

Disrupting Terrorist Financing Networks: A scoping Review of Countering Funding for Political Violence and Extremist Operations in the U.S

Clement Aryee¹ and Juliana Popoola²

^{1,2}Texas Tech University.

Abstract: Terrorist financing is a major fuel for political violence and extremist operations in the world. The increasing advancement of digital technologies, cryptocurrencies, crowdfunding platforms, and social media has significantly transformed how extremist groups raise, transfer, and conceal funds, yet little has been done to examine the broader digital transformation of terrorist financing and its implications for the United States. This scoping review examined evolving trends, financing strategies, and operational challenges associated with terrorist financing networks and assessed their implications for the United States counterterrorism agenda. Following the Arksey and O'Malley guidelines for scoping reviews, relevant studies were identified through systematic database searches and screened using predefined inclusion and exclusion criteria. Ten studies were selected and analyzed thematically. The findings underscored four major themes: the digitalization of terrorist financing, the fusion of lawful and unlawful funding mediums, administrative and institutional weaknesses, and the growing need for collaborative and intelligence-driven disruption strategies. The review found that extremist financing increasingly operates within ordinary digital and financial ecosystems, making detection more difficult for regulators, financial institutions, and law enforcement agencies. The study concludes that terrorist financing has become more decentralized, adaptive, and technologically sophisticated than many existing counterterrorism frameworks are prepared to address. Hence, strengthening United States national security will require a more proactive digital financial monitoring, sophisticated regulatory systems, and stronger inter-sectoral collaborations to disrupt evolving extremist financing networks before they escalate into acts of violence.

Keywords: Terrorist Financing, Political Violence, Violent Extremism, United States, Counterterrorism.

INTRODUCTION

Terrorism or violent extremism cannot survive without sustainable financing. According to Freeman (2016) and Jacobson (2010), whether extremist groups are organizing attacks, spreading propaganda, recruiting supporters, purchasing weapons, or sustaining operations across borders, access to financial resources remains central to their survival and growth. After the September 11 attacks, the United States invested heavily in counterterrorism strategies designed to disrupt terrorist organizations and protect national security (Ola, 2025). However, as military operations and intelligence efforts keep advancing significantly, terrorist financing systems have also become more advanced, adaptive, and difficult to track (Farber & Yehezkel, 2025; Zahari *et al.*, 2024). This rapid growth of digital technology has significantly changed the way extremist groups raise and engage in financial transactions. For instance, studies have shown that social media platforms, cryptocurrencies, crowdfunding systems, online payment applications, and decentralized financial technologies now provide terrorist groups with reliable, quicker, cost-effective, and anonymous ways of financing their activities (Alley-Young, 2023; Salami, 2018). Unlike traditional financing systems that relied heavily on banks or physical cash transfers, contemporary terrorist financing occurs within online spaces that millions of people

use daily (Akartuna *et al.*, 2022). This shift has muddled the line between lawful financial activities and unlawful extremist financing. Notably, research has shown that terrorist organizations increasingly blend both lawful and unlawful funding mediums to evade detection (Popoola & Aryee, 2026). For example, it has been revealed that some terrorist organizations may operate legal businesses, solicit charitable donations, capitalize on crowdfunding campaigns, engage in cyber fraud, or use cryptocurrency to conceal transactions (Mursyid *et al.*, 2025; Farber & Yehezkel, 2025). Such strategies as the above make counterterrorism financing efforts more complicated, as suspicious financial activities are often buried in conventional economic and digital behavior. In most cases, terrorist financing networks acclimate more quickly than most governments and regulatory institutions ever would. This situation is particularly problematic within the United States Context, given its highly interconnected digital economy and the growing use of Fintech (Popoola & Aryee, 2026). The proliferation of decentralized financing, peer-to-peer payment systems, and anonymous digital transactions creates new vulnerabilities that can be exploited by both international terrorist organizations and domestic extremist actors (Popoola & Aryee, 2026). At the same time, social

media and online platforms have become powerful spaces not only for propaganda and recruitment, but also for fundraising and financial mobilization (Keatinge & Keen, 2020). These developments raise important questions about whether current United States counterterrorism financing mechanisms are adequately prepared for evolving digital threats. Despite growing attention to terrorism financing, important gaps remain within the existing literature. Much of the research focuses on international terrorist organizations, with comparatively limited attention given to the broader digital transformation of extremist financing and its implications for the United States (Mursyid *et al.*, 2025; Zahari *et al.*, 2024; Ola, 2025; Popoola & Aryee, 2026). Also, there are limited syntheses of emerging evidence regarding cryptocurrencies, crowdfunding, social media fundraising, and the nexus between cybercrime and terrorism financing (Akartuna *et al.*, 2022; Manning *et al.*, 2025). Consequently, not understanding these emerging terrorist financing mechanisms puts counterterrorism efforts at risk of becoming reactive rather than preventive.

Given the above, this scoping review examines the evolving methods and strategies associated with terrorist financing networks. By doing so, the study seeks to contribute to ongoing discussions on strengthening the United States financial security, improving regulatory responses, and disrupting extremist operations before they translate into acts of violence.

METHODS

The study adopted a scoping review design to examine existing studies on terrorist financing networks and their implications for countering political violence and extremist operations in the United States. The review was guided by the

scoping review framework developed by Hilary Arksey and Lisa O'Malley, which emphasizes mapping key concepts, identifying research gaps, and synthesizing evidence across a broad body of literature (Arksey & O'malley, 2005). The review process involved four main stages, which included the identification of relevant studies, screening studies for eligibility, selecting studies for inclusion, and conducting thematic synthesis of the findings. Several electronic databases such as Google Scholar, Scopus, Web of Science, JSTOR, ProQuest, and ScienceDirect were searched using keyword combinations like “terrorist financing,” “terrorism funding,” “cryptocurrency and terrorism,” “social media financing,” “crowdfunding and extremism,” and “counterterrorism financing.” Studies were included if they: (1) focused on terrorist or extremist financing mechanisms, (2) examined digital or traditional financing methods, (3) discussed counterterrorism financing strategies, (4) were published in English, and (5) provided sufficient conceptual, empirical, or policy-related insights relevant to the study objective. Studies were, however, excluded if they did not meet the above inclusion criteria, lacked full-text availability, were duplicate publications, or had limited relevance to extremist financing activities. After removing the duplicates, the titles and abstracts were screened for relevance. Full-text articles that met the inclusion criteria were then reviewed in detail. Afterwards, a total of 10 studies were included in the final synthesis. Data analysis was conducted using thematic synthesis. The thematic approach allowed for the identification of trends, knowledge gaps, and implications for countering terrorism financing in the United States.

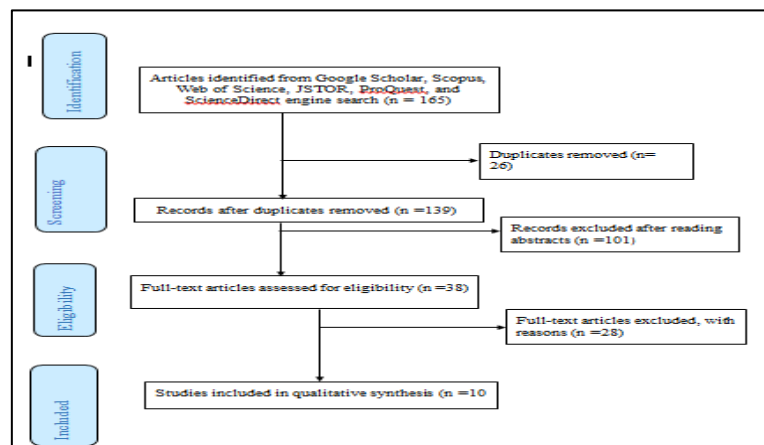


Figure 1: PRISMA-ScR Flow diagram showing the article selection process
Sources; Author's Construct 2026.

Table 1: Characteristics of included studies

Author(s) & Year	Country/Context	Study Focus	Methodology/Approach	Key Findings	Relevance to U.S. Counterterrorism
Alley-Young (2023)	Global	Social media and terrorist financing	Conceptual/analytical chapter	Social media facilitates fundraising, recruitment, propaganda dissemination, and operational support for extremist groups	Highlights vulnerabilities in U.S.-based social media ecosystems and online extremist mobilization
Mursyid <i>et al.</i> (2025)	Indonesia	Terrorism financing modus operandi	Field-based legal and criminological analysis	Terrorist groups combine legal businesses, donations, cybercrime, and cryptocurrency to fund operations	Demonstrates hybrid financing methods relevant to domestic extremist financing in the U.S.
Ola (2025)	Global/USAID	Extremism financing and international aid systems	Process tracing and discourse analysis	Raises concerns regarding geopolitical and institutional dynamics connected to extremist financing	Highlights the need for policy accountability and oversight in international counterterrorism operations
Zahari <i>et al.</i> (2024)	Malaysia	Financial innovations in terrorism financing	Focus groups with enforcement officers	Terrorist groups use innovative financial techniques to evade regulators and law enforcement	Emphasizes the importance of adaptive intelligence and financial monitoring systems in the U.S.
Farber & Yehezkel (2025)	Middle East/Global	Crowdfunding and terrorism	Systematic case analysis	Online crowdfunding and cryptocurrency strengthen extremist resilience and fundraising capacity	Relevant to online fundraising threats and digital extremism in the United States
Andrianova (2019)	Russia/Global	Terrorism financing in the digital economy	Policy and analytical assessment	Digital technologies, crowdfunding, and virtual currencies are transforming	Demonstrates the need for modernized digital-era counterterrorism policies in the

				terrorist financing globally	U.S.
Salami (2018)	Global/high-risk states	Virtual currencies and terrorism financing	Regulatory and policy analysis	Cryptocurrencies create cross-border financing risks requiring coordinated global regulation	Relevant to U.S. cryptocurrency regulation and blockchain surveillance efforts
Burgess <i>et al.</i> (2024)	Global	Crypto-crime-terror nexus	Comparative case study/proof of concept	FATF standards are inadequate for addressing crypto-enabled terrorist financing	Highlights international regulatory gaps affecting U.S. counterterrorism effectiveness
Ehrenfeld (2016)	Global	Nexus between terrorism and criminal organizations	Historical and analytical overview	Terrorist groups rely on both legitimate funding and organized criminal activity	Relevant to understanding organized crime-extremism linkages within and beyond the U.S.
Keatinge & Keen (2020)	Global	Social media and counter-terrorist finance	Policy and analytical discussion	Social media platforms can support both terrorist fundraising and counterterrorism disruption	Supports public-private collaboration in U.S. counterterrorism financing efforts

FINDINGS

The review demonstrates that terrorist financing has moved beyond traditional criminal activities or physical cash transfers. Rather, terrorist financing networks have become increasingly decentralized, technology-driven, adaptive, and very difficult to detect. Four major themes emerged from the literature: (1) the digitalization of terrorist financing, (2) the fusion of lawful and unlawful funding mediums, (3) Administrative and institutional weaknesses, and (4) the need for collaboration and intelligence-led disruptions.

The Digitalization of Terrorist Financing

The rapid digital transformation of terrorist financing emerged as a major theme across several studies. The exploitation of digital platforms, cryptocurrencies, crowdfunding systems, and social media to raise, transfer, and conceal funds among terrorist organizations has increased significantly in recent times.

For instance, Alley-Young (2023) explained that social media has evolved beyond a communication

tool into a financial ecosystem that supports extremist recruitment, propaganda dissemination, and fundraising. According to the author, platforms that were originally designed to connect people are now being exploited by violent extremist organizations to crowdsource financial support from sympathizers across the world. Similarly, Keatinge and Keen (2020) argued that, social media itself has become a very crucial fundraising infrastructure for extremist groups mainly because of the alacrity, anonymity, and global reach it provides.

Further, the role of cryptocurrency and the decentralized nature of terrorist financing is strongly emphasized in the literature. Salami (2018) identified several virtual currencies as specifically attractive for terrorist financing because they enable cross-border transfers with reduced visibility and limited government oversight. Also, Burgess *et al.* (2024) revealed how further terrorist agencies blend cryptocurrency with traditional financial systems

to create advanced hybrid financing models. This implies that decentralized finance technologies are creating new pathways for criminal-terrorist networks that existing regulatory frameworks fail to monitor effectively.

In Mursyid *et al.* (2025) and Zahari *et al.* (2024), both studies demonstrate how extremist groups have increasingly become innovative in adapting digital tools for fundraising and operational support. They argue that extremist organizations mostly use investment scams, cyber fraud, hacked platforms, and anonymous digital transactions to generate revenue. This is because most of the time, these digital platforms permit extremist actors to operate in smaller, disorganized cells that are very difficult for law enforcement agencies to detect.

Additionally, Andrianova (2019) expands the discourse by marrying the digital economy directly to evolving terrorist financing strategies. The study maintains that the internet, virtual currencies, crowdfunding systems, and encrypted communication channels have basically altered the landscape of terrorism financing. Thus, terrorist financing has therefore become faster, less geographically restricted, and increasingly resistant to conventional surveillance systems.

The Fusion of Lawful and Unlawful Funding Mediums

Another major theme is the unclear line between legitimate economic activities and illegal extremist financing. The review shows that terrorist organizations rarely depend on a single source of funding. However, they blend both lawful and unlawful financial practices to sustain their operations while avoiding being caught.

In Indonesia, Mursyid *et al.*, (2025) provided one of the clearest examples of this pattern. Their study revealed that extremist organizations use lawful businesses, charity events, donations, and legal commercial activities alongside unlawful methods like armed robbery, online fraud, theft, and cybercrime. Thus, the strategy of fusing both lawful and unlawful funding channels enables extremist actors to hide financial flows within mainstream financial systems.

Similarly, Ehrenfeld (2016) also explained that terrorist organizations usually depended on both “clean” money and criminal enterprises. This is because financial support that is framed as political or ideological solidarity often entered extremist systems through apparently lawful donations or charitable activities. Nevertheless, these funds are

mostly insufficient to sustain operations, ultimately leading terrorist organizations to establish relationships with organized criminal networks.

Further, Farber and Yehezkel (2025) also highlighted how online crowdfunding has become a powerful tool for anonymizing extremist financing through humanitarian or political appeals. They argued that crowdfunding campaigns linked to extremist organizations may appear legal to donors, especially when emotional narratives or humanitarian language are used appropriately. This concern is reinforced by Zahari *et al.* (2024), who argued that terrorist organizations frequently use innovative and flexible financial arrangements that epitomize conventional commercial transactions. Thus, the above strategies employed by terrorist groups make it difficult for financial institutions to differentiate suspicious activities from standard economic behavior.

The above review demonstrates that terrorist financing networks are deeply rooted within broader economic and social systems. Particularly, the nexus between lawful and unlawful funding channels undermines law enforcement efforts because suspicious financial behavior may closely mimic conventional business transactions or charitable fundraising donations.

Administrative and Institutional Weaknesses

Another theme that runs through the reviewed literature was the identification of major weaknesses in existing oversight frameworks, international supervision mechanisms, and enforcement systems.

For instance, Salami (2018) argued that although regulatory technologies offered prospective solutions to disrupting terrorist financing, several countries still lacked advanced systems capable of addressing the risks associated with virtual currencies. According to the author, weak international coordination allows terrorist financiers to exploit differences in national laws and enforcement strengths.

Consequently, Burgess *et al.*, (2024) heavily criticized existing Financial Action Task Force (FATF) standards, maintaining that they are insufficiently nuanced to address the rapidly evolving relationship between cryptocurrency, crime, and terrorism. According to the authors, even the current standards are abysmally

implemented in many countries, leading to gaps that extremist actors capitalize on.

Andrianova (2019) similarly noted that technological innovations have advanced more quickly than regulatory adaptations. The author further noted that, due to the rapid evolution of these technological innovations, governments and financial institutions still fumble with detecting new financing strategies that operate within decentralized digital spaces.

Further, the review noted a concern regarding institutional accountability and unintended policy consequences. For instance, Ola (2025) presented a controversial but important discussion regarding allegations that international aid systems and geopolitical interventions can indirectly create avenues where extremist financing networks thrive. While the study's claims are heavily contentious, it underscores the broader issue of how international political and institutional systems can unintentionally contribute to instability and the growth of extremist movements and activities.

Thus, the literature clearly demonstrates that counterterrorism financing frameworks are often reactive rather than proactive. This means that regulatory frameworks often respond only after extremist groups have already adapted to new technologies and financial channels.

The Need for Collaborative and Intelligence-Led Disruption Strategies

The final theme identified had to do with the increasing recognition that terrorist financing cannot be disrupted only through isolated enforcement efforts. However, the reviewed literature underscored the need for organized, intelligence-driven, and multi-sectoral approaches.

According to Keatinge and Keen (2020), social media companies, financial institutions, and law enforcement agencies must effectively work together to identify suspicious fundraising activities online. They further stressed that digital spaces should not only be used to remove extremist propaganda, but also to actively surveil financial exploitations ongoing within their systems.

Zahari *et al.* (2024) also underscored the importance of practitioner expertise and interagency collaborations. They opined that frontline enforcement officers possessed valuable operational knowledge that can and should inform

broader policy development and prevention strategies.

Further, Salami (2018) advocated for internationally standardized regulatory technologies capable of detecting suspicious virtual currency transactions across different jurisdictions. Similarly, Burgess *et al.*, (2024) recommended stronger interagency collaborations and more specialized regulatory frameworks tailored specifically to crypto-enabled terrorism financing.

Moreover, Alley-Young (2023) also highlighted the importance of adaptive responses that evolve alongside extremist innovations. The study suggested that governments should frequently upgrade and update legal frameworks, monitoring systems, and public awareness strategies to deal with terrorist financing strategies as and when they emerge.

DISCUSSION

The findings of this scoping review demonstrate that terrorist financing has progressively become digital, decentralized, and very difficult to track. Terrorist organizations now capitalize on social media, crowdfunding platforms, cryptocurrencies, and other digital financial systems to raise and move funds quickly without a trace (Alley-Young, 2023; Salami, 2018; Farber & Yehezkel, 2025). What this implies for the United States is that, traditional counterterrorism financing approaches focused mainly on banks and cash transactions are no longer sufficient, hence the need for robust and sophisticated digitalized approaches in counterterrorism financing efforts. The review also highlighted how terrorist financing is often hidden within legitimate activities such as charities, businesses, online donations, and conventional commercial transactions (Mursyid *et al.*, 2025; Ehrenfeld, 2016). This makes detection more difficult because extremist financing may mimic standard financial behavior. In the U.S. context, this increases the need for intelligence-driven monitoring systems that can identify suspicious patterns across digital platforms. Another major concern is that technological innovation is advancing faster than regulation. As a result, existing frameworks struggle to address decentralized finance and cryptocurrency-based transactions effectively (Salami, 2018; Burgess *et al.*, 2024). For the United States context, this implies the urgent need for counterterrorism financing policies to become more adaptive and technologically informed to respond effectively to

evolving threats. The review further highlighted the growing role of social media and fintech companies in counterterrorism efforts. Several studies affirm the fact that digital platforms are no longer just communication spaces; they are being used for recruitment, propaganda, and extremist fundraising simultaneously (Alley-Young, 2023; Keatinge & Keen, 2020). This suggests that stronger collaboration between government agencies such as the Department of Homeland Security, financial institutions, and technology companies is critical for disrupting extremist financing networks in the United States. Finally, the studies reveal an important research gap regarding domestic extremist financing in the United States. Much of the existing literature focuses on international terrorist organizations, with limited attention given to how domestic extremist groups use crowdfunding systems, cryptocurrencies, and peer-to-peer payment platforms (Farber & Yehezkel, 2025; Burgess *et al.*, 2024). Addressing this gap in future studies is critical as domestic violent extremism continues to evolve within the United States security landscape.

LIMITATIONS

This review cannot be said to be without limitations. As a scoping review, the aim was to map and synthesize the breadth of existing evidence rather than critically appraise the methodological quality of included studies or determine causal relationships among them. The review is further limited by the availability of published literature, which may not fully capture rapidly evolving terrorist financing practices, particularly those emerging within digital environments. Additionally, the relatively limited number of eligible studies may affect the generalizability of the findings; hence, care should be taken when generalizing the findings to other contexts.

CONCLUSION

This study has demonstrated that terrorist financing has advanced into a highly adaptive and technologically driven system that increasingly capitalizes on digital platforms, cryptocurrencies, crowdfunding networks, and decentralized financial technologies. The findings reveal that extremist groups no longer rely on traditional funding methods; rather, they blend both lawful and unlawful financial mediums to avoid detection and sustain their operations. The review further highlighted how existing counterterrorism financing frameworks often struggle to keep up

with increasingly changing digital financial systems. Social media platforms, fintech applications, and cryptocurrency networks have created new vulnerabilities that extremist actors now exploit for fundraising, recruitment, and operational support. The findings carry important national security implications for the United States, as countering modern terrorist financing will require more adaptive regulatory systems, stronger digital financial intelligence capabilities, and closer collaboration between government agencies, financial institutions, and technology companies.

REFERENCES

1. Akartuna, E. A., Johnson, S. D., & Thornton, A. E. "The money laundering and terrorist financing risks of new and disruptive technologies: a futures-oriented scoping review." *Security Journal* (2022): 1.
2. Alley-Young, G. "Social Media and terrorist Financing." *Countering Terrorist and Criminal Financing*. CRC Press, 2023. 85-96.
3. Andrianova, A. "Countering the financing of terrorism in the conditions of digital economy." *Digital transformation of the economy: Challenges, trends and new opportunities*. Cham: Springer International Publishing, 2019. 20-31.
4. Arksey, H., & O'malley, L. "Scoping studies: towards a methodological framework." *International journal of social research methodology* 8.1 (2005): 19-32.
5. Burgess, A., Hamilton, R., & Leuprecht, C. "Terror on the blockchain: The emergent crypto-crime-terror nexus." *Financial crime, law and governance: Navigating challenges in different contexts*. Cham: Springer Nature Switzerland, 2024. 203-227.
6. Davis, J. "Understanding the effects and impacts of counter-terrorist financing policy and practice." *Terrorism and political violence* 36.1 (2024): 1-17.
7. Ehrenfeld, R. "Funding evil: How terrorism is financed and the nexus of terrorist and criminal organizations." *Terronomics*. Routledge, 2016. 27-48.
8. Farber, S., & Yehezkel, S. A. "Financial Extremism: The Dark Side of Crowdfunding and Terrorism." *Terrorism and political violence* 37.5 (2025): 651-670.
9. Freeman, M. "Sources of terrorist financing: theory and typology." *Financing Terrorism*. Routledge, 2016. 7-25.

10. Jacobson, M. "Terrorist financing and the Internet." *Studies in Conflict & Terrorism* 33.4 (2010): 353-363.
11. Johnston, T., Mueller, E. E., Chindea, I. A., Byrne, H. J., Vest, N., Clarke, C. P., & Shatz, H. J. "Countering violent nonstate actor financing: Revenue sources, financing strategies, and tools of disruption." (2023).
12. Keatinge, T., & Keen, F. "Social media and (counter) terrorist finance: A fund-raising and disruption tool." *Islamic State's online activity and responses*. Routledge, 2020. 178-205.
13. Manning, M., Akartuna, E. A., & Johnson, S. "Opportunities to future crime: Scoping the future of money laundering and terrorist financing through cryptoassets." *Technological Forecasting and Social Change* 210 (2025): 123894.
14. Mursyid, A. M., Ghoni, M. H., Utari, I. S., Niravita, A., & Azzam, M. "Terrorism Financing Modus Operandi In Indonesia." *Indonesian Journal of Criminal Law Studies* 10.2 (2025): 685-722.
15. Ola, T. P. "Understanding the United States Agency for International Development's relationship with extremism financing." *Third World Quarterly* 46.17 (2025): 2278-2292.
16. Popoola, J. G., & Aryee, C. "Leveraging Behavioral Analytics to Prevent Lone-Actor Terrorism in the United States: A Scoping Review." *Journal Of Humanities And Cultural Studies* 5.1 (2026): 12-18.
17. Popoola, J. G., & Aryee, C. "Countering Cross-Border Radicalization Pipelines: A Comprehensive Analysis of How Foreign Terrorist Ideologies Amplify Domestic Extremist Violence in the US." *Sarcouncil Journal of Arts, Humanities and Social Sciences*, 5.2 (2026): 5–11.
18. Salami, I. "Terrorism financing with virtual currencies: can regulatory technology solutions combat this?." *Studies in Conflict & Terrorism* 41.12 (2018): 968-989.
19. Zahari, A. I., Said, J., Abdullah, K., & Mohd Noor, N. "Financial innovations in terrorism financing: a case study of Malaysian terror financing." *Journal of Criminological Research, Policy and Practice* 10.1 (2024): 1-18.

Source of support: Nil; **Conflict of interest:** Nil.

Cite this article as:

Aryee, C. & Popoola, J. "Disrupting Terrorist Financing Networks: A scoping Review of Countering Funding for Political Violence and Extremist Operations in the U.S." *Sarcouncil journal of Arts humanities and social sciences* 5.6 (2026): pp 8-15.