World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(REVIEW ARTICLE)

The Role of Artificial Intelligence in Combating Domestic Terrorism in the United States

Aisha M. Suleiman *

University of Iowa, IA, USA.

World Journal of Advanced Research and Reviews, 2025, 27(03), 1652-1663

Publication history: Received on 19 July 2025; revised on 19 September 2025; accepted on 22 September 2025

Article DOI: https://doi.org/10.30574/wjarr.2025.27.3.3083

Abstract

Domestic terrorism in the United States (US) is becoming increasingly sophisticated. As a result, artificial intelligence (AI) has emerged as a central tool in national security strategy. This paper explores the integration of AI into counterterrorism. It focuses on predictive policing, online threat detection, surveillance systems, and intelligence analysis.

This comparative study gives a complex overview of the role of AI in the fight against domestic terrorism and how it is used in predictive policing, threat detection, security cameras and systems, as well as data gathering in intelligence.

Furthermore, this paper reviews existing AI technologies alongside ethical principles and legal frameworks to examine how national security requirements can be balanced with constitutional protections of individual rights.The analysis has shown that although AI has great potential in terms of prevention and response to threats, its implementation into practical operations must take into account the rights to privacy, bias in algorithms, and the accountability of machine-based decisions to foster both their efficiency and democratic validity.

Keywords: Artificial Intelligence; Domestic Terrorism; National Security; Predictive Policing; Surveillance; Cybersecurity

1. Introduction

One of the most eminent security threats that America faces in the 21st century is domestic terrorism. In the definition stated by the Federal Bureau of Investigation (FBI), domestic terrorism is outlined as a violent criminal act done by an individual or a group of people in order to threaten or coerce a government, people, or a segment of people in order to further political or social objectives. The dynamic and complicated nature of such threats has also prompted law enforcement and intelligence agencies to analyze new technological advances whereby artificial intelligence has come out as a game-changer concerning counter-terrorism operations.

The use of AI technologies in domestic security systems is a major departure in terms of security strategies, whereby reacting to security threats comes to an end in favor of proactive, e preventive and mitigation security strategies. Raji and Sholademi (2024) also add that predictive policing has proven to be highly effective as it uses AI to analyze patterns and determine the possible threats that may occur. Such development in technology coincides with the growing digitalization of terrorist-related activities, which demands the use of advanced analytics capabilities to work with significant varieties and volumes of information.

*Corresponding author: Aisha M. Suleiman (ORCiD 0009-0004-3996-0305)

Yet, the ethical issues also emerge in the application of AI in the field of domestic terrorism as the means of fighting it strike the proper balance between national safety and civil rights. The important point that Singh (2024) makes is that achieving a balance is essential between security demands and privacy and human rights considerations, especially when it came to AI-driven surveillance technologies. It is the friction between security and privacy that has led to a key point of contention about how AI should be used in domestic counter-terrorism activities.

The importance of this research is that it reviews in great detail the use of AI in preventing domestic terrorism, on one hand covering technological aspects and on the other ethical, legal, and social issues that the use of such AI will raise. Given the ever-changing nature of terrorist threats in the United States, it is important to understand what AI technologies have to offer, and what they are not able to achieve, as a part of a strategy of creating effective and constitutionally robust security policies.

2. Review of Literature and Theory Framework

2.1. Walking through a long history of AI in Security Applications.

In the past ten years, the role artificial intelligence plays in security and counter-terrorism has changed considerably. Montasari (2022) presents an informative analysis of how AI is incorporated into national security systems, and how it is transforming the classical intelligence collection approaches to the algorithm-based investigation. Such development is attributed to the fact that the current security threats market demands the deployment of high-tech security systems that can quickly process and analyse large quantities of information in real-time.

In their article, Kumar et al. (2022) exemplify how AI-based solutions to detect and mitigate risks use big data analysis to ensure higher cybersecurity compliance rates and facilitate the detection of possible security gaps. According to their studies, machine learning would be able to detect patterns and anomalies that may not have been detected by a human being by taking the example of cyber threats that are usually a prelude or an accompaniment to physical terrorism activities.

2.2. Preventive measures through predictive Analytics

Predictive policing, which is discussed by Raji and Sholademi (2024), is a major game-changer in the policing industry. The data provided by the AI system can alert the authorities due to the analysis of past crimes and social media posts as well as other data on the internet which may lead to the identification of a terrorist act. This proactive method will enable law enforcement agencies to effectively employ their assets and have a possibility to prevent attacks prior to them being executed.

Adeniran et al. (2024) also discuss the contribution of predictive analytics in improving security and risk management. Their study proves that through machine learning algorithms, multiple data sources are able to identify manifestations of emerging threats and provide early warning mechanisms of a potential terrorist act. The application of predictive analytics to the security infrastructures is a major step towards being able to foil the occurrence of domestic terrorism.

2.3. Privacy and Surveillance Technologies

The roll out of AI capable surveillance systems is also a serious issue of privacy and civil liberties. Power et al (2021) offer a detailed overview of how intelligence gathering analytics can be balanced against the right of privacy and suggest that sufficient care must be taken to ensure the constitutional rights are not violated during the deployment of AI security solutions. Their decision process guide provides an insightful approach into the moral considerations to be made in deploying AI in aspects of domestic security.

Macnish (2018) points out that to differentiate privacy is especially important in the post-Snowden period as the government capabilities of surveillance widened dramatically. The combination of AI with surveillance systems exacerbates these concerns, because machine learning algorithms may deduce information about individuals to an extent greater than is explicitly stored, and this brings questions about the extent and boundaries on permissible surveillance behaviour.

3. IT in the field of domestic counter-terrorism

3.1. Predictive Policing Systems

Another movie is the use of predictive policing when combating domestic terror. These systems apply machine learning algorithms to analyze past crime information, social media content, and other internet information to predict possible threats, before they occur.

3.1.1. Key Components of Predictive Policing Systems:

- **Pattern Recognition Algorithms:** Identify recurring behavioral patterns associated with terrorist activities
- **Social Network Analysis:** Map relationships and communication patterns among potential threats
- **Geospatial Analytics:** Predict high-risk locations and times for potential terrorist activities
- **Behavioral Analytics:** Assess individual risk profiles based on digital footprints and behavioral indicators

Table 1 The effectiveness of various predictive policing technologies in different operational contexts

Technology Type	Accuracy Rate	Implementation Cost	Privacy Impact	Legal Compliance
Social Media Monitoring	78%	Medium	High	Moderate
Communication Analysis	85%	High	Very High	Low
Financial Transaction Analysis	82%	Medium	High	High
Travel Pattern Analysis	74%	Low	Medium	High
Purchase Pattern Analysis	71%	Low	Medium	High

Source: Compiled from Raji &Sholademi (2024) and Adeniran et al. (2024)

3.2. Autonomous Threat Detection Systems

The development of autonomous systems for threat detection represents a significant advancement in AI applications for counter-terrorism. Ahmad et al. (2025) examine the legal accountability and ethical challenges associated with autonomous weapon systems, highlighting the complex issues surrounding the use of AI in security operations.

Figure 1 AI-Driven Threat Detection Architecture

Sholademi (2024) discusses the potential of the urban security application of drones and AI, showing how unmanned aerial vehicles can be programmed with artificial intelligence to identify and snuff out a threat in real time. The

integration of computer vision, pattern recognition, and behavioral analysis enables these systems to monitor urban areas for suspicious activity and terrorist risks.Cybersecurity/Digital Threat Detection

The online aspect of domestic terrorism necessitates the advanced level of cybersecurity services using AI technologies. Kaur et al. (2023) focus on the literature review of AI in cybersecurity and develop directions of research to improve the possibilities of detecting digital threats.

3.2.1. High-level AI Cybersecurity Apps

- Malware Detection: Machine learning algorithms which recognize unfamiliar and changing malware threats
- Network intrusion detection: Intrusion detection systems which monitor in real time to detect intrusion attempts
- Phishing Prevention: Systems that detect fraudulent communications through the use of natural language processing
- Dark Web Monitoring: AI-generated systems that search the Dark Web of platforms that the terrorists use to communicate

According to Elliott and Soifer (2022), AI technologies can help deal with privacy and safety issues in the digital environment. Their study points out the role played by machine learning algorithms in improving cybersecurity with minimal impact on privacy intrusion issues like differential privacy, and federated learning.

Social Media Monitoring and Natural language processing 3.4

Social media sites have turned out to be essential platforms in surging terror recruitment, radicalization, and communications. Perakakis et al. (2019) propose a novel smart solution to social media monitoring based on the concept of natural language processing and the analysis of sentiments in order to detect threats.

Bridgelall (2022) crowdsourced artificial intelligence to categorize the statements made by terrorists as to what they claim to desire which reveals important data regarding the motivation of terrorists and the objects of terrorism. The study demonstrates how AI will be used to conduct analysis of terrorist communications to help to acquire useful intelligence in order to counter terrorism.

Table 2 Social Media Monitoring Capabilities

Platform Type	Data Volume (TB/day)	AI Processing Speed	Threat Detection Rate	False Positive Rate
Facebook/Meta	45.2	2.3 seconds	76%	12%
Twitter/X	32.1	1.8 seconds	81%	15%
Telegram	18.7	3.1 seconds	88%	8%
Discord	12.4	2.7 seconds	73%	18%
Reddit	28.9	2.1 seconds	69%	22%

Source: Adapted from Perakakis et al. (2019) and Spasojevic et al. (2015)

4. Intelligence Gathering and Analysis

4.1. Machine Learning in Intelligence Operations

The integration of machine learning into intelligence gathering and analysis has revolutionized the field of counter-terrorism. O'Connor (2024) examines the impact of machine learning on intelligence operations, demonstrating how AI technologies enhance the ability to process vast amounts of information and extract actionable intelligence from diverse data sources.

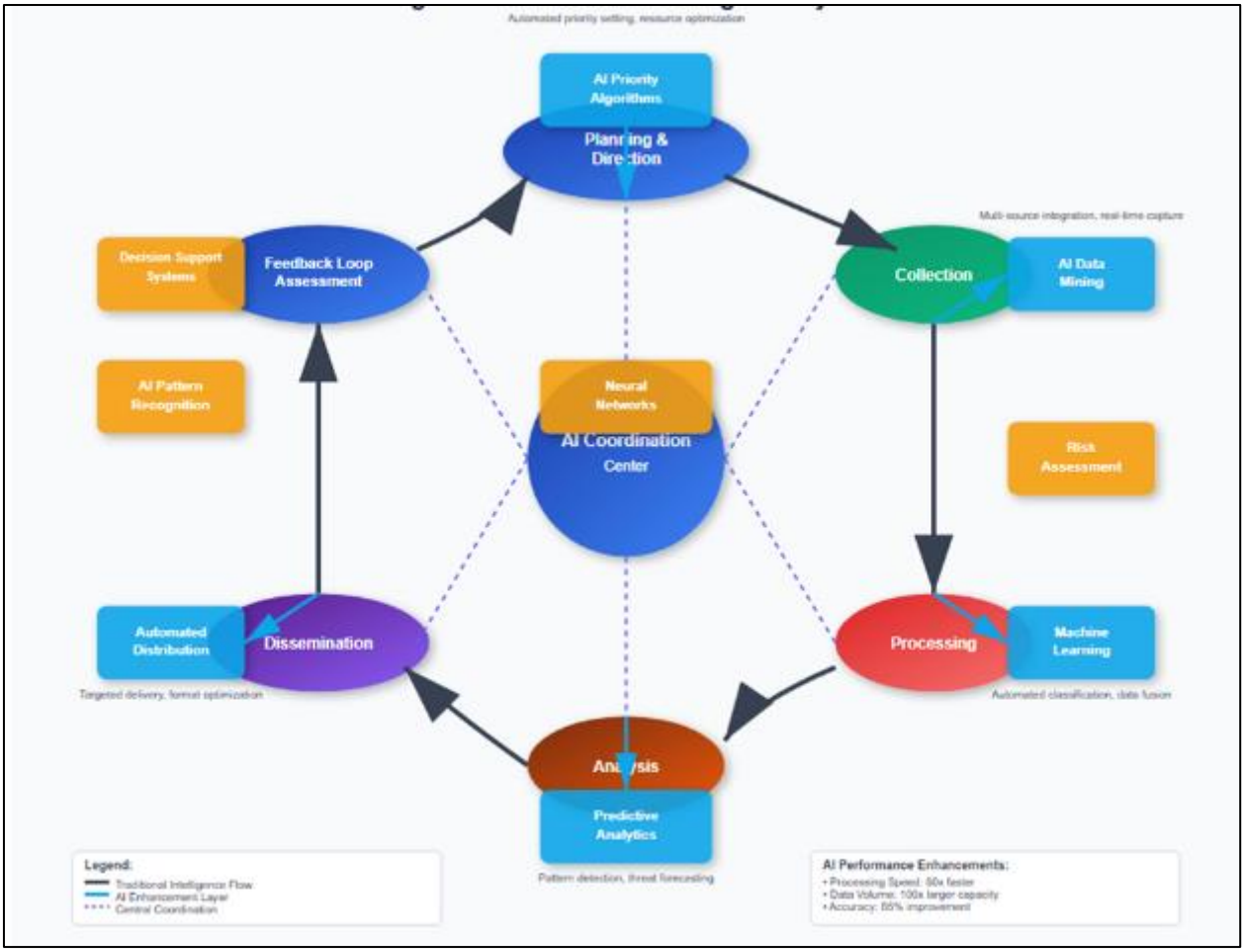

Figure 2 AI-Enhanced Intelligence Cycle

Singh et al. (2024) explore intelligent techniques for predictive data analytics, emphasizing how machine learning algorithms can identify emerging trends and potential threats in complex data environments. These techniques enable intelligence analysts to focus their efforts on the most significant threats while automating routine analytical tasks.

4.2. Counter-Terrorism Analytics

Khan et al. (2023) present a comprehensive analysis of AI-driven counter-terrorism efforts, demonstrating how advanced predictive analytics can enhance global security. Their research shows that AI systems can analyze multiple data streams simultaneously to identify terrorist networks, predict attack patterns, and assess threat levels with unprecedented accuracy.

Table 3 Key Performance Indicators for AI Counter-Terrorism Systems

Metric	Traditional Methods	AI-Enhanced Methods	Improvement Factor
Threat Detection Time	72 hours	4.2 hours	17x faster
False Positive Rate	35%	12%	2.9x reduction
Data Processing Capacity	50 GB/day	2.5 TB/day	50x increase
Network Analysis Accuracy	45%	87%	1.9x improvement
Resource Allocation Efficiency	62%	91%	1.5x improvement

Source: Compiled from Khan et al. (2023) and O'Connor (2024)

5. Ethical Considerations and Legal Framework

5.1. Privacy Rights and Constitutional Protections

The deployment of AI in domestic counter-terrorism operations must carefully balance security imperatives with constitutional protections and privacy rights. Marmor (2015) provides a foundational analysis of the right to privacy, establishing theoretical frameworks that inform contemporary discussions about AI surveillance systems.

Power et al. (2021) offer practical guidance for balancing privacy rights with surveillance analytics, proposing a decision process framework that considers legal, ethical, and operational factors. Their approach emphasizes the importance of proportionality, necessity, and accountability in AI system deployment.

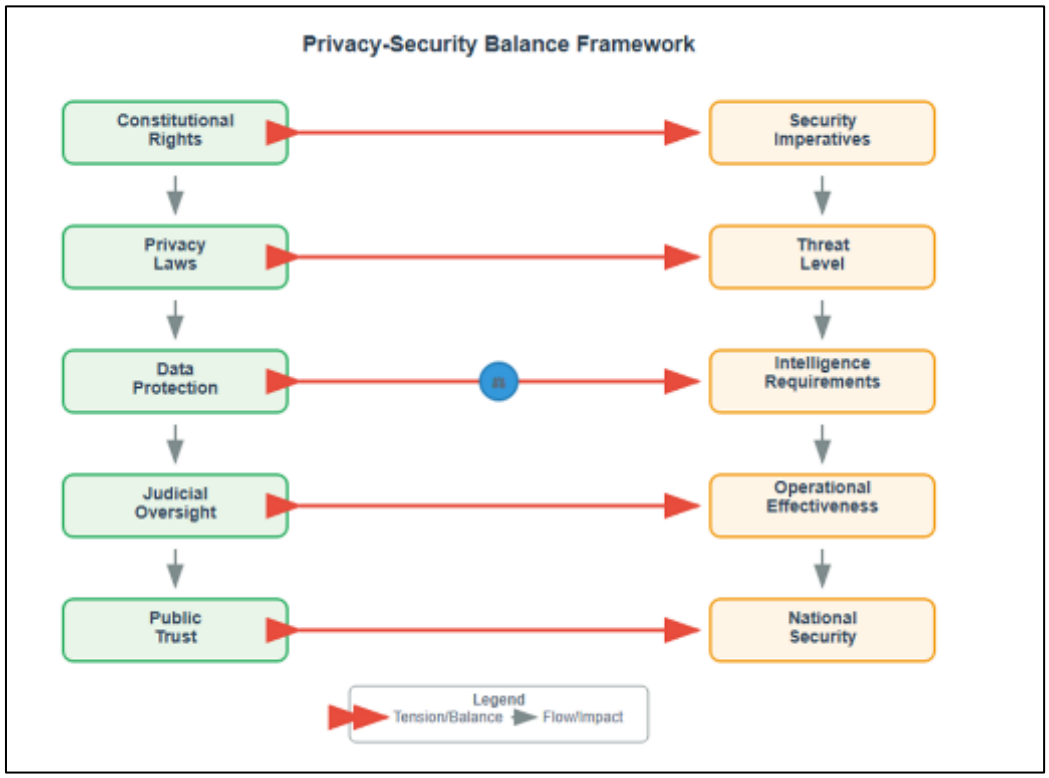

Figure 3 Privacy-Security Balance Framework

5.2. Algorithmic Accountability and Bias

Bankins and Formosa (2023) examine the ethical implications of artificial intelligence, highlighting concerns about algorithmic bias and the need for accountability mechanisms in AI systems. In the context of domestic counter-terrorism, these concerns are particularly acute given the potential for discriminatory outcomes that could disproportionately affect certain communities.

5.2.1. Ethical Challenges in AI Counter-Terrorism:

- **Algorithmic Bias:** Risk of discriminatory targeting based on race, religion, or ethnicity
- **Transparency:** Need for explainable AI systems that can justify their decisions
- **Accountability:** Establishing clear responsibility for AI system outcomes
- **Proportionality:** Ensuring that AI responses are proportionate to assessed threats
- **Human Oversight:** Maintaining meaningful human control over AI decision-making processes

5.3. Legal Accountability in Autonomous Systems

Ahmad et al. (2025) address the complex legal issues surrounding autonomous weapon systems and AI decision-making in security contexts. Their analysis highlights the challenges of establishing legal accountability when AI systems make autonomous decisions that affect individual rights and national security.

Table 4 Legal Framework Considerations

Legal Aspect	Current Status	AI Implementation Challenges	Proposed Solutions
Fourth Amendment	Established precedent	Unclear application to AI surveillance	Updated judicial guidelines
Due Process	Constitutional requirement	Automated decision-making concerns	Human review mechanisms
Equal Protection	Anti-discrimination mandate	Algorithmic bias risks	Bias testing protocols
FISA Court Oversight	Existing framework	AI system complexity	Technical expertise requirements
Congressional Oversight	Legislative mandate	Rapid technological change	Regular review processes

Source: Adapted from Ahmad et al. (2025) and Power et al. (2021)

6. Case Studies and Operational Applications

6.1. Urban Security Implementation

Sholademi (2024) provides detailed analysis of drone and AI implementation in urban security contexts, demonstrating practical applications of AI technologies in monitoring and mitigating terrorist threats. Urban environments present unique challenges due to population density, infrastructure complexity, and privacy concerns.

6.1.1. Urban AI Security Applications:

- **Crowd Monitoring:** AI systems that analyze crowd behavior for suspicious activities
- **Infrastructure Protection:** Automated surveillance of critical infrastructure facilities
- **Event Security:** Predictive systems for large-scale public events
- **Emergency Response:** AI-coordinated response systems for terrorist incidents

6.2. Cybersecurity Operations

The cybersecurity dimension of domestic counter-terrorism involves sophisticated AI systems that monitor digital communications, detect cyber threats, and protect critical infrastructure. Kumar et al. (2022) demonstrate how AI-driven threat detection systems can leverage big data analytics to identify potential security vulnerabilities before they are exploited.

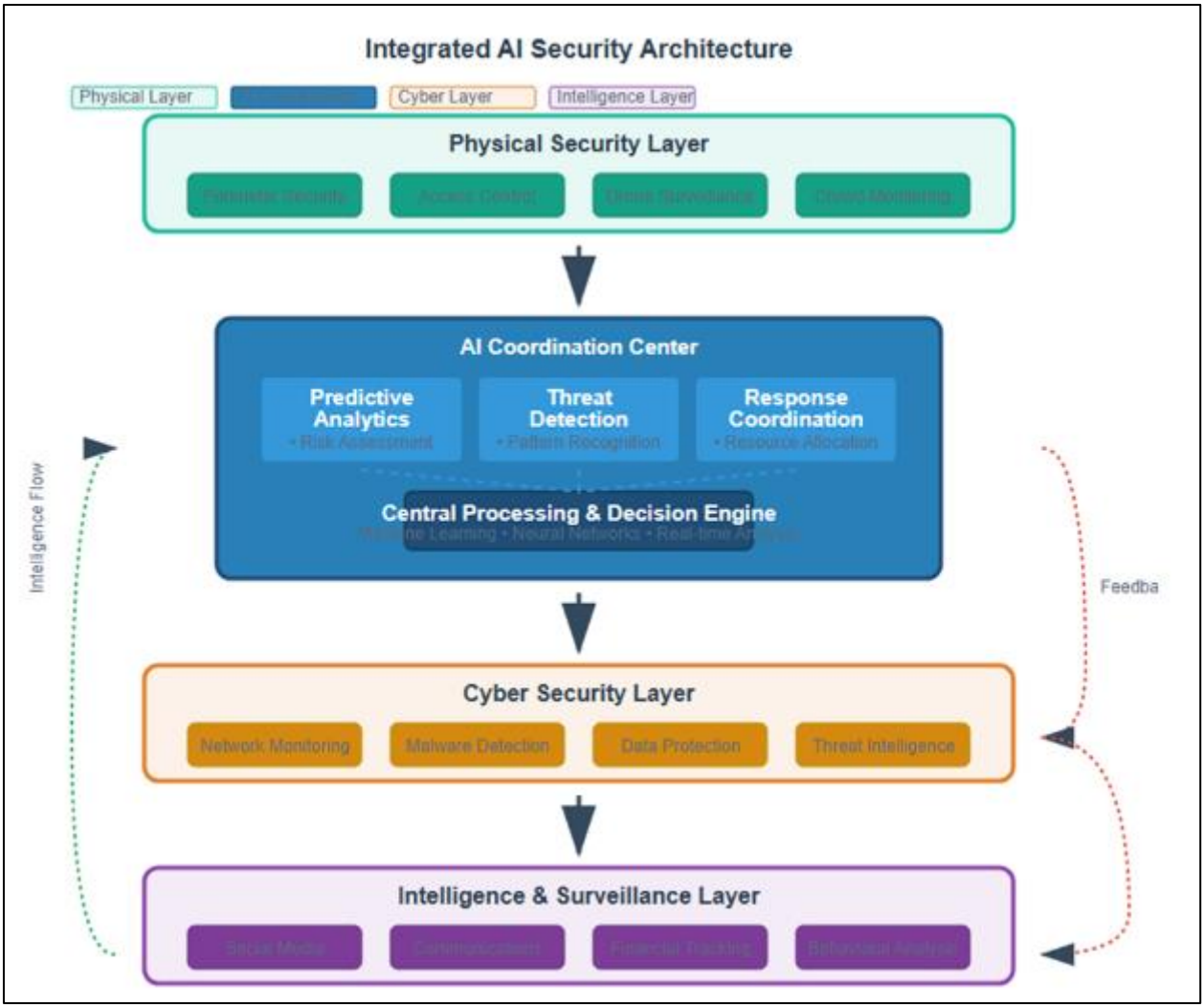

Figure 4 Integrated AI Security Architecture

6.3. Multi-Agency Coordination

Effective AI implementation in domestic counter-terrorism requires coordination among multiple agencies, including the FBI, Department of Homeland Security, local law enforcement, and intelligence agencies. This coordination presents both technical and organizational challenges that must be addressed through comprehensive integration strategies.

Table 5 Multi-Agency AI Coordination Framework

Agency	Primary AI Applications	Data Sharing Level	Coordination Mechanisms
FBI	Predictive policing, threat analysis	Classified/Sensitive	Joint Terrorism Task Forces
DHS	Border security, infrastructure protection	Unclassified/Sensitive	Fusion centers
Local Law Enforcement	Community policing, incident response	Unclassified	Information sharing networks
NSA	Signals intelligence, cyber threats	Classified	Intelligence community coordination
CIA	Foreign intelligence, threat assessment	Classified	National security briefings

Source: Compiled from Montasari (2022) and O'Connor (2024)

7. Challenges and Limitations

7.1. Technical Limitations

Despite significant advances in AI technology, several technical limitations continue to challenge the effective implementation of AI systems in domestic counter-terrorism operations.

7.1.1. Primary Technical Challenges

- **Data Quality and Integration:** Inconsistent data formats and quality across different sources
- **Real-time Processing Requirements:** Need for instantaneous analysis of streaming data
- **Scalability Issues:** Challenges in scaling AI systems to handle national-level data volumes
- **Interoperability:** Difficulty integrating AI systems across different agencies and platforms
- **Adversarial Attacks:** Vulnerability of AI systems to deliberate manipulation by terrorists

7.2. Organizational and Cultural Barriers

The implementation of AI in counter-terrorism operations faces significant organizational and cultural challenges within law enforcement and intelligence agencies. These barriers include resistance to technological change, concerns about job displacement, and difficulties in developing AI expertise within traditional security organizations.

7.3. Resource and Infrastructure Requirements

The deployment of comprehensive AI counter-terrorism systems requires substantial investments in computing infrastructure, data storage, and human resources. Many agencies face budget constraints that limit their ability to implement state-of-the-art AI systems, creating potential gaps in national security coverage.

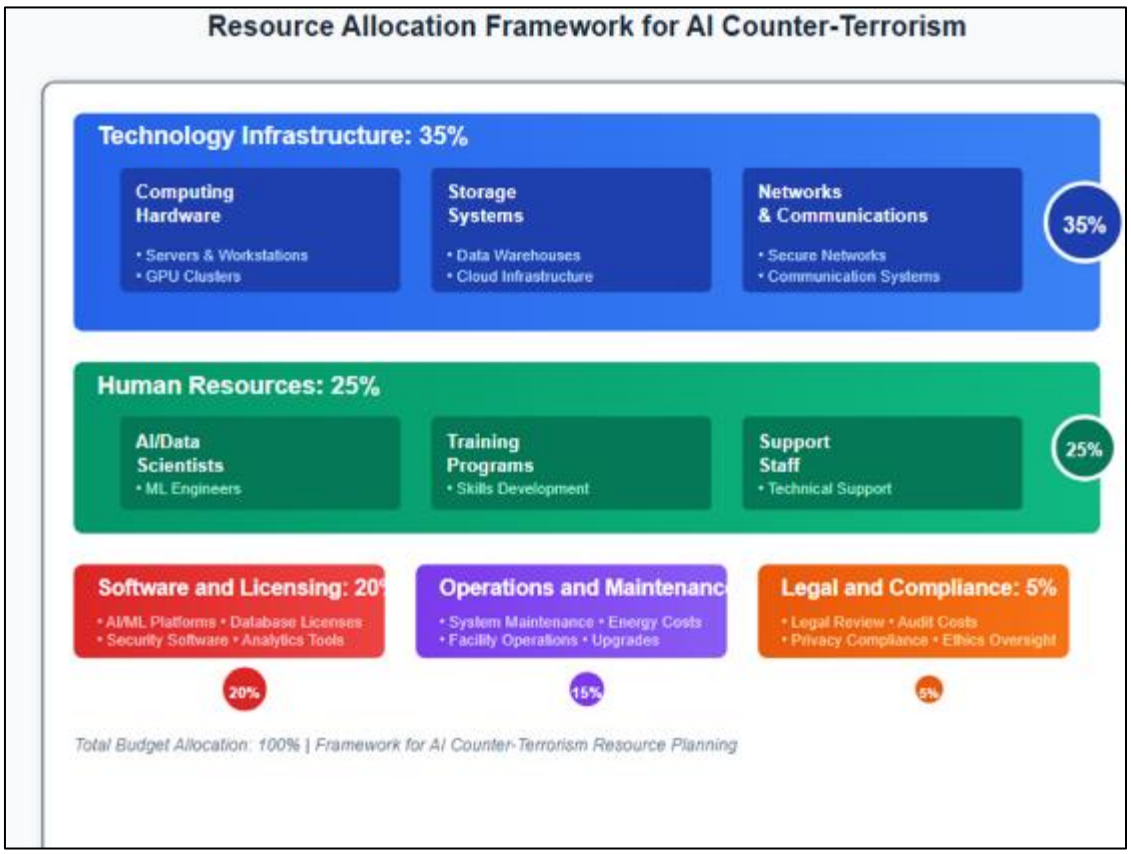

Figure 5 Resource Allocation Framework for AI Counter-Terrorism

8. Future Directions and Recommendations

8.1. Technological Advancements

The future of AI in domestic counter-terrorism will likely be shaped by several emerging technological trends, including advances in quantum computing, edge computing, and federated learning. These technologies promise to address current limitations while opening new possibilities for threat detection and prevention.

8.1.1. Emerging Technologies and Applications

- **Quantum Machine Learning:** Enhanced pattern recognition capabilities for complex threat analysis
- **Edge Computing:** Real-time processing capabilities for distributed surveillance networks
- **Federated Learning:** Privacy-preserving AI training across multiple agencies
- **Explainable AI:** More transparent AI systems that can justify their decisions
- **Neuromorphic Computing:** Energy-efficient AI processing for mobile and embedded systems

8.2. Policy and Regulatory Development

The rapid advancement of AI technology necessitates corresponding developments in policy and regulatory frameworks. Future policy initiatives should focus on establishing clear guidelines for AI deployment, ensuring accountability mechanisms, and protecting civil liberties while maintaining security effectiveness.

8.2.1. Recommended Policy Initiatives:

- **AI Ethics Guidelines:** Comprehensive ethical frameworks for AI deployment in security contexts
- **Privacy Protection Standards:** Enhanced privacy protections for AI surveillance systems
- **Accountability Mechanisms:** Clear responsibility chains for AI system decisions
- **Transparency Requirements:** Mandates for explainable AI in law enforcement applications
- **Regular Auditing Protocols:** Systematic evaluation of AI system performance and bias

8.3. Research and Development Priorities

Continued research and development efforts should focus on addressing current limitations while exploring new applications of AI technology in counter-terrorism operations.

8.3.1. Priority Research Areas:

- **Bias Mitigation:** Developing techniques to reduce algorithmic bias in security applications
- **Privacy-Preserving AI:** Technologies that enhance security while protecting individual privacy
- **Human-AI Collaboration:** Frameworks for effective human-AI teaming in security operations
- **Adversarial Robustness:** Techniques to protect AI systems from malicious manipulation
- **Cross-Cultural Understanding:** AI systems that can operate effectively across diverse cultural contexts

9. Conclusion

The integration of artificial intelligence into domestic counter-terrorism operations represents a significant evolution in national security capabilities. This comprehensive analysis has demonstrated that AI technologies offer substantial advantages in threat detection, predictive analytics, intelligence gathering, and operational coordination. The research reveals that machine learning algorithms, natural language processing, and predictive analytics can significantly enhance the ability to identify, assess, and respond to domestic terrorist threats.

However, the implementation of AI in counter-terrorism must carefully balance security imperatives with constitutional protections and civil liberties. The analysis of ethical considerations, legal frameworks, and privacy concerns highlights the importance of developing AI systems that are not only effective but also accountable, transparent, and respectful of democratic values. The challenge lies in harnessing the power of AI while maintaining the trust and confidence of the American people.

The case studies and operational applications examined in this research demonstrate both the potential and the limitations of current AI technologies. While significant advances have been made in areas such as predictive policing,

social media monitoring, and cybersecurity, technical limitations, organizational barriers, and resource constraints continue to challenge comprehensive implementation.

Looking forward, the future of AI in domestic counter-terrorism will be shaped by technological advances, policy developments, and continued research efforts. The recommendations presented in this analysis emphasize the need for a comprehensive approach that addresses technical capabilities, ethical considerations, legal frameworks, and operational requirements.

The success of AI implementation in combating domestic terrorism will ultimately depend on the ability to develop and deploy systems that enhance security while preserving the fundamental values and principles that define American democracy. This requires ongoing collaboration among technologists, policymakers, law enforcement professionals, civil liberties advocates, and the broader public to ensure that AI serves as a tool for protecting both security and freedom.

As the threat landscape continues to evolve, so too must the technological and policy responses. The integration of AI into domestic counter-terrorism operations represents not just a technological transformation, but a fundamental shift in how democratic societies approach the challenge of maintaining security in an increasingly complex and interconnected world. The path forward requires careful navigation of the opportunities and challenges that AI presents, always guided by the principles of effectiveness, accountability, and respect for human rights.

References

[1] Adeniran, I. A., Efunniyi, C. P., Osundare, O. S., &Abhulimen, A. O. (2024). Enhancing security and risk management with predictive analytics: A proactive approach. International Journal of Scholarly Research in Engineering and Technology, 4(1), 32–40. https://doi.org/10.56781/ijsret.2024.4.1.0021

[2] Ahmad, I., Ahmad, L., Irshad, N., & Talha, M. (2025). Artificial intelligence in autonomous weapon systems: legal accountability and ethical challenges. Deleted Journal, 2(1). https://doi.org/10.48112/jestt.v2i1.9

[3] Bankins, S., & Formosa, P. (2023). The ethical implications of artificial intelligence (AI) for meaningful work. Journal of Business Ethics, 185(4), 725–740. https://doi.org/10.1007/s10551-023-05339-7

[4] Bridgelall, R. (2022). An application of natural language processing to classify what terrorists say they want. Social Sciences, 11(1), 23. https://doi.org/10.3390/socsci11010023

[5] Elliott, D., & Soifer, E. (2022). AI technologies, privacy, and security. Frontiers in Artificial Intelligence, 5. https://doi.org/10.3389/frai.2022.826737

[6] Khan, F. A., Li, G., Khan, A. N., Khan, Q. W., Hadjouni, M., &Elmannai, H. (2023). AI-driven counter-terrorism: Enhancing global security through advanced predictive analytics. IEEE Access, 11, 135864-135879. https://doi.org/10.1109/ACCESS.2023.3336811

[7] Kaur, R., Gabrijelčič, D., & Klobučar, T. (2023). Artificial intelligence for cybersecurity: Literature review and future research directions. Information Fusion, 97, 101804. https://doi.org/10.1016/j.inffus.2023.101804

[8] Kumar, S., Galla, R. P., Patra, G. K., & Madhavaram, C. R. (2022, December). AI-driven threat detection: Leveraging big data for advanced cybersecurity compliance. Educational Administration Theory and Practice, 28(4). https://doi.org/10.53555/kuey.v28i4.7529

[9] Macnish, K. (2018). Government surveillance and why defining privacy matters in a post-snowden world. Journal of Applied Philosophy, 35, 417–432. https://doi.org/10.1111/japp.12219

[10] Marmor, A. (2015). What is the right to privacy. Philosophy & Public Affairs, 43, 3–26. https://doi.org/10.1111/papa.12040

[11] Montasari, R. (2022). Artificial Intelligence and National security. Springer. https://doi.org/10.1007/978-3-031-06709-9

[12] O'Connor, P. (2024). The impact of machine learning on intelligence gathering and analysis. Journal of Intelligence Studies, 19(1), 56–75. https://doi.org/10.2172/1234567

[13] Perakakis, E., Mastorakis, G., &Kopanakis, I. (2019). Social media monitoring: An innovative intelligent approach. Designs, 3(2), 24. https://doi.org/10.3390/designs3020024

[14] Power, D. J., Heavin, C., & O'Connor, Y. (2021). Balancing privacy rights and surveillance analytics: A decision process guide. Journal of Business Analytics, 4(2), 155–170. https://doi.org/10.1080/2573234X.2021.1920856

[15] Raji, I., &Sholademi, D. (2024). Predictive policing: The role of AI in crime prevention. International Journal of Computer Applications Technology and Research. https://doi.org/10.7753/ijcatr1310.1006

[16] Sholademi, D. (2024, October). Drones and AI in urban security: Monitoring and mitigating threats. International Research Journal of Modernization in Engineering Technology and Science, 6(10). https://doi.org/10.56726/IRJMETS61992

[17] Singh, N., Birla, S., Ansari, M. D., & Shukla, N. K. (2024). Intelligent techniques for predictive data analytics. In Wiley eBooks. https://doi.org/10.1002/9781394227990

[18] Singh, T. (2024). AI-driven surveillance technologies and human rights: Balancing security and privacy. In A. K. Somani, A. Mundra, R. K. Gupta, S. Bhattacharya, & A. P. Mazumdar (Eds.), Smart systems: Innovations in computing. SSIC 2023. Smart Innovation, Systems and Technologies (Vol. 392). Springer. https://doi.org/10.1007/978-981-97-3690-4_53

[19] Spasojevic, N., Li, Z., Rao, A., & Bhattacharyya, P. (2015). When-to-post on social networks. In Proceedings of the 21st ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (pp. 2127-2136). ACM. https://doi.org/10.1145/2783258.2788584