THROUGH A LOOKING GLASS:

AN EXAMINATION OF U.S. COUNTER DOMESTIC VIOLENT EXTREMIST ACTIVITIES

Avante Edge Research

June 2025

Table of Contents

Introduction

Violence has been a tool throughout humanity, it is neither good nor evil, but simply mirrors the purpose and intent of its usage. Terrorism is the use of violence, being politically or ideologically motivated, against targets to induce fear and aim to cause change (FBI, 2020). Countering terrorism and violent extremists of all kinds is not something that is easily accomplished. The U.S. has been one of the leading counter violent extremism (CVE) actors since the 2001 attacks against the World Trade Center in New York. Heavily focused externally, the U.S. realized it also needed to match effectiveness to domestic counter terror operations as yet it still has difficulties with domestic terror on its sovereign soil. In this paper we will analyze the U.S. Governments 2011 approach to CVE domestically and how it has been executed along with the nuances of influence and radicalism and how technology plays a role.

Investigating Success

The Strategic Implementation Plan for Empowering Local Partners to Prevent Violent Extremism in the United States (SIP) is a document that assigns a whole of government effort to strengthen state and local Law Enforcement Agencies (LEA) with both capabilities and education to combat extremism. Beyond that, it also attempts to designate agencies to engage with communities that are in danger of radicalization, while simultaneously countering propaganda with the promotion of ideals (SIP 2011, 2). It attempted to be thorough yet flexible, as it recognized that changes in forms and functions of radicalization would occur.

As we assess the effectiveness, let us state some initial key aspects of the document. This document was created with heavy emphasis on Islamic extremism and the terror group Al Qaeda. Meaning that the ideas and solutions presented are not effective against all kinds of radicalization. There is also an interesting assumption that is characterized by the tone of the work, which seems to believe that there is no possibility of internal issues of influences, bias, or extremism among the government entities involved. The paper, besides one aspect of the DoD (Department of Defense) has zero insight on the fact that society makes up its agencies, thus the same type of people abroad in the country are the same people inside their own organizations. Humans are humans and they act relatively the same unless they are extremely cognizant of themselves and how humans operate.

Between the years of 2010 and 2021, there were 231 events that fell in the realm of domestic terror or a plot to commit and attack (GAO, 2023). When examining the data surrounding attacks on the U.S. Homeland, the Department of States (DoS) archived reports on terror reveal that though no Islamic based terror attacks were successful in the US in 2011 (DoS 2012, 6), and when looking down the line towards the present, there were increases of Jihadist plots and attacks that rose until ~2015/2016 time frame and have been in decline since (Palmer et al 2025, 4). There were recorded successful attacks/attempts the year before and after the document according to CSIS, so either this was a coincidence or there was an initially successful effect of the SIP. With these facts, we can see that the document and ideas were possibly initially effective in its scope towards Islamic extremism, but certainly had seemingly little ability to stop both domestic terror from racial/ethnic, anti-government, environmental rights, or other groups (GAO, 2023) and Islamic terror. With regards towards domestic extremism, the government, after analyzing this in 2023, it sought the need to further strengthen collaboration and integration among federal agencies. This statement is interesting as it is reflected in an opposite manner from earlier document in 2016, which was the SIP's fourth year review. This document stated the need to strengthen collaboration yes, but instead with private sectors and academia to capitalize on technologies and specialists outside of government agencies (SIP 2016, 14). That is an excellent recommendation, and we will focus on that in the following section.

Effective Elements

The 2011 document would be assessed as a solid initial effort to begin addressing the issues at the time, especially with its focused target. The emphasis on LEA training, community engagement, and counter-messaging are important functions that need to be executed to this day. In order to contend with the contemporary threat, there needs to be some modifications and additions. The issue of the modern domestic threat is that there are not simply easily identifiable *in-person* communities that can readily engaged with. Though there is a connection between offline and online factors, users may intentionally or accidently encounter radical and extremist content (NIJ, 2023). Users are largely introduced to content and individuals virtually where radicalization can begin. Swinging back to the 2016 NIP, it made a very important point. In a country like ours, there needs to be cooperation between government and private sectors for law enforcement to attain successful "Pre-bang" incident interdiction. The private sector owns and facilitates unbelievable amounts of data on every U.S. Citizen and their data transactions. From car manufacturers to social media companies, they collect and maintain gargantuan amounts of information on messaging, biometrics, searches, habits, etc. (Pillar, 2013). Both training and cooperation between the realms would greatly impact the successes in locating recruitment pools, material procurement, and propaganda. Extremist communities from all aspects are online, the integration of commercial data and federal entities would absolutely raise concerns, but there must be plain and direct language instituted purposing the intelligence to be derived from the data being analyzed. The fact that the government can locate geographically and in cyberspace extremists of all kinds proves that an effective strategy must include private data and tech companies working with Federal Agencies, as the first flags and triggers of such extremism could be found online first.

When breaking down the U.S. messaging on countering mis/disinformation and propaganda, it is very difficult to ascertain an actual effect. Public trust in U.S. Government is significantly low. According to a 2024 PEW Research Center study, it sits at an average of 19-22% of the public trusts that the government always/most of the time (PEW, 2024). Though this may not be inherently indicative of messaging effectiveness, it certainly plays a role in either degrading the value of a message or increasing in polarizing effects which break away at social trust as well. A lack of trust in government and society undermines cohesion and collective action (Lee 2022, 1533) which removes the ability for government messaging to be an arbiter, as any message stated is easily viewed as untrue to someone who identifies as the opposite political party. Understanding government trust, its messaging, and societal perceptions is important when looking at domestic terror actors, as they span across spectrum and ideology. Failing competence, ability, or legitimacy fosters mistrust (Bagozzi et al 2022, 366). Lacking in trust allows for extremist messaging and ideologies to fester and limits the effectiveness of any entities messaging tied to the government. There are seemingly limitless conspiracy theories that are out there, many these are inflamed more when there is a lack of clarity, truthfulness, or perceived duplicity in messaging and actions via the government. The continued political turmoil of the U.S. Government is easily seen in the increasing violence of public demonstrations and riots. Not only are the demonstrations the targets of attack, they are a symptom of a spiraling radicalization disease that is affecting the society (Doxsee et al 2022, 2) Extremism will continue to affect the US on a political spectrum if there is not a sense of community and societal connection to one another. An effective strategy therefore must include the regaining of trust and legitimacy through transparency, reliability, and responsibility.

Media and Terrorism

Terrorism relies on the need to send a message, that is what the attack is all about. Many of these groups also count on might of the global media to further increase their effectiveness. This relationship is one of mainly legitimacy and constituency, as the attack itself is valued not by genuine gains of material, but in influence. Media is the ultimate weapon of influence. Be it legacy medias (television, print, and radio) or modern medias (Blogs, Social Platforms, Vlogs, etc.) (Voyles, 2022), terror actors look to spread their ideology or political end states to the masses. There will be no way to stop reporting on terror attacks, we are a curious race and the worse a situation is the more will need to be reported for clarity reasons. Large events such as the September 11th attacks in the US and the recent October 7th attack in Gaza are instances where continued media coverage will be conducted in the long term to release facts. This is where authorities can be extremely helpful in stopping mis/disinformation. Governing bodies must immediately release any and all information that is factual as fast as possible.

The key in denying the media in being as effective is in the message wording and context. Words are the medium in which we understand, feel, discern, control and so much more. The power of words is rightly coined in the phrase, "The pen is mightier than the sword." Our outlooks and beliefs are shaped by words; thus they control our reaction and emotions and how we look at an event (Lysiuk 2019, 136). How a story is broadcast and what it portrays in both messaging and imagery impacts the influence of the story (Burke et al 2016, 4). Also, denying significant amounts of time in front of an audience can assist in decreased effectiveness of terror messaging. The unbelievable attack on the World Trade Center in 2001 received hundreds of hours of continuous airtime (CFR, 2019). To positively effect change, there would need to be training by experts in the field of information advantage and marketing. The U.S. Government cannot, with extreme emphases, cannot establish an organization managing media releases. What can happen is government agencies or preferably non-governmental organizations (NGO) could brief journalists and other media influencers on the intricacies and dangers of poor messaging practices. There could be no mandate for it as well, but participating companies and organizations could voluntarily attend or receive information on the matter. This could not only hinder the goals of a terror organization but also reduce possible copycat attackers. Though all lone attackers or copy-cat attackers may not fall into the exact realm of domestic terror in some senses due to the mental illness factor, there are realities surrounding a rippling effect of attacks.

Internet and Terrorism

With the advent of the internet, comes new forms of media and tools used by terrorists to coordinate, finance, plan, and recruit. The endless connection points and wireways allow cells to maintain continuous presence while remaining nearly untraceable in cyberspace. Though there are ways to use it as an attack, the primary use for this is extending a groups reach. This technology enables it to recruit abroad, fundraise by locating sympathizers, and expands the audience to their influence. The nature of the internet is conducive to their modus operandi, it offers rapid and flexible means of achieving these uses (Lewis 2005, 114). The solution lies in a true understanding of where they operate and how to recognize their actions online.

To combat terror use of the internet, there needs to be a broader emphasis on private and commercial companies. The execution of all of these activities are done across the private websites, games, chatrooms, and platforms. Recognizing how and where the operate is key to interdiction. For example, the Islamic State (IS) uses various forms of social media platforms to conduct various tasks. Twitter was used to recruit, influence, and communicate to target audiences of their choosing, but for training videos and longer form propaganda they utilized YouTube and other video streaming platforms (Fishman 2019, 86). Moderation and content removal on these platforms must be enforced. Though it is an imperfect solution and will be met with scrutiny, extremist content of all sorts must be banned.

Social Media platforms have editing rights, the same as those of print media. This is incredibly important to understand by the citizenry and must be consciously messaged, there are no ultimate free speech protections on a social media platform, if a social media company wishes to remove the content (Greene, 2024). As for internet based messaging applications, besides identification and deletion, there is opportunity to collect or corral communications. If legalities and authorities are set, agreements between private and federal entities could be used to locate and collect information on these platforms. Action on collected sources would not only be benefit to the destruction of the cell, but an inherent fear of using social messaging applications may arise in other groups. From a government position, there should be efforts to remove open source published information on TTPs (Techniques, Tactics, and Procedures) and other training documentation. With regards to the most modern and emerging of internet applications, Artificial Intelligence poses a great risk via its many uses. This incredibly powerful tool for analysis, research, and planning can be used just as simply by terrorists. To limit abuses, there should be entities within companies that ensure compliance to counter-terror efforts. This would mean that there are no simple ways to circumnavigate security protocols along with an immediate reporting to a reviewing entity of potentially unsafe searches.

Conclusion

Terrorism is a difficult beast to defeat due to its everchanging forms, functions, and tools. In the end though, there are critical vulnerabilities that can be identified and subsequently capitalized on. To completely stop all terror attacks is an idea that is too far to attain. End states for CVE should be realistic and achievable, founded in both capability and necessity. We have analyzed the 2011 SIP and found it to be wanting, but as an initial formal effort we can find successes. There are many decades of work and efforts to draw from, the most difficult task is learning lessons and making proper decision when it comes to genuinely defeating domestic terror. With that, the United States Government and politicians must begin to close the both real and perceived fault lines in its society to reduce and prevent extremist ideologies and domestic terror attacks from being executed. Political and Social distrust will continue to drive attacks, but if the county can begin to mend and come together, there will be change.

When it comes to media both legacy and modern, there must be an emphasis placed on the dangers of over exerting government intervention on the matter. We the People, have our rights and they must be respected. There also must be different steps taken to deny terrorists such a powerful tool as media. For the internet, Federal agencies must work, train with, and inform private sector and entities in a wide variety of aspects be it media or internet applications to have both sides up to date on the most recent TTPs of terrorists on the internet. There is a long way to go but as one nation, acting together, there is nothing that we cannot achieve protect, prevent, and mitigate terror attacks of all kinds.

References

Bagozzi, R. (2022). Responses of the public towards the government in times of crisis. *British Journal of Social Psychology*. https://doi.org/10.1111/bjso.12566

Burke, S., Sims, A., & Sterman, D. (2016). The context: Terrorism, public reaction, and the media. In *War and tweets: Terrorism in America in the digital age* (pp. 3–6). New America. http://www.jstor.org/stable/resrep10512.4

Department of State. (2012). *Country reports on terrorism 2011*. United States Department of State. https://2009-2017.state.gov/documents/organization/195768.pdf

Doxsee, C., Seth, J., Thompson, J., Halstead, K., & Hwang, G. (2022). *Pushed to extremes: Domestic terrorism amid polarization and protest*. Center for Strategic and International Studies. https://www.csis.org/analysis/pushed-extremes-domestic-terrorism-amid-polarization-and-protest

Federal Bureau of Investigation. (2020). *Domestic terrorism: Definitions, terminology, and methodology*. https://www.fbi.gov/file-repository/counterterrorism/fbi-dhs-domestic-terrorism-definitions-terminology-methodology.pdf/view

Fishman, B. (2019). Crossroads: Counter-terrorism and the internet. *Texas National Security Review, 2*(2), 82–100. https://tnsr.org/2019/02/crossroads-counter-terrorism-and-the-internet/

Government Accountability Office. (2023). *The rising threat of domestic terrorism in the U.S. and federal efforts to combat it*. https://www.gao.gov/blog/rising-threat-domestic-terrorism-u.s.-and-federal-efforts-combat-it

Greene, D. (2024). Platforms have First Amendment right to curate speech. *Electronic Frontier Foundation*. https://www.eff.org/deeplinks/2024/07/platforms-have-first-amendment-right-curate-speech-weve-long-argued-supreme-1

Lee, A. H. (2022). Social trust in polarized times: How perceptions of political polarization affect Americans' trust in each other. *Political Behavior, 44*(3), 1533–1554. https://doi.org/10.1007/s11109-022-09787-1

Lewis, J. (2005). The internet and terrorism. *Proceedings of the Annual Meeting (American Society of International Law), 99*, 112–115. http://www.jstor.org/stable/25659982

Lysiuk, L. (2020). How words and emotions control behavior. *Acta Neuropsychologica, 18*(1), 127–140. https://doi.org/10.5604/01.3001.0014.0190

National Institute of Justice. (2023). *The role of the internet and social media in domestic radicalization*. https://nij.ojp.gov/topics/articles/five-things-about-role-internet-and-social-media-domestic-radicalization

Palmer, A., Skyeler, J., & Byman, D. (2025). *Jihadist terrorism in the United States*. Center for Strategic and International Studies. https://www.csis.org/analysis/jihadist-terrorism-united-states

Pew Research Center. (2024). *Public trust in government: 1958–2024*. https://www.pewresearch.org/politics/2024/06/24/public-trust-in-government-1958-2024/

Pillar, P. (2013). Big data, public and private. *Brookings Institution*. https://www.brookings.edu/articles/big-data-public-and-private/

Voyles, S. (2022). What is legacy media? *Logos Communications*. https://logos-communications.com/2022/09/26/what-is-legacy-media/