MAPPING THE TERROR: A SOCIAL NETWORK ANALYSIS OF AL-QAEDA AND ITS AFFILIATES' OPERATIONS

Sarthak Sahu[a], **Shivani Singh**[b] **and Payal**[c]

[1]*Department of Applied Mathematics*
[1]*DELHI TECHNOLOGICAL UNIVERSITY*

Abstract—This paper presents an in-depth Social Network Analysis (SNA) of Al-Qaeda and its affiliates' terrorist activities spanning from 2000 to 2020, offering new insights into the structural, temporal, and geospatial dimensions of transnational terrorism. Drawing on data collated from reputable sources—including RAND reports, the Global Terrorism Database (GTD), National Counterterrorism Center (NCTC) reports, and United Nations publications—the study constructs a comprehensive network capturing the multifaceted relationships among terrorist perpetrator groups, influential leaders, and targeted countries. Initially, an overall network is constructed using edge lists derived from both group-to-leader and group-to-country interactions. This network is then analyzed using various centrality measures—degree, betweenness, closeness, and eigenvector centrality—to identify key nodes that serve as hubs and bridges within the network. By filtering the top 10Additionally, a bipartite network is developed that explicitly links perpetrator groups with the countries where terrorist incidents have occurred. Projections of this bipartite graph into single-mode networks uncover clusters of countries sharing similar terrorist threats and highlight overlapping operational domains among different groups. Temporal analysis is incorporated by segmenting the dataset into defined intervals, thereby illuminating the dynamic evolution of the network. This approach uncovers shifting centralities and the emergence or dissolution of sub-networks, reflecting the adaptive strategies employed by terrorist organizations in response to counterterrorism interventions and broader geopolitical shifts. Furthermore, this paper employs link prediction techniques, notably the Adamic/Adar index, to forecast potential future connections within the network. This predictive component is critical for anticipating emerging alliances and operational collaborations that may not yet be evident. Despite the absence of precise geographic coordinates, geospatial analysis is conducted at the country level by aggregating incident counts and mapping them onto global boundaries, which highlights regional hotspots and strategic operational zones. Collectively, the methodologies and findings of this study contribute to a deeper academic understanding of decentralized terrorist networks while providing practical recommendations for intelligence and counterterrorism agencies. The research underscores the resilience and adaptability of Al-Qaeda's network and emphasizes the necessity of integrated, network-based strategies to effectively disrupt its operations.

Keywords—*Social Network Analysis, Al-Qaeda, Terrorism, Link Prediction, Centrality Measures, Bipartite Network*

1. Introduction

Terrorism has been a persistent global threat, impacting national stability, economic growth, social cohesion, and international relations. Over the past few decades, terrorism has evolved from localized insurgencies to transnational networks, exploiting digital platforms, financial systems, and geopolitical conflicts to expand their reach. The consequences of terrorism include loss of life, economic downturns, and the destabilization of entire regions. Traditional counterterrorism strategies have struggled to address the complexity of networked terrorist organizations. Social Network Analysis (SNA) provides a systematic approach to understanding these networks by identifying key actors, hidden structures, and vulnerabilities.

Al-Qaeda, founded in 1988 by Osama bin Laden, initially emerged as an anti-Soviet resistance movement in Afghanistan and evolved into a global jihadist network responsible for major attacks, including the September 11, 2001 attacks in the United States. Over time, Al-Qaeda has established regional affiliates, including Al-Qaeda in the Arabian Peninsula (AQAP), Al-Qaeda in the Islamic Maghreb (AQIM), Al-Shabaab, Jama'at Nusrat al-Islam wal-Muslimin (JNIM), and Al-Qaeda in the Indian Subcontinent (AQIS). These affiliates collaborate strategically by sharing resources, training, and operational knowledge, making them highly adaptive and resilient against counterterrorism measures.

Terrorist organizations like Al-Qaeda operate through decentralized, networked structures rather than hierarchical command chains, which increases their adaptability. However, limited research has been conducted on the structural evolution of these networks over time from an SNA perspective. Existing studies focus primarily on individual attacks or ideological narratives rather than the dynamic relationships between different actors, regions, and operational tactics. This study aims to fill this gap by applying SNA techniques to analyze the structure, temporal evolution, and spatial dynamics of Al-Qaeda's network from 2000 to 2020.

The key research questions focus on understanding the structural characteristics of Al-Qaeda's network, identifying the most influential actors, studying the evolution of terrorist alliances, predicting future connections using link prediction, and analyzing geospatial patterns influencing Al-Qaeda's operations. The main objectives include constructing a comprehensive dataset of Al-Qaeda-related attacks, analyzing network structure using SNA, studying network evolution, applying link prediction, conducting geospatial analysis, and providing actionable insights for counterterrorism efforts.

The study's significance lies in both theoretical and practical contributions. Theoretically, it enhances the application of SNA in terrorism studies by integrating structural, temporal, and geospatial dimensions. Practically, it helps intelligence agencies and policymakers identify critical nodes and potential threats, offers data-driven insights to disrupt networks, and supports predictive policing through network-based threat assessments.

The study focuses on Al-Qaeda and its affiliates from 2000 to 2020, using data from RAND reports, GTD, NCTC, and UN reports. It examines terrorist networks, affiliations, and organizational changes over time using SNA, link prediction, and geospatial mapping. However, limitations include potential gaps in open-source data, hidden networks not being publicly documented, and the influence of complex geopolitical factors that are difficult to quantify.

2. Background

Terrorism is broadly defined as the use of violence and intimidation, particularly against civilians, to achieve political, religious, or ideological goals. Various definitions provided by institutions like the United Nations (UN), the Federal Bureau of Investigation (FBI), and the Global Terrorism Database (GTD) differ slightly, which influences how terrorism is studied and countered. Counter-terrorism strategies are generally classified into four major categories.

First, **Military and Law Enforcement Responses** involve direct operations aimed at eliminating terrorist groups and dismantling their infrastructure.

Second, **Legislative Measures** include anti-terror laws, increased surveillance, and intelligence-sharing to prevent terrorist activities.

Third, **De-radicalization Programs** focus on rehabilitating extremists and preventing recruitment by addressing ideological and psychological factors.

Lastly, **Cyber and Financial Countermeasures** target online propaganda and disrupt financial networks that support terrorist operations.

Studies have shown that terrorist networks, particularly Al-Qaeda, have adapted to counter-terrorism measures by shifting from a centralized command structure to a decentralized network of affiliates. This structural evolution allows terrorist organizations to maintain operational flexibility and resilience despite leadership losses and increased surveillance.

Social Network Analysis (SNA) has become a key tool for understanding terrorist networks by examining how groups and individuals are connected and how information flows within these networks. Krebs (2002) analyzed the 9/11 hijackers' network, revealing a core-periphery structure where a few key figures controlled operations. Carley et al. (2003) used dynamic networks to study how terrorist cells communicate and coordinate attacks, showing that these groups adapt their communication strategies to avoid detection. Everton (2012) explored jihadist networks and demonstrated how fragmented groups can sustain their operations through decentralized communication.

Key SNA metrics used in terrorism research include Degree Centrality, which identifies individuals with the most direct connections; Betweenness Centrality, which reveals nodes that act as intermediaries controlling information flow; Clustering Coefficient, which measures the cohesion of subgroups within the network; and Community Detection, which helps identify clusters within terrorist networks, useful for targeting key operational cells. These metrics provide insight into how terrorist networks are structured and how they adapt to external pressures.

Al-Qaeda operates as a transnational network with regional affiliates that adapt to local geopolitical conditions. **Gunaratna (2002)** examined Al-Qaeda's financial and organizational structure, revealing how the group secures funding through donations, illicit trade, and state sponsorship. **Hoffman (2006)** explored the ideological and strategic shifts within Al-Qaeda, showing how leadership changes influenced operational priorities. **Mendelsohn (2016)** studied affiliation patterns within Al-Qaeda, demonstrating how the group forms and dissolves alliances based on geopolitical factors. While regional affiliates maintain varying degrees of operational autonomy, they generally adhere to Al-Qaeda's broader ideological framework. External factors such as post-9/11 counter-terrorism efforts, leadership changes (e.g., the death of Osama bin Laden), and technological advancements (e.g., encrypted communication and social media) have significantly influenced Al-Qaeda's evolution.

Terrorist networks are not static but evolve over time in response to external pressures. Longitudinal studies using SNA have identified patterns in terrorist recruitment, attack frequency, and network resilience. State crackdowns, such as intensified military operations following major terrorist attacks, often lead terrorist organizations to decentralize and adopt more flexible operational structures. Leadership changes, including the death or capture of key figures, can disrupt the hierarchy of terrorist networks and force operational adjustments. Technological advancements, such as encrypted communication and the use of social media, have transformed how terrorist groups coordinate attacks and recruit new members. These temporal dynamics highlight the need for adaptive counter-terrorism strategies that respond to the changing nature of terrorist threats.

Geospatial analysis has emerged as a valuable tool for understanding the spatial patterns of terrorist activity. Studies have used Geographic Information Systems (GIS) and spatial econometrics to identify attack hotspots and track terrorist mobility between conflict zones. For example, Al-Qaeda's ability to operate across borders highlights the importance of studying international networks of financing and logistics. Geospatial analysis helps identify high-risk regions and cross-border terrorist activity, enabling more targeted counter-terrorism efforts. Tracking how fighters move between conflict zones and how terrorist groups secure funding and logistical support across borders provides insight into the operational strategies of transnational terrorist networks.

Link prediction has been applied in criminology to anticipate future collaborations between criminal or terrorist entities. Techniques such as the Adamic/Adar Index measure the likelihood of a connection forming based on shared links within a network. The Jaccard Coefficient calculates the similarity between nodes, indicating the potential for future connections. Preferential Attachment assesses whether well-connected nodes are more likely to form new links, reflecting the tendency of influential figures within a network to attract new connections. Although link prediction has been widely used in criminal network analysis, its application to terrorist networks remains limited. This presents an opportunity to enhance counter-terrorism strategies by using predictive analytics to anticipate and prevent future terrorist alliances.

Despite significant advancements in understanding terrorist networks, existing research has notable limitations. Few studies have comprehensively analyzed Al-Qaeda's network evolution over a sustained period, such as from 2000 to 2020. Most research relies on static network models, which fail to capture the dynamic and adaptive nature of terrorist networks. There is also limited use of predictive techniques, such as link prediction, to anticipate future alliances and operational strategies. Furthermore, interdisciplinary approaches combining SNA, geospatial analysis, and predictive modeling remain underexplored. This study addresses these gaps by applying a comprehensive SNA framework to analyze Al-Qaeda and its affiliates, incorporating structural, temporal, and geospatial dimensions to provide a more holistic understanding of terrorist networks.

3. Theoretical Framework

Social Network Theory (SNT) examines relationships between entities (nodes) and their interactions (edges). It provides insights into how terrorist groups are connected, how power is distributed within the network, and how intelligence and resources are transferred between actors. In the context of terrorism, SNT helps identify key actors (central nodes), how terrorist cells are clustered into operational units, and how coordinated attacks are executed across different regions. It also helps analyze how network disruptions, such as the arrest of a leader, impact the overall functionality of the group. Degree centrality, betweenness centrality, and community detection are key metrics used to identify influential leaders, operational hubs, and vulnerable subgroups. For instance, analyzing Al-Qaeda's network structure reveals that the group has shifted from a centralized structure to a decentralized one, which enhances its resilience against counter-terrorism measures.

The **Organizational Theory of Terrorism** views terrorist organizations as adaptive systems that adjust their structures and strategies in response to external pressures. Early Al-Qaeda followed a **Hierarchical Model** with centralized leadership and a clear command structure. However, modern jihadist networks increasingly follow a **Networked Model** of loosely connected autonomous cells. A **Hybrid Model** combines elements of both, where central leadership provides ideological guidance while regional affiliates execute operations independently. Terrorist organizations enhance resilience by decentralizing leadership, using encrypted communication to evade surveillance, and forming cross-border alliances to secure funding and logistical support. For example, after the death of Osama bin Laden, Al-Qaeda adapted by shifting control to regional affiliates, ensuring operational continuity despite leadership losses.

The **Diffusion of Innovation Theory** (Rogers, 1962) explains how new ideas, behaviors, and technologies spread within a network. Applied to terrorism, it helps analyze how attack strategies, recruitment techniques, and operational models are adopted by different terrorist groups. The diffusion process occurs in four stages: Innovation Introduction involves the first use of a new tactic (e.g., suicide bombings or vehicle-borne IEDs) by a pioneering group. In the Early Adoption phase, close affiliates experiment with the tactic. During the Expansion phase, the tactic spreads through training camps, propaganda, and online forums. Finally, in the Institutionalization phase, the tactic becomes a standard operational practice within the network. Historical patterns show how Al-Qaeda's strategies, such as suicide bombings, were adopted by affiliates like Al-Shabaab, AQIM, and JNIM through this diffusion process. This model helps explain the rapid spread of new attack methods and the adaptive capacity of terrorist organizations.

The **Conceptual Framework** for this study integrates Social Network Theory, Organizational Theory, and Diffusion of Innovation to construct a multidimensional approach for analyzing Al-Qaeda and its affiliates. Structural analysis involves identifying core leaders, influential cells, and examining the density and connectivity of the network. Temporal evolution focuses on mapping changes in the network from 2000 to 2020 and understanding how counter-terrorism measures have affected the group's operational strategies. Bipartite and geospatial dimensions link perpetrator groups to their countries of operation, helping to identify geographical hotspots for terrorist activities. Predictive modeling uses link prediction algorithms to forecast future alliances and assess the likelihood of emerging terrorist factions. By combining these components, this framework enables a comprehensive analysis of Al-Qaeda's network structure, operational tactics, and future behavior.

4. Approach

4.1. Data Collection and Processing

The dataset for this study is compiled from multiple reliable sources, ensuring comprehensive coverage of terrorist activities and organizational structures. The primary data sources include the **RAND Database of Worldwide Terrorism Incidents (RAND)**, which provides detailed records of terrorist attacks; the **Global Terrorism Database (GTD)**, which contains incident-level data on terrorist activities; **National Counterterrorism Center (NCTC)** Reports, which offer information on terrorist organizations and their affiliations; and **United Nations Security Council (UNSC)** Reports, which provide insights into transnational terrorist financing and movement. These datasets are cross-referenced to enhance accuracy and address missing information, ensuring a more complete and consistent dataset.

To ensure consistency and usability for analysis, several data preprocessing steps were applied. First, in the data cleaning phase, event dates and locations were standardized to resolve inconsistencies. Entity name variations, such as "Al-Qaeda in the Arabian Peninsula" versus "AQAP," were aligned to prevent duplication. Duplicate records were removed using fuzzy matching techniques to eliminate redundancy. Next, the data was structured for Social Network Analysis (SNA) by transforming it into a graph-compatible format. In this structure, nodes represent terrorist groups, attack locations, and key individuals, while edges represent connections based on joint operations, alliances, and financial ties. This allows for effective analysis of network relationships and operational patterns.

Finally, missing data handling was addressed using interpolation techniques to estimate missing time series data. Cross-referencing with secondary sources further improved data completeness, ensuring the dataset is robust and suitable for network analysis. These preprocessing steps ensured that the final dataset was accurate, structured, and ready for comprehensive Social Network Analysis (SNA).

4.2. Network Metrics

Network metrics are essential for understanding the structural and functional properties of the Al-Qaeda terrorist network. They provide insights into how terrorist groups coordinate and influence each other within the network.

Network Density measures how interconnected the network is, defined as the ratio of actual edges to the maximum possible edges:

$$Density = \frac{2E}{N(N-1)}$$

where E is the number of edges and N is the number of nodes.

A low density suggests a decentralized network where most groups operate independently, while high density reflects frequent collaboration among terrorist factions. The observed density indicates a moderately connected network with localized clusters of high interaction, suggesting that while Al-Qaeda maintains a broad influence, its operational structure is somewhat fragmented.

Degree Distribution reflects how many direct connections each node has within the network. It is defined as:

$$Degree(v) = \sum_i A_{vi}$$

where A_{vi} is the adjacency matrix.

A power-law degree distribution is observed, where a few nodes (key terrorist hubs) have a very high number of connections, while most nodes have relatively few. Key hubs include Al-Qaeda (Core), Al-Qaeda in Iraq, AQAP, and AQIM, indicating their dominant role in coordinating operations and facilitating communication within the network.

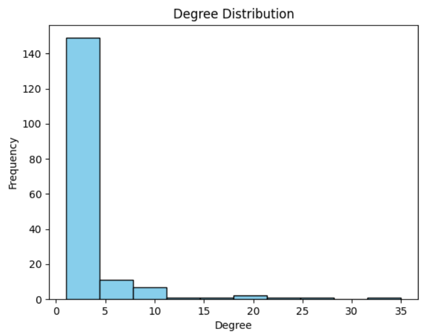


Figure 1. Degree Distribution

Centrality Measures identify the most influential nodes within the network:

- **Degree Centrality** highlights nodes with the most direct connections. It is defined as:

$$C_D(v) = \frac{deg(v)}{N-1}$$

  Al-Qaeda Core shows the highest degree centrality, reinforcing its central role in the network.
- **Betweenness Centrality** identifies nodes that serve as key intermediaries for information flow. It is calculated as:

$$C_B(v) = \sum_{s\neq v\neq t} \frac{\sigma_{st}(v)}{\sigma_{st}}$$

  where $\sigma_{st}(v)$ is the number of shortest paths passing through node v. AQAP and AQIM function as important brokers, controlling the flow of resources and intelligence across different factions.
- **Closeness Centrality** measures how quickly information can spread from a node. It is defined as:

$$C_C(v) = \frac{1}{\sum_u d(v,u)}$$

  Terrorist groups with high closeness centrality are well-positioned for rapid communication and mobilization.
- **Eigenvector Centrality** assigns importance based on connections to other highly connected nodes. It is given by:

$$C_E(v) \propto \sum_{u\in N(v)} C_E(u)$$

  Al-Qaeda Core and Al-Qaeda in Iraq dominate in this regard, reflecting their strategic significance.

The **Clustering Coefficient** measures the tendency of nodes to form tightly connected subgroups or triangles. It is defined as:

$$C(v) = \frac{2T(v)}{deg(v)(deg(v)-1)}$$

where $T(v)$ is the number of triangles through node v. A high clustering coefficient indicates that terrorist cells often collaborate within smaller operational units, enhancing cohesion and resilience. The analysis shows that localized terrorist cells are common within the Al-Qaeda network.

Connected Components identify isolated subgroups within the network. The largest connected component includes approximately 85% of the nodes, suggesting that Al-Qaeda maintains a broad operational reach despite regional differences. Smaller components represent autonomous or emerging factions that still align with Al-Qaeda's ideological framework. —

Top 4 Nodes by Centrality Measures

Degree Centrality:

1. Al-Qaeda – 0.1191
2. ISIS (Al-Qaeda roots) – 0.0978
3. ISIS (Al-Qaeda-inspired) – 0.0894
4. Al-Qaeda-inspired – 0.0766

Betweenness Centrality:

1. Al-Qaeda – 0.1896
2. ISIS (Al-Qaeda roots) – 0.1313
3. Al-Qaeda-inspired – 0.1211
4. United States – 0.1119

Closeness Centrality:

1. Al-Qaeda – 0.3331
2. France – 0.1344

Eigenvector Centrality:

1. ISIS (Al-Qaeda-inspired) - 0.29242258461884746
2. Al-Qaeda - 0.2903418750739722
3. United Kingdom - 0.18537580807471146

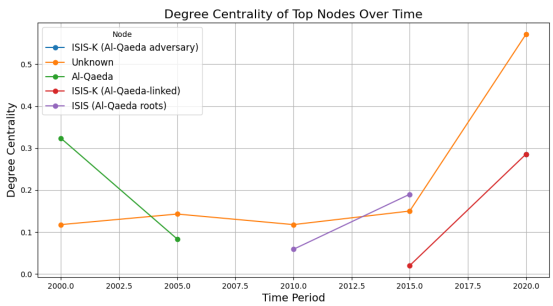


Figure 2. Degree centrality

4.3. Network Creation and Visualization

To analyze the structural properties of **Al-Qaeda** and its affiliates, a graph representation was created where:

- **Nodes** represent terrorist organizations, key individuals, and attack locations.
- **Edges** represent connections such as joint attacks, financial ties, or ideological affiliations.

The network is visualized using Gephi and Python's NetworkX.
Steps in Network Construction:

1. **Data Extraction:** Events from GTD, RAND, NCTC, and UN reports were filtered for Al-Qaeda-related incidents between 2000–2020.
2. **Graph Representation:**
   - **Unipartite Graph:** Terrorist groups were represented as nodes, with edges representing known interactions.
   - **Bipartite Graph:** Groups were connected to the countries where attacks occurred.
3. **Visualization Techniques:**
   - Force-directed layouts (Fruchterman-Reingold, Kamada-Kawai) were used for clarity.
   - **Color coding:**
     - **Purple nodes** → Al-Qaeda and core affiliates.
     - **Blue nodes** → Leaders.
     - **Yellow nodes** → Geographic locations.
   - **Edge thickness** indicates the strength of relationships.

4.3.1. Figures

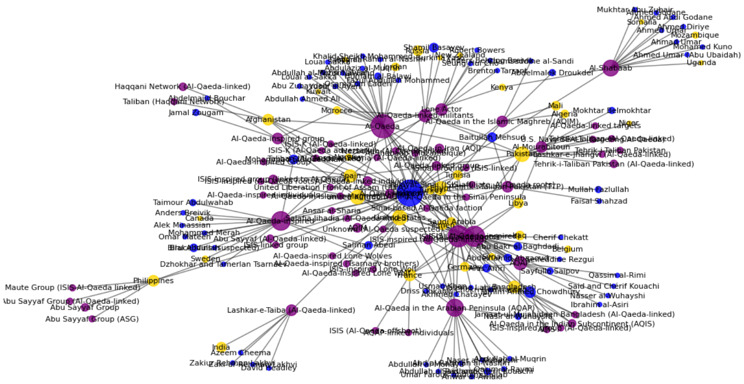


Figure 3. Filtered Terrorism Network

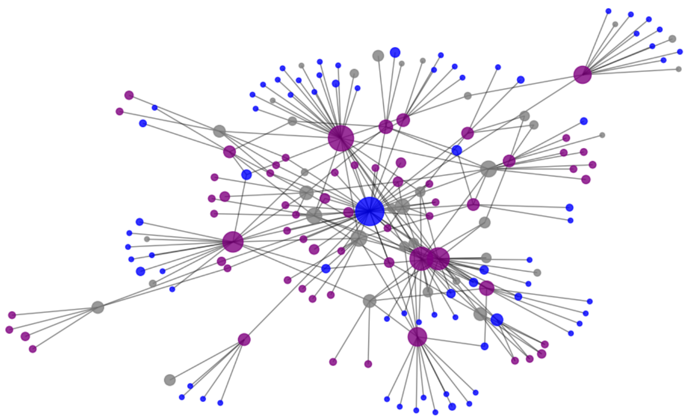
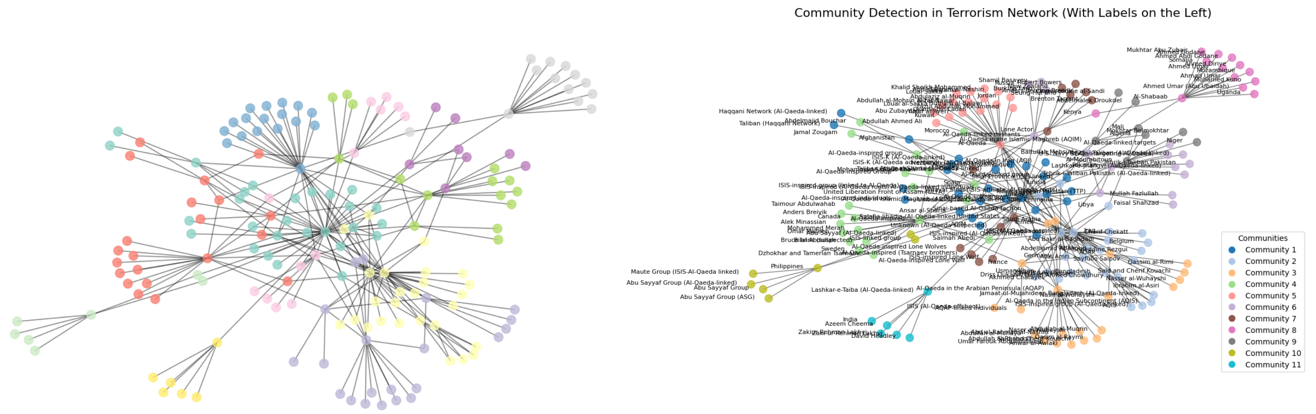


Figure 4. Filtered Terrorism Network [without labels]

4.4. Community Detection

Community detection plays a crucial role in understanding the structural organization of terrorist networks. It helps reveal clusters of interconnected groups, highlighting operational alliances and strategic collaborations. In this analysis, the Louvain method was employed to detect clusters within the Al-Qaeda-affiliated terrorist network. The Louvain method is widely used in network analysis due to its efficiency in identifying communities based on modularity optimization. By maximizing the modularity score, the algorithm partitions the network into clusters where the density of edges within clusters is higher than between clusters.

The analysis identified few major clusters of terrorist groups and their corresponding operational regions:



(a) without labels   **(b)** with labels

Figure 5. Community Detection

- **Al-Qaeda (Core) and Middle East Networks:** This cluster includes Al-Qaeda's central leadership and affiliated groups operating primarily in the Middle East. It reflects the core operational strength and strategic leadership of Al-Qaeda.
- **AQIM (Al-Qaeda in the Islamic Maghreb) and North African Networks:** This cluster highlights the operational reach of AQIM in North Africa, indicating coordinated activities and shared resources among groups in the region.
- **AQAP (Al-Qaeda in the Arabian Peninsula) and Arabian Peninsula Networks:** This cluster includes AQAP and its affiliated groups operating in the Arabian Peninsula, showing patterns of collaboration and strategic alignment among groups in this region.

Community detection using the Louvain method provides insights into the hierarchical and regional structure of terrorist networks. Identifying these clusters allows for targeted counterterrorism strategies by focusing on high-risk clusters and their operational dependencies. The modular structure revealed by the Louvain method reflects the strategic alliances and decentralized nature of Al-Qaeda's operational model.

4.5. Temporal Analysis

Temporal analysis is essential for understanding the evolving nature of terrorist networks and explore the dynamic structure of Al-Qaeda and its affiliates from 2000 to 2020, focusing on how key network metrics change annually and how nodes (terrorist groups, leaders, and countries) gain or lose influence over time. Terrorist networks are not static; they adapt in response to counterterrorism measures, leadership changes, and geopolitical events. By analyzing these temporal changes, the study provides insights into the resilience, adaptability, and long-term operational trends of terrorist organizations.

Temporal Community Structure

Community structure also evolves over time. Temporal community detection methods, such as the Louvain or Girvan-Newman algorithms, reveal the formation of new clusters, dissolution of existing clusters, and shifts in alliances. While detailed community evolution analysis was not implemented here, it remains a critical area for future study.

4.5.1. Interpretation of Temporal Dynamics

The temporal analysis offers several key insights:

- **Network Resilience:** The network's ability to reconfigure after the removal of key nodes highlights its resilience.
- **Shifting Centers of Influence:** Shifts in degree centrality reveal emerging power centers within the network.
- **Correlation with External Events:** Variations in network metrics often correlate with major geopolitical events, demonstrating that terrorist networks are highly reactive to external pressures.
- **Forecasting Future Trends:** Understanding historical trends helps to forecast future alliances and link predictions, which is vital for developing proactive counterterrorism strategies.

4.5.2. Figures

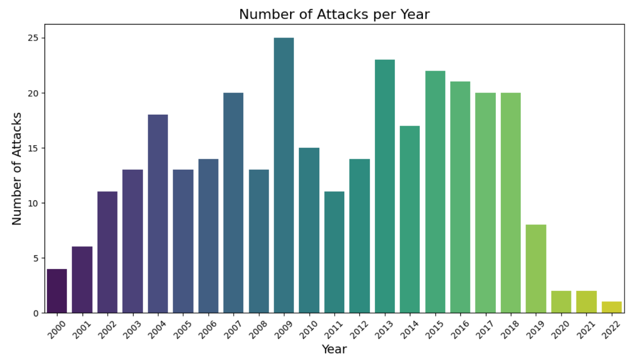


Figure 6. Temporal Ananlysis

4.6. Geospatial Analysis

Geospatial analysis provides a critical perspective on understanding terrorist activities by situating them within a geographic context. By mapping the frequency of terrorist attacks and overlaying network insights onto a world map, this analysis uncovers geographic patterns and highlights regional hotspots of activity. This geospatial perspective enhances the understanding of transnational terrorism and helps in identifying strategic vulnerabilities.

4.6.1. Mapping Terrorist Activities by Country

Mapping terrorist incidents at the country level allows for a clear visualization of the distribution of terrorist activities across different nations. This helps in identifying countries with high frequencies of terrorist incidents, which may indicate strategic importance or heightened vulnerability. The dataset includes a "Country" column (sourced from the RAND report, GTD, National Counterterrorism Center (NCTC), and UN reports), which specifies the location of each terrorist incident.

To create a country-level map, the following steps are performed:

1. **Data Aggregation:** The data is aggregated by country, counting the total number of terrorist incidents for each nation.
2. **Geographic Merging:** The aggregated data is merged with a global shapefile (such as GeoPandas' `naturalearth_lowres` dataset) to associate each country with its geographic boundaries.
3. **Visualization:** A choropleth map is generated to display the frequency of terrorist incidents by country, using color intensity to represent variations in incident counts.

4.6.2. Hotspot Analysis Using Country-Level Data

Hotspot analysis focuses on identifying countries and regions with concentrated terrorist activities. This involves:

- **Incident Aggregation:** The total number of terrorist attacks is computed for each country.
- **Density Visualization:** A choropleth map is used to visualize density, where darker or more intense colors indicate higher incident frequencies.
- **Interpretation:**
  - **High-Incident Countries:** Countries with high counts (depicted in deeper red) likely serve as operational hubs or strategic targets for terrorist activities. (Pakistan, Somaliya, UK)
  - **Regional Patterns:** Clusters of neighboring countries with similar incident levels may point to shared geopolitical or logistical factors facilitating terrorism.
  - **Outliers:** Countries with unexpectedly low incident counts might either be less targeted or underreported, suggesting the need for further investigation.

4.6.3. Interpretation of Spatial Patterns

Regional Hotspots: Certain regions, such as the Middle East, North Africa, and South Asia, exhibit higher frequencies of terrorist activities. **Geopolitical Implications:** Countries with high incident counts may require targeted counterterrorism strategies. **Correlation with Network Metrics:** When combined with network metrics, geospatial patterns provide a multidimensional view of terrorist operations.

4.6.4. Figures

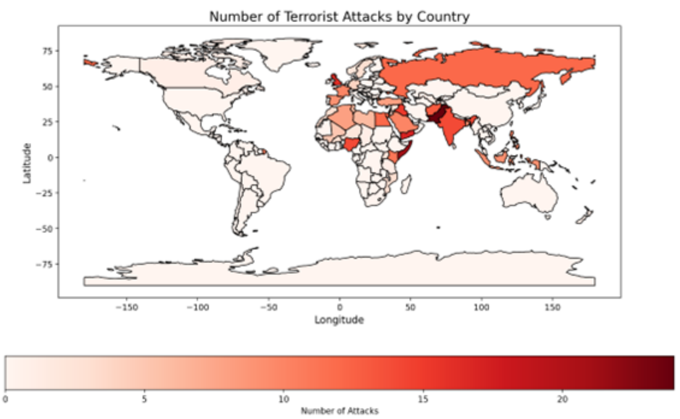


Figure 7. Geospatial Ananlysis

4.7. Bipartite Graph Analysis

A bipartite graph is constructed, focusing on the relationships between terrorist perpetrator groups and the countries they target, to represent these two distinct types of entities, followed by projections onto single-mode networks to analyze cross-border terrorist dynamics and operational patterns.

Construction of the Bipartite Graph

The bipartite graph consists of two node types:

Perpetrator Groups: Terrorist organizations and affiliates.

Countries: Locations where terrorist attacks have been carried out.

The data was cleaned to remove duplicates and missing values. Each record defines an edge between a perpetrator group and a country, creating an undirected bipartite graph using NetworkX in Python. Perpetrator groups were assigned a bipartite attribute value of 0, while countries were assigned a value of 1.

Visualization of Perpetrator Groups and Countries

Perpetrator groups – Pink

Countries – Cyan

This visualization highlights the overall network structure and operational overlaps between groups and nations.

4.7.1. Figures

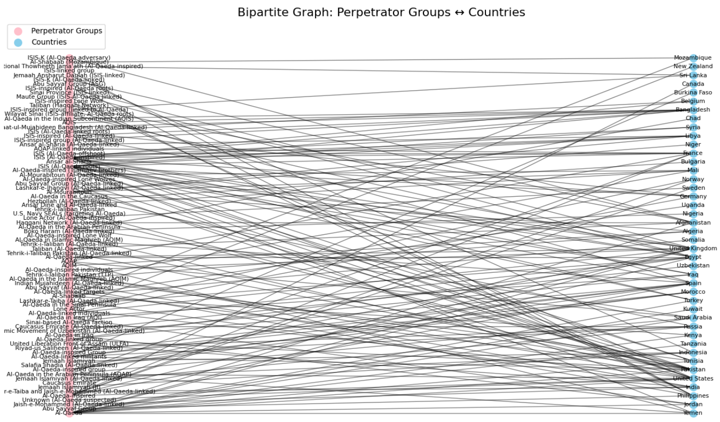


Figure 8. Bipartite Graph

4.8. Link Prediction in Terrorist Networks

Link prediction is a crucial aspect of SNA that aims to forecast the emergence of new connections based on the existing network structure, identifying terrorist groups or countries that may form new operational ties in the future, enhance counterterrorism strategies by highlighting emerging connections that could pose vulnerabilities, and complement other analyses such as static, temporal, and geospatial approaches to build a holistic understanding of the network's dynamics.

In the context of terrorist networks, particularly those associated with **Al-Qaeda** and its affiliates, predicting future links can assist intelligence agencies and policymakers in identifying potential alliances, emerging cells, or covert operational collaborations before they fully materialize.

Application of the Adamic/Adar Index

The **Adamic/Adar index** is a well-established link prediction metric that assigns higher scores to pairs of nodes sharing many common neighbors, giving more weight to rarer (more informative) neighbors. This makes it particularly useful for analyzing terrorist networks, as it identifies key nodes that act as bridges between disconnected sub-networks.

4.8.1. Projection of the Bipartite Graph:

The bipartite graph was visualized using a layout that clearly separates perpetrator groups from countries. Color coding was used to distinguish between the two node sets, and predicted links in red, making the interconnections between them more visible.

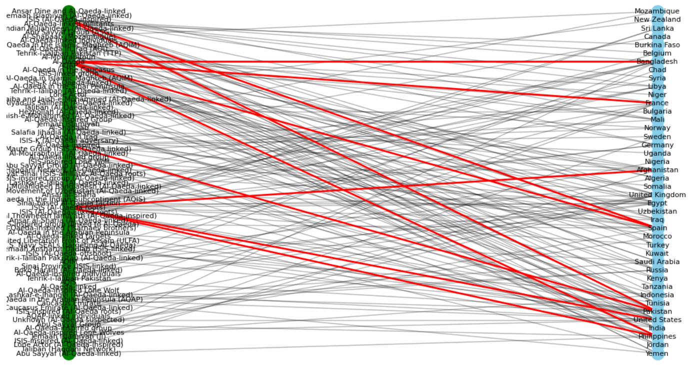


Figure 9. Predicted Links in Bipartite Graph

Interpretation of Bipartite Relationships:
The bipartite graph and its projections provide valuable insights into the structure of Al-Qaeda's network:
Inter-Nodal Relationships: Direct connections between perpetrator groups and countries highlight how terrorist operations spread across national boundaries.
Strategic Implications for Counter-Terrorism: Understanding these bipartite relationships aids policymakers in developing targeted strategies to disrupt terrorist operations.

4.8.2. Country Projection:

Nodes represent countries, and an edge is drawn if they have been targeted by the same terrorist group. The purpose of this projection is to identify clusters of countries that face similar threats and understand transnational operational links between countries.

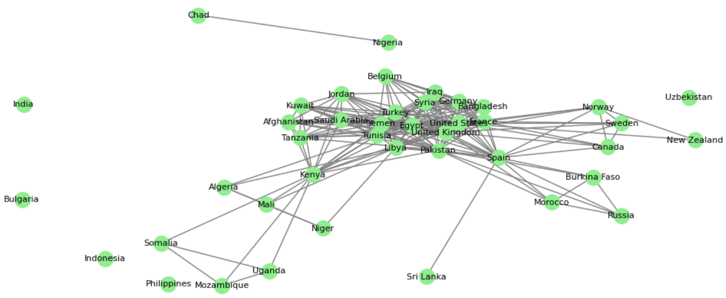


Figure 10. Country Projection

Country Projection Analysis:
The country projection graph reveals the degree of similarity between nations based on shared terrorist activities, i.e.,
high-risk countries - nations frequently targeted by the same perpetrator groups and
geographical or political clusters that exhibit common vulnerability patterns.

4.8.3. Perpetrator Group Projection:

Nodes represent terrorist groups, and edges indicate shared attack locations. The purpose of this projection is to highlight collaborations or similar operational footprints among terrorist groups and identify clusters that could indicate coordinated actions or shared resources.

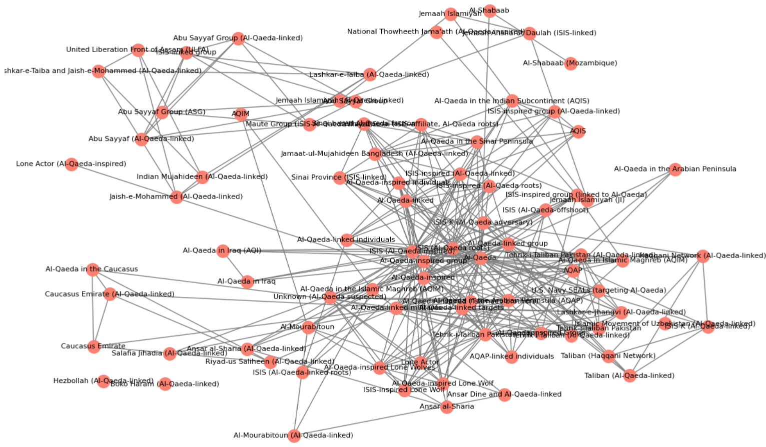


Figure 11. Perpetrator Group Projection

Perpetrator Group Projection Analysis:
This projection focuses on the relationships between different terrorist groups:
Collaborative Clusters: Groups with similar attack patterns may form operational alliances.
Influential Nodes: Groups with high centrality metrics are critical for the overall network connectivity.
Strategic Implications: Patterns of connectivity suggest potential for future collaboration or strategic convergence among groups.

4.8.4. Interpretation and Implications

Key Findings:

- **Emerging Alliances:** Highlights potential new connections.
- **Country Projection:** Identifies transnational terrorism patterns.
- **Perpetrator Group Projection:** Suggests potential operational alliances.

Strategic Implications for Counter-Terrorism:

- **Preventive Measures:** Enables proactive counterterrorism.
- **Resource Allocation:** Helps prioritize intelligence efforts.
- **Policy Formulation:** Supports international cooperation.

4.9. Shortest Path Analysis

The shortest path in a network determines the minimum number of steps required to traverse between two nodes. In the context of this study, the shortest path analysis was applied to the country projection network to investigate the structural relationships between terrorist activities in different nations.

For this analysis, we utilized NetworkX's `shortest_path()` function to compute the shortest path between nodes representing different countries. For instance, a key observation from our results was that the shortest path between **Pakistan** and **Afghanistan** played a crucial role in linking multiple terrorist networks. This suggests a high level of connectivity between groups operating in these two regions.

To visualize the shortest path, we plotted the entire network while highlighting the path in red to emphasize its significance.

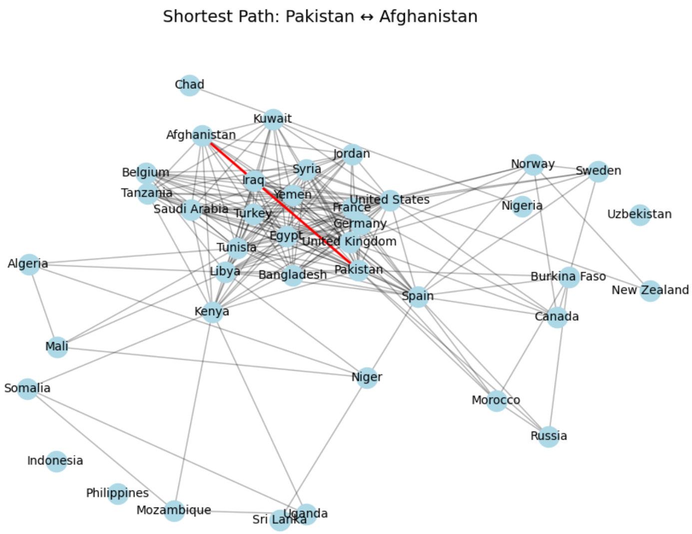


Figure 12. Shortest path between Pakistan and Afghanistan

The results from this analysis highlight the strategic importance of pathways between key countries in terrorism networks. By identifying these paths, we can gain insights into possible communication channels and operational dependencies between different terrorist organizations.

5. Conclusion

The study applied multiple analytical methods to analyze Al-Qaeda's terrorist network. The static network analysis revealed that the network exhibits a decentralized structure, with certain nodes such as the core Al-Qaeda organization, AQAP, and AQIM functioning as central hubs. These nodes consistently demonstrated high centrality measures (degree, betweenness, closeness, and eigenvector), underscoring their critical roles in maintaining operational connectivity. Bipartite graph analysis uncovered strong transnational relationships by linking perpetrator groups with countries where attacks occurred. Projections of the bipartite network highlighted clusters of countries facing similar threats and operational overlaps among terrorist groups. Temporal network analysis demonstrated that the network's structure evolved over time, with key nodes gaining or losing influence due to counterterrorism interventions or geopolitical events. The Adamic/Adar index was used for link prediction, identifying potential future alliances that could enhance the network's operational capacity. Geospatial analysis, despite relying on country-level data, identified high-incident regions such as the Middle East, South Asia, and parts of Africa. In-depth case studies reinforced these findings, highlighting vulnerabilities and operational patterns within the network.

The research successfully answered key questions about Al-Qaeda's network. The network is structured as a decentralized system with core groups like Al-Qaeda, AQAP, and AQIM acting as communication and operational hubs. Influential nodes were identified based on centrality measures, highlighting strategic regions like Pakistan, Afghanistan, and Yemen. Temporal analysis showed that alliances are highly dynamic, with leadership changes and counterterrorism operations causing rapid reconfigurations. Link prediction models demonstrated the potential for new operational ties among terrorist groups and countries. Geospatial analysis revealed that terrorist activities are concentrated in specific regions, reflecting strategic operational choices.

This research makes important contributions to the field. Methodologically, it integrates static, bipartite, temporal, link prediction, and geospatial analyses, enhancing the application of SNA in counterterrorism research. The findings validate existing theories about the adaptability and resilience of decentralized terrorist networks. The study provides practical intelligence by identifying key nodes, emerging alliances, and spatial patterns, offering insights for early-warning systems and targeted counterterrorism strategies.

Recommendations for future research include incorporating more granular geospatial data (e.g., latitude and longitude) and more accurate data about leaders or masterminds of the attacks for finer-scale spatial analysis and hotspot detection. Integrating additional link prediction models, including the Jaccard coefficient, Preferential Attachment, and machine learning approaches, could improve predictive accuracy. Developing real-time network models would enable dynamic monitoring of terrorist networks for more responsive counterterrorism measures. Cross-disciplinary approaches for future work could benefit from integrating insights from political science, sociology, and behavioral psychology to provide a more holistic understanding of terrorist motivations and network evolution.
By integrating predictive models and detailed case studies, this research offers valuable insights that can inform both academic inquiry and practical counterterrorism strategies.Ultimately, the multidimensional approach presented herein not only enhances our understanding of terrorist networks but also lays the groundwork for more proactive and effective security measures. As global terrorism continues to evolve, the methodologies and insights from this study will be essential for anticipating future threats and developing strategies to safeguard international security.

References

1. Krebs, V. E. (2002). *Mapping networks of terrorist cells.* Connections, 24(3).
2. Gunaratna, R. (2002). *Inside Al Qaeda: Global Network of Terror*. Columbia University Press.
3. Hoffman, B. (2006). *Inside Terrorism*. Columbia University Press.
4. Everton, S. (2012). *Network Analysis of Terrorist Organizations*. Journal of Strategic Studies, 35(5), 597–622.
5. Xu, J., & Chen, H. (2005). *Learning the Structure of Dynamic Social Networks.* IEEE Transactions on Knowledge and Data Engineering, 17(3), 346–360.
6. LaFree, G., & Dugan, L. (2009). *Introducing the Global Terrorism Database (GTD).* Perspectives on Terrorism, 3(6).
7. RAND Corporation. (Year). *RAND Database of Worldwide Terrorism Incidents.* [Dataset].
8. National Counterterrorism Center (NCTC). (Year). *NCTC Reports.* [Dataset].
9. United Nations. (Year). *UN Reports on Transnational Terrorism.* [Dataset].

Refer [1] for the GitHub link to the code used in this paper.

[1] https://github.com/mrsarthak41/Terrorism-Network-Analysis?tab=readme-ov-file#terrorism-network-analysis