**Research Paper Addressing Topics on Domestic Terrorism Threats and Internet and Media Use in Extremism**

Student

Institution

Instructor Name

Course

Date

**Research Paper Addressing Topics on Domestic Terrorism Threats and Internet and Media Use in Extremism**

**1. Domestic Terrorism Threats**

**Introduction**

Almost a decade ago, the White House through the Obama Administration sought to reinforce America's fight against violent extremists by acknowledging that the U.S. government cannot solely address terrorism and violent extremism. Therefore, through the *Empowering Local Partners to Prevent Violent Extremism in the United States* the administration endorsed the idea that success demands mobilizing local law enforcement and communities in a collaborative effort towards this cause (White House, 2011). The strategy implied that the U.S. government's goal at the time included expanding intelligence collection and analysis to prevent terrorist attacks both domestically and internationally. How would they accomplish this goal? By increasing collection sources with information shared across local, state, and federal levels. As such, law enforcement was, and still is, empowered to identify concerning behaviors among the public while communities are called upon to be vigilant and notify authorities of any suspicious activities. According to Ahmad and Monaghan (2022), expanding the number of ears and eyes allows intelligence to flow from the ground up and guide counterterrorism efforts. The approach hinges on an informed, engaged public partnering with local police as a force multiplier. As such, this decentralized, collective approach is deemed more effective than isolated federal efforts to detect and disrupt terrorist plots (Ahmad & Monaghan, 2022).

It is necessary to understand that the idea of mobilizing local law enforcement for intelligence gathering is not a fresh one, with varying implementations dating back to shortly after World War I. In 1919-1920, the local law enforcement agencies and the Federal Bureau of Investigation (FBI) reacted to fears of leftist radicals in the *Palmer Raids*, arresting and deporting thousands of immigrants based on suspicions of radical beliefs informed by local intelligence (George & Klosová, n.d.). The FBI again extensively used local police for intelligence during the mid-1900s Counter Intelligence Program (COINTELPRO) targeting subversive groups including civil rights activists (Stieva, 2018). Given major technological advances since these earlier eras, such collaborative programs have far greater potential today as intelligence-gathering tools. Still, past localized intelligence efforts also demonstrate potential for overreach, as evidenced by the Palmer Raids and COINTELPRO's civil liberties violations. Therefore, safeguards are highly necessary to guarantee lawful, ethical information sharing between federal and local partners.

Police departments in major cities recognized early the need for in-house counterterrorism abilities, initially to serve their jurisdictions which soon expanded to federal partnerships. The first Joint Terrorism Task Force (JTTF) began in the late 1900s as a collaboration between the Federal Bureau of Investigation and NYPD (New York City Police Department), comprising 20 agents and officers spread across each department (Erickson, 2021). This modest start catalyzed the growth and proliferation of the JTTF model. From these local roots, joint terrorism task forces sprouted nationally to fuse grassroots intelligence with expansive federal capabilities under one roof. The intended goal and priority were coordinating multi-agency counterterrorism efforts within the local areas. Fortunately, the task force (JTTFs) evolved into vital nodes in a national network generating terror alerts, investigations, and disruption operations (Erickson, 2021). Notably, the joint operations center concept bridged gaps between federal intelligence priorities and police street-level awareness of potential threats.

Additionally, the JTTF framework has proliferated, with over 190 units now spanning every FBI field office nationwide. This collaborative and supportive intelligence framework between local law enforcement and federal agencies can claim successes, yet also shortcomings that have pushed some departments to withdraw. Compared to the civil liberties violations within programs like COINTELPRO, contemporary partnerships are plagued by controversies bringing negative attention. Even though broad integration and cohesion initiatives promise national security gains, the approach lacks sufficient safeguards against local political firestorms that have dogged joint operations historically (Erickson, 2021). Despite the evident potential, convincing individual jurisdictions the hassles are worthwhile remains an uphill climb. Therefore, it is paramount forthe enticement of shared information and resourcesto be balanced against vulnerability to public scrutiny of opaque intelligence activities. In this digital age, privacy and oversight expectations are much higher; thus, as joint terrorism task forces become broader, balancing civil rights with security would determine whether communities embrace or reject an enlarging surveillance state apparatus leveraging technology and local partners to root out threats.

**Missing elements or Needed Integration Processes.**

Still, the approach mentioned above struggles to reconcile civil liberties with the surveillance required to preempt attacks. This is because controversial law enforcement actions have sparked public outrage, like the NYPD's warrantless monitoring of Muslims. It is important to acknowledge that legal challenges are likely to persist against overbroad intelligence gathering that tests Constitutional bounds. This pre-empts a precarious balancing act (allowing domestic spying to uncover threats and at the same time respecting rights). Nevertheless, mass surveillance of ordinary Americans without sufficient reason or reasonable suspicion risks crossing red lines. The potential solution to this occurrence may be training more selective spotlights (Ferguson, 2019). Rather than dragnet monitoring, law enforcement in local areas could focus on specific individuals of concern based on articulable suspicion. This middle path limits widespread rights infringements yet empowers urgent intervention against high-risk actors. But it requires trust in local police judgment, oversight on determinations, as well as faith in the judicial system to catch oversteps. According to Ferguson (2019), no framework can guarantee security and liberty in equal measure. Still targeted surveillance based on particularized evidence, prompt destruction of non-pertinent data, and swift accountability for misconduct could increase public confidence.

**2. Reduction of Media and Interest**

The media has a responsibility to report on major events, regardless of what caused them to occur. Terrorist attacks are theatrical happenings that typically receive media coverage, therefore, terrorists tend to get publicity, while media outlets get content, and the public gets captivated by the occurrences. A majority of these terrorist organizations exploit this symbiotic relationship by planning attacks designed to attract maximum attention (Sardarnia & Safizadeh, 2019). Thus, receiving extensive media exposure is not unexpected for terrorists and has become a useful tool for them. In this symbiotic association, media outlets benefit by gaining and keeping viewership and readership whereas terrorists benefit by gaining exposure. The saying "there is no such thing as bad publicity" is a concept that terrorist groups value greatly.

According to studies including Kearns et al. (2019), the extent of media coverage of a terrorist attack is directly proportional to the number of casualties. Before the internet and social media, terrorists exploited this media attention like businesses used advertising - as the most effective way to promote their cause. Even asmany viewers reacted angrily or became repulsive,it was noticeable that some fringe sympathizers were still watching. As such, terrorists relied on connecting with these fringe individuals for recruitment and funding. Despite knowing this dynamic, there has been little effort to limit terrorists' media exploitation and the justification exists to restrict their media access, yet the status quo persists.

As Kearns et al. (2019) highlight, progress has stalled in curtailing terrorists' exploitation of mass media. For instance, in a democratic society like America where the government cannot control media reporting and the press is free to cover what it chooses, a core tenet of democracy. Therefore, encouraging greater awareness in the media community about responsible reporting and potential consequences is key to reducing terrorists' media manipulation. Research shows that there exists a direct link between the amount of media attention an issue receives and the perceived importance of the issue. Considering it would be inaccurate to claim a terrorist incident has minor societal implications, it is the media’s core duty to moderate public panic and perceived significance by keeping coverage factual without over-sensationalizing things (Jetter, 2019).

**Tools to help reduce Terrorists Use of Media and Internet**

Governments in countries with free media use official speeches as one way to shape coverage of terrorist events. Media outlets are naturally inclined to repeat information from high-ranking government officials. This allows those governments to frame terrorist incidents in whatever manner may lessen public psychological impact (Kearns et al., 2019). Besides, if a government just reports factual details without indicating potential responses, it leaves the impression the incident is unresolved. Thus, providing the public with a sense the government is actively handling the terrorist situation and outlining the next steps, even if vague, helps mitigate panic.

Second, all stakeholders including the government and technology companies should monitor and restrict violent extremist content while protecting lawful speech. Algorithms can identify and remove propaganda videos or posts inciting violence, though human oversight is critical to avoid over-censorship. Moreover, companies need to limit accounts spreading terrorist content through bans or enhanced monitoring, an approach that has been noted to help monitor as well as track unorthodox activities online (Dias Oliva, 2020).

Next, media outlets should craft ethical guidelines for covering terrorist attacks. Establishing standards could limit the use of propaganda materials, advise discretion in airing graphic content, and encourage focused coverage of victims over perpetrators (Dias Oliva, 2020). Besides, responsible reporting can deny terrorists the dramatic coverage they seek without suppressing free speech. Additionally, governments need to foster and encourage counter-messaging and alternative narratives. As such, activists, non-profits, and victims' groups can utilize media and social platforms to denounce terrorism and offer positive alternatives. Yeneakal (2019) notes that drowning out extremist voices with moderate ones counters radicalization, a move that can be pivotal in supporting the cause of minimizing or alleviating terrorists' use of media sources.

Another approach that could yield positive results is authorities partnering with communities to identify individuals at risk of radicalization and provide counseling. There is a likely chance that early intervention guidance away from violence can prove more effective than post-hoc limits on internet usage (Yeneakal, 2019). Also, ensuring and fostering global cooperation among governments, companies, and organizations is essential for a unified approach. Considering terrorism transcends borders, strategies to curtail media exploitation need also be multinational in scope.

**Internet-based Media**

Undoubtedly, internet-based media faces comparable challenges as traditional media in propagating terrorism. Private social media agencies are not government-controlled, and free speech protections apply online as they do elsewhere. Therefore, it falls to each institution to recognize its role in spreading terrorism and act responsibly to reduce it. For instance, Twitter highlighted this dilemma in 2015 by proclaiming it would never censor its platform, defying demands from the U.S. and other countries to remove known terrorist accounts (Margetts, 2018). Nevertheless, the social media platform (Twitter) eventually relented under mounting public and government pressure, deleting thousands of accounts. Even though no law required such an action, public disapproval compelled Twitter to voluntarily remove terrorist content as well as other content that was associated with these groups. Now other social media platforms confront the same issues with extremist content. But acting in their self-interest, they have increasingly purged such material from their sites. Like traditional media, internet companies are not obligated by law yet may choose to restrict terrorist propaganda in response to public expectations.

**Conclusion**

The initiative adopted by the White House during the Obama administration proved crucial for the cause as it empowered local stakeholders in the intelligence and law enforcement community to improve intelligence collaboration between police officers and agencies and the government across the nation. This significantly reinforced a history of similar initiatives going forward. Besides, the expansion of the network of reporting sources and data integration solidifies authorities’ objective of identifying and thwarting terrorist radicalization and attacks. Still, addressing the approach's drawbacks is important. Past occurrences like the Palmer Raids and COINTELPRO underscore the potential for overreach when the intelligence apparatus becomes too diffuse and opaque. Ongoing controversies continue to risk alienating partners and eroding public trust. Steps to ensure rights protections and oversight are essential. Additionally, reliance on local authorities risks inconsistent implementation across jurisdictions. Nevertheless, proactive security depends on early threat detection. Overall, the decentralized framework offers advantages if applied judiciously. Similarly, while traditional media's influence on terrorism is hard to restrict, there are ways to mitigate the adverse impacts as highlighted. As the internet has become a platform for terrorist messaging, private technology companies have taken action to reduce extremist content and preempt government intervention.

**References**

Ahmad, F., & Monaghan, J. (2022). Socializing the high policing métier: Exploring counterterrorism trainings for frontline workers. *Surveillance & society*, *20*(3), 248-264.

Dias Oliva, T. (2020). Content moderation technologies: Applying human rights standards to protect freedom of expression. *Human Rights Law Review*, *20*(4), 607-640. <https://doi.org/10.1093/hrlr/ngaa032>

Erickson, S. G. (2021). Center for Homeland Security and Immigration Twenty Years After 9/11: Strong Federal, State, and Local Law Enforcement Collaboration Remains Essential in the Fight Against Terror–But It’s Under Attack. *Center for Homeland Security and Immigration*.

Ferguson, A. G. (2019). The exclusionary rule in the age of blue data. *Vand. L. Rev.*, *72*, 561.

George, M., &Klosová, B. M. The Red Scare: The Fear of Communism in American Society of 1919-1920.

Jetter, M. (2019). More bang for the buck: Media coverage of suicide attacks. *Terrorism and political violence*, *31*(4), 779-799. <https://doi.org/10.1080/09546553.2017.1288112>

Kearns, E. M., Betus, A. E., & Lemieux, A. F. (2019). Why do some terrorist attacks receive more media attention than others?. *Justice Quarterly*, *36*(6), 985-1022. <https://doi.org/10.1080/07418825.2018.1524507>

Margetts, H. (2018). Rethinking democracy with social media. *Political Quarterly*, *90*(S1).

Sardarnia, K., &Safizadeh, R. (2019). The internet and its potentials for networking and identity seeking: A study on ISIS. *Terrorism and Political Violence*, *31*(6), 1266-1283. <https://doi.org/10.1080/09546553.2017.1341877>

Stieva, K. (2018). *‘What Colour are You?’: FBI Counter-Intelligence and the Targeting of White Hate and Black Extremist Groups in the 1960s* (Doctoral dissertation, UNIVERSITY OF CALGARY).

White House. (2011). *Empowering Local Partners to Prevent Violent Extremism in the United States*. [Www.ojp.gov](http://Www.ojp.gov).

Yeneakal, T. Y. (2019). *AI and extremism in social networks* (Master's thesis, The University of Bergen). <https://hdl.handle.net/1956/21061>