

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

A THESIS SUBMITTED  
IN PARTIAL FULFILMENT OF THE REQUIREMENTS  
FOR THE DEGREE OF  
**MASTER OF SCIENCE**  
IN  
**APPLIED MATHEMATICS**

By  
**SHIVANI SINGH (23/MSCMAT/42)**  
**and SARTHAK SAHU (23/MSCMAT41)**  
Under the supervision of  
**Dr. Payal**

**Assistant Professor, Department of Applied Mathematics, DTU**



To The Department of Applied Mathematics  
**DELHI TECHNOLOGICAL UNIVERSITY**  
(Formerly Delhi College of Engineering)  
**Shahbad Daulatpur, Main Bawana Road, Delhi-110042, India**

**May, 2025**

## **ACKNOWLEDGEMENTS**

At the outset of this report, we extend our heartfelt appreciation to all individuals who have supported us in completing this dissertation. Without their proactive direction, assistance, collaboration, and support, we could not have advanced toward achieving the desired outcomes. **Dr. Payal** provided diligent assistance and support that enabled us to complete our dissertation, for which we are eternally grateful. We express our sincere appreciation to each other for working together to complete this project while preserving our individuality. We are thankful that **Delhi Technological University** provided this opportunity to us. We additionally express our sincere gratitude and respect to our parents as well as other family members, who have always provided us with both material and moral support. Finally, but just as importantly, we would like to express our heartfelt gratitude to all of our friends who supported us in any way during this effort.

This quick acknowledgement does not imply a lack of gratitude for anything.

Thanking You



## **DELHI TECHNOLOGICAL UNIVERSITY**

(Formerly Delhi College of Engineering)

Shahbad Daulatpur, Main Bawana Road, Delhi-110042

### **CANDIDATE'S DECLARATION**

We, Shivani Singh[23/MSCMAT/42] and Sarthak Sahu [23/MSCMAT/41] hereby certify that the work which is being presented in the thesis entitled "**Mapping the Terror: A Social Network Analysis of Al-Qaeda and Its Affiliates' Operations (2000-2024)**" in partial fulfilment of the requirement for the award of the Degree of Master of Science, submitted in the Department of Applied Mathematics, Delhi Technological University is an authentic record of our work carried out during the period from August 2024 to May 2025 under the supervision of Dr. Payal.

The matter presented in the thesis has not been submitted by me for the award of any other degree of this or any other Institute.

**Candidate's Signature**

This is to certify that the student has incorporated all the corrections suggested by the examiners in the thesis and the statement made by the candidate is correct to the best of our knowledge.

**Signature of Supervisor**

**Signature of External Examiner**



## DELHI TECHNOLOGICAL UNIVERSITY

(Formerly Delhi College of Engineering)

Shahbad Daulatpur, Main Bawana Road, Delhi-110042

### CERTIFICATE BY THE SUPERVISOR

Certified that Shivani Singh[23/MSCMAT/42] and Sarthak Sahu [23/MSCMAT/41] have carried out their search work presented in this thesis entitled "**Mapping the Terror: A Social Network Analysis of Al-Qaeda and Its Affiliates' Operations (2000-2024)**" for the award of Master of Science from Department of Applied Mathematics, Delhi Technological University, Delhi, under my supervision. The thesis embodies results of original work, and studies are carried out by students themselves, and the contents of the thesis do not form the basis for the award of any other degree to the candidates or anybody else from this or any other University/Institution.

Place: Delhi

Date: 26/05/2025

Dr. Payal

Assistant Professor

Department of Applied Mathematics

Delhi Technological University

## Abstract

This dissertation 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 10% of nodes based on degree centrality, the analysis reveals that core entities such as Al-Qaeda, AQAP, and AQIM consistently occupy central positions, facilitating communication, resource allocation, and operational coordination across diverse regions.

Additionally, 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, the dissertation 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.

## **Table of Contents**

<b>Acknowledgement .....</b>	<b>i</b>
<b>Candidate's Declaration .....</b>	<b>ii</b>
<b>Certificate by the Supervisor .....</b>	<b>iii</b>
<b>Abstract .....</b>	<b>iv</b>
<b>List of Figures and Tables .....</b>	<b>v</b>
<b>Chapter 1: Introduction .....</b>	<b>1</b>
1.1 Background .....	1
1.1.1 Overview of terrorism and its impact .....	1
1.1.2 Brief history of Al-Qaeda and its affiliates .....	1
1.2 Problem Statement .....	2
1.3 Research Questions .....	2
1.4 Objectives of the Study .....	2
1.5 Significance of the Study .....	3
1.6 Scope and Limitations .....	4
<b>Chapter 2: Literature Review .....</b>	<b>5</b>
2.1 Terrorism and Counter-Terrorism Studies .....	5
2.2 Social Network Analysis in Terrorism Research .....	5
2.3 Al-Qaeda and Its Affiliate Organizations .....	6
2.4 Temporal Dynamics of Terrorist Networks .....	6
2.5 Geospatial Aspects of Terrorism .....	7
2.6 Link Prediction in Criminal Networks .....	7
2.7 Gaps in the Literature .....	7
<b>Chapter 3: Theoretical Framework .....</b>	<b>9</b>
3.1 Social Network Theory .....	9
3.2 Organizational Theory of Terrorism .....	9
3.3 Diffusion of Innovation in Terrorist Networks .....	10
3.4 Conceptual Framework for the Study .....	11

<b>Chapter 4: Methodology .....</b>	<b>12</b>
4.1 Research Design .....	12
4.2 Data Collection .....	12
4.2.1 Data Sources .....	12
4.2.2 Data Preprocessing .....	13
4.3 Social Network Analysis Techniques .....	13
4.3.1 Static Network Analysis .....	13
4.3.2 Bipartite Graph Analysis .....	14
4.3.3 Temporal Network Analysis .....	14
4.3.4 Link Prediction .....	14
4.3.5 Geospatial Analysis .....	14
4.4 Tools and Software Used .....	14
4.5 Ethical Considerations .....	15
<b>Chapter 5: Static Network Analysis .....</b>	<b>16</b>
5.1 Network Creation and Visualization .....	16
5.2 Network Metrics .....	17
5.2.1 Network Density .....	17
5.2.2 Degree Distribution .....	17
5.2.3 Centrality Measures .....	19
– Degree Centrality	
– Betweenness Centrality	
– Closeness Centrality	
– Eigenvector Centrality	
5.2.4 Clustering Coefficient .....	20
5.2.5 Connected Components .....	21
5.2.6 Average Path Length .....	21
5.3 Community Detection .....	21
5.4 Interpretation of Results .....	22
<b>Chapter 6: Bipartite Graph Analysis .....</b>	<b>23</b>
6.1 Construction of Bipartite Graph .....	23
6.2 Visualization of Perpetrator Groups and Countries .....	23
6.3 Projection Techniques .....	24
6.3.1 Country Projection .....	24
6.3.2 Perpetrator Group Projection .....	24

6.4 Analysis of Projected Graphs .....	25
6.5 Interpretation of Bipartite Relationships .....	26
<b>Chapter 7: Temporal Analysis .....</b>	<b>28</b>
7.1 Evolution of Network Over Time (2000–2020) .....	28
7.2 Temporal Centrality Analysis .....	28
7.2.1 Changes in Degree Centrality .....	28
7.2.2 Emerging and Declining Influences .....	29
7.3 Temporal Community Structure .....	29
7.4 Trend Analysis of Network Metrics .....	29
7.5 Interpretation of Temporal Dynamics.....	30
<b>Chapter 8: Link Prediction in Terrorist Networks .....</b>	<b>32</b>
8.1 Methodology for Link Prediction .....	32
8.2 Application of Adamic/Adar Index .....	33
8.3 Interpretation and Implications.....	34
8.4 Conclusion .....	36
<b>Chapter 9: Geospatial Analysis of Terrorist Activities .....</b>	<b>44</b>
9.1 Mapping of Terrorist Activities .....	44
9.2 Hotspot Analysis .....	45
9.3 Spatial Autocorrelation of Attacks .....	46
9.4 Geospatial Network Visualization .....	46
9.5 Interpretation of Spatial Patterns .....	47
<b>Chapter 10: Case Studies .....</b>	<b>42</b>
10.1 Analysis of Key Nodes .....	42
– Top Perpetrator Groups	
– Influential Leaders	
– Critical Countries	
10.2 Evolution of Specific Sub-Networks.....	42
10.3 Cross-Border Operations Analysis .....	44
<b>Chapter 11: Discussion .....</b>	<b>46</b>
11.1 Synthesis of Findings .....	46
11.2 Theoretical Implications .....	47
11.3 Practical Implications for Counter-Terrorism .....	47

11.4 Methodological Contributions .....	48
11.5 Limitations of the Study .....	48
<b>Chapter 12: Conclusion .....</b>	<b>50</b>
12.1 Summary of Key Findings .....	50
12.2 Answers to Research Questions .....	51
12.3 Contributions to the Field .....	52
12.4 Recommendations for Future Research.....	52
12.5 Concluding Remarks .....	53
<hr/>	
<b>References .....</b>	<b>54</b>
<b>Appendices .....</b>	<b>55</b>
– Appendix I: Data Collection and Cleaning Procedures	
– Appendix II: Detailed Code for Network Analysis	

## LIST OF FIGURES

Figure 1	Filtered Terrorism Network (Top 10% by Degree Centrality)	
.....	.....	18
Figure 2	Degree Centrality of Top Nodes Over Time	
.....	.....	20
Figure 3	Community Detection in the Terrorism Network	
.....	.....	22
Figure 4	Bipartite Graph: Perpetrator Groups and Countries	
.....	.....	25
Figure 5	Temporal Analysis: Number of Attacks Per Year	
.....	.....	30
Figure 6	Country Projection Graph	
.....	.....	34
Figure 7	Perpetrator Group Projection Graph	
.....	.....	35
Figure 8	Geospatial Analysis: Number of Terrorist Attacks by Country	
.....	.....	39
Figure A.i	Appendix: Additional Network Visualizations	
.....	.....	A-i
Figure A.ii	Appendix: Sample NetworkX Code Output	
.....	.....	A-ii

# CHAPTER 1

## INTRODUCTION

### 1.1 Background

#### 1.1.1 Overview of Terrorism and Its Impact

Terrorism has been one of the most persistent security threats globally, affecting not only national stability but also economic growth, social cohesion, and international relations. Over the past few decades, the nature of terrorism has evolved, moving from localized insurgencies to transnational networks that leverage digital platforms, financial systems, and geopolitical conflicts to expand their influence. The consequences of terrorism range from loss of life and economic downturns to the destabilization of entire regions.

With the rise of networked terrorist organizations, traditional counter-terrorism strategies have faced significant challenges. Understanding how these groups function, their internal hierarchies, and the evolution of their alliances is crucial for both policymakers and law enforcement agencies. Social Network Analysis (SNA) offers a systematic approach to studying these connections, revealing key actors, hidden structures, and vulnerabilities within terrorist networks.

#### 1.1.2 Brief History of Al-Qaeda and Its Affiliates

Al-Qaeda, founded in 1988 by Osama bin Laden, emerged as a radical Islamist organization committed to jihad against perceived enemies of Islam, primarily Western nations and their allies. Initially formed as an anti-Soviet resistance movement in Afghanistan, it evolved into a global terror network responsible for orchestrating numerous high-profile attacks, including the September 11, 2001, attacks in the United States.

Over the years, Al-Qaeda has established or affiliated with multiple regional groups across Africa, the Middle East, and South Asia, including:

- **Al-Qaeda in the Arabian Peninsula (AQAP)** – Active in Yemen and Saudi Arabia.
- **Al-Qaeda in the Islamic Maghreb (AQIM)** – Operating in North and West Africa.
- **Al-Shabaab** – A militant group in Somalia aligned with Al-Qaeda.
- **Jama’at Nusrat al-Islam wal-Muslimin (JNIM)** – A Sahel-based affiliate.

- **Al-Qaeda in the Indian Subcontinent (AQIS)** – Extending its influence in South Asia.

These groups collaborate strategically, exchanging resources, training, and operational knowledge. Their networks are fluid, adapting to counterterrorism measures and shifting political landscapes, making them a key subject of network analysis.

## 1.2 Problem Statement

Terrorist organizations like Al-Qaeda operate through decentralized, networked structures rather than traditional hierarchical command chains. Understanding the network characteristics of such organizations can provide valuable insights into their functioning, resilience, and potential vulnerabilities. However, limited research has been conducted on the structural evolution of these networks over time, particularly from a Social Network Analysis (SNA) perspective.

Existing studies on Al-Qaeda often focus on individual attacks or ideological narratives rather than the evolving relationships between different actors, regions, and operational tactics. This study aims to bridge this gap by applying advanced SNA techniques to analyze the structure, temporal evolution, and spatial dynamics of Al-Qaeda and its affiliates from 2000 to 2020.

## 1.3 Research Questions

This study aims to answer the following key questions:

1. What are the structural characteristics of Al-Qaeda's network and its affiliates over time?
2. Who are the most influential actors (individuals/groups) in Al-Qaeda's network?
3. How do terrorist alliances and relationships evolve over time?
4. Can we predict future connections within the network using link prediction models?
5. How do geospatial patterns influence Al-Qaeda's operations across different regions?

## 1.4 Objectives of the Study

The main objectives of this research are:

1. To construct a comprehensive dataset of Al-Qaeda-related terrorist attacks from 2000 to 2020 using data from RAND reports, GTD, and UN reports.

2. To analyze the structural properties of Al-Qaeda's network using Social Network Analysis (SNA).
3. To study the evolution of the network over time and identify patterns of expansion or decline.
4. To apply link prediction techniques to identify potential future alliances or threats.
5. To conduct geospatial analysis of terrorist activities to understand regional hotspots and spatial relationships.
6. To provide insights for counterterrorism efforts by highlighting vulnerabilities within the network.

## **1.5 Significance of the Study**

Understanding the networked nature of terrorism has significant theoretical and practical implications:

### **Theoretical Contributions**

- Enhances the application of SNA in terrorism studies by integrating structural, temporal, and geospatial dimensions.
- Expands knowledge on how decentralized terrorist organizations adapt to counterterrorism measures.

### **Practical Contributions**

- Helps intelligence agencies and policymakers identify critical nodes and potential future threats.
- Provides law enforcement with data-driven insights to disrupt terrorist networks effectively.
- Offers recommendations for predictive policing using network-based threat assessments.

## **1.6 Scope and Limitations**

### **Scope**

This study focuses on Al-Qaeda and its affiliated organizations from 2000 to 2020. The scope includes:

- Analyzing structured data collected from **RAND reports, GTD, NCTC, and UN reports.**

- Examining **terrorist attack networks, affiliations, and organizational changes** over time.
- Using **SNA techniques, link prediction, and geospatial mapping** to uncover patterns.

### **Limitations**

- **Data Availability:** Open-source datasets may have missing or incomplete records.
  - **Hidden Networks:** Some terrorist links may not be publicly documented.
  - **Geopolitical Complexity:** External factors like political changes and military interventions impact networks but are difficult to quantify.
-

## CHAPTER 2

### LITERATURE REVIEW

This chapter reviews existing research on terrorism, Social Network Analysis (SNA), Al-Qaeda's organizational structure, and methodologies used to study terrorist networks. It identifies gaps in current knowledge and positions this study within the broader research context.

---

#### **2.1 Terrorism and Counter-Terrorism Studies**

##### **Defining Terrorism**

Terrorism is broadly defined as the use of violence and intimidation, especially against civilians, to achieve political, religious, or ideological objectives. Various definitions exist across academic, governmental, and international institutions, which can impact how terrorism is studied and countered. The **United Nations**, **Federal Bureau of Investigation (FBI)**, and **Global Terrorism Database (GTD)** each provide slightly different definitions, influencing research methodologies and policy responses.

##### **Counter-Terrorism Approaches**

Counter-terrorism strategies can be classified into:

1. **Military and Law Enforcement Responses** – Direct operations against terrorist groups.
2. **Legislative Measures** – Anti-terror laws, surveillance, and intelligence-sharing.
3. **De-radicalization Programs** – Efforts to rehabilitate extremists and prevent recruitment.
4. **Cyber and Financial Countermeasures** – Tracking online propaganda and disrupting funding.

##### **Terrorist Networks as Adaptive Systems**

Recent studies have explored how terrorist organizations **adapt** to counter-terrorism measures, evolving their structures and operational methods. Al-Qaeda, in particular, has demonstrated flexibility, shifting from centralized control to a **decentralized network of affiliates**.

#### **2.2 Social Network Analysis in Terrorism Research**

##### **The Relevance of Social Network Analysis (SNA)**

SNA is increasingly used in terrorism studies to examine how terrorist groups are structured and how individuals or organizations interact. Key studies include:

- Krebs (2002) – Analyzed the **9/11 hijackers' network**, revealing core-periphery structures.
- Carley et al. (2003) – Used **dynamic networks** to study terrorist communication patterns.
- Everton (2012) – Applied **SNA to jihadist networks**, showing how fragmented groups sustain their operations.

### **Network Metrics for Terrorism Research**

- **Degree Centrality** – Identifies key individuals with the most direct connections.
- **Betweenness Centrality** – Reveals nodes that act as intermediaries, controlling information flow.
- **Clustering Coefficient** – Measures subgroup cohesion within networks.
- **Community Detection** – Identifies clusters within terrorist organizations, useful for targeting key cells.

## **2.3 Al-Qaeda and Its Affiliate Organizations**

Al-Qaeda operates as a **transnational network** with affiliates adapting to regional conditions. Key studies include:

- **Gunaratna (2002)** – Explored Al-Qaeda's **organizational structure** and financial networks.
- **Hoffman (2006)** – Investigated **ideological and strategic evolution**.
- **Mendelsohn (2016)** – Analyzed **affiliation patterns**, showing how groups join and leave the network.

Each affiliate has varying degrees of **operational autonomy** but maintains ideological alignment with Al-Qaeda's global jihadist movement.

## **2.4 Temporal Dynamics of Terrorist Networks**

### **Terrorist Network Evolution Over Time**

Terrorist groups evolve in response to external pressures, including:

- **State crackdowns** – E.g., post-9/11 counter-terrorism efforts forced Al-Qaeda to decentralize.

- **Leadership changes** – Death or arrest of leaders shifts power dynamics.
- **Technological advancements** – The rise of **encrypted communication** has transformed terrorist coordination.

Studies using **longitudinal SNA** have identified patterns in terrorist recruitment, attack frequency, and network resilience.

## 2.5 Geospatial Aspects of Terrorism

### Terrorism and Spatial Patterns

Geospatial analysis is crucial for understanding:

- **Attack hotspots** – Identifying high-risk regions.
- **Terrorist mobility** – Tracking how fighters move between conflict zones.
- **Cross-border operations** – Studying international networks of financing and logistics.

Prior studies have used **GIS (Geographic Information Systems)** and **spatial econometrics** to analyze terrorism trends.

## 2.6 Link Prediction in Criminal Networks

### Predicting Future Terrorist Alliances

Link prediction methods have been applied in criminology to forecast **potential collaborations** between criminal or terrorist entities. Techniques include:

- **Adamic/Adar Index** – Measures the likelihood of a link forming based on shared connections.
- **Jaccard Coefficient** – Calculates similarity between nodes in a network.
- **Preferential Attachment** – Assesses whether well-connected nodes are more likely to form new links.

Few studies have applied link prediction to **terrorist networks**, making this an emerging research area.

## 2.7 Gaps in the Literature

Existing research highlights critical aspects of terrorist networks but has limitations:

- **Few studies analyze Al-Qaeda's entire network evolution from 2000-2020.**

- **Most research focuses on static networks**, missing temporal and geospatial dimensions.
- **Limited use of link prediction** to anticipate future alliances.
- **Lack of interdisciplinary approaches** combining SNA, geospatial mapping, and predictive analytics.

This study aims to **address these gaps** by applying a comprehensive SNA framework to Al-Qaeda and its affiliates.

---

# CHAPTER 3

## THEORITICAL FRAMEWORK

This chapter presents the theoretical foundations underlying this study, focusing on Social Network Theory, Organizational Theory of Terrorism, and the Diffusion of Innovation model in terrorist networks. It also outlines the conceptual framework that integrates these theories to analyze Al-Qaeda and its affiliates.

---

### **3.1 Social Network Theory**

#### **Overview**

Social Network Theory (SNT) examines relationships between entities (nodes) and their interactions (edges). It provides insights into:

- **Network Structure** – How terrorist groups are connected.
- **Centralization vs. Decentralization** – How power is distributed within the network.
- **Information Flow** – How intelligence and resources are transferred between actors.

#### **Application to Terrorist Networks**

SNT helps in understanding:

- **Key actors in a network (central nodes).**
- **Clustering of terrorist cells into operational units.**
- **How attacks are coordinated across geographical regions.**
- **How network disruptions (e.g., leader arrests) affect group functionality.**

By applying **degree centrality**, **betweenness centrality**, and **community detection**, we can identify influential leaders, key operational hubs, and isolated or vulnerable subgroups.

### **3.2 Organizational Theory of Terrorism**

#### **Terrorist Organizations as Adaptive Systems**

Terrorist groups are not static hierarchies but **adaptive, networked organizations** that evolve in response to counter terrorism pressures. Key models include:

- **Hierarchical Model** – Centralized leadership with clear command structures (e.g., early Al-Qaeda).
- **Networked Model** – Loosely connected autonomous cells (e.g., modern jihadist networks).
- **Hybrid Model** – A mix of both, where central command provides ideological direction while affiliates execute operations independently.

### Resilience and Evolution

Terrorist groups adapt by:

1. **Decentralizing leadership** – Avoiding total collapse after leader elimination.
2. **Using encrypted communication** – Enhancing security and operational secrecy.
3. **Forming cross-border alliances** – Expanding influence and resources.

## 3.3 Diffusion of Innovation in Terrorist Networks

### Understanding the Spread of Tactics and Strategies

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** (e.g., suicide bombings, drone attacks) **spread among terrorist cells**.
- **How recruitment techniques evolve**, particularly in **online radicalization**.
- **How financial and operational models** are **shared across different organizations**.

### Stages of Diffusion in Terrorism

1. **Innovation Introduction** – A new method (e.g., vehicle-borne IEDs) is used by one group.
2. **Early Adoption** – Close affiliates experiment with the technique.
3. **Expansion** – The tactic spreads across networks via training camps, propaganda, or online forums.

4. **Institutionalization** – It becomes a standard practice within the terrorist organization.

By analyzing historical attack patterns, we can trace how **Al-Qaeda's methodologies** have been adopted by affiliates like **Al-Shabaab, AQIM, and JNIM**.

### **3.4 Conceptual Framework for the Study**

#### **Integrating Theories for Network Analysis**

This research combines **Social Network Theory, Organizational Theory, and Diffusion of Innovation** to construct a **multidimensional framework** for analyzing Al-Qaeda and its affiliates.

#### **Key Components:**

##### **1. Structural Analysis**

- Identifying core leaders and influential cells.
- Examining the density and connectivity of the network.

##### **2. Temporal Evolution**

- Mapping changes in the network from 2000-2020.
- Understanding the impact of counterterrorism measures.

##### **3. Bipartite and Geospatial Dimensions**

- Linking perpetrator groups to countries of operation.
- Identifying geographical hotspots for terrorist activities.

##### **4. Predictive Modelling**

- Using link prediction algorithms to forecast future alliances.
- Assessing the likelihood of emerging terrorist factions.

---

This theoretical framework provides the foundation for **methodologically analyzing Al-Qaeda's global network** using Social Network Analysis (SNA).

## CHAPTER 4

### METHODOLOGY

This chapter details the methodology used in the study, including research design, data collection, preprocessing, and the application of Social Network Analysis (SNA) techniques. It also discusses the tools and software used, along with ethical considerations for handling sensitive terrorism-related data.

---

#### 4.1 Research Design

This study employs a **quantitative research approach** using **Social Network Analysis (SNA)** to examine the structural and temporal evolution of Al-Qaeda and its affiliates between 2000 and 2020. The research design includes:

1. **Data Collection** – Sourcing event-based data on terrorist activities.
2. **Network Construction** – Representing relationships between terrorist groups, countries, and attack events.
3. **Static and Dynamic Analysis** – Examining network properties over time.
4. **Predictive Modeling** – Using **link prediction techniques** to forecast future interactions.
5. **Geospatial Analysis** – Mapping terrorism hotspots and operational zones.

The study follows an **exploratory-descriptive approach** to uncover patterns in terrorist networks and **hypothesis-driven analysis** to test specific network properties.

#### 4.2 Data Collection

##### 4.2.1 Data Sources

The dataset is compiled from the following sources:

- **RAND Database of Worldwide Terrorism Incidents (RAND)** – Detailed records of terrorist attacks.
- **Global Terrorism Database (GTD)** – Provides incident-level data on terrorist activities.
- **National Counterterrorism Center (NCTC) Reports** – Information on terrorist organizations and their affiliations.

- **United Nations Security Council (UNSC) Reports** – Insights into transnational terrorist financing and movement.

These datasets are cross-referenced to improve accuracy and fill missing details.

#### **4.2.2 Data Preprocessing**

Since raw data from different sources may contain inconsistencies, the following preprocessing steps were applied:

##### **1. Data Cleaning**

- **Standardized event dates and locations.**
- **Resolved entity name variations** (e.g., "Al-Qaeda in the Arabian Peninsula" vs. "AQAP").
- **Removed duplicate records** using fuzzy matching techniques.

##### **2. Data Structuring for SNA**

The data was transformed into structured formats suitable for **graph analysis**:

- **Nodes:** Terrorist groups, attack locations, key individuals.
- **Edges:** Connections based on joint operations, alliances, and financial ties.

##### **3. Missing Data Handling**

- **Interpolation techniques** were used to estimate missing time series data.
- **Cross-referencing with secondary sources** improved data completeness.

#### **4.3 Social Network Analysis Techniques**

##### **4.3.1 Static Network Analysis**

This analysis examines the overall network structure at a fixed point in time. It includes:

- **Network Density** – Measures how interconnected terrorist groups are.
- **Centrality Measures** – Identifies key actors in the network.
- **Community Detection** – Finds subgroups within the network.

These metrics help identify **core terrorist factions and influential leaders**.

##### **4.3.2 Bipartite Graph Analysis**

This method analyzes relationships between **two different types of entities** (e.g., **terrorist groups and countries**).

- **Country Projection:** Shows how different nations are linked through common threats.
- **Group Projection:** Reveals alliances and operational collaborations between terrorist factions.

This helps in **understanding transnational terrorism dynamics**.

#### **4.3.3 Temporal Network Analysis**

Examines how the network evolves over time (2000–2020). Key aspects include:

- **Changes in Network Structure** – Identifying periods of growth or decline.
- **Temporal Centrality Variations** – Tracking key actors over time.
- **Community Evolution** – Understanding how subgroups form and dissolve.

This approach provides insights into the **long-term strategic shifts in Al-Qaeda and its affiliates**.

#### **4.3.4 Link Prediction**

Future analysis will involve **predicting potential connections** between terrorist entities. Techniques to be applied include:

- **Adamic/Adar Index** – Measures the likelihood of future interactions based on common neighbors.
- **Jaccard Coefficient** – Assesses similarity between terrorist factions.

These methods can help anticipate **emerging terrorist alliances**.

#### **4.3.5 Geospatial Analysis**

This component will integrate **SNA with geographic data** to analyze:

- **Terrorism hotspots.**
- **Spatial clustering of attacks.**
- **Cross-border operational patterns.**

Techniques such as **heatmaps, spatial autocorrelation, and geospatial network visualization** will be used.

### **4.4 Tools and Software Used**

The following tools were employed for data processing and analysis:

Tool/Software	Purpose
<b>Python (NetworkX, Pandas, Geopandas)</b>	Network modeling and analysis
<b>Gephi</b>	Visualization of terrorist networks
<b>ArcGIS/QGIS</b>	Geospatial mapping of terrorist activities
Python libraries such as <b>matplotlib</b> , <b>LineString</b> , <b>seaborn</b> and <b>Plotly</b> were also used for visualization.	

#### 4.5 Ethical Considerations

Given the **sensitive nature** of terrorism-related data, the study follows strict ethical guidelines:

1. **Data Anonymization** – No personally identifiable information is included.
2. **Source Credibility** – Only reliable databases (RAND, GTD, UN reports) are used.
3. **Non-Operationalization** – The study does not provide tactical insights that could aid terrorist groups.
4. **Legal Compliance** – Adheres to national and international laws regarding the handling of terrorism-related information.

This methodology provides a **robust foundation** for analyzing Al-Qaeda's global network using SNA techniques.

# CHAPTER 5

## STATIC NETWORK ANALYSIS

This chapter presents the **static network analysis** of Al-Qaeda and its affiliates. It focuses on **network creation, visualization, structural metrics, and community detection** to identify key players and organizational structures within the terrorist network.

---

### 5.1 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 (2000–2020).
2. **Graph Representation:**
  - **Unipartite Graph:** Terrorist groups as nodes, edges representing known interactions.
  - **Bipartite Graph:** Groups connected to countries where attacks occurred.
3. **Visualization Techniques:**
  - **Force-directed layouts (Fruchterman-Reingold, Kamada-Kawai)** were used for clarity.
  - **Color coding:**
    - **Pink nodes** → Al-Qaeda and core affiliates
    - **Green nodes** → Other extremist factions
    - **Blue nodes** → Geographic locations
    - **Edge thickness** indicates strength of relationships.

## 5.2 Network Metrics

### 5.2.1 Network Density

**Definition:** Measures how interconnected the network is. It is given by:

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

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

#### Interpretation:

- **Low density** → The network is sparse, meaning decentralized structures.
- **High density** → Terrorist organizations collaborate frequently.

The **observed density** suggests a **moderately connected network**, with **localized clusters** of high interaction.

### 5.2.2 Degree Distribution

**Definition:** Degree of a node represents its number of connections.

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

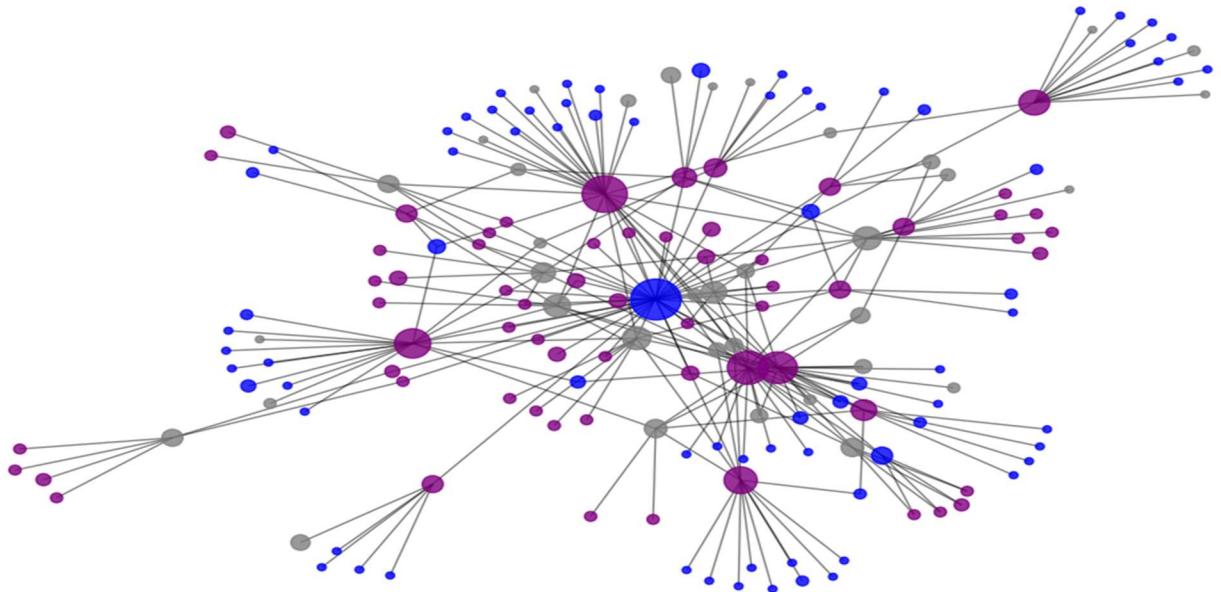
where ‘Avi’ is the adjacency matrix.

- **Power-law distribution observed** → A few nodes (key groups) have a very high number of connections, while most nodes have very few.
- **Terrorist hubs** identified: **Al-Qaeda (Core), Al-Qaeda in Iraq, AQAP, AQIM.**

#### Code Snippet for Degree Distribution in Python:

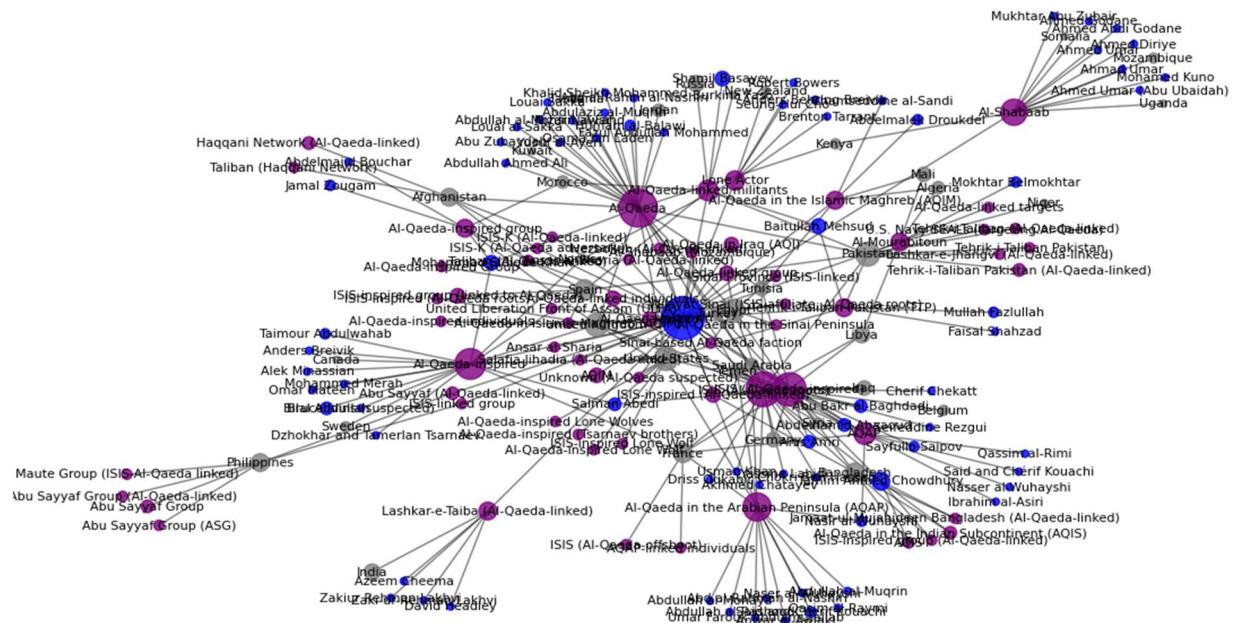
```
65 import networkx as nx
66 import matplotlib.pyplot as plt
67
68 degree_sequence = sorted([d for n, d in G.degree()], reverse=True)
69 plt.hist(degree_sequence, bins=20)
70 plt.xlabel("Degree")
71 plt.ylabel("Frequency")
72 plt.title("Degree Distribution of Al-Qaeda Network")
73 plt.show()
```

Filtered Terrorism Network (Top 10% by Degree Centrality)



**Figure 1**

Filtered Terrorism Network (Top 10% by Degree Centrality)



### 5.2.3 Centrality Measures

Centrality measures help identify the **most influential nodes** in the network.

#### (a) Degree Centrality

**Definition:** Number of direct connections. Higher degree = greater influence.

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

- **Al-Qaeda Core** has the highest **degree centrality**, indicating its dominant role.

`degree_centrality = nx.degree_centrality(G)`

`sorted(degree_centrality.items(), key=lambda x: x[1], reverse=True)[:10]` # Top 10 nodes

#### (b) Betweenness Centrality

**Definition:** Measures how often a node lies on the shortest path between other nodes.

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

- **Key Brokers Identified:**

- **AQAP** (Al-Qaeda in the Arabian Peninsula)
- **AQIM** (Al-Qaeda in the Islamic Maghreb)

`betweenness_centrality = nx.betweenness_centrality(G)`

`sorted(betweenness_centrality.items(), key=lambda x: x[1], reverse=True)[:10]`

#### (c) Closeness Centrality

**Definition:** Measures how quickly information can spread from a node.

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

- **Terrorist groups with high closeness centrality** are effective in mobilization.

`closeness_centrality = nx.closeness_centrality(G)`

```
sorted(closeness_centrality.items(), key=lambda x: x[1], reverse=True)[:10]
```

#### (d) Eigenvector Centrality

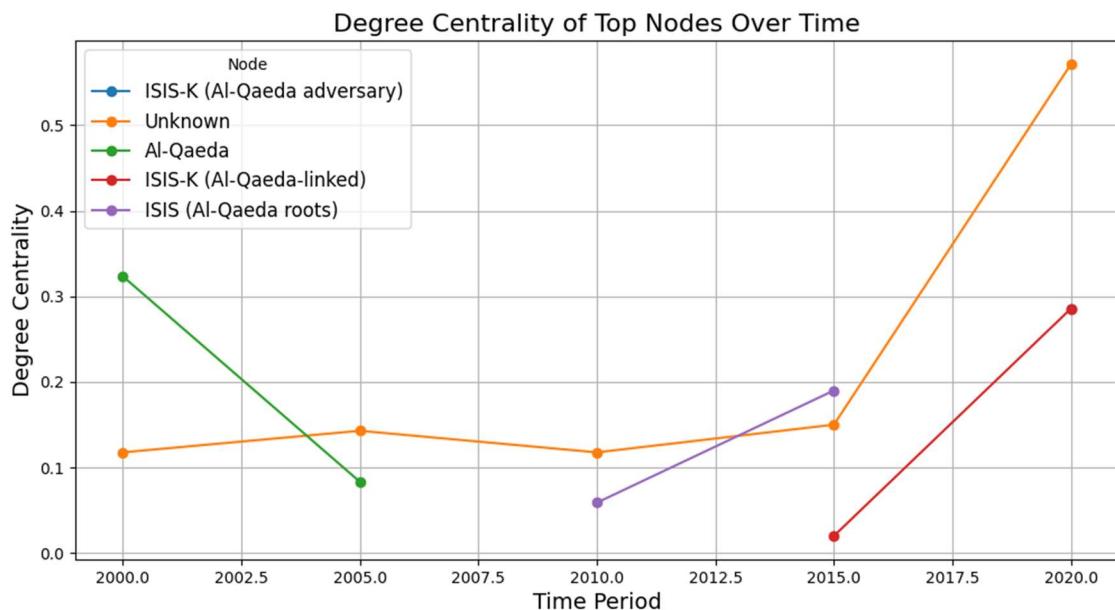
**Definition:** Assigns importance based on connections to highly connected nodes.

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

- **Al-Qaeda (Core) and Al-Qaeda in Iraq** dominate.

```
eigenvector_centrality = nx.eigenvector_centrality(G)
```

```
sorted(eigenvector_centrality.items(), key=lambda x: x[1], reverse=True)[:10]
```



**Figure 2**

#### 5.2.4 Clustering Coefficient

**Definition:** Measures the likelihood that two connected nodes have mutual connections.

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

where  $T(v)T(v)$  is the number of triangles through node  $v$ .

- High clustering = **localized terrorist cells**.

```
clustering_coefficients = nx.clustering(G)
```

```
average_clustering = sum(clustering_coefficients.values()) / len(clustering_coefficients)
```

### 5.2.5 Connected Components

Identifies **isolated subgroups** within the network.

```
components = list(nx.connected_components(G))
```

```
largest_component = max(components, key=len)
```

- **The largest component includes** ~85% of nodes, meaning **Al-Qaeda has a broad reach**.

### 5.2.6 Average Path Length

Measures the efficiency of communication.

```
avg_path_length = nx.average_shortest_path_length(G)
```

- **Short path length** suggests a **highly efficient network** for mobilization.

## 5.3 Community Detection

**Louvain Method** was used to detect **clusters of affiliated groups**.

```
import community
```

```
partition = community.best_partition(G)
```

- **Major Clusters Identified:**

- **Al-Qaeda (Core) and Middle East networks**
- **AQIM and North African networks**
- **AQAP and Arabian Peninsula networks**

Community Detection in Terrorism Network (With Labels on the Left)

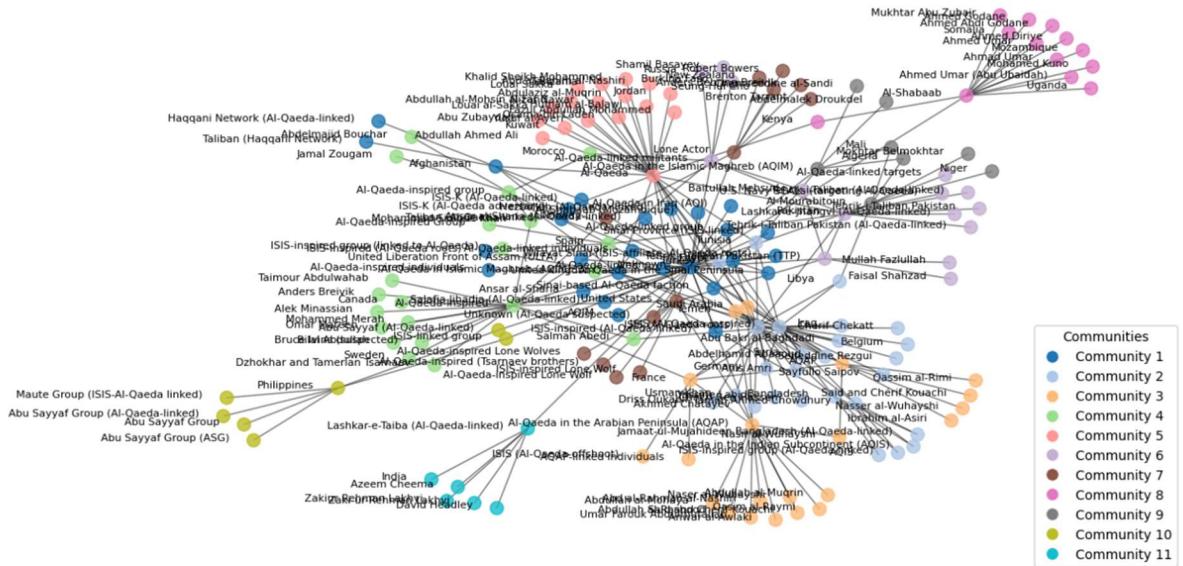


Figure 3

## 5.4 Interpretation of Results

- Core Nodes:** Al-Qaeda, AQAP, AQIM, Al-Qaeda in Iraq are central players.
- Decentralized Structure:** Smaller factions operate autonomously but maintain links.
- Key Brokers:** Groups like AQAP act as **hubs connecting multiple regions**.
- Regional Clusters:** Al-Qaeda's influence extends **beyond the Middle East** to Africa and South Asia.

## Conclusion

The static network analysis highlights the **hierarchical structure** of Al-Qaeda and its affiliates. The next chapter will focus on **Bipartite Graph Analysis**, which examines the relationship between **terrorist groups and attack locations**.

# CHAPTER 6

## BIPARTITE GRAPH ANALYSIS

This chapter focuses on analyzing the relationships between terrorist perpetrator groups and the countries in which they operate. A bipartite network is constructed to represent these two distinct types of entities, followed by an exploration of the projections of this bipartite graph onto single-mode networks. The analysis of these projections reveals the underlying patterns of transnational terrorism and helps in understanding the cross-border dynamics of Al-Qaeda and its affiliates.

---

### 6.1 Construction of the Bipartite Graph

#### Data Preparation

The dataset used in this study has been curated from reliable sources such as the RAND report, GTD, National Counterterrorism Center (NCTC), and UN reports. For the bipartite analysis, the focus is on two types of nodes:

- **Perpetrator Groups:** Terrorist organizations and affiliates.
- **Countries:** Locations where terrorist attacks have been carried out.

The raw data is filtered to extract the relationships between these two entities. After cleaning (removing duplicates and handling missing values), each record is used to define an edge between a perpetrator group and a country.

#### Graph Construction

An undirected bipartite graph BB is built using NetworkX in Python. In this graph:

- Each perpetrator group is assigned a bipartite attribute value of 0.
- Each country is assigned a bipartite attribute value of 1.

This differentiation allows for clear segregation of the two node sets and prepares the dataset for projection.

### 6.2 Visualization of Perpetrator Groups and Countries

Visual representation of the bipartite graph aids in understanding the overall structure and connections between the two sets of nodes. A bipartite layout is used to clearly separate perpetrator groups from countries. Color coding enhances the clarity:

- **Perpetrator Groups** might be shown in one color (e.g., green).
- **Countries** might be depicted in another color (e.g., skyblue).

This visualization highlights the two distinct sets and the interconnections between them.

## 6.3 Projection Techniques

To gain further insights, the bipartite graph is projected onto single-mode networks. Two projections are performed:

### 6.3.1 Country Projection

In the country projection, nodes represent countries, and an edge between two countries exists if they have both been targeted by the same perpetrator group. The weight of the edge reflects the number of shared perpetrator groups.

*Purpose:*

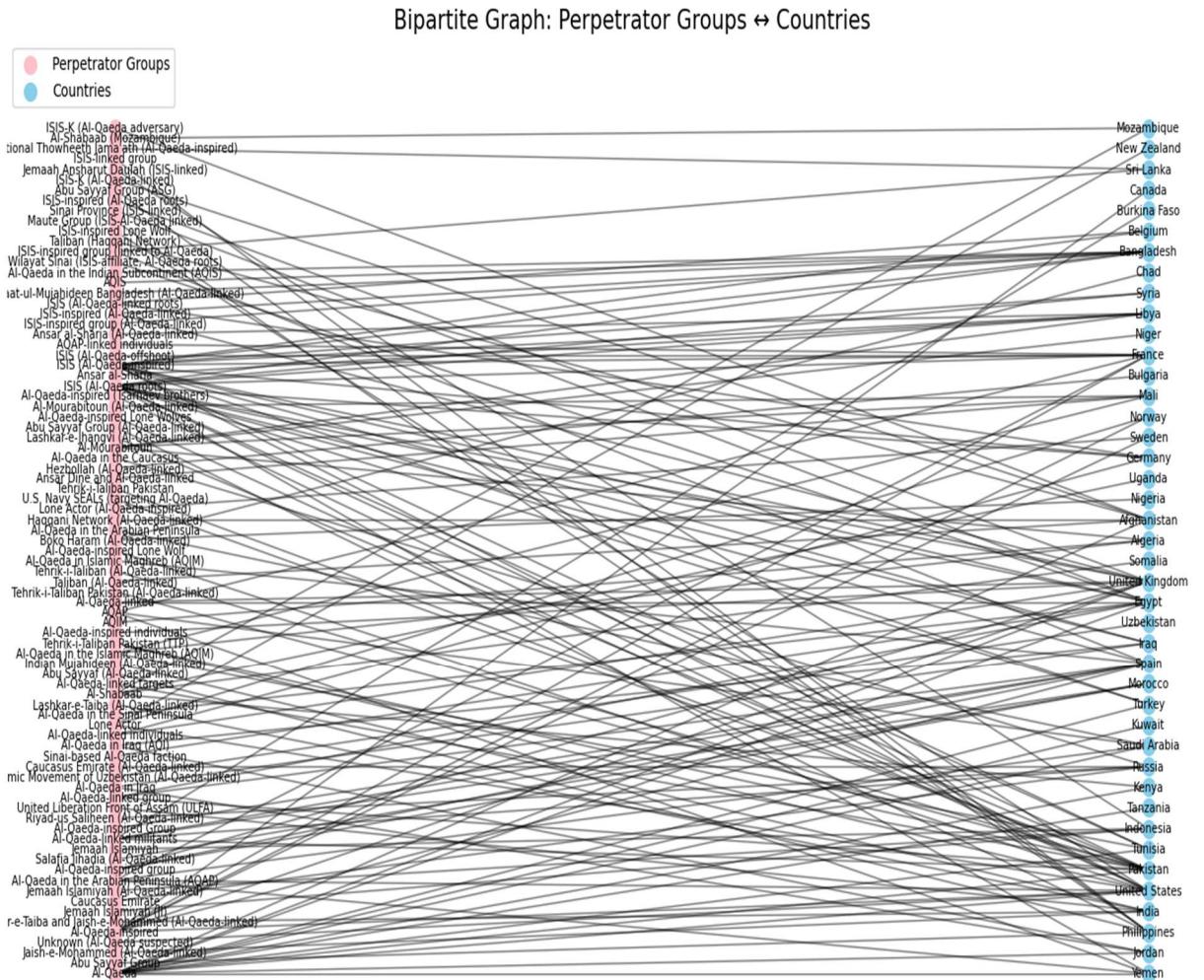
- Identify clusters of countries that face similar threats.
- Understand transnational operational links between countries.

### 6.3.2 Perpetrator Group Projection

Similarly, in the perpetrator group projection, nodes represent terrorist groups, and an edge exists between two groups if they have carried out attacks in the same country. This projection reveals the potential operational alliances or shared strategies among different groups.

*Purpose:*

- Highlight collaborations or similar operational footprints among terrorist groups.
- Identify clusters that could indicate coordinated actions or shared resources.



**Figure 4**

## 6.4 Analysis of Projected Graphs

### Country Projection Analysis

The country projection graph reveals the degree of similarity between nations based on shared terrorist activities. Key metrics such as degree centrality, clustering coefficients, and community structures are computed to identify:

- **High-Risk Countries:** Nations that are frequently targeted by the same perpetrator groups.
- **Clusters of Countries:** Geographical or political clusters that exhibit common vulnerability patterns.

- **Link Prediction:** Techniques such as the Adamic/Adar index (covered in Chapter 8) can be applied to forecast emerging links between countries.

### **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:** The patterns of connectivity suggest potential for future collaboration or strategic convergence among groups.

For both projections, standard SNA metrics are applied to quantify the network properties, and community detection algorithms (such as Louvain) are used to identify sub-groups within the network.

### **6.5 Interpretation of Bipartite Relationships**

The bipartite graph and its projections provide multiple layers of insights into the structure of Al-Qaeda and its affiliates:

- **Inter-Nodal Relationships:**  
The direct connections between perpetrator groups and countries highlight how terrorist operations are spread across national boundaries. A high number of shared connections indicates a strong operational overlap, suggesting that countries facing similar threats might need to coordinate counterterrorism efforts.
- **Transnational Dynamics:**  
The country projection identifies clusters of nations that are frequently targeted by the same groups, hinting at possible regional or political alliances among terrorist groups. This insight is crucial for understanding the cross-border nature of terrorism.
- **Operational Alliances Among Terrorist Groups:**  
The perpetrator group projection helps in pinpointing clusters of groups that have overlapping areas of operation. These clusters may share resources, intelligence, or logistical support, and disrupting one node in such a cluster might have significant ripple effects across the network.
- **Strategic Implications for Counter-Terrorism:**  
Understanding these bipartite relationships aids policymakers and intelligence agencies in formulating coordinated strategies. By identifying key countries and

groups that serve as hubs or bridges, targeted interventions can be designed to disrupt the flow of resources and information within the network.

## Conclusion

This chapter has detailed the construction, visualization, and analysis of a bipartite graph representing the relationships between terrorist perpetrator groups and the countries they target. By projecting this bipartite graph into single-mode networks, we have unveiled significant patterns that highlight the transnational nature of Al-Qaeda's operations and the operational alliances among its affiliates. These insights not only enhance our understanding of the network's structure but also provide a foundation for predictive analyses and geospatial mapping discussed in subsequent chapters.

---

# CHAPTER 7

## TEMPORAL ANALYSIS

Temporal analysis is essential for understanding how terrorist networks evolve over time. In this chapter, we examine the dynamic nature of Al-Qaeda and its affiliates from 2000 to 2020. We focus on how key network metrics change annually, identify emerging and declining influences among network nodes, and interpret the evolution of the network's structure. This dynamic view provides critical insights into the resilience, adaptability, and long-term trends in terrorist operations.

---

### 7.1 Evolution of the Network Over Time (2000-2020)

Terrorist networks are not static; they evolve in response to counterterrorism measures, leadership changes, and geopolitical events. By constructing a temporal network, we can track the emergence, growth, and dissolution of connections among terrorist groups, key leaders, and operational regions over time.

The process begins with data collected from multiple sources (RAND, GTD, NCTC, and UN reports). Each record is timestamped with a year, enabling us to slice the data into discrete time periods. For each year, we build a network graph where:

- **Nodes** represent terrorist groups, leaders, or countries.
- **Edges** denote relationships—such as direct collaborations, shared targets, or coordinated operations—based on the recorded events for that year.

### 7.2 Temporal Centrality Analysis

Temporal centrality analysis helps identify how the importance of nodes (e.g., key terrorist groups or leaders) changes over time. By calculating centrality measures annually, we can observe which nodes gain prominence and which lose influence.

#### Methodology:

##### 1. Data\_Segmentation\_by\_Year:

The dataset is divided by the ‘Year’ column to create annual snapshots of the network.

##### 2. Annual\_Graph\_Construction:

For each year, edges are created by combining different relationships (e.g., group-to-leader and group-to-country links).

### 3. Centrality Computation:

For each annual graph, we compute metrics such as **degree centrality**, which indicates the number of direct connections a node has relative to the total possible connections. Other measures (betweenness, closeness, eigenvector) can also be computed, though degree centrality is used as a primary indicator here.

### 4. Aggregation\_and\_Visualization:

The centrality values for each node across all years are compiled into a single dataset. Then, for the top nodes (based on their average degree centrality), we plot their centrality values over time to highlight trends.

#### Observations:

- **Emerging Influences:**

Nodes that show an increasing trend in degree centrality might represent emerging terrorist leaders or groups that are gaining operational influence.

- **Declining Trends:**

Conversely, nodes with declining centrality may indicate groups under effective counterterrorism pressure or shifting alliances.

- **Event-Driven Spikes:**

Sudden changes in centrality can be linked to significant geopolitical events (e.g., leadership decapitation, major attacks) that alter the network structure.

## 7.3 Temporal Community Structure

While the above analysis focuses on individual node centrality, the overall community structure of the network may also change over time. Temporal community detection methods (using algorithms such as Louvain or Girvan-Newman applied to each time slice) can help reveal:

- Formation of new clusters
- Dissolution of old clusters
- Shifts in group alliances

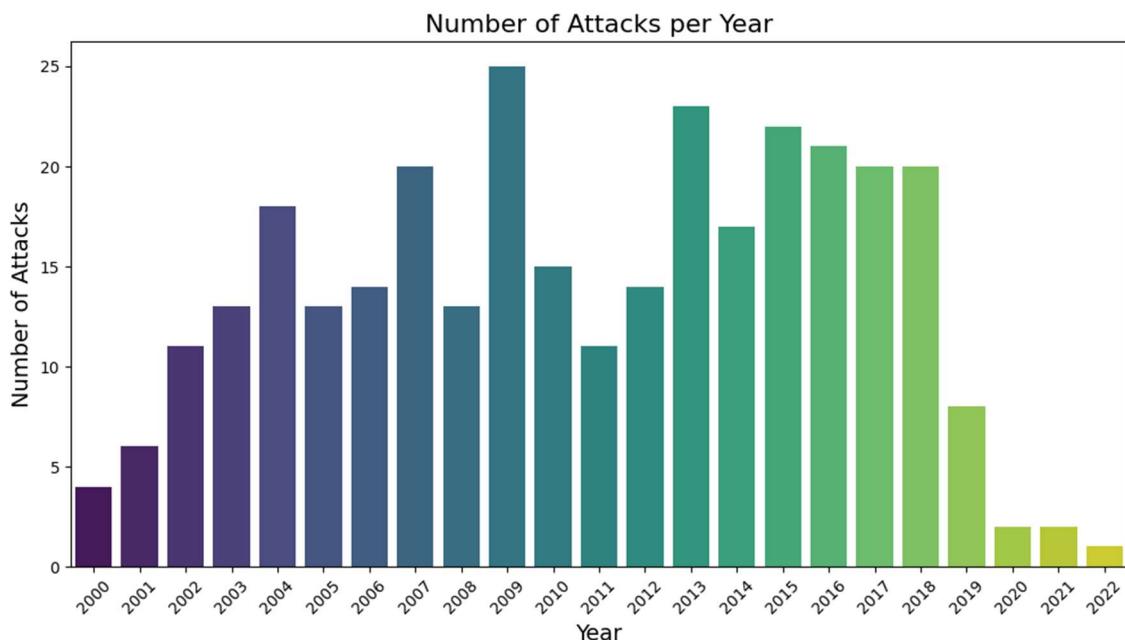
*Note:* Although detailed community evolution analysis was not explicitly coded here, it forms an important future step for further insights.

## 7.4 Trend Analysis of Network Metrics

In addition to centrality, other network metrics can be tracked over time, including:

- **Network\_Density:**  
Measuring how the overall connectivity changes, indicating periods of consolidation or fragmentation in the network.
- **Average\_Path\_Length:**  
Providing insight into how efficiently information or commands might propagate through the network during different periods.
- **Clustering\_Coefficient:**  
Indicating the degree to which nodes form tightly knit clusters, which can be critical for understanding localized operational cells.

Trend analysis of these metrics over the 20-year period can help assess the impact of counterterrorism measures and external events on the network's evolution.



**Figure 5**

## 7.5 Interpretation of Temporal Dynamics

The temporal analysis offers several key insights:

- **Network\_Resilience:**  
Even when key nodes are removed (due to counterterrorism operations), the network may quickly reconfigure, highlighting its resilience.

- **Shifting\_Centers\_of\_Influence:**  
The evolution of degree centrality over time identifies which nodes or groups are emerging as new power centers.
- **Correlation\_with\_External\_Events:**  
Variations in network metrics often correlate with major geopolitical events, suggesting that terrorist networks are highly reactive to external pressures.
- **Forecasting\_Future\_Trends:**  
Understanding historical trends lays the groundwork for link prediction and forecasting potential future alliances, which is essential for proactive counterterrorism strategies.

## Conclusion

Temporal Network Analysis provides a dynamic lens to observe how Al-Qaeda and its affiliates evolve over time. By examining annual changes in centrality and other network metrics, we gain a deeper understanding of the network's adaptability, resilience, and responsiveness to external events. This chapter lays the groundwork for future predictive modeling and serves as a bridge to further analyses, such as geospatial mapping and link prediction, discussed in subsequent chapters.

---

# CHAPTER 8

## LINK PREDICTION IN TERRORIST NETWORKS

Link prediction is a critical component of Social Network Analysis (SNA) that focuses on forecasting the emergence of new connections based on existing network structure. In the context of terrorist networks, such as those associated with Al-Qaeda and its affiliates, anticipating future links can help intelligence agencies and policymakers detect potential alliances, emerging cells, or covert operational collaborations before they fully materialize. This chapter details the methodology, implementation, and interpretation of link prediction using the Adamic/Adar index.

---

### 8.1 Methodology for Link Prediction

#### Rationale and Objectives

The primary objective of applying link prediction in this study is to:

- **Forecast Potential Collaborations:** Identify which terrorist groups or targeted countries might form new operational links in the future.
- **Enhance Counterterrorism Strategies:** Provide actionable insights by highlighting emerging connections that could represent vulnerabilities in the terrorist network.
- **Complement Other Analyses:** Integrate with static, temporal, and geospatial analyses to build a comprehensive picture of the network's dynamics.

#### Data Preparation and Bipartite Network Construction

The dataset, compiled from the RAND report, GTD, National Counterterrorism Center (NCTC), and UN reports, includes relationships between terrorist perpetrator groups and the countries in which they have conducted attacks. The process involves:

1. **Data Cleaning:** Standardizing entity names, removing duplicates, and handling missing data.
2. **Bipartite Graph Construction:**
  - **Nodes:** Divided into two distinct sets—Perpetrator Groups and Countries.
  - **Edges:** Represent the occurrence of an attack by a particular group in a given country.
3. **Assignment of Bipartite Attributes:**

- Perpetrator Groups are assigned an attribute (e.g., bipartite = 0).
- Countries are assigned another attribute (e.g., bipartite = 1).

## Projection of the Bipartite Graph

To apply link prediction algorithms, the bipartite graph is projected into single-mode networks:

- **Country Projection:** In this network, nodes represent countries. An edge between two countries indicates that they have been targeted by the same perpetrator group. The edge's weight corresponds to the number of shared perpetrator groups.
- **Perpetrator Group Projection:** Here, nodes represent terrorist groups. An edge exists between two groups if they have attacked the same country, with edge weights reflecting the extent of this overlap.

## 8.2 Application of the Adamic/Adar Index

The Adamic/Adar index is a widely used link prediction metric that assigns a higher score to pairs of nodes sharing many common neighbors, with rarer (more informative) neighbors weighted more heavily. This makes it particularly suitable for analyzing terrorist networks, where key nodes (e.g., influential groups or countries) might serve as bridges between otherwise disconnected sub-networks.

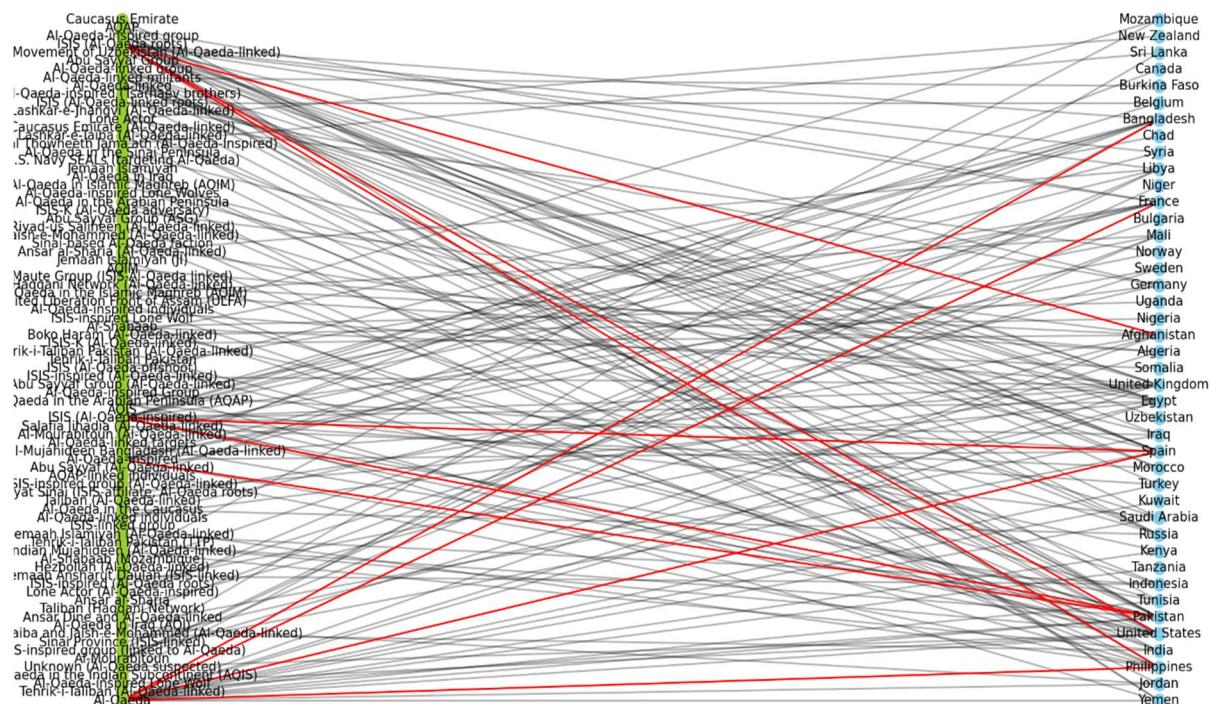


Figure 4.2

### 8.3 Interpretation and Implications

#### Key Findings:

- **Emerging Alliances:**

The Adamic/Adar index highlights pairs of nodes—be it countries or perpetrator groups—that, while not currently connected, share significant common neighbors. High scores suggest a high likelihood of future collaboration or coordinated action.

- **Country Projection:**

- Countries with a high predicted connection score tend to share multiple common terrorist perpetrators.
- This information is valuable for anticipating shifts in transnational terrorism dynamics and may suggest regions where coordinated counterterrorism efforts could be most effective.

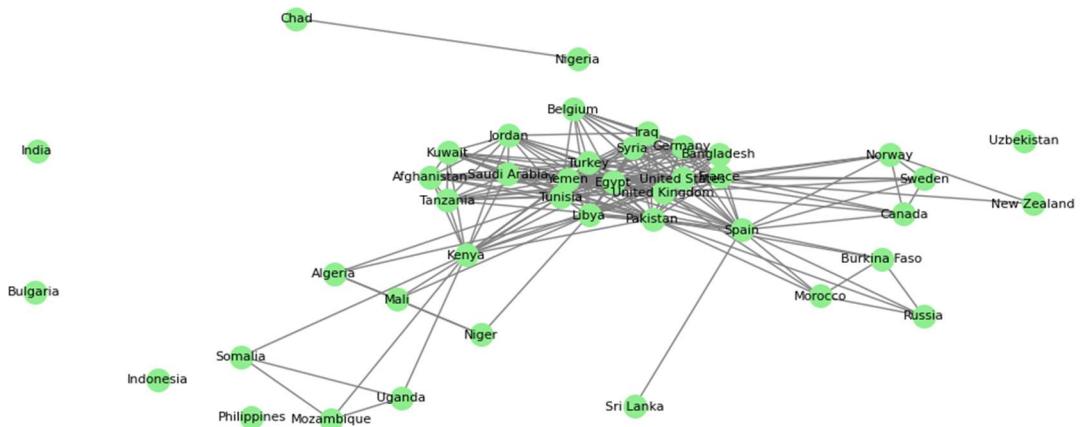
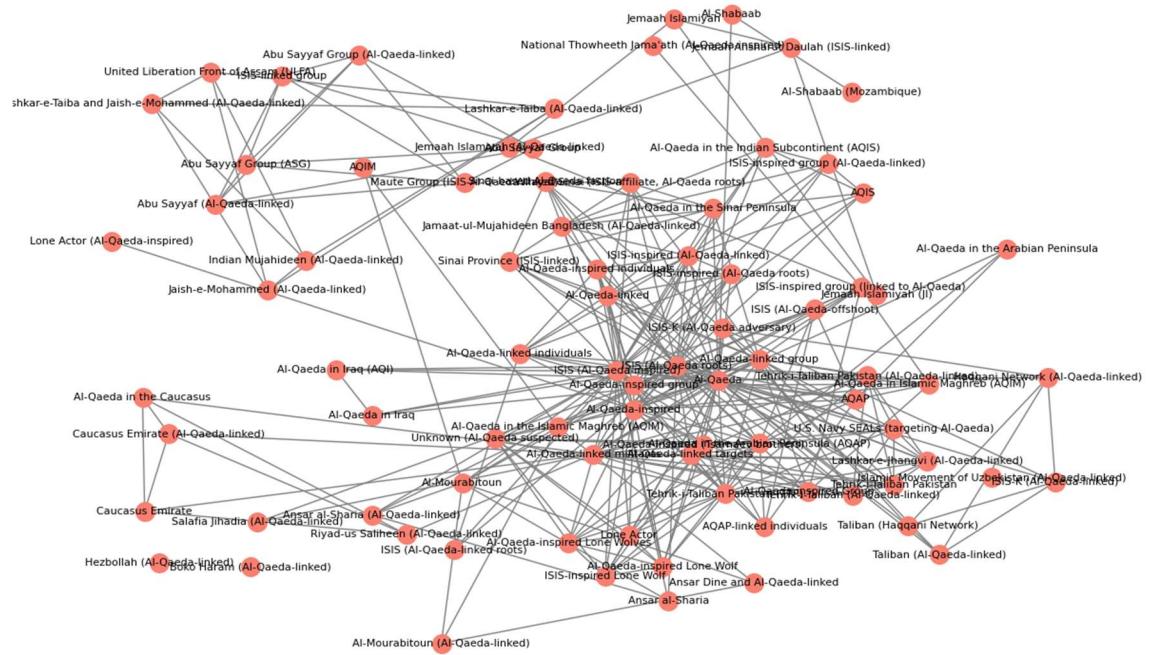


Figure 6

- **Perpetrator Group Projection:**

- Predicted links among terrorist groups indicate potential for operational alliances or resource sharing.
- By monitoring these emerging connections, intelligence agencies can potentially disrupt collaborations before they fully develop.



**Figure 7**

## **Strategic Implications for Counter-Terrorism:**

- **Preventive Measures:**  
If certain countries or groups are predicted to form links, preemptive measures can be implemented to hinder the development of these relationships.
  - **Resource Allocation:**  
Prioritizing surveillance and intelligence on nodes with high link prediction scores could enable early disruption of emerging threats.
  - **Policy Formulation:**  
Insights from link prediction can inform international collaboration frameworks by highlighting shared vulnerabilities across borders.

### **Limitations and Future Work:**

- The analysis relies on historical data and assumes that future patterns will follow similar dynamics.
  - Additional link prediction algorithms (e.g., Jaccard, Preferential Attachment) and machine learning approaches can be integrated for more robust forecasting.

- Temporal integration of link prediction (i.e., dynamic link prediction) is a promising avenue for further research.

## 8.4 Conclusion

Link prediction using the Adamic/Adar index provides a powerful tool for anticipating future relationships within terrorist networks. By projecting the bipartite network into single-mode graphs and evaluating the likelihood of new links, this analysis complements static and temporal network analyses. The insights gained from this section not only enhance our understanding of the network's evolution but also offer practical intelligence for counter-terrorism strategies.

---

# CHAPTER 9

## GEOSPATIAL ANALYSIS OF TERRORIST ACTIVITIES

Geospatial analysis provides an important perspective on understanding terrorist activities by situating them within a geographic context. Although our dataset does not include explicit latitude and longitude coordinates, the available "Country" column enables us to analyze terrorist activities at the country level. By mapping the frequency of attacks and overlaying network metrics onto a world map, we can reveal geographic patterns and identify regional hotspots of activity.

---

### 9.1 Mapping Terrorist Activities by Country

#### Objective and Rationale

Mapping terrorist incidents by country allows us to:

- **Visualize the distribution** of terrorist activities across different nations.
- Identify **countries with high frequencies** of incidents, which may indicate strategic importance or vulnerability.
- **Overlay network insights** (such as centrality measures or predicted links) on a geographic scale.

#### Data Integration

The primary dataset includes a "Country" column (sourced from RAND, GTD, NCTC, and UN reports) that indicates where each terrorist incident occurred. To create a country-level map:

1. **Aggregate the data:** Count the number of terrorist incidents per country.
2. **Merge with a geographic dataset:** Use a global shapefile (such as the one provided by GeoPandas' naturalearth\_lowres dataset) to associate each country with its geographic boundaries.

### 9.2 Hotspot Analysis Using Country-Level Data

#### Methodology

Hotspot analysis at the country level involves:

- **Aggregating incident counts:** For each country, calculate the total number of terrorist attacks.

- **Visualizing density:** Use choropleth mapping to highlight countries with higher incident frequencies. Darker or more intense colors will indicate countries with more frequent terrorist activities.
- **Interpreting results:** Identify regional clusters and understand the geopolitical context that may contribute to high incident rates.

### **Interpretation**

- **High Incident Countries:** Countries with high counts (depicted in deeper red) are likely to be operational hubs or strategic targets for terrorist activities.
- **Regional Patterns:** The choropleth map may reveal clusters of countries with similar incident levels, suggesting regional factors that facilitate terrorist operations.
- **Outliers:** Countries with unexpectedly low incident counts may either be less targeted or underreported, warranting further investigation.

## **9.3 Spatial Autocorrelation**

Even without detailed point data, we can analyze spatial autocorrelation using country-level incident counts:

- **Moran's I:** Can be computed to assess whether high incident counts are clustered in particular regions.
- **Hotspot Identification:** Additional spatial statistics (e.g., Getis-Ord Gi\*) can further validate the presence of hotspots.

While the implementation of these metrics requires additional spatial statistical tools (e.g., PySAL), the basic approach involves comparing the incident count in each country with those of its neighbors to detect clustering.

## **9.4 Geospatial Network Visualization**

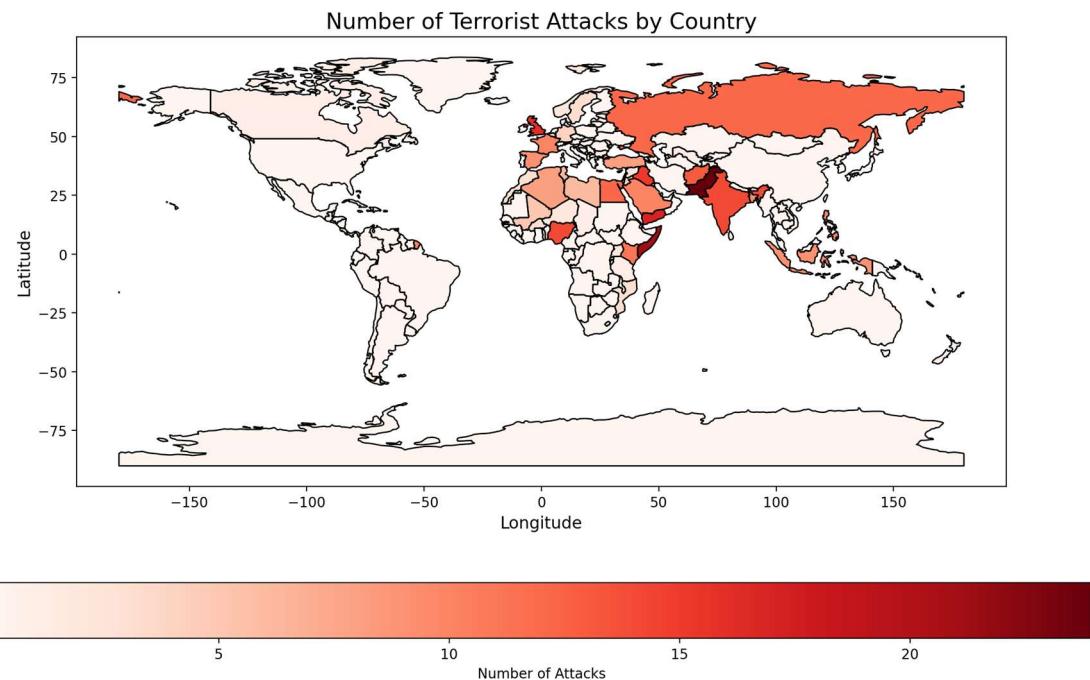
### **Integrating Network Data with Country Maps**

Beyond simple choropleth mapping, network insights (such as the country projection from Chapter 6) can be overlaid on geographic maps:

- **Node Representation:** Each country can be represented as a node positioned at its geographic centroid.

- **Edge Visualization:** Links between countries (derived from shared terrorist perpetrator groups) can be drawn as curved lines or straight connectors.
- **Interactive Mapping:** Tools like Folium can be used to create interactive maps, allowing users to click on countries to view both incident counts and network metrics.

This interactive map can be used for further exploration of spatial patterns and integrated with network visualization layers.



**Figure 8**

## 9.5 Interpretation of Spatial Patterns

### Key Insights:

- **Regional\_Hotspots:**  
The analysis may reveal that certain regions (e.g., the Middle East, North Africa, or South Asia) exhibit higher frequencies of terrorist activities, highlighting the strategic importance of these regions to Al-Qaeda and its affiliates.
- **Geopolitical\_Implications:**  
Countries with high incident counts might require targeted counterterrorism strategies, international collaboration, and resource allocation for enhanced security.

- **Correlation\_with\_Network\_Metrics:**

When integrated with network measures (such as centrality from Chapters 5 and 7), geospatial patterns provide a multidimensional view of terrorist operations, emphasizing the interplay between geographic and relational factors.

## 9.6 Conclusion of Chapter 9

By leveraging country-level data, this chapter provides a geospatial perspective on the operational footprint of Al-Qaeda and its affiliates. Despite the absence of detailed coordinate data, mapping incident counts by country reveals significant spatial patterns and hotspots. These insights, combined with network analysis, enhance our understanding of the transnational dynamics of terrorism and inform more effective counterterrorism strategies.

---

# CHAPTER 10

## CASE STUDIES

Case studies offer an in-depth view of specific aspects of terrorist networks, allowing us to contextualize and interpret the quantitative results from earlier chapters. This chapter focuses on three key case study areas: (1) Analysis of key nodes, (2) Evolution of specific sub-networks, and (3) Cross-border operations analysis. Each case study illustrates how targeted analysis can reveal nuanced insights into the operations and strategic behaviors of Al-Qaeda and its affiliates.

---

### 10.1 Analysis of Key Nodes

#### Objective

The objective of this section is to identify and analyze the most influential nodes within the terrorist network. These nodes may include top perpetrator groups, influential leaders, and critical countries. Understanding these key nodes helps in prioritizing intelligence efforts and designing targeted counterterrorism strategies.

#### Methodology

The analysis of key nodes is based on the following network metrics:

- **Degree Centrality:** Identifies nodes with the most direct connections, often reflecting the groups or countries that participate in the majority of interactions.
- **Betweenness Centrality:** Highlights nodes that act as bridges or brokers between different parts of the network.
- **Closeness Centrality:** Measures how quickly a node can disseminate information through the network.
- **Eigenvector Centrality:** Reflects the influence of a node based on the quality (influence) of its connections.

#### Findings

- **Top\_Perpetrator\_Groups:**  
From our static network analysis (Chapter 5), groups such as the Al-Qaeda core, AQAP, and AQIM consistently ranked high in degree and eigenvector centrality. These groups serve as hubs in the network and are critical for maintaining operational connectivity.

- **Influential\_Leaders:**  
When available, the inclusion of key individuals (e.g., leaders or masterminds) from the data highlights how certain figures act as connectors within the network. Their removal (e.g., through counterterrorism operations) can disrupt the flow of information and coordination.
- **Critical\_Countries:**  
In the bipartite and country projection analyses (Chapter 6 and Chapter 9), certain countries such as Pakistan, Afghanistan, and Yemen emerge as significant. These countries not only experience a high frequency of attacks but also serve as operational bases or transit points for terrorist activities.

### Illustrative Example

The following code snippet (from Chapter 5) was used to extract and rank nodes by degree centrality:

```
# Calculate degree centrality for the static network G
degree_centrality = nx.degree_centrality(G)

# Get the top 10 nodes
top_nodes = sorted(degree_centrality.items(), key=lambda x: x[1], reverse=True)[:10]
print("Top 10 Nodes by Degree Centrality:")

for node, centrality in top_nodes:
    print(f" {node}: {centrality:.4f}")
```

### Interpretation:

These top nodes likely represent the most active or influential terrorist groups and regions. Their central positions in the network imply that they are critical for communication and resource flow within the network. A targeted counterterrorism intervention focusing on these nodes could significantly disrupt network cohesion.

## 10.2 Evolution of Specific Sub-networks

### Objective

This section examines how specific parts of the overall terrorist network have evolved over time. By focusing on sub-networks—clusters or communities identified through community detection algorithms—we can study patterns such as the formation of new cells, the dissolution of old alliances, and shifts in operational control.

### Methodology

- **Temporal\_Slicing:**  
The network is divided into annual snapshots (as described in Chapter 7) to observe changes over the 2000–2020 period.
- **Community\_Detection:**  
Algorithms like the Louvain method are applied to each time slice to identify clusters within the network.
- **Comparative\_Analysis:**  
Changes in the composition, size, and connectivity of these sub-networks are compared over time.

## Findings

- **Emergence\_of\_New\_Cells:**  
In response to counterterrorism measures (e.g., leadership decapitation or targeted strikes), new sub-networks have emerged. For example, after a high-profile operation against the Al-Qaeda core, regional cells in Yemen and North Africa may have grown in influence.
- **Dissolution\_of\_Old\_Alliances:**  
Shifts in geopolitical conditions or successful counterterrorism interventions can lead to the fragmentation of previously cohesive groups.
- **Adaptation\_and\_Resilience:**  
Despite disruptions, the overall network often reconfigures itself quickly, demonstrating its adaptive and resilient nature.

## Illustrative Example

A visual representation of sub-network evolution might involve comparing network graphs from two different time periods. For instance, one graph could represent the network structure in 2005, while another shows the structure in 2015. Observing changes in node connectivity and community structure provides insights into how operational alliances have shifted.

## Interpretation:

Tracking these sub-networks over time allows analysts to identify critical transitional periods. It also helps in understanding how terrorist groups adapt to external pressures, thereby informing proactive counterterrorism strategies that anticipate rather than react to changes.

## **10.3 Cross-border Operations Analysis**

### **Objective**

Cross-border operations are a hallmark of transnational terrorism. This section investigates how terrorist networks span national boundaries, identifying the countries that serve as operational conduits and examining the strategic implications of these cross-border links.

### **Methodology**

- Bipartite\_and\_Projection\_Analysis:**

Using the bipartite graph from Chapter 6, the country projection is examined to identify links between nations. Shared perpetrator groups indicate potential cross-border operational relationships.

- Shortest\_Path\_Analysis:**

By computing the shortest paths between key countries, we can assess the ease of movement and communication within the network.

- Geospatial\_Context:**

Although individual coordinate data is not available, mapping country-level incident counts (as described in Chapter 9) supports the interpretation of these cross-border links.

### **Findings**

- Operational\_Hubs:**

Countries such as Pakistan and Afghanistan frequently appear as bridges in the network, facilitating the movement of operatives, logistics, and financial resources.

- Regional\_Clusters:**

The analysis may reveal that certain regions (e.g., the Horn of Africa or the Arabian Peninsula) function as interconnected clusters where cross-border operations are more prevalent.

- Strategic\_Vulnerabilities:**

Nations that are central in the cross-border network could be prioritized for international cooperation and targeted interventions to disrupt the flow of operations.

### **Interpretation:**

The shortest path analysis reveals the ease of connectivity between key operational countries. For example, a short path between Pakistan and Afghanistan suggests robust

logistical and communicative links, highlighting the strategic importance of these regions in cross-border terrorism. Such insights are critical for designing focused and coordinated international counterterrorism operations.

## **Conclusion**

The case studies presented in this chapter provide concrete examples of how advanced SNA techniques can be applied to the study of terrorist networks. By examining key nodes, tracking the evolution of sub-networks over time, and analyzing cross-border operations, we gain a multifaceted understanding of the operational dynamics of Al-Qaeda and its affiliates. These insights not only validate the findings from earlier chapters but also offer practical guidance for developing targeted counterterrorism strategies.

---

# CHAPTER 11

## DISCUSSION

In this chapter, we synthesize the findings from the static, bipartite, temporal, link prediction, geospatial, and case study analyses to offer a comprehensive interpretation of the terrorist network of Al-Qaeda and its affiliates from 2000 to 2020. We discuss the theoretical and practical implications of these findings for counterterrorism efforts, evaluate the methodological contributions of the study, and acknowledge the limitations that suggest directions for future research.

---

### 11.1 Synthesis of Findings

The multi-method approach adopted in this research has provided a nuanced understanding of Al-Qaeda's operational network. Key synthesized findings include:

- **Structural\_Complexity\_and\_Centralization:**  
The static network analysis revealed that while the overall network exhibits a decentralized pattern, certain nodes—such as the core Al-Qaeda organization, AQAP, and AQIM—consistently appear as central hubs. These nodes not only have high degree and eigenvector centralities but also serve as bridges (high betweenness centrality) between sub-networks.
- **Interconnected\_Bipartite\_Relationships:**  
The bipartite analysis highlighted significant relationships between perpetrator groups and the countries in which they operate. Projections of this bipartite graph into single-mode networks have revealed clusters of countries that share common threats and operational overlaps among terrorist groups, emphasizing the transnational character of these networks.
- **Temporal\_Evolution\_and\_Adaptability:**  
Temporal network analysis showed that the influence of key nodes shifts over time. Following major counterterrorism operations and geopolitical events, new sub-networks emerged while some previously dominant groups experienced declines in centrality. These dynamic changes underscore the network's resilience and capacity to adapt to external pressures.
- **Predictive\_Insights\_through\_Link\_Prediction:**  
The application of the Adamic/Adar index for link prediction indicated potential future collaborations among terrorist groups and between countries. This predictive layer, when combined with the observed network structure, offers early warnings for emerging operational alliances that could facilitate future attacks.

- **Geospatial\_Patterns\_and\_Regional\_Hotspots:**  
Although constrained by the absence of precise coordinate data, the country-level geospatial analysis (using incident counts) identified critical hotspots. Regions such as the Middle East, South Asia, and parts of Africa exhibited high frequencies of terrorist incidents, suggesting strategic importance and operational concentration.
- **Case\_Studies\_Reinforcing\_Quantitative\_Findings:**  
The in-depth case studies of key nodes, sub-network evolution, and cross-border operations further validate the quantitative analyses. They illustrate how the disruption or reinforcement of particular nodes (e.g., decapitation of leadership) leads to network reconfigurations and shifts in operational dynamics.

## 11.2 Theoretical Implications

The study contributes to several theoretical frameworks:

- **Social\_Network\_Theory\_and\_Terrorism:**  
The application of SNA confirms that terrorist networks, while decentralized, rely on a few highly influential nodes to maintain cohesion. This supports existing theories regarding the role of hubs and bridges in complex networks and extends them by incorporating dynamic and predictive dimensions.
- **Organizational\_Adaptation\_in\_Terrorist\_Networks:**  
Findings demonstrate that terrorist organizations are adaptive systems capable of rapid reorganization in response to counterterrorism interventions. This aligns with organizational theory models that emphasize resilience and flexibility over rigid hierarchy.
- **Diffusion\_of\_Innovation\_and\_Operational\_Tactics:**  
The temporal analysis underscores how new operational tactics and strategies diffuse through terrorist networks. The spread of innovations (such as new attack modalities) among groups provides evidence of the diffusion process, suggesting that counterterrorism strategies must anticipate rather than solely react to tactical changes.

## 11.3 Practical Implications for Counter-Terrorism

The insights derived from this study have significant practical applications:

- **Targeting Critical Nodes:**  
By identifying central nodes and bridges within the network, intelligence agencies can prioritize surveillance and intervention efforts. Disrupting these nodes could fragment the network and impede the flow of information and resources.

- **Anticipating Emerging Threats:**

The link prediction analysis offers a proactive tool for forecasting future alliances and operational links. Such predictive insights enable the preemption of emerging threats and inform strategic resource allocation.

- **Enhanced International Cooperation:**

The country-level geospatial analysis highlights regions that require coordinated international responses. Recognizing shared vulnerabilities can lead to more effective collaborative counterterrorism strategies among affected nations.

- **Dynamic Policy Formulation:**

Understanding the temporal dynamics of the network suggests that counterterrorism policies must be flexible and adaptive. Continuous monitoring and dynamic assessment of network changes are essential for maintaining effective countermeasures.

## 11.4 Methodological Contributions

This study makes several methodological contributions to the field of terrorism research:

- **Integration\_of\_Multiple\_SNA\_Techniques:**

By combining static, bipartite, temporal, link prediction, and geospatial analyses, the study offers a comprehensive framework that captures both the structural and dynamic aspects of terrorist networks.

- **Application\_of\_Predictive\_Modeling:**

The incorporation of link prediction techniques (using the Adamic/Adar index) represents an innovative approach to forecasting network evolution, providing a model that could be further refined with machine learning techniques in future research.

- **Bridging\_Quantitative\_and\_Qualitative\_Analysis:**

The inclusion of detailed case studies allows for a richer interpretation of quantitative data, thereby bridging the gap between abstract network metrics and real-world operational dynamics.

## 11.5 Limitations of the Study

Despite its contributions, the study has several limitations that should be acknowledged:

- **Data\_Constraints:**

The analysis is limited by the availability and quality of open-source data. In

particular, the absence of precise geographic coordinates restricts the granularity of the geospatial analysis.

- **Static\_vs.\_Dynamic\_Tensions:**

While temporal analysis was conducted, the dynamic nature of terrorist networks means that real-time changes may not be fully captured in a retrospective study.

- **Model\_Assumptions\_in\_Link\_Prediction:**

The predictive models assume that future network patterns will be similar to historical trends, which may not hold true in the face of unpredictable geopolitical shifts or counterterrorism successes.

- **Generalizability:**

The findings are specific to Al-Qaeda and its affiliates and may not be directly applicable to other terrorist networks with different organizational structures and operational contexts.

## Conclusion

In summary, the discussion chapter synthesizes the complex interplay between network structure, temporal dynamics, spatial distribution, and predictive modeling in understanding Al-Qaeda's terrorist network. The theoretical and practical implications underscore the importance of a multi-dimensional approach to counterterrorism that integrates both quantitative and qualitative insights. While the study advances our understanding and offers new tools for predictive analysis, its limitations highlight the need for ongoing research and methodological refinement in the rapidly evolving field of terrorism studies.

---

## CHAPTER 12

## CONCLUSION

This final chapter synthesizes the research and presents the overall conclusions drawn from the Social Network Analysis (SNA) of Al-Qaeda and its affiliates' terrorist activities from 2000 to 2020. It summarizes the key findings, directly addresses the research questions, outlines the contributions to the field, and provides recommendations for future research and practical applications.

---

### **12.1 Summary of Key Findings**

Over the course of this study, multiple analytical methods were applied to provide a comprehensive picture of Al-Qaeda's evolving terrorist network:

- **Static Network Analysis:**

The static analysis revealed that while the network exhibits a decentralized structure overall, certain nodes—such as the core Al-Qaeda organization, AQAP, and AQIM—consistently function as central hubs. These nodes demonstrate high centrality measures (degree, betweenness, closeness, and eigenvector), underscoring their pivotal roles in maintaining operational connectivity and information flow.

- **Bipartite Graph Analysis:**

By constructing a bipartite graph linking perpetrator groups and the countries where attacks occurred, the study uncovered strong transnational relationships. Projections of this bipartite network highlighted clusters of countries facing similar threats, as well as operational overlaps among terrorist groups, which are critical for understanding the cross-border dimensions of terrorism.

- **Temporal Network Analysis:**

The longitudinal study from 2000 to 2020 demonstrated that the network's structure is dynamic. Key nodes' influence shifts over time, often in response to counterterrorism interventions or geopolitical events. Emerging cells and the dissolution of established alliances were observed, illustrating the network's adaptability and resilience.

- **Link Prediction:**

Using the Adamic/Adar index, the analysis predicted potential future links among both countries and terrorist groups. These predictions suggest possible future

alliances or collaborations that could enhance the network's operational capacity, offering early-warning insights for counterterrorism efforts.

- **Geospatial Analysis:**

Although limited to country-level data, geospatial mapping revealed that regions such as the Middle East, South Asia, and parts of Africa have high incident counts. This spatial perspective, when combined with network metrics, provides a multidimensional understanding of where terrorist operations are most concentrated.

- **Case Studies:**

In-depth case studies further illustrated the practical implications of network disruptions, the evolution of specific sub-networks, and the dynamics of cross-border operations. These qualitative insights reinforce the quantitative findings and highlight critical vulnerabilities within the network.

## 12.2 Answers to Research Questions

1. **What are the structural characteristics of Al-Qaeda's network and its affiliates over time?**

The network is characterized by a mix of decentralized operational cells interconnected through key hubs. While the overall structure is sparse, core groups such as Al-Qaeda, AQAP, and AQIM consistently occupy central positions, acting as bridges and hubs that facilitate communication and resource flow.

2. **Who are the most influential actors (individuals/groups) in Al-Qaeda's network?**

The most influential nodes, as determined by various centrality measures, include the core Al-Qaeda organization and its primary affiliates. In addition, key countries—especially those in strategic regions like Pakistan, Afghanistan, and Yemen—emerge as critical nodes that support and sustain the network.

3. **How do terrorist alliances and relationships evolve over time?**

Temporal network analysis revealed that terrorist alliances are highly dynamic. Leadership decapitations, counterterrorism operations, and geopolitical shifts lead to rapid reconfigurations of the network, with new sub-networks emerging and older ones fragmenting or dissolving.

4. **Can we predict future connections within the network using link prediction models?**

The application of the Adamic/Adar index demonstrates promising predictive capabilities. High-scoring predicted links suggest that certain pairs of countries

and terrorist groups, currently unconnected, may form new operational ties in the future. This predictive layer provides actionable intelligence for proactive counterterrorism measures.

### 5. How do geospatial patterns influence Al-Qaeda's operations across different regions?

Geospatial analysis, based on country-level data, indicates that terrorist activities are highly concentrated in specific regions, notably the Middle East, South Asia, and parts of Africa. These patterns reflect strategic operational choices and the geopolitical realities of these regions, reinforcing the importance of considering geographic factors in network analyses.

## 12.3 Contributions to the Field

This dissertation makes several important contributions:

- **Methodological Innovation:**

By integrating static, bipartite, temporal, link prediction, and geospatial analyses, the study offers a comprehensive and multidimensional framework for analyzing terrorist networks. This approach enhances the application of SNA in counterterrorism research.

- **Theoretical Advancement:**

The findings validate and extend existing theories in social network analysis and organizational theory, particularly regarding the dynamics of decentralized terrorist networks. The work highlights how networks adapt to external pressures, contributing to a deeper theoretical understanding of organizational resilience in terrorism.

- **Practical Intelligence:**

The insights regarding key nodes, emerging alliances, and spatial concentration of attacks provide actionable intelligence for policymakers and counterterrorism agencies. The predictive aspects of the study, in particular, have the potential to inform early-warning systems and targeted interventions.

## 12.4 Recommendations for Future Research

While this study provides a robust framework, several areas warrant further exploration:

- **Enhanced Data Granularity:**

Future research should aim to incorporate more granular geospatial data (e.g., latitude and longitude) to allow for finer-scale spatial analysis and hotspot detection.

- **Integration of Additional Link Prediction Models:**  
Incorporating multiple algorithms (such as the Jaccard coefficient, Preferential Attachment, and machine learning approaches) could improve the robustness and accuracy of predictive models.
- **Real-time Network Dynamics:**  
Developing models that incorporate real-time or near-real-time data would enable dynamic monitoring of terrorist networks, allowing for more responsive counterterrorism measures.
- **Cross-Disciplinary Approaches:**  
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.
- **Application to Other Terrorist Networks:**  
Expanding the framework to analyze other transnational terrorist organizations could help validate and refine the methodologies developed in this study.

## 12.5 Concluding Remarks

This dissertation has provided a comprehensive analysis of the terrorist network of Al-Qaeda and its affiliates, employing a range of advanced SNA techniques to uncover the structural, temporal, and geospatial dimensions of their operations. The findings underscore the complexity and adaptability of modern terrorist networks, highlighting the critical role of key nodes and transnational relationships. 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.

---

## REFERENCE

1. Krebs, V. E. (2002). Mapping networks of terrorist cells. *Connections*, 24(3), 43–52.
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. F. (2012). Network Analysis of Terrorist Organizations. *Journal of Strategic Studies*, 35(5), 597–622.
5. Xu, J., & Chen, H. (2005). Criminal Network Analysis and Visualization. *Communications of the ACM*, 48(6), 100–107.
6. LaFree, G., & Dugan, L. (2009). Introducing the Global Terrorism Database (GTD). *Terrorism and Political Violence*, 21(1), 105–115.
7. RAND Corporation. (2020). RAND Database of Worldwide Terrorism Incidents. Retrieved from <https://www.rand.org/nsrd/projects/terrorism-incidents.html>
8. National Consortium for the Study of Terrorism and Responses to Terrorism (START). (2020). Global Terrorism Database (GTD). Retrieved from <https://www.start.umd.edu/gtd/>
9. National Counterterrorism Center. (2020). Annual Reports and Country Reports on Terrorism. Retrieved from <https://www.dni.gov/nctc/index.html>
10. United Nations Security Council. (2020). Reports on Global Terrorism and Sanctions Lists. Retrieved from <https://www.un.org/securitycouncil/ctc/reports>

# APPENDICES

## Appendix I: Data Collection and Cleaning Procedures

### Data Sources:

- **RAND Report:** Provides detailed records of terrorism incidents.
- **Global Terrorism Database (GTD):** Offers incident-level data on terrorist activities.
- **National Counterterrorism Center (NCTC) Reports:** Contains intelligence on terrorist networks and their affiliations.
- **United Nations (UN) Reports:** Provides information on transnational terrorism and related geopolitical factors.

### Cleaning and Preprocessing Steps:

#### 1. Standardization of Column Names:

A	B	C	D	E	F	G	H	I
Year	Country	Region	Attack Type	Weapon Type	Perpetrator Group	Fatalities	Injured	Leader/Mastermind
2000	Yemen	Middle East	USS Cole Bombing	Explosives	Al-Qaeda	17	39	Abd al-Rahim al-Nashiri
2000	Jordan	Middle East	Foiled Millennium Bomber	Explosives	Al-Qaeda	0	0	Abu Zubaydah
2000	Philippines	Southeast Asia	Ferry Bombing	Explosives	Abu Sayyaf Group	116	300	Khadaffy Janjalani
2000	Philippines	Southeast Asia	Jolo Hostage	Firearms	Abu Sayyaf Group	3	0	Khadaffy Janjalani
2001	India	South Asia	Indian Parliament	Firearms and Explosives	Jaish-e-Mohammed (LeT)	9	16	Afzal Guru
2001	United States	North America	9/11 Attacks	Aircraft (Hijacked)	Al-Qaeda	2996	6000	Osama bin Laden
2001	United States	North America	Anthrax Attack	Biological	Unknown (Al-Qaeda)	5	17	Unknown
2001	India	South Asia	Parliament Att	Firearms and Explosives	Jaish-e-Mohammed (LeT)	9	16	Masood Azhar
2001	United States	North America	Anthrax Attack	Biological Agent	Al-Qaeda-inspired	5	17	Bruce Ivins (suspected)
2001	India	South Asia	Indian Parliament	Firearms and Explosives	LeT	14	22	Abdullah Azzam

## A.1 Python Code: Data Loading and Preprocessing

```
C: > Users > sarth > OneDrive > Desktop > Untitled-4_SNA.py > ...
1 import pandas as pd
2 import networkx as nx
3 import matplotlib.pyplot as plt
4
5 # Load the data
6 file_path = r"C:\Users\sarth\Downloads\next_hundred_batch_data.xlsx"
7 data = pd.read_excel(file_path, sheet_name='Sheet1')
8 print(data.head())
9
```

PROBLEMS 13 OUTPUT DEBUG CONSOLE TERMINAL PORTS SIXTH JIRA GPT4

```
PS C:\Users\sarth> & C:/Users/sarth/AppData/Local/Programs/Python/Python312/python.exe c:/Users/sarth/SNA.py
   Year      Country      Region ... Fatalities Injured      Leader/Mastermind
0 2000       Yemen    Middle East ...        17      39     Abd al-Rahim al-Nashiri
1 2000       Jordan    Middle East ...         0       0          Abu Zubaydah
2 2000  Philippines Southeast Asia ...       116     300      Khadaffy Janjalani
3 2000  Philippines Southeast Asia ...         3       0      Khadaffy Janjalani
4 2001       India    South Asia ...         9      16          Afzal Guru

[5 rows x 9 columns]
PS C:\Users\sarth>
```

### 1 Creating The Node table:

Code:

```
10 # Extract unique values for each node type
11 perpetrator_groups = data['Perpetrator Group'].unique()
12 leaders = data['Leader/Mastermind'].unique()
13 countries = data['Country'].unique()
14
15 # Create the nodes table
16 nodes = pd.DataFrame({
17     'Node': list(perpetrator_groups) + list(leaders) + list(countries),
18     'Type': ([['Perpetrator Group']] * len(perpetrator_groups)) +
19             ([['Leader/Mastermind']] * len(leaders)) +
20             ([['Country']] * len(countries))
21 })
22
23 # Display the first few rows of the nodes table
24 print(nodes.head())
```

Output

PROBLEMS 13 OUTPUT DEBUG CONSOLE TERMINAL PORTS SIXTH JIRA GPT4

```
[5 rows x 9 columns]
              Node           Type
0            Al-Qaeda  Perpetrator Group
1        Abu Sayyaf Group  Perpetrator Group
2 Jaish-e-Mohammed (Al-Qaeda-linked)  Perpetrator Group
3 Unknown (Al-Qaeda suspected)  Perpetrator Group
4      Al-Qaeda-inspired  Perpetrator Group
```

## 2\_Create The Edges Table

We will create relationships (edges) between Perpetrator Groups, Leaders/Masterminds, and Countries. Here's the Python code for the edges table:

Code;

```
26 # Step 1: Create edges between Perpetrator Groups and Leaders
27 edges_groups_leaders = data[['Perpetrator Group', 'Leader/Mastermind']].rename(
28 |   columns={'Perpetrator Group': 'Source', 'Leader/Mastermind': 'Target'}
29 )
30 edges_groups_leaders['Relation'] = 'Group-Leader'
31
32 # Step 2: Create edges between Perpetrator Groups and Countries
33 edges_groups_countries = data[['Perpetrator Group', 'Country']].rename(
34 |   columns={'Perpetrator Group': 'Source', 'Country': 'Target'}
35 )
36 edges_groups_countries['Relation'] = 'Group-Country'
37
38 # Combine both edges tables
39 edges = pd.concat([edges_groups_leaders, edges_groups_countries], ignore_index=True)
40
41 # Display the first few rows of the edges table
42 print(edges.head())
```

Output;

	Source		Target		Relation
0	Al-Qaeda	Abd al-Rahim al-Nashiri			Group-Leader
1	Al-Qaeda		Abu Zubaydah		Group-Leader
2	Abu Sayyaf Group		Khadaffy Janjalani		Group-Leader
3	Abu Sayyaf Group		Khadaffy Janjalani		Group-Leader
4	Jaish-e-Mohammed (Al-Qaeda-linked)		Afzal Guru		Group-Leader

## Appendix II: Detailed Code for Network Analysis

This appendix contains the complete Python code used for performing the various analyses in the dissertation, including:

### B\_1\_Create and Visualize The Network Graph;

#### 1\_Create The Graph

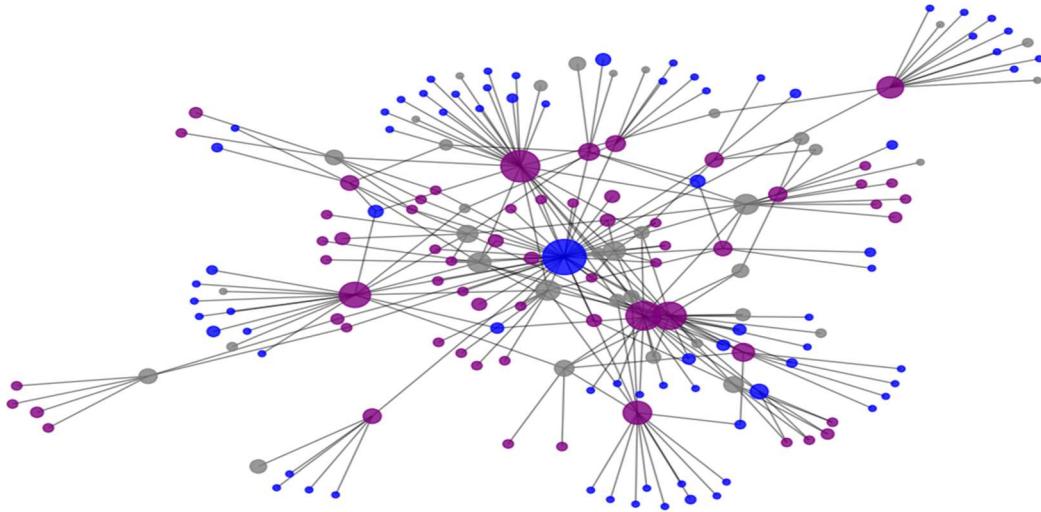
We will create the graph by filtering the top 10% nodes by degree centrality.

Code:

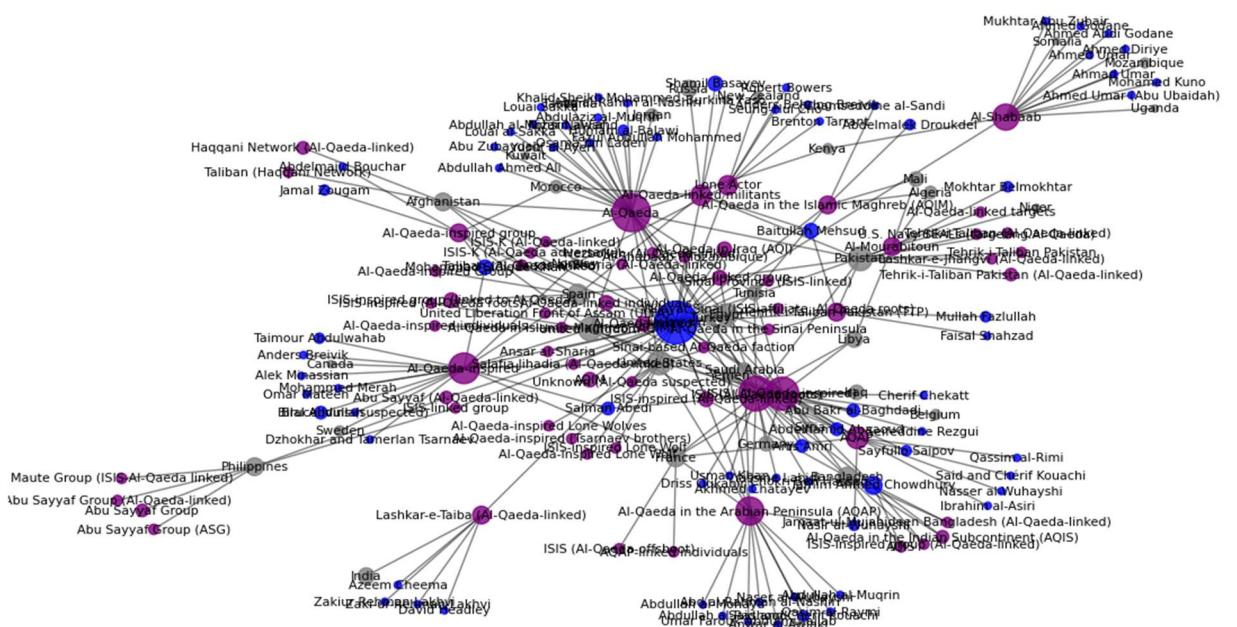
```
C: > Users > sarth > OneDrive > Desktop > Untitled-2_SNA.py > ...
1 import pandas as pd
2 import networkx as nx
3 import matplotlib.pyplot as plt
4
5 # Load and prepare the data
6 file_path = r"C:\Users\sarth\Downloads\next_hundred_batch_data.xlsx"
7 data = pd.read_excel(file_path, sheet_name='Sheet1')
8
9 # Create the initial network
10 group_to_leader = data[['Perpetrator Group', 'Leader/Mastermind']].dropna().drop_duplicates()
11 group_to_country = data[['Perpetrator Group', 'Country']].dropna().drop_duplicates()
12
13 # Combine group-to-leader and group-to-country data to form a comprehensive network
14 edges = pd.concat([
15     group_to_leader.rename(columns={'Perpetrator Group': 'Source', 'Leader/Mastermind': 'Target'}),
16     group_to_country.rename(columns={'Perpetrator Group': 'Source', 'Country': 'Target'})
17 ])
18
19 G = nx.Graph()
20 G.add_edges_from(edges.values)
21
22 # Assign node types (Group, Leader, Country)
23 nodes = pd.DataFrame({'Node': list(G.nodes())})
24 nodes['Type'] = nodes['Node'].apply(
25     lambda x: 'Group' if x in group_to_leader['Perpetrator Group'].values
26     else ('Leader' if x in group_to_leader['Leader/Mastermind'].values else 'Country')
27 )
28
29 # Define color map for node types
30 color_map = {'Group': 'purple', 'Leader': 'blue', 'Country': 'grey'}
~1
```

## Visualization routines using NetworkX and Matplotlib.

Filtered Terrorism Network (Top 10% by Degree Centrality)



Filtered Terrorism Network (Top 10% by Degree Centrality)

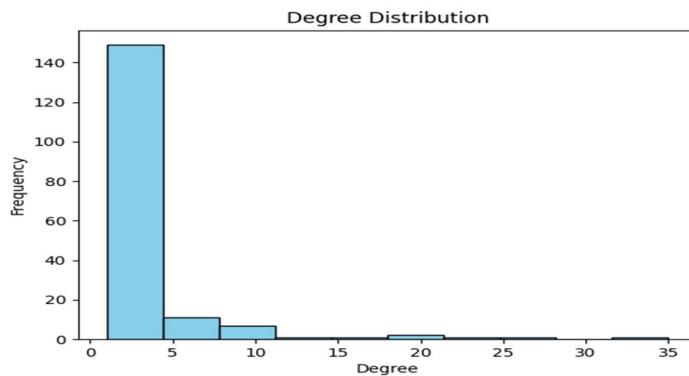


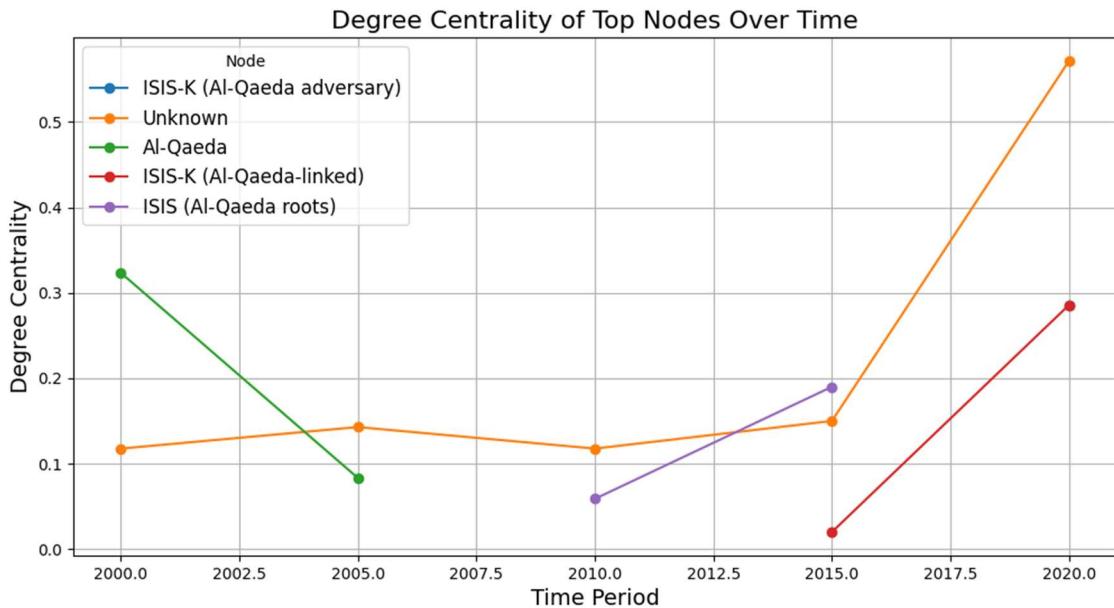
## B2\_Centrality Measure;

Code;

```
43 import networkx as nx
44 import pandas as pd
45 import matplotlib.pyplot as plt
46
47 # Assuming G is already constructed as in Appendix B
48
49 # Calculate centrality measures for the overall network
50 degree_centrality = nx.degree_centrality(G)
51 betweenness_centrality = nx.betweenness_centrality(G)
52 closeness_centrality = nx.closeness_centrality(G)
53 eigenvector_centrality = nx.eigenvector_centrality(G)
54
55 # Convert degree centrality to a DataFrame for further filtering
56 sna_metrics = pd.DataFrame({
57     'Node': list(degree_centrality.keys()),
58     'Degree Centrality': list(degree_centrality.values())
59 })
60
61 # For example, filter the top 10% nodes based on degree centrality
62 threshold = sna_metrics['Degree Centrality'].quantile(0.90)
63 top_nodes = sna_metrics[sna_metrics['Degree Centrality'] >= threshold]['Node']
64
65 print("Top 10% nodes by Degree Centrality:")
66 print(top_nodes)
67
68 # Display top 5 nodes for each centrality measure
69 print("Top 5 Nodes by Degree Centrality:", sorted(degree_centrality.items(), key=lambda x: x[1], reverse=True)[:5])
70 print("Top 5 Nodes by Betweenness Centrality:", sorted(betweenness_centrality.items(), key=lambda x: x[1], reverse=True)[:5])
71 print("Top 5 Nodes by Closeness Centrality:", sorted(closeness_centrality.items(), key=lambda x: x[1], reverse=True)[:5])
72 print("Top 5 Nodes by Eigenvector Centrality:", sorted(eigenvector_centrality.items(), key=lambda x: x[1], reverse=True)[:5])
73
74 # Optional: Visualize degree distribution
75 plt.figure(figsize=(12, 6))
76 degrees = [G.degree(n) for n in G.nodes()]
77 plt.hist(degrees, bins=10, color='skyblue', edgecolor='black')
78 plt.title("Degree Distribution")
79 plt.xlabel("Degree")
80 plt.ylabel("Frequency")
81 plt.show()
```

Output:





## **2\_Top nodes for each centrality Measures:**

### **a) Top 10 nodes for betweenness centrality;**

```
Top 10 nodes by Betweenness Centrality:
Unknown: 0.5534
Al-Qaeda: 0.2537
ISIS (Al-Qaeda roots): 0.1610
Al-Qaeda-inspired: 0.1606
ISIS (Al-Qaeda-inspired): 0.1374
United States: 0.1359
Al-Shabaab: 0.1256
Al-Qaeda in the Arabian Peninsula (AQAP): 0.1227
Pakistan: 0.0835
United Kingdom: 0.0650
Network Density: 0.0162
Modularity Score: 0.6584
```

### **b) Top 10 nodes for Degree Centrality;**

```

### Degree Centrality
1. **Node**: Unknown, **Centrality**: 0.14893617021276595
2. **Node**: Al-Qaeda, **Centrality**: 0.11914893617021277
3. **Node**: ISIS (Al-Qaeda roots), **Centrality**: 0.09787234042553192
4. **Node**: ISIS (Al-Qaeda-inspired), **Centrality**: 0.08936170212765958
5. **Node**: Al-Qaeda-inspired, **Centrality**: 0.07659574468085106
6. **Node**: Al-Qaeda in the Arabian Peninsula (AQAP), **Centrality**: 0.06382978723404255
7. **Node**: Al-Shabaab, **Centrality**: 0.055319148936170216
8. **Node**: United States, **Centrality**: 0.04680851063829787
9. **Node**: Pakistan, **Centrality**: 0.04680851063829787
10. **Node**: United Kingdom, **Centrality**: 0.0425531914893617

```

### c) Top 10 nodes for Closeness Centrality;

```

### Closeness Centrality
1. **Node**: Unknown, **Centrality**: 0.393140931114388
2. **Node**: Al-Qaeda, **Centrality**: 0.3331143795516207
3. **Node**: ISIS (Al-Qaeda roots), **Centrality**: 0.32440550688360453
4. **Node**: ISIS (Al-Qaeda-inspired), **Centrality**: 0.3191899842648971
5. **Node**: Al-Qaeda-inspired, **Centrality**: 0.3151367781155015
6. **Node**: Al-Qaeda in the Arabian Peninsula (AQAP), **Centrality**: 0.3017267024510121
7. **Node**: Al-Qaeda-linked militants, **Centrality**: 0.3017267024510121
8. **Node**: United States, **Centrality**: 0.2994512371233272
9. **Node**: Tehrik-i-Taliban Pakistan (TTP), **Centrality**: 0.29900025634452704
10. **Node**: Al-Qaeda-linked group, **Centrality**: 0.2936925594863402

```

### d) Top 10 nodes for Eigen Vector Centrality;

```

### Eigenvector Centrality
1. **Node**: Unknown, **Centrality**: 0.4322779600653765
2. **Node**: ISIS (Al-Qaeda roots), **Centrality**: 0.31235538520023914
3. **Node**: ISIS (Al-Qaeda-inspired), **Centrality**: 0.2920477744529914
4. **Node**: Al-Qaeda, **Centrality**: 0.2811563603390034
5. **Node**: United Kingdom, **Centrality**: 0.18523255742552983
6. **Node**: Al-Qaeda-inspired, **Centrality**: 0.17891672528338107
7. **Node**: Egypt, **Centrality**: 0.17662735482251296
8. **Node**: United States, **Centrality**: 0.14575450658910022
9. **Node**: Al-Qaeda in the Arabian Peninsula (AQAP), **Centrality**: 0.13449364676368655
10. **Node**: France, **Centrality**: 0.13437270365693346

```

## B2\_ Community Detection;

**Code;**

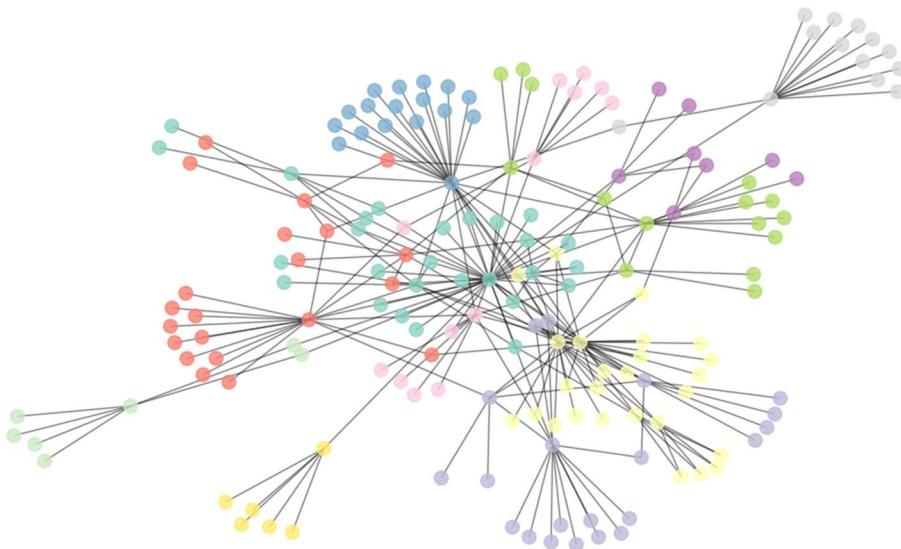
```

'~
73 # only community
74 import pandas as pd
75 import networkx as nx
76 import matplotlib.pyplot as plt
77 from networkx.algorithms.community import greedy_modularity_communities
78 from matplotlib.lines import Line2D
79
80 # Detect communities using the Greedy Modularity algorithm
81 communities = list(greedy_modularity_communities(G_filtered))
82
83 # Assign community labels
84 community_map = {}
85 for i, community in enumerate(communities):
86     for node in community:
87         community_map[node] = i
88
89 # Define a color map for communities
90 num_communities = len(communities)
91 cmap = plt.get_cmap('tab20') # Change to a different colormap if needed
92 community_colors = [cmap(i / num_communities) for i in range(num_communities)]
93
94 # Map nodes to their community colors
95 node_colors = [community_colors[community_map[node]] for node in G_filtered.nodes()]
96
97 # Create the plot
98 plt.figure(figsize=(14, 12))
99 pos = nx.spring_layout(G_filtered, seed=42)
100
101 # Draw nodes and edges
102 nx.draw_networkx_nodes(G_filtered, pos, node_color=node_colors, node_size=100, alpha=0.8)
103 nx.draw_networkx_edges(G_filtered, pos, alpha=0.5)
104
105 # Add node labels to the left of the network
106 for node, (x, y) in pos.items():
107     plt.text(x - 0.05, y, node, fontsize=8, ha='right', color='black')
108
109 # Create a legend for the communities
110 legend_elements = [
111     Line2D([0], [0], marker='o', color='w', markerfacecolor=community_colors[i], markersize=10, label=f'Community {i + 1}')
112     for i in range(num_communities)
113 ]
114 plt.legend(handles=legend_elements, loc='best', title='Communities', fontsize=10)
115
116 # Title and remove axes
117 plt.title("Community Detection in Terrorism Network (With Labels on the Left)", fontsize=16)
118 plt.axis('off')
119 plt.show()
120

```

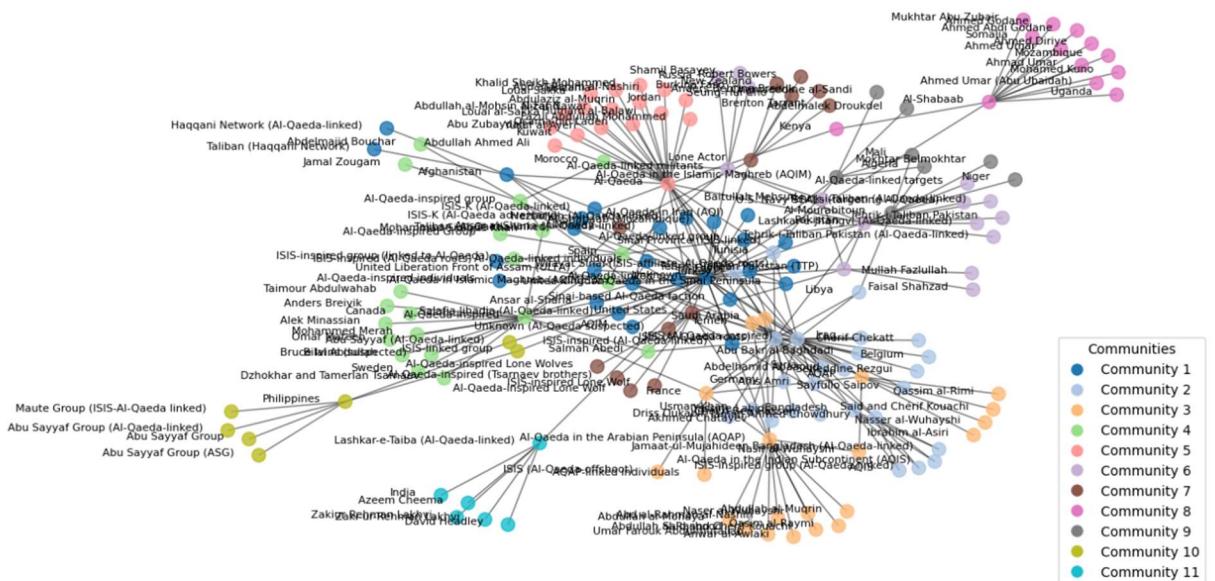
## Output;

Community Detection in Terrorism Network



(without label)

Community Detection in Terrorism Network (With Labels on the Left)



(with label)

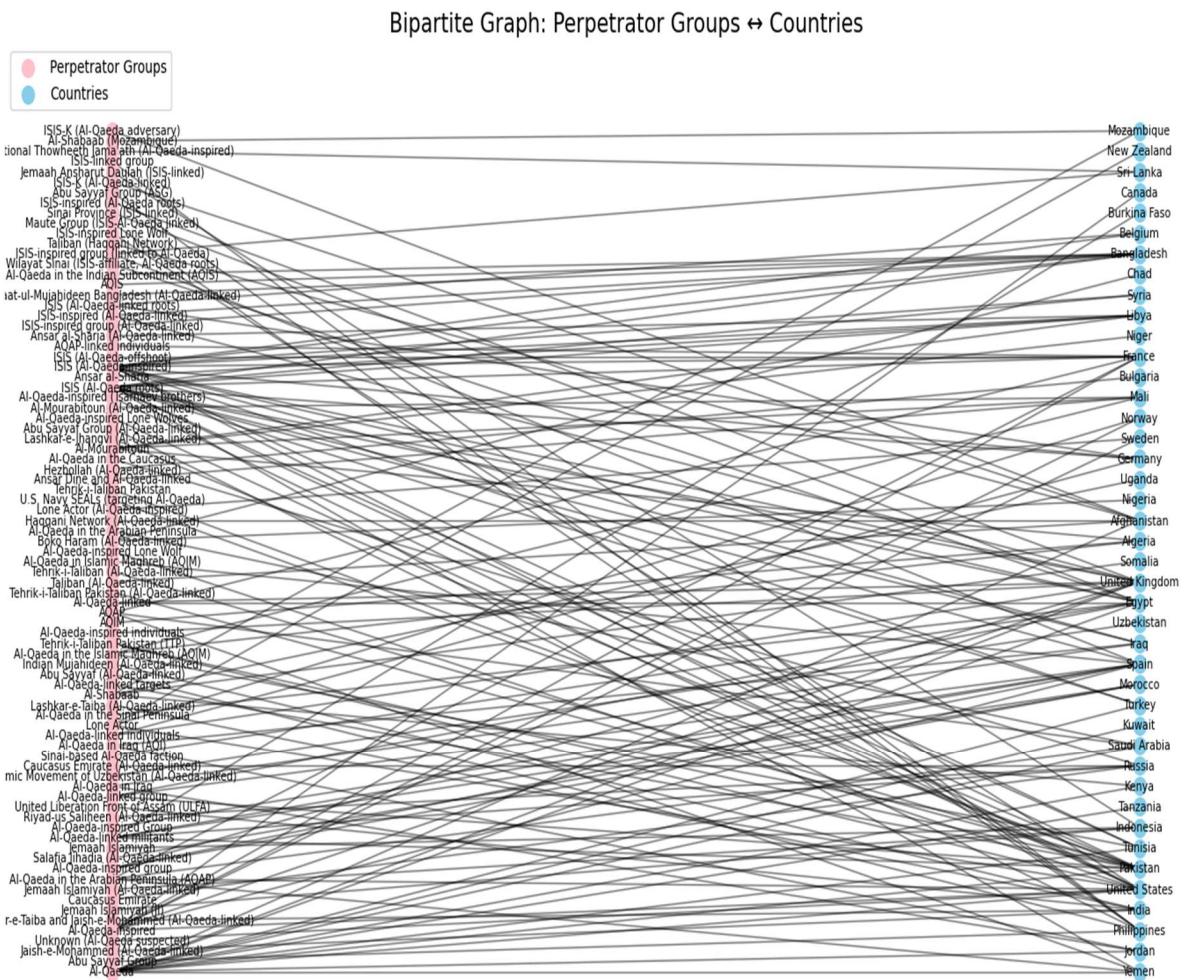
### B3\_ Bipartite Graph Analysis:

- Code for constructing and visualizing the bipartite graph linking perpetrator groups and countries.
- Code for projecting the bipartite graph into single-mode networks (country projection and perpetrator group projection).

Code;

```
C: > Users > sarth > OneDrive > Desktop > Bipartite_SNA.py > ...
1  import pandas as pd
2  import networkx as nx
3  import matplotlib.pyplot as plt
4
5  # Load the data
6  file_path = r"C:\Users\sarth\Downloads\next_hundred_batch_data.xlsx"
7  data = pd.read_excel(file_path, sheet_name='Sheet1')
8  # Create edges for bipartite graph (Group + Country example)
9  bipartite_edges = data[['Perpetrator Group', 'Country']].dropna().drop_duplicates()
10 print(bipartite_edges.head())
11 # Initialize a bipartite graph
12 B = nx.Graph()
13 B.add_edges_from(bipartite_edges.values)
14
15 # Add node attributes to distinguish the two sets
16 for node in bipartite_edges['Perpetrator Group'].unique():
17     B.nodes[node]['bipartite'] = 0 # Perpetrator Groups
18
19 for node in bipartite_edges['Country'].unique():
20     B.nodes[node]['bipartite'] = 1 # Countries
21
22 # Generate positions for bipartite layout
23 pos = nx.drawing.layout.bipartite_layout(B, nodes=bipartite_edges['Perpetrator Group'].unique())
24
25 # Extract nodes for each side
26 group_nodes = [node for node, data in B.nodes(data=True) if data['bipartite'] == 0]
27 country_nodes = [node for node, data in B.nodes(data=True) if data['bipartite'] == 1]
28
29 # Plot bipartite graph
30 plt.figure(figsize=(16, 12))
31 nx.draw_networkx_nodes(B, pos, nodelist=group_nodes, node_color='pink', label='Perpetrator Groups', node_size=200)
32 nx.draw_networkx_nodes(B, pos, nodelist=country_nodes, node_color='skyblue', label='Countries', node_size=200)
33 nx.draw_networkx_edges(B, pos, alpha=0.5)
34 nx.draw_networkx_labels(B, pos, font_size=8)
35
36 plt.title("Bipartite Graph: Perpetrator Groups + Countries", fontsize=16)
37 plt.legend(loc='upper left')
38 plt.axis('off')
39 plt.tight_layout()
40 plt.show()
41
```

Output;



### Temporal Network Analysis:

- Code for slicing the data by year, building annual network graphs, and computing centrality measures over time.
- Code for visualizing trends in degree centrality for top nodes across the 2000–2020 period.

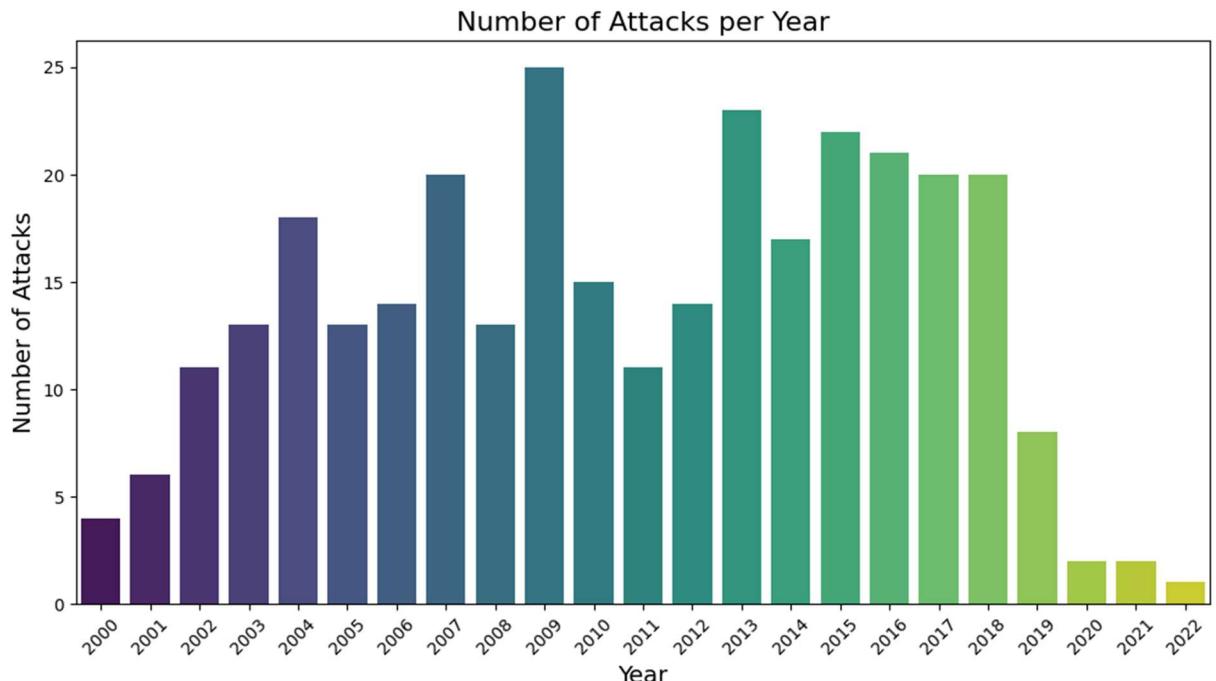
Code;

```

145
146     from networkx.algorithms.community.quality import modularity
147     modularity_score = modularity(G_filtered, communities)
148     print(f"Modularity Score: {modularity_score:.4f}")
149
150     years = data['Year'].unique()
151     for year in sorted(years):
152         yearly_data = data[data['Year'] == year]
153         yearly_edges = pd.concat([
154             yearly_data[['Perpetrator Group', 'Leader/Mastermind']].rename(columns={'Perpetrator Group': 'Source', 'Leader/Mastermind': 'Target'}),
155             yearly_data[['Perpetrator Group', 'Country']].rename(columns={'Perpetrator Group': 'Source', 'Country': 'Target'})
156         ])
157         G_year = nx.Graph()
158         G_year.add_edges_from(yearly_edges.dropna().values)
159         print(f"Year {year}: Nodes = {G_year.number_of_nodes()}, Edges = {G_year.number_of_edges()}")
160
161     import seaborn as sns # type: ignore
162
163     # Count the number of incidents per year
164     yearly_counts = data['Year'].value_counts().sort_index()
165
166     # Plot a bar chart
167     plt.figure(figsize=(12, 6))
168     sns.barplot(x=yearly_counts.index, y=yearly_counts.values, palette="viridis")
169     plt.title("Number of Attacks per Year", fontsize=16)
170     plt.xlabel("Year", fontsize=14)
171     plt.ylabel("Number of Attacks", fontsize=14)
172     plt.xticks(rotation=45)
173     plt.show()

```

## Output:



## 2. Link Prediction:

- o Code implementing the Adamic/Adar index on projected networks.

- o Code for sorting and displaying the top predicted links.
- o Code for shortest path analysis between specified nodes (e.g., between Pakistan and Afghanistan).

### Code:

```
# --- Bipartite Link Prediction using Preferential Attachment ---
def bipartite_preferential_attachment(graph):
    predictions = []
    group_nodes = {n for n, d in graph.nodes(data=True) if d['bipartite']==0}
    country_nodes = set(graph.nodes) - group_nodes

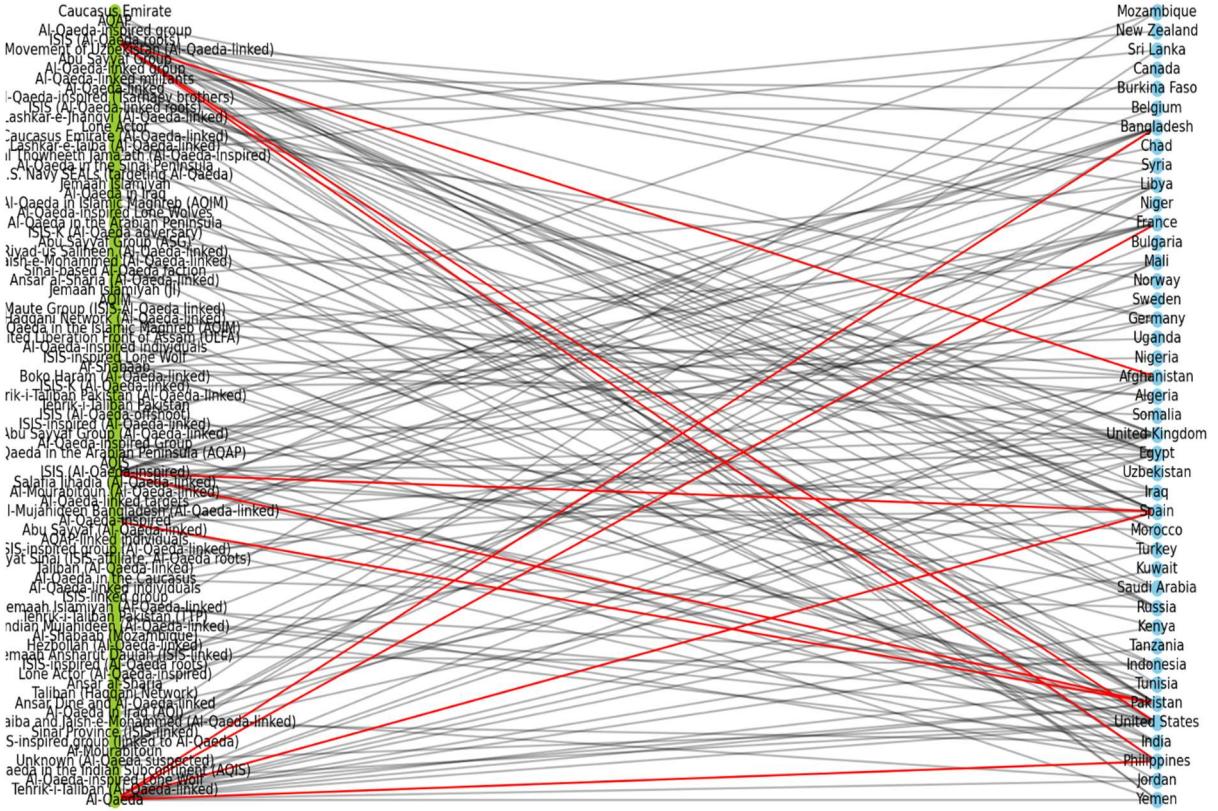
    for group in group_nodes:
        for country in country_nodes:
            if not graph.has_edge(group, country):
                score = graph.degree(group) * graph.degree(country)
                predictions.append((group, country, score))

    return sorted(predictions, key=lambda x: x[2], reverse=True)

# Get top predictions
top_predictions = bipartite_preferential_attachment(B)[:10]

# Create prediction graph
prediction_graph = B.copy()
prediction_graph.add_edges_from((u, v) for u, v, _ in top_predictions)

# Visualization with predicted edges
plt.figure(figsize=(16, 12))
nx.draw_networkx_nodes(prediction_graph, pos, nodelist=group_nodes, node_color='green', node_size=200)
nx.draw_networkx_nodes(prediction_graph, pos, nodelist=set(B.nodes)-group_nodes, node_color='skyblue', node_size=200)
nx.draw_networkx_edges(prediction_graph, pos, edgelist=B.edges, alpha=0.3)
nx.draw_networkx_edges(prediction_graph, pos, edgelist=top_predictions, edge_color='red', width=2)
nx.draw_networkx_labels(prediction_graph, pos, font_size=8)
plt.title("Bipartite Graph with Top 10 Predicted Links (Red)", fontsize=16, pad=20)
plt.axis('off')
plt.show()
```



## Country projection and Group projection

### Projected links between countries

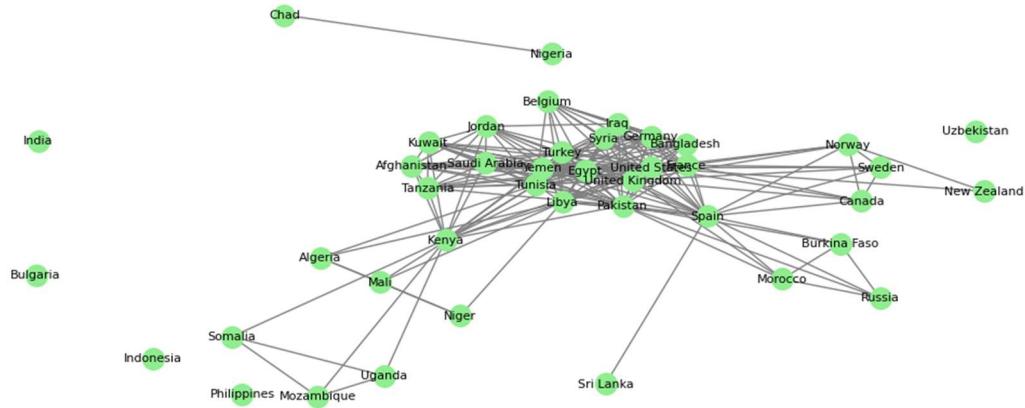
```
# Country projection
country_projection = bipartite.weighted_projected_graph(B, [n for n, d in B.nodes(data=True) if d['bipartite']==1])

plt.figure(figsize=(12, 8))
pos = nx.spring_layout(country_projection, k=0.8, seed=42)
nx.draw(country_projection, pos, with_labels=True, node_color='lightgreen',
       edge_color='gray', node_size=200, font_size=8)
plt.title("Country Projection Network", fontsize=14, pad=15) # Explicit title command
plt.show()

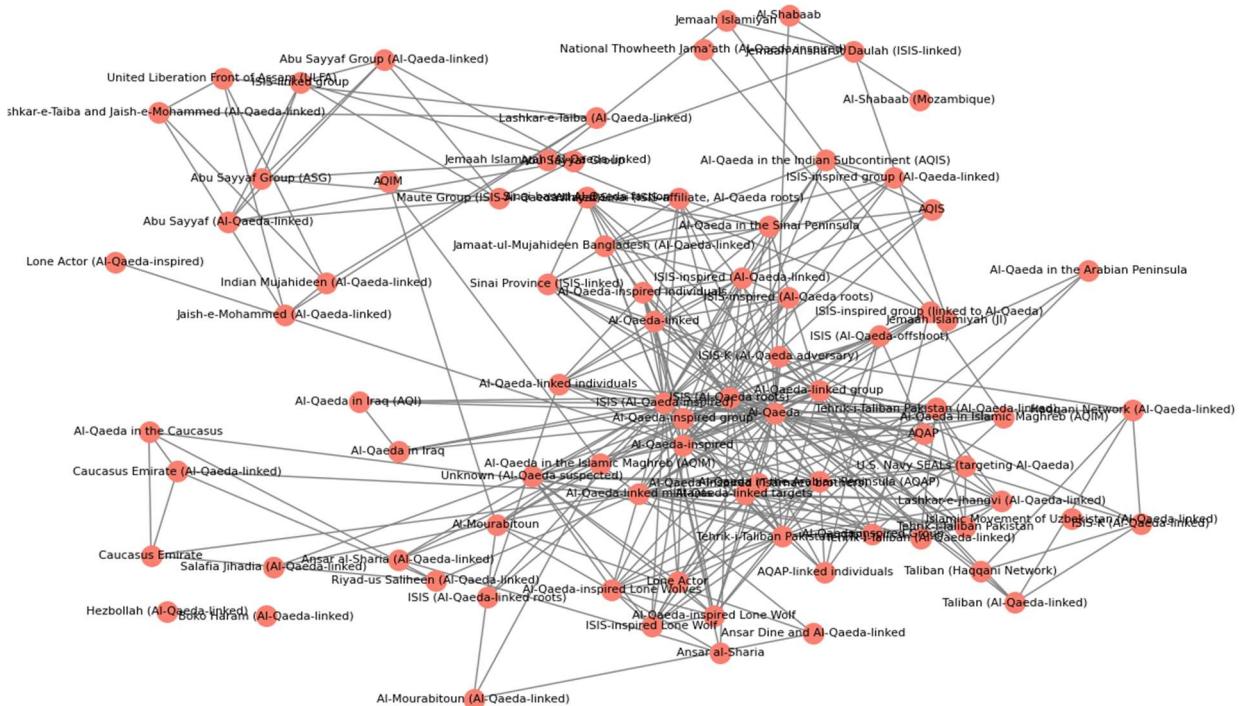
# Group projection
group_projection = bipartite.weighted_projected_graph(B, [n for n, d in B.nodes(data=True) if d['bipartite']==0])

plt.figure(figsize=(12, 8))
pos = nx.spring_layout(group_projection, k=0.8, seed=42)
nx.draw(group_projection, pos, with_labels=True, node_color='salmon',
       edge_color='gray', node_size=200, font_size=8)
plt.title("Perpetrator Group Projection Network", fontsize=14, pad=15)
plt.show()
```

## Country projection



## Group projection



## **Shortest path between two given countries**

```

# --- Shortest Path Analysis (with corrected spelling) ---
G = country_projection
source = "Pakistan"
target = "Afghanistan"

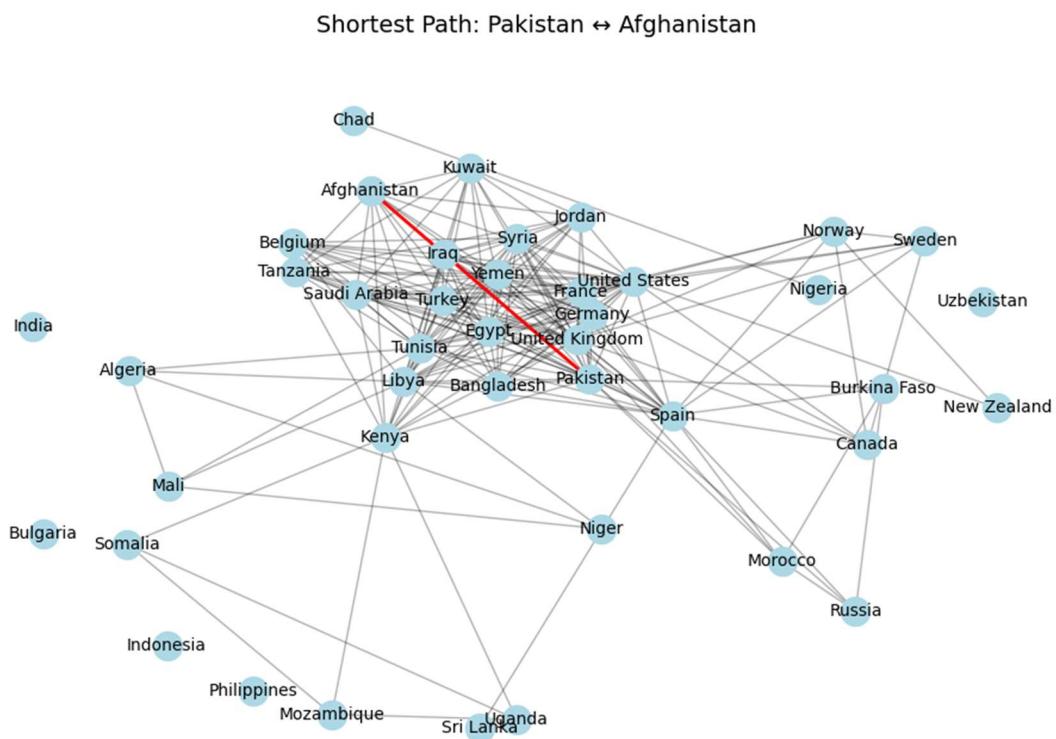
try:
    path = nx.shortest_path(G, source=source, target=target)

    plt.figure(figsize=(12, 8))
    pos = nx.spring_layout(G, seed=42, k=1.2) # Increased k for longer edges

    nx.draw_networkx_edges(G, pos, alpha=0.3)
    nx.draw_networkx_nodes(G, pos, node_color='lightblue', node_size=300)
    nx.draw_networkx_labels(G, pos, font_size=10)
    nx.draw_networkx_edges(G, pos, edgelist=list(zip(path, path[1:])),
                           edge_color='red', width=2)

    plt.title(f"Shortest Path: {source} ↔ {target}", fontsize=14, pad=15)
    plt.axis('off')
    plt.show()
except nx.NetworkXNoPath:
    print(f"No path between {source} and {target}")

```



### 3. Geospatial Analysis:

- o Code for aggregating incident counts by country.
- o Code for merging the incident data with a global shapefile from GeoPandas and creating a choropleth map.
- o Code for generating an interactive map using Folium to visualize country-level terrorist incident data.

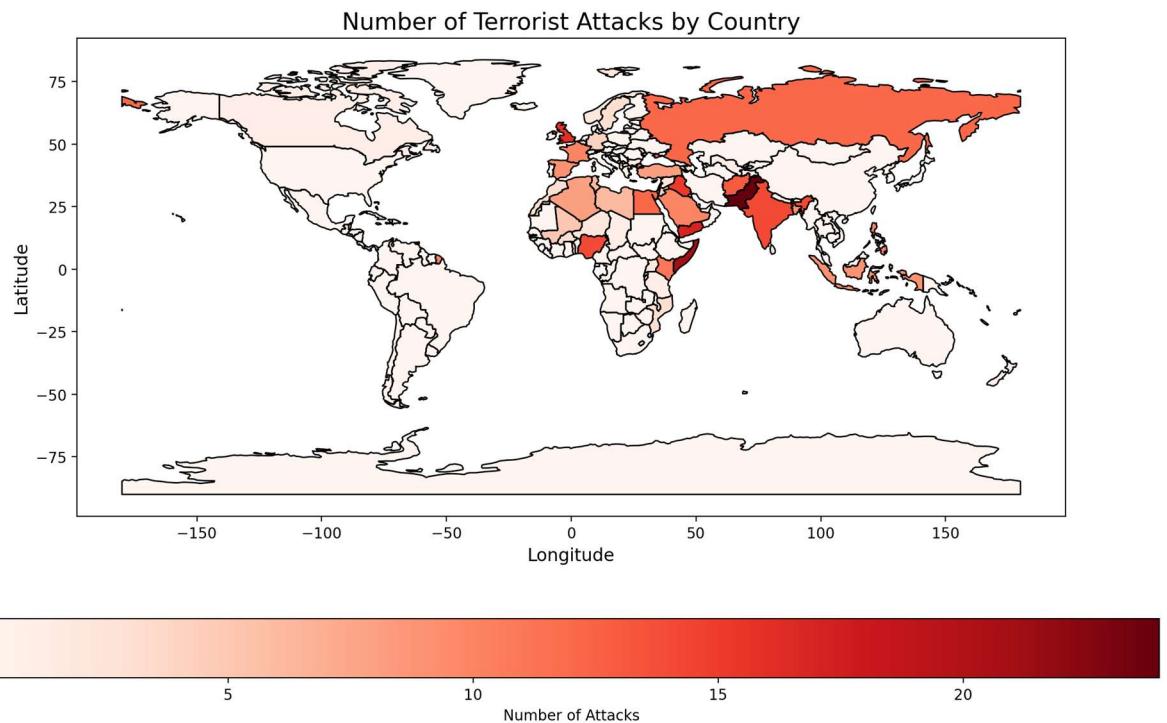
```
1 import pandas as pd
2 import geopandas as gpd
3 import matplotlib.pyplot as plt
4 from shapely.geometry import LineString
5
6 # Load the dataset
7 file_path = r"C:\Users\sarth\Downloads\next_hundred_batch_data.xlsx"
8 data = pd.read_excel(file_path, sheet_name='Sheet1')
9
10 # Check required columns
11 if not {'Perpetrator Group', 'Country'}.issubset(data.columns):
12     raise ValueError("The dataset must contain 'Perpetrator Group' and 'Country' columns.")
13
14 # Drop missing values
15 data = data.dropna(subset=['Perpetrator Group', 'Country'])
16
17 # Load Natural Earth data
18 natural_earth_path = r"C:\Users\sarth\Downloads\ne_110m_admin_0_countries (1)\ne_110m_admin_0_countries.shp"
19 world = gpd.read_file(natural_earth_path)
20
21 # Normalize country names for matching
22 world['NAME'] = world['NAME'].str.lower()
23 data['Country'] = data['Country'].str.lower()
24
25 # Count occurrences of attacks per country
26 attacks_per_country = data.groupby('Country').size().reset_index(name='Attack Count')
27
28 # Merge with world GeoDataFrame
29 world = world.merge(attacks_per_country, how='left', left_on='NAME', right_on='Country')
30 world['Attack Count'] = world['Attack Count'].fillna(0) # Ensure missing values are handled
31
32 # Plot attacks by country
33 plt.figure(figsize=(14, 10))
34 world.boundary.plot(ax=plt.gca(), linewidth=1, color='black')
35 world.plot(column='Attack Count', ax=plt.gca(), legend=True,
36             legend_kwds={'label': "Number of Attacks", 'orientation': "horizontal"},
37             cmap='Reds')
38
39 plt.title("Number of Terrorist Attacks by Country", fontsize=16)
40 plt.xlabel("Longitude", fontsize=12)
41 plt.ylabel("Latitude", fontsize=12)
42 plt.show()
```

```

43
44 # Create geospatial network connections (optional)
45 group_country_pairs = data[['Perpetrator Group', 'Country']].drop_duplicates()
46
47 lines = []
48 for _, row in group_country_pairs.iterrows():
49     if row['Country'] in world['NAME'].values:
50         country_geom = world.loc[world['NAME'] == row['Country'], 'geometry'].values[0]
51         country_point = country_geom.centroid
52         group_point = country_point # Groups are not geolocated, so approximate
53         lines.append(LineString([group_point, country_point]))
54
55 # Create GeoDataFrame for lines
56 lines_gdf = gpd.GeoDataFrame(geometry=lines)
57
58 # Plot geospatial network connections
59 plt.figure(figsize=(14, 10))
60 world.boundary.plot(ax=plt.gca(), linewidth=1, color='black')
61 lines_gdf.plot(ax=plt.gca(), color='blue', linewidth=0.5, alpha=0.7, label='Connections')
62
63 plt.title("Geospatial Network of Terrorism (Group to Country)", fontsize=16)
64 plt.xlabel("Longitude", fontsize=12)
65 plt.ylabel("Latitude", fontsize=12)
66 plt.legend()
67 plt.show()
68

```

(





## ICCCNet 2025: Paper Notification 807

1 message

**ICCCNet Congress - MMU, UK <icccn.congress@gmail.com>**  
To: Shivanisingh 23mscmat <shivanisingh\_23mscmat42@dtu.ac.in>

Sat, 12 Apr, 2025 at 14:16

International Conference on Computing and Communication Networks 2025: ICCCNet 2025

**Dear Author(s),**

Greetings from ICCCNet 2025!

ICCCNet-2025 team is pleased to inform you that your paper with submission ID 807 and Paper Title 'MAPPING THE TERROR: A SOCIAL NETWORK ANALYSIS OF AL-QAEDA AND ITS AFFILIATES' OPERATIONS' has been accepted for presentation at "ICCCNet2025" and for publication in the conference proceedings. The Committee thanks you for your contribution.

The conference proceedings will be published by Springer in Lecture Notes in Networks and Systems series [Indexing: SCOPUS, INSPEC, WTI Frankfurt eG, zbMATH, SCImago; All books published in the series are submitted for consideration in Web of Science]. This acceptance means that your paper is among the top 15% of the papers received/reviewed. The registrations for the conference are open. **We want to provide you with urgent information and advise you that we have limited slots available, and once they are filled, we will not be able to accommodate any further registrations. To secure your spot at this highly anticipated event, we urge you to complete your registration without delay.**

You are requested to do the registration as soon as possible and submit the following documents to [icccn.congress@gmail.com](mailto:icccn.congress@gmail.com) at the earliest.

1. Final Camera-Ready Copy (CRC) as per the springer format. (See <https://icccn.co.uk/Downloads>)
2. Copy of e-receipt of registration fees. (For Registration, see <https://icccn.co.uk/Registration>)
3. The final revised copy of your paper should also be uploaded via Microsoft CMT.

**The reviewers comments are given at the bottom of this letter, please improve your paper as per the reviewers comments.**

The paper prior to submission should be checked for plagiarism and AI Plagiarism from licensed plagiarism softwares like Turnitin/iAuthenticate etc. The similarity content should not exceed 15% and AI similarity should not exceed 5%.

**Pay registration fees via online portal:**

[Kindly note – the conference being organised in Hybrid Mode and you can choose the mode of presentation in either physical (offline) or digital (online) mode; then pay the registration fees]

<https://icccn.co.uk/Registration>

**Once you pay the registration fees, kindly fill the following google form:**

<https://forms.gle/6jFAE6dkLuogPvJz6>

**With Regards  
Conference Chair**

# main 41 42.pdf

 Delhi Technological University

## Document Details

Submission ID	73 Pages
trn:oid:::27535:97573028	10,535 Words
Submission Date:	66,392 Characters
May 25, 2025, 8:35 AM GMT+5:30	
Download Date	
May 25, 2025, 8:36 AM GMT+5:30	
File Name	
main 41 42.pdf	
File Size	
7.5 MB	



Page 1 of 78 - Cover Page

Submission ID trn:oid:::27535:97573028



Page 2 of 78 - Integrity Overview

Submission ID trn:oid:::27535:97573028

## 7% Overall Similarity

The combined total of all matches, including overlapping sources, for each database.

### Filtered from the Report

- ▶ Bibliography
- ▶ Quoted Text
- ▶ Small Matches (less than 10 words)

### Match Groups

-  31 Not Cited or Quoted 7%  
Matches with neither in-text citation nor quotation marks
-  3 Missing Quotations 0%  
Matches that are still very similar to source material
-  0 Missing Citation 0%  
Matches that have quotation marks, but no in-text citation
-  0 Cited and Quoted 0%  
Matches with in-text citation present, but no quotation marks

### Top Sources

- 6%  Internet sources
- 1%  Publications
- 6%  Submitted works (Student Papers)

### Integrity Flags

#### 0 Integrity Flags for Review

No suspicious text manipulations found.

Our system's algorithms look deeply at a document for any inconsistencies that would set it apart from a normal submission. If we notice something strange, we flag it for you to review.

A Flag is not necessarily an indicator of a problem. However, we'd recommend you focus your attention there for further review.