iJRASET
International Journal For Research in
Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH
IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 Issue: VIII Month of publication: August 2025

DOI: https://doi.org/10.22214/ijraset.2025.73912

Survey on a New Model for Predicting and Dismantling a Complex Terrorist Network

Shwetha A B[1], Arpitha G[2], Chirantana Prashanth[3], Divya N[4]
[1]Assistant Professor,Dept. of CSE , Sapthagiri College of Engineering
[2, 3, 4]Dept. of CSE , Sapthagiri College of Engineering

Abstract: Terrorist attacks keep happening around the world, which has led researchers to use Social Network Analysis (SNA) as a way to study terrorism. Terrorist groups function like secretive networks, strengthening their operations while staying hidden. This study introduces a new approach to reveal and break apart such networks by using four different centrality measures. First, the method predict hidden or missing link in the network using these centrality measures. Then, the network is dismantled by applying the Galton-Watson extinction probability model, which helps estimate the chances of the network collapsing. The study looks at real-world cases, such as the 9/11 terrorist attacks and the M-19 group, to test how well link prediction works. It shows that removing the most influential members (highly ranked nodes) is essential for weakening and destroying a terrorist network. Additionally, the research examines how dangerous the network is (lethality) and how tightly connected its members are (bonding), since cohesiveness is critical for a network's survival. The results demonstrate that link prediction is a key tool for exposing hidden terrorist networks, making it an important strategy for counterterrorism efforts.

Keywords: Social Network Analysis (SNA), lethality, centrality measures.

I. INTRODUCTION

In recent years, terrorist attacks have grown in frequency worldwide, with such groups responsible for massive destruction of lives and property. Because of this, counterterrorism strategies are essential, and one of the first step is to understand how terrorist organization actually function. Research on how to uncloak hidden terror networks has expanded rapidly.

However, many official counterterrorism efforts have struggled, largely because modern terrorist groups are highly adaptable and resilient. According to the Global Terrorism Database (GTD), between 1970 and 2019 there were over 180,000 recorded terrorist incidents, showing the scale of the challenge. Since then, numerous studies have tried to find better ways to tackle the problem.Terrorism itself is dynamic, not static. Both old and new groups learn from each other, sharing knowledge and tactics, especially when a particular approach succeeds.

This means that counterterrorism methods must also evolve and remain flexible. One useful tool is Social Network Analysis (SNA), which studies how individuals in these groups are connected. Unlike ordinary social networks, terrorist networks are layered. They typically have a core, which acts as the command and control center, and a periphery, which carries out instructions. The structure is hierarchical, with each member playing a defined role.Understanding this operational structure is crucial. Scholars note that modeling terrorist networks is extremely complex (an NP-complete problem), making them difficult to analyze. The 9/11 attack brought this challenge to the front, when Valdis Krebs first mapped the network of hijackers, which later became a reference point for many studies.

Terrorist networks act like hidden social networks with organizational features. Their secrecy makes it hard for intelligence agencies to track them. Data about their operations is often vague or incomplete, again making analysis difficult. As a result, researchers argue that dismantling such networks requires heuristic and brute-force methods, supported by advanced network models. Terrorist activities are designed to be stealthy and lethal. Borrowing from David Mitrany's theory of functionalism, terrorist cooperation often spreads into other areas, producing a cascading effect that increases their ability to cause large-scale damage. Moreover, these groups usually operate only in environments that act as safe havens, giving them cover and helping them thrive.

In this study, the authors treat a terrorist network as a graph (TN = G), where actors (nodes) are connected through shared information (edges). They assume that when one group achieves success, other groups often imitate those tactics. For example, since the Colombian M-19 group carried out successful operations, its methods provide valuable lessons for understanding and countering other terrorist organizations.

II. BACKGROUND

Terrorist groups operate like hidden social networks, where members (nodes) are connected by communication, training, family, or financial ties (edges).

1) Centrality measures (degree, closeness, betweenness, eigenvector) identify important or suspicious nodes.
2) Social Network Analysis (SNA) is applied to map visible members and relationships.
3) Link prediction helps detect hidden or missing ties that are not directly observable in intelligence data.
4) This process reveals the structure of the network and highlights key figures who are central to its operations.
5) By existing patterns, it estimates where new ties are likely to form (for example, training links, funding channels, or communication pathways)
6) Remove highly central actors (leaders, brokers) whose elimination fragments the network.
7) Apply the Galton-Watson extinction model: this uses probability theory to estimate how removing certain nodes leads to network collapse.
8) Measure network lethality (ability to conduct deadly attacks) and cohesiveness (bonding strength). Breaking high-cohesion links reduces survival chances.

III. LITERATURE SURVEY

A. V. Krebs, ''Uncloaking terrorist networks,'' FM, vol. 7, no. 4, Apr. 2002.

METHODOLOGY: Relied on publicly available information (news reports, court documents, government releases). Individuals (terrorists and associates) were represented as nodes. Strength of ties was classified into strong, moderate, and weak, based on how much time individuals spent together. Examined redundancy and resilience due to trusted long-term ties (e.g., Hamburg cell).

LIMITATION:Not all nodes and ties are visible.Some relationships may never be uncovered (hidden or destroyed).Some information reported in the media was incorrect or planted deliberately.Incomplete or inaccurate data could distort network maps. Because covert networks deliberately minimize visible ties, making them hard to detect beforehand.

B. S. J. Dixon et al., ''A neural network for counter-terrorism,'' in Intell. London, U.K.: Springer, 2011

METHODOLOGY: The study explored the use of artificial neural networks (ANNs) to identify deceptive or terrorist behavior in a controlled environment. Data was generated through a simulation game where participants acted as either genuine builders or terrorists disguised as builders. A feed-forward backpropagation neural network was implemented with 122 input variables, one hidden layer of 10 neurons, and a single output neuron. Using supervised learning and sigmoid activation, the network was trained and tested on 144 game records, achieving an average success rate of 60–68% in distinguishing builders from terrorists.

LIMITATION: Despite showing potential, the approach faced several limitations. The dataset was small and imbalanced, with more builder than terrorist samples, creating bias in learning. The high dimensionality of input variables increased computational complexity and risk of overfitting. Accuracy remained modest, leading to false positives and negatives that are unacceptable in real-world counter-terrorism. Moreover, the reliance on simulated game data restricted generalizability, as actual terrorist behavior may differ significantly from modeled scenarios.

C. A. Berzinji, L. Kaati, and A. Rezine, ''Detecting key players in terrorist networks,'' in Proc. Eur. Intell. Secur. Informat. Conf. (EISIC), Aug. 2012, pp. 297–302.

METHODOLOGY: The study applies Social Network Analysis (SNA) to identify critical terrorists within covert networks. Terrorists are modeled as nodes, and their connections—such as communication, organizational ties, or family links—are represented as edges. The network is then examined using centrality measures like degree (most active members), betweenness(information brokers), closeness (quick reachability), and eigenvector centrality (connections to influential individuals). To refine this, Key Player Analysis (KPP) is applied in two ways: KPP-Pos, which identifies individuals whose removal would fragment and weaken the network, and KPP-Neg, which highlights those most effective at spreading influence or information. These methods are demonstrated through case studies, where the removal of key individuals is shown to disrupt communication, cohesion, and operational efficiency.

LIMITATION: While effective in theory, this approach faces several practical challenges. Terrorist networks are dynamic and covert, making data collection incomplete or inaccurate, as many ties remain hidden or deliberately obscured. Static snapshots of networks also fail to capture their adaptive and evolving nature. Moreover, centrality-based rankings can be misleading since high visibility does not always equate to true leadership or operational significance, as leaders may intentionally keep a low profile.

Beyond technical issues, there are ethical and legal risks, including the possibility of misidentifying innocent individuals due to indirect associations. Finally, even when key players are identified, real-world interventions depend on intelligence quality, timing, and political constraints, making implementation complex.

D. Z. Su, K. Ren, R. Zhang, and S.-Y. Tan, ‘‘Disrupting terrorist networks based on link prediction: A case study of the 9–11 hijackers network,’’ IEEE Access, vol. 7, pp. 61689–61696, 2019.

METHODOLOGY: This study proposes a link prediction–based disintegration model to identify and remove critical nodes in terrorist networks, particularly when link information is incomplete. The authors model the terrorist network as a graph, with terrorists as nodes and relationships as edges. They employ similarity-based link prediction algorithms to estimate missing ties and reconstruct a more accurate network structure. After evaluating 20 algorithms, the Resource Allocation (RA) index was chosen for its superior performance. Using the September 11th hijackers as a case study, the reconstructed networks were analyzed under different node removal strategies (degree, betweenness, closeness, and eigenvector centrality). The efficiency of disruption was measured by the reduction in the size of the largest connected component after successive node removals. Results show that adding predicted links improves disruption outcomes significantly, sometimes even outperforming complete-data scenarios due to a “comic effect,” where predicted links exaggerate important structures and emphasize critical nodes.

LIMITATION: Despite its promise, the approach faces several limitations. Accuracy depends heavily on the amount of missing information: when more than 50% of links are absent, prediction adds noise and reduces disintegration effectiveness. The comic effect, while beneficial in some cases, may also distort network structure and introduce false “noise nodes” that do not reflect actual importance. Moreover, the method primarily considers structural relationships while ignoring contextual factors such as resources, skills, tasks, and dynamic changes in terrorist networks. The authors also acknowledge that in real-world intelligence settings, the exact proportion of missing links is unknown, making it difficult to tune prediction magnitude optimally. Finally, computational complexity for path-based strategies (like betweenness) can hinder applicability in large-scale networks. These limitations highlight the need for hybrid approaches that combine structural prediction with domain-specific intelligence for reliable network disruption.

IV. METHODOLOGY

The paper presents an agent-based modeling (ABM) approach as a tool to simulate, analyze, and forecast the behavior of terrorist organizations and the evolution of their attack patterns. Unlike conventional statistical models or purely network-structural approaches, ABM provides a bottom-up simulation environment in which individual actors are represented as autonomous agents endowed with specific behavioral rules, capabilities, and decision-making logics. Each agent may correspond to a terrorist operative, a recruiter, a leader, or even a counter-terrorism entity such as intelligence officers or security agencies. Agents are not static; they interact with their environment and with each other, forming emergent structures and collective behaviors that resemble real-world organizational dynamics.

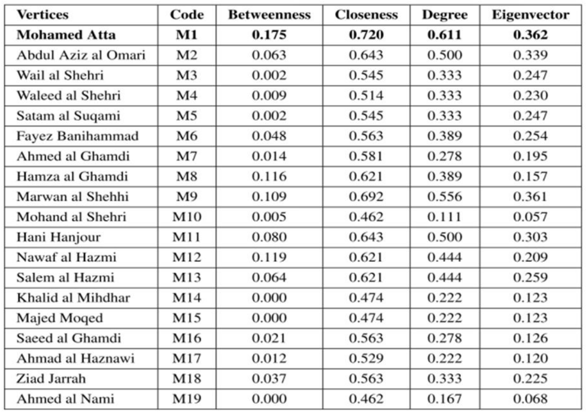
The modeling framework incorporates several important features. First, it embeds heterogeneity among agents, recognizing that terrorists differ in ideology, skills, resources, and influence. Second, it introduces probabilistic and adaptive decision-making: agents choose actions (e.g., joining a group, conducting reconnaissance, launching attacks) based on probabilities that evolve over time according to experiences, environmental pressures, and feedback from past successes or failures. Third, the environment itself is dynamic and includes contextual factors such as socio-political conditions, counter-terrorism pressure, and opportunities for radicalization or recruitment.

A central element of the methodology is the ability to run “what-if” simulations under different counter-terrorism strategies. For example, the model allows testing the impact of leadership decapitation (removal of top leaders), disruption of recruitment pipelines, or the restriction of financial and logistical resources. By simulating multiple iterations, the model yields insights into how these interventions may influence future attack frequency, group survival, or network resilience. Furthermore, the methodology integrates historical data from past terrorist events to calibrate agent behaviors, making the simulation partially grounded in empirical evidence. This combination of data-driven calibration and rule-based simulation allows researchers to experiment with complex scenarios that cannot be easily captured using purely mathematical or network-theoretic models.

Ultimately, the ABM framework provides a flexible, exploratory platform for examining terrorism as a dynamic, adaptive system. Rather than producing point predictions, it enables analysts and policymakers to explore possible futures, uncover nonlinear relationships, and evaluate how small changes in behavior or policy can cascade into large-scale impacts on the stability and lethality of terrorist organizations.

A. Figures and Tables

1) Table 1 outlines the key features of the agent-based simulation model, describing how different elements of the system are represented and how they interact. The model treats both terrorists and counter-terrorism forces as autonomous agents, each equipped with attributes such as resources, skills, motivations, and levels of commitment. These attributes are not static but evolve dynamically as the simulation progresses, reflecting the adaptive and changing behavior of real-world actors. The behavior of agents is governed by probabilistic rules, meaning decisions—such as whether to recruit, plan an attack, or attempt disruption—are made under uncertainty and influenced by external conditions like opportunities or threats. The environment provides the broader context, incorporating social, political, and security conditions that shape agent decisions and interactions. Within this environment, agents continuously interact: terrorists recruit, form cells, and attempt attacks, while counter-terrorism agents try to identify, monitor, and dismantle these structures. From these micro-level interactions, the model produces emergent outcomes such as attack frequency, lethality, organizational survival, and the resilience or fragmentation of terrorist networks. Thus, the table captures the model's multi-layered design, emphasizing that a combination of agent heterogeneity, adaptive decision-making, environmental dynamics, and interactions leads to system-level behaviors that can be studied to evaluate different counter-terrorism strategies.



Vertices	Code	Betweenness	Closeness	Degree	Eigenvector
Mohamed Atta	**M1**	**0.175**	**0.720**	**0.611**	**0.362**
Abdul Aziz al Omari	M2	0.063	0.643	0.500	0.339
Wail al Shehri	M3	0.002	0.545	0.333	0.247
Waleed al Shehri	M4	0.009	0.514	0.333	0.230
Satam al Suqami	M5	0.002	0.545	0.333	0.247
Fayez Banihammad	M6	0.048	0.563	0.389	0.254
Ahmed al Ghamdi	M7	0.014	0.581	0.278	0.195
Hamza al Ghamdi	M8	0.116	0.621	0.389	0.157
Marwan al Shehhi	M9	0.109	0.692	0.556	0.361
Mohand al Shehri	M10	0.005	0.462	0.111	0.057
Hani Hanjour	M11	0.080	0.643	0.500	0.303
Nawaf al Hazmi	M12	0.119	0.621	0.444	0.209
Salem al Hazmi	M13	0.064	0.621	0.444	0.259
Khalid al Mihdhar	M14	0.000	0.474	0.222	0.123
Majed Moqed	M15	0.000	0.474	0.222	0.123
Saeed al Ghamdi	M16	0.021	0.563	0.278	0.126
Ahmad al Haznawi	M17	0.012	0.529	0.222	0.120
Ziad Jarrah	M18	0.037	0.563	0.333	0.225
Ahmed al Nami	M19	0.000	0.462	0.167	0.068

TABLE I. RESULTS OF 4-CENTRALITY MEASURES OF M-19 NETWORK

2) Figure 1 presents the results of the simulation experiments, showing how different counter-terrorism strategies influence the long-term dynamics of terrorist attacks within the agent-based model. The figure plots the number of attacks over time under several intervention scenarios, such as leadership targeting, recruitment disruption, and resource constraints, and compares them against a baseline where no intervention is applied. The visual trend illustrates that leadership targeting alone produces only a temporary decline in attacks, as organizations are able to replace leaders and adapt relatively quickly. In contrast, recruitment disruption yields a more sustained reduction, since limiting the inflow of new members gradually weakens the network's size and capacity. Resource constraint strategies also prove effective, as reducing financial and logistical support directly lowers operational capability and the ability to conduct coordinated strikes. The figure highlights the nonlinear and adaptive nature of terrorist organizations, as the effectiveness of interventions varies not only in magnitude but also in duration, with some strategies producing delayed but compounding effects. Overall, Figure 7 demonstrates that while single strategies may have limited or temporary impacts, a combination of approaches—especially those targeting recruitment and resources—provides the most significant long-term disruption to terrorist activity.

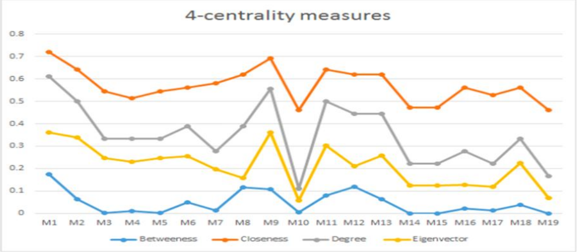


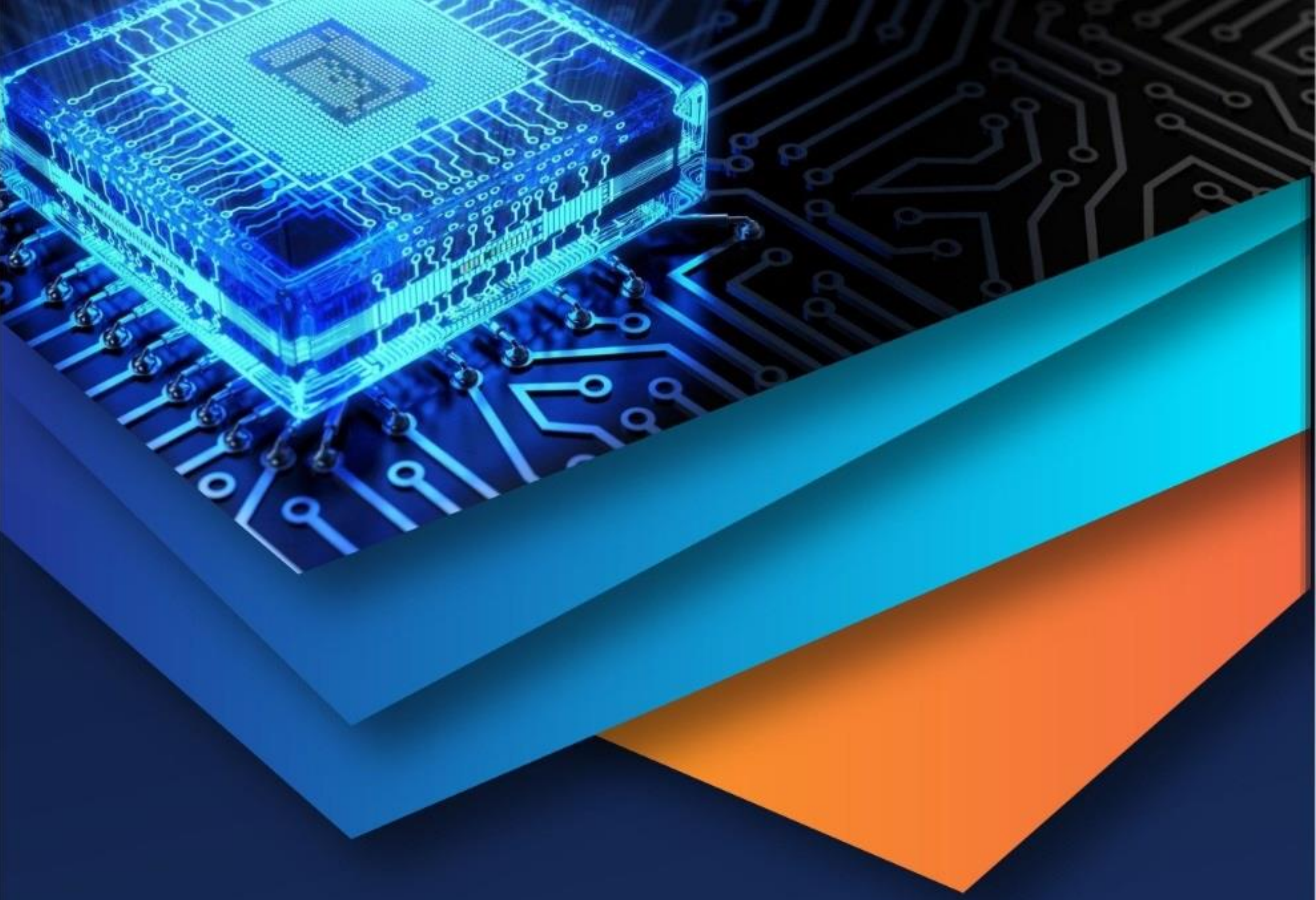
Fig. 1. Example of a figure caption. (*figure caption*)

V. CONCLUSION

The study shows that agent-based modeling (ABM) provides a flexible and dynamic framework for understanding the adaptive nature of terrorist organizations by simulating terrorists, leaders, recruiters, and counter-terrorism agents as autonomous actors operating in a changing environment. By running scenario-based experiments, the model reveals that interventions focused on recruitment disruption and resource constraints generate more sustained long-term impacts than leadership decapitation alone, which often produces only temporary effects. While ABM is not intended as a predictive tool, it serves as an exploratory laboratory that helps uncover possible futures, nonlinear responses, and unintended consequences of counter-terrorism strategies. Despite challenges such as limited data, sensitivity to assumptions, and validation difficulties, the approach remains valuable when integrated with statistical models, network analysis, and expert insights, offering policymakers a richer and more adaptive toolkit for anticipating and countering terrorism in a complex and evolving landscape.

REFERENCES

[1] G. Eason, B. Noble, and I. N. Sneddon, “On certain integrals of Lipschitz-Hankel type involving products of Bessel functions,” Phil. Trans. Roy. Soc. London, vol. A247, pp. 529–551, April 1955. *(references)*
[2] J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.
[3] I. S. Jacobs and C. P. Bean, “Fine particles, thin films and exchange anisotropy,” in Magnetism, vol. III, G. T. Rado and H. Suhl, Eds. New York: Academic, 1963, pp. 271–350.
[4] K. Elissa, “Title of paper if known,” unpublished.
[5] R. Nicole, “Title of paper with only first word capitalized,” J. Name Stand. Abbrev., in press.
[6] Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, “Electron spectroscopy studies on magneto-optical media and plastic substrate interface,” IEEE Transl. J. Magn. Japan, vol. 2, pp. 740–741, August 1987 [Digests 9th Annual Conf. Magnetics Japan, p. 301, 1982].
[7] M. Young, The Technical Writer’s Handbook. Mill Valley, CA: University Science, 1989.



10.22214/IJRASET

INDEX COPERNICUS

45.98

IMPACT FACTOR:
7.129

TOGETHER WE REACH THE GOAL

IMPACT FACTOR:
7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY