding experimental efforts. Innovative ideas should be encouraged, particularly in a field where effectiveness and success are difficult to measure (Rosand, 2017b).

Recommendation 4: Trustworthy Alternatives

The government must develop clear alternatives to law enforcement where community members can report alarming behavior. Early intervention tools are most effectively utilized on the local level (Hadra, 2016). Teachers, family members, counselors, and other community members must feel comfortable conducting interventions without fear of prosecution. Even if intervention programs are funded by the federal government, they should be tailored to specific needs, replicating community drug courts that deal with addiction (McKenzie, 2016). Social and educational programs like conflict resolution and youth engagement must be situated explicitly outside the counterterrorism umbrella. When community members choose to report their suspicions to law enforcement, there should be clear, customized federal guidelines for such referrals (Rosand, 2017a).

Recommendation 5: Rehabilitation and Reintegration

The government must support the development of off-ramps for extremist offenders. The criminal justice system lacks adequate policies and programs to address extremist offenders. The traditional zero-tolerance approach towards terrorism inhibits the possible rehabilitation and reintegration of previously radicalized persons. Instead, the government should establish federal policy that allows judges greater sentencing authority (Rosand, 2017a). When appropriate, judges should have the ability to issue reduced or alternative sentences for extremist offenders who agree to participate in rehabilitation or reintegration programs (Rosand, 2016). Alternatives to criminal prosecution and incarceration are more likely to facilitate the cooperation of family, friends, and other community members to assist in the deradicalization process. For persons already imprisoned, the Federal Bureau of Prisons needs to do more. Although there is a growing number of persons in federal prison for nonviolent terrorism charges, there are no tailored plans for rehabilitating them in prison or reintegrating them into society upon release. Customized counseling and vocational training should be provided for this unique type of prisoner (Hadra, 2016). During the development of such programs, criminal justice officials and the public must understand that the government is not going “soft” on terrorism. Rather, it is implementing processes that will reduce the threat (Rosand, 2016).

Recommendation 6: Name the Problem

A study of the National Strategy and its auxiliary documents reveals a tendency towards vague language and unhelpful platitudes. These documents delineate a number of drivers, ranging from the psychological to the conditional. Yet, there is no mention of what is arguably the most potent driver: religion—specifically, Islam. This is a stunning omission considering that former Secretary of State John Kerry used the term “Muslim majority countries” in his foreword to the Department of State & USAID Joint Strategy on Countering Violent Extremism (Simcox, 2016). From there, the document quickly retreated from any mention of Islamist extremism or Islam broadly. This highlights an overall dishonesty in the government’s policy approach to CVE. It is nearly impossible to address “root causes” when policymakers are unwilling to name and address a primary root cause in the name of political correctness. Islam is, and has been, a primary driver of violent extremism. It is a religion that encourages and incites violence among its radically devoted adherents. By failing to acknowledge the role of Islam in radicalization, policymakers create a knowledge gap in CVE strategy and thus fall short of fully understanding the root causes of extremism.

Conclusion

Actors across all levels of government and society must continue to make strides in the CVE space. They must progress, however, with the awareness that CVE will always be controversial and that its success will be difficult to measure. Current problems with U.S. CVE efforts are not limited to lack of funding or poor coordination. Rather, the underlying problem is that CVE is an ambiguous concept that does not always adhere to the standard American method of fighting evil (McKenzie, 2016). The partisan divide has further impeded efforts to develop a comprehensive and sustainable plan to prevent future terrorist attacks. Politicians will inevitably ask for quantifiable successes, even in a field where success is difficult to quantify (Challgren et al., 2016). CVE successes are “non-events.” Effective CVE efforts in the United States will consist of community members looking out for one another, law enforcement foiling planned attacks, and the criminal justice system rehabilitating and reintegrating at-risk persons.

Reference List

- Anyadike, O. (2016, August 10). Does countering violent extremism work? *IRIN*. Retrieved from <https://www.irinnews.org/analysis/2016/08/10/does-countering-violent-extremism-work>
- Challgren, J., Kenyon, T., Kervick, L., Scudder, S., Walters, M., & Whitehead, K. (2016). Countering violent extremism: Applying the public health model. *Georgetown Security Studies Review, National Security Critical Issues Task Force*. Retrieved from <http://georgetownsecuritystudiesreview.org/wp-content/uploads/2016/10/NSCITF-Report-on-Countering-Violent-Extremism.pdf>
- Cottee, S. (2015, October 27). The pre-terrorists among us. *The Atlantic*. Retrieved from <https://www.theatlantic.com/international/archive/2015/10/counterterrorism-prevention-britain-isis/412603/>
- Executive Office of the President. (2016). *Strategic implementation plan for empowering local partners to prevent violent extremism in the United States*. Retrieved from https://www.brennancenter.org/sites/default/files/2016_strategic_implementation_plan_empowering_local_partners_prev%20%282%29.pdf
- Frazer, O., & Nunlist, C. (2015). The concept of countering violent extremism. *Center for Security Policy Analyses in Security Policy*, 183. Retrieved from <http://www.css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/CSSAnalyse183-EN.pdf>
- The future of the violent extremist threat. (2016). *Center for Strategic & International Studies*. Retrieved from <https://medium.com/center-for-strategic-and-international-studies/the-future-of-the-violent-extremist-threat-780a86aaec5a>
- Glazzard, A., & Rosand E. (2017, June 11) . Is it all over for CVE? *Lawfare*. Retrieved from <https://www.lawfareblog.com/it-all-over-cve>
- Green, S., & Proctor, K. (2016). *Turning point: A new comprehensive strategy for countering violent extremism*. Center for Strategic & International Studies. Retrieved from <https://www.csis.org/features/turning-point>

Simcox, R. (2016). The unmentionable origins of terrorism. *Heritage Foundation*. Retrieved from http://www.heritage.org/defense/commentary/the-unmentionable-origins-terrorism?_ga=2.80139415.141239306.1511484080-439873825.1511484080

White House/Office of the Press Secretary. (2014, September 24). *Remarks by President Obama in address to the United Nations General Assembly* [Press release]. Retrieved from <https://obamawhitehouse.archives.gov/the-press-office/2014/09/24/remarks-president-obama-address-united-nations-general-assembly>