NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

TERRORISM FROM A GLOBAL PERSPECTIVE: INFLUENCE AND NETWORK STRUCTURE ANALYSIS

by

Ee Hong Aw

September 2018

Thesis Advisor: Ralucca Gera
Co-Advisor: Michelle L. Isenhour

Approved for public release. Distribution is unlimited.

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			*Form Approved OMB No. 0704-0188*

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington, DC 20503.

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** September 2018	**3. REPORT TYPE AND DATES COVERED** Master's thesis

4. TITLE AND SUBTITLE TERRORISM FROM A GLOBAL PERSPECTIVE: INFLUENCE AND NETWORK STRUCTURE ANALYSIS	**5. FUNDING NUMBERS**
6. AUTHOR(S) Ee Hong Aw	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	**10. SPONSORING / MONITORING AGENCY REPORT NUMBER**

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release. Distribution is unlimited.	**12b. DISTRIBUTION CODE** A

13. ABSTRACT (maximum 200 words)

While terrorism is not new, today's terrorist threat is different from that of the past. Terrorism has evolved, and terrorist groups today are more structured and better organized. Modern technology enables terrorists to plan and operate worldwide as never before. Through the constant exchange of information between parties, perpetrator groups may influence or be influenced by other perpetrator groups to improve their efficacy. This study moves away from the traditional analysis of terrorist groups and examines terrorist networks from a global perspective. Using network science and our proposed methodology to calculate influence strength, this thesis looks at the extent of influence of one perpetrator group with another based on their activities and locations. We observe that some perpetrator groups, like ISIL and Al–Nusrah Front, have high and increasing influence strength. Some of these perpetrator groups are, from a network science perspective, neighbors. In addition, the community detection algorithm shows that most of the perpetrator groups with high influence strength exist within the same network-defined community. Our proposed influence score metric allows measurement of a node's actual influence score based on the responses of other nodes around it, as compared to existing measures, which determine the node's influential strength by its position in the network. We hope our study provides insights into terrorism and how influence spreads among perpetrators.

14. SUBJECT TERMS network science, terrorist networks, network analysis	**15. NUMBER OF PAGES** 75
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	**18. SECURITY CLASSIFICATION OF THIS PAGE**	**19. SECURITY CLASSIFICATION OF ABSTRACT**	**20. LIMITATION OF ABSTRACT**
Unclassified	Unclassified	Unclassified	UU

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89) Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

TERRORISM FROM A GLOBAL PERSPECTIVE: INFLUENCE AND NETWORK STRUCTURE ANALYSIS

Ee Hong Aw
Major, Singapore Army
BE, Nanyang Technological University, 2013

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN APPLIED MATHEMATICS

from the

NAVAL POSTGRADUATE SCHOOL
September 2018

Approved by: Ralucca Gera
Advisor

Michelle L. Isenhour
Co-Advisor

Wei Kang
Chair, Department of Applied Mathematics

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

While terrorism is not new, today's terrorist threat is different from that of the past. Terrorism has evolved, and terrorist groups today are more structured and better organized. Modern technology enables terrorists to plan and operate worldwide as never before. Through the constant exchange of information between parties, perpetrator groups may influence or be influenced by other perpetrator groups to improve their efficacy. This study moves away from the traditional analysis of terrorist groups and examines terrorist networks from a global perspective. Using network science and our proposed methodology to calculate influence strength, this thesis looks at the extent of influence of one perpetrator group with another based on their activities and locations. We observe that some perpetrator groups, like ISIL and Al–Nusrah Front, have high and increasing influence strength. Some of these perpetrator groups are, from a network science perspective, neighbors. In addition, the community detection algorithm shows that most of the perpetrator groups with high influence strength exist within the same network-defined community. Our proposed influence score metric allows measurement of a node's actual influence score based on the responses of other nodes around it, as compared to existing measures, which determine the node's influential strength by its position in the network. We hope our study provides insights into terrorism and how influence spreads among perpetrators.

THIS PAGE INTENTIONALLY LEFT BLANK

Table of Contents

List of Figures

THIS PAGE INTENTIONALLY LEFT BLANK

List of Tables

THIS PAGE INTENTIONALLY LEFT BLANK

List of Acronyms and Abbreviations

GTD	Global Terrorism Database
ISIL	Islamic State of Iraq and the Levant
START	Study of Terrorism and Responses to Terrorism
TTP	Tehrik-i-Taliban Pakistan
TVG	Time-Varying Graph

THIS PAGE INTENTIONALLY LEFT BLANK

Executive Summary

Network science has gained much traction in today's academic field. Researchers have applied many mathematical and analytical tools from the field of network science to allow the visualization of large data sets in the form of a mathematical model. In the digital age, we exchange information, opinions, and attitudes, and in the process of interaction, impart influence on each other.

Influence is a complex dynamic process, which evolves with the structure of the network. As such, influence and network structure are closely related. Existing algorithms such as eigenvalue centrality, closeness centrality, and betweenness centrality, can be implemented in a network to identify influential nodes. However, none of these algorithms account for the response or modification of behavior due to influence, hence may not be reflective of a node's actual influential strength.

This thesis leverages a large amount of terrorist data and examines terrorism. Unlike much of the other research which focuses on individual perpetrator groups, this thesis views terrorism from a global perspective. We believe that perpetrator groups are exchanging information with each other, thereby influencing each other in their operations. We propose a method to rank the influence strength of each perpetrator group by developing a scoring metric based on the location of operations, as well as the similarities and differences between their operations. In the process, we identify certain perpetrator groups of key interest.

We believe that perpetrators of terrorism have grown more networked and complex in nature. Our research can help in identifying perpetrator groups which show high and increasing influence strength, which can then allow the channeling of resources to isolate these groups, thus disrupting influence and information spreading among the terrorist network.

THIS PAGE INTENTIONALLY LEFT BLANK

Acknowledgments

This thesis would not have been possible without the support of my family. Special thanks to my girlfriend, Leticia, who has been more than a source of motivation throughout my time here at the Naval Postgraduate School.

I would also like to thank my thesis advisors, Professor Ralucca Gera, and LTC Michelle Isenhour, for their precious guidance in this arduous intellectual journey of discovery. Both the advisors have invested a lot of time in the development of this thesis. The weekly discussions with my advisors have helped me view my research from different perspectives, enlightened my knowledge, and improved the overall quality of this thesis.

THIS PAGE INTENTIONALLY LEFT BLANK

CHAPTER 1:
Introduction

Around 280 years ago in 1736, Leonhard Euler wrote a historical paper entitled "Seven Bridges of Königsberg," which laid the foundation of graph theory, and later on served as the foundation of network science in mathematical academia. The problem facing Euler was to devise a way to walk to all parts of the city by walking across all the bridges once and only once. Euler proved that there is no solution to the problem [1]. Since then, graph theory has been a focus area for mathematicians, and later the ideas of graph theory expanded across many disciplinary fields to give rise to network science, with applications of neural networks in medical fields, social behavior in sociology, and airline networks in transportation.

Today, the evolution of technology has brought mankind closer together. With the established roads, railways, sea line of communications, and air lines, we are able to commute to places around the world faster. Not only have transportation systems improved, communications technology has also pushed boundaries. Social media platforms, such as Facebook and Twitter, have allowed users to be informed on the latest news trending on the other side of the world with a simple press of the finger. The spread of such information may effect changes in our behaviors and perspectives as individuals, communities or at a larger scale, society.

In the digital age, we exchange information, opinions, and attitudes, and in the process of interaction, impart influence on each other. Influence is a complex dynamic process, which evolves with the structure of the network. It intertwines with many other factors that may determine how influence spreads across a network. Our attitude and behaviors are shaped by those who influence us or by our ability to influence others. The inherent ability to model complex interactions and flow characteristics using network science may enable network science techniques to become a leading approach to understanding how ideology and influence spread. On the surface, influence defines the basic structure of the network. Beneath it, lie the characteristics and intertwined relationships defining dynamic complex behavior and individual attitudes of each actor in an ever-evolving environment.

Network science has gained much traction in academia. With today's technology, coupled with the ability to collect large amounts of data from the digital world, we can leverage information availability to study and understand dynamic complex problems faced by the world today. The digital era provides an opportunity for us to observe and study human behavior at a wider and larger scale.

We can model interactions using tools from network science. Each entity can be visually described as a node or vertex, and any two entities that are related by certain attributes can form a connection or edge with each other. Expanding such a model to a wider database of entities will turn the model into a graph, which enables us to study the properties of the graph. For example, we can categorize the nodes into different communities, or identify nodes with special importance. The most important decision when modeling with network science is to identify the type of attributes which determine the relationship between two nodes. For example, when determining a terrorist network, we can arrange perpetrator groups based on certain attributes such as location of attacks, casualties, types of attacks or lifespan of the groups. Different attributes will result in different connections, giving rise to different graphs. Depending on the objectives and goal of the research, one arrangement may be more appropriate than the other.

1.1 Problem Description

Terrorism remains as one of the greatest threats that national security faces today. Added to the increasing complex security landscape, the rapid evolution of terrorism is partially a result of rapid technological advancement. The threat is further exacerbated with countries such as Iran sponsoring terrorism, destabilizing regions around the world [2]. Terrorism remains as a dire condition driven by extreme ideology in regions with unstable political, economical and social structures. Such trans-boundary activity threatens peace and stability at home, making it a pertinent issue to be addressed by every country in the world. With an objective of assisting the 2018 US National Defense Strategy in preventing terrorism, we set out to investigate how perpetrator groups form a network of influence at the global view. In this paper, we examine how the influence of a perpetrator group can affect other perpetrator groups, and in the process, we will identify certain perpetrator groups of interest.

Influence is "a special instance of causality namely, the modification of one person's re-

sponses by the action of another" [3]. It does not require constant and deliberate attempts to change an actor's behavior or attitude. At times, it could be a spontaneous imitation of others by observing the action of others and their outcomes [4].

Influence and network structure are related. Influence drives the network structure, and also the network structure drives the ability to spread influence among the actors in a network. Based on their position in the network, some nodes, which represent the individual actors, are ranked more important than others based on centrality values. Existing algorithms such as eigenvalue centrality, closeness centrality, and betweenness centrality, can be implemented in a network to identify these important nodes. However, due to the various interpretations of the term "importance", a vast number of network algorithms have been developed over the years to identify different nodes of differing importance in a network. Depending on the analyst's definition of importance, these algorithms will often result in different answers. Strategically located nodes in a network could possess the potential to be highly influential, but yet they may not be reflective of their actual influential strength [5].

Influence is also a dynamic process. With connotation of time, it is crucial to analyze the evolution of influence over time. However, most network science algorithms do not consider time in the calculations, making the use of these tools particularly challenging when applying to temporal networks. To analyze how influence evolves with time, we need to develop a temporal graph, in which each layer reflects a certain time segment. There are two ways to create a temporal graph. One way is to create each network layer by reflecting separate blocks of time segments without overlapping. Consider the following 2-year non-overlapping example: the first network layer would cover events from the beginning of 1970 to the end of 1971; the second layer would then be from the start of 1972 to the end of 1973; and the third layer would encompass events from the start of 1974 to the end of 1975. This method of segmenting the time layers will result in an independent analysis of each layer; however, we would not be able to study the network holistically. Another method, and the one we adopt in this thesis, is to allow each time layer to have a time overlap where the first network layer would still cover events from the beginning of 1970 to the end of 1971 but the second layer would now start at the beginning of 1971 and cover events up to the end of 1972. The third layer, correspondingly, would encompass events from the start of 1972 to the end of 1973. This allows the data transition to be smoother between each layer and results in a more holistic analysis.

1.2 Research Questions and Contributions

The purpose of this research is to examine terrorism on a global scale and to determine how influential a perpetrator group is temporally. While there are many on-going research initiatives to disrupt terror operations by identifying, isolating, and capturing key personnel of a perpetrator group, little has been done to look at terrorism on a global scale. There are existing network algorithms that provide ranking of influential nodes based on their positions in a network, but most do not account for attributes which reflect the status or strength of influence. The aim of this thesis is to present an analysis of global terrorism and develop a method to assess each actor's influence strength by incorporating other attributes available from an online database.

The database we use provides an opportunity to examine the temporal evolution of terrorism. The data is tagged with a vast amount of information on global terror activities such as the date, location, and the type of terror incident, which we use as indicators to determine the influence strength of a perpetrator group and examine how influence strength changes with time. In Chapter 3, we provide a summary of the terrorist activities and insights to terrorism at a global scale, such as lifespan of a perpetrator group, spread of terror activities from 1970 to 2016, and recorded terror activities since 1970.

In this thesis, we examine the data from as early as 1970 through the year 2016. We are interested in analyzing (1) how influence strength differs across perpetrator groups, as well as (2) how influence strength evolves with time. To analyze the data, we create a network representing perpetrator groups as nodes, and two nodes x and y are adjacent to each other if x and y conduct at least one incident in the same city. We then apply our methodology in assessing influence strength of a perpetrator group to the terrorist network at a global scale. We seek to understand and determine what causes the rise and fall of certain perpetrator groups, as well as which perpetrator groups are persistent and exist for many years. In order to evaluate the strength of influence, we propose a method to rank the strength of each actor's influence by tabulating their influence score. The influence score is calculated based on the number neighboring nodes which show similarity in the type of operations that they conduct. We expect certain perpetrator groups, like Islamic State of Iraq and the Levant (ISIL), to show high influence score and signs of growing influence among the perpetrator groups in the network. In the process, we identify other similar perpetrator groups with high influence score, and groups that show signs of increasing influence.

1.3 Thesis Structure

This thesis is organized into six chapters: 1) Introduction; 2) Background, 3) Data, 4) Methodology, 5) Results and Analysis, and 6) Conclusion and Future Work. In the next chapter, we provide a literature review on prior work in network science as well as in areas of terrorism. In Chapter 3, we provide a summary of the Global Terrorism Database, which we obtain from an open source platform. The database provides information on more than 170,000 terrorist attacks from 1970 to 2016 around the world. The completeness of the database provides an opportunity to examine the temporal evolution of terrorism. We then illustrate our method to determine influence strength in Chapter 4, and we present the results and analysis in Chapter 5. In Chapter 5, we also identify perpetrator groups of key interest. In the final chapter, we summarize our findings and recommend future work to strengthen our approach in determining measures of influence among terrorist organizations.

THIS PAGE INTENTIONALLY LEFT BLANK

CHAPTER 2:
Background

In this chapter, we present prior research contributions to network science. We also explore prior research contributions to the study of terrorism, especially in the identification of terrorist networks and their circle of influence.

This chapter is organized into four main sections: 1) Network Science Overview; 2) Topological Characteristics; 3) Measure of Influence; and 4) Terrorist Networks. In the network science overview, we present basic terms and concepts that are prescribed in this academia field. Topological characteristics will cover existing structural characteristics that define the network such as centralities, which identify nodes of importance. We also present some of the influence measures previously presented in prior research. In the last section, we highlight previous research to describe the structure of terrorist networks.

2.1 Network Science Overview

Network science has gained much traction in today's academic field. Researchers have applied many analytical tools from the field of network science to study airline networks, development of human brains, and even the worldwide web. Recently, network science has been adopted to model social networks in order to understand complex human behaviors in society. Researchers use nodes or vertices to describe objects or actors inside a network, and edges or arcs to connect the vertices if they show similar attributes determined by the researcher. In the previous chapter, we introduced the concept of a graph, which contains vertices and edges. According to Bollabas, a graph G is defined as:

Definition 1 (Graph)

> *A **graph** is an ordered pair of finite disjoint sets (V,E) such that E is a subset of the set VxV of unordered pairs of V. The set V is the set of vertices V and E is the set of edges. If G is a graph, then $V = V(G)$ is the vertex set of G, $E = E(G)$ is the edge set. An edgex,y is said to join the vertices x and y and*

is denoted by xy. Thus xy and yx mean exactly the same edge; the vertices x and y are the end vertices of this edges G [6].

Figure 2.1 illustrates how we can model the “Seven Bridges of Königsberg" problem as a graph.

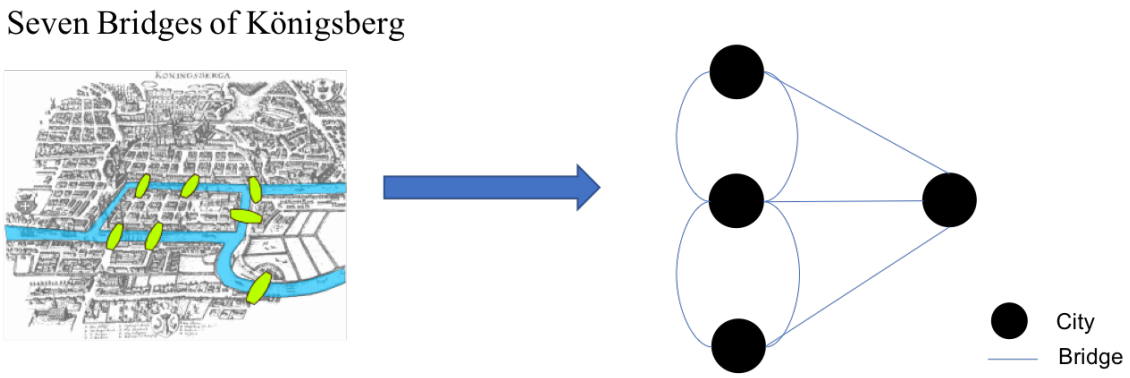

Figure 2.1. Modeling of Konigsberg Bridges as a Graph

Each vertex in the graph represents a region inside the city, and each edge represents the bridge which spans between the regions. A simple exhaustive search shows that there is clearly no way to walk through all the regions by walking across all the bridges once and only once.

Many graphs representing real-life scenarios end up having too many nodes and edges. Such large graphs are difficult to visualize and analyze. We instead focus on and analyze certain sub-areas of a graph, which contain smaller quantities of nodes and edges. A smaller portion of the graph is known as a subgraph and is defined as:

Definition 2 (Subgraph)

*A **subgraph** of a graph G is a graph H such that $V(H) \subseteq V(G)$ and $E(H) \subseteq E(G)$ and the assignment of endpoints to edges in H is the same as in G. We then write $H \subseteq G$* [7].

Rather than having a binary value on an edge, where 1 depicts the presence of an edge between two vertices, and 0 depicts no edge, we can sometimes place a weighted value on

an edge to depict values such as cost, or importance of the edge in comparison to others. For example, the bandwidth between nodes can be indicated on all the edges of a digital communications network.

Another definition used in this thesis is neighborhood. Node b is adjacent to node a when it is connected to node a by an edge. Node b is said to be a neighbor of node a. A neighborhood is a set of nodes, and is defined as:

Definition 3 (Neighborhood)

> ***Neighborhood**, $N_G(a)$, is a set of nodes which are adjacent to node a* [8].

A graph can be extended to become a network. A network is a complex graph which captures more information than a graph. It is a mathematical representation of interactions by using a simplified model for an analytical purpose. According to Newman, a network is defined as:

Definition 4 (Network)

> *A **network** is a simplified representation that reduces a system to an abstract structure capturing only the basics of connection patterns and little else* [9].

A network may consist of different sets of nodes. In particular for this thesis, we used a two mode network and it is defined as:

Definition 5 (Two Mode Network)

> *A **two mode network** is a network that contains two different sets of nodes* [10].

A network which contains time information is called a temporal network in which the nodes and edges exist only for a certain period of time. It can depict the rise and fall of nodes, and also describe transmission processes such as information, diseases, and influence. Each

edge depicts a contact opportunity. With the addition of time information, the order in which each node contacts other nodes can be illustrated in the temporal network. Arnaud introduces the concept of a Time-Varying Graph (TVG) [11], by integrating various existing dynamic network concepts into a unified framework.

TVG is a useful mathematical model that represents dynamic (evolving or temporal) networks. Dynamic networks such as mobile communications networks, social networks, and internet networks, are always changing and evolving. For example, mobile phones need to establish new connections with broadcast stations as they move across coverage areas. The bandwidth and latency of the communications are always changing, and the quality of communications is also dependent on various factors such as the traveling speed and traveling mechanism. The traditional static network would be less useful in describing and analyzing these types of networks, which are clearly dynamic in nature.

2.2 Topological Characteristics

As network science became more established, numerous topological metrics were developed to study, analyze, and categorize the various forms of networks. These metrics include centralities, modularities, clustering coefficients, and network diameters. In this section, we will introduce some of the topological metrics which are used in this paper to analyze the structure of our terrorist networks.

2.2.1 Centrality

Before we introduce the concept of centrality, we need to define what is meant by a path and a walk. First, a walk is defined as:

Definition 6 (Walk)

> *A $u - v$* ***walk*** *is a sequence of vertices in graph, beginning with vertex u and ending at vertex v such that consecutive vertices in the sequence are adjacent* [8].

The difference between a path and a walk is that a path is a walk where the vertices are distinct. This means that the vertices in a path do not repeat.

In a network, centrality refers to the importance of a vertex as compared to the other vertices. As the term “importance" can differ depending on the context and environment, there are many centrality measures that have been proposed. The more popular centrality measures are 1) eigenvector centrality; 2) closeness centrality; and 3) betweenness centrality. They are defined as follows:

Definition 7 (Centrality)

> *1)* ***Eigenvector Centrality****: a degree centrality score proportionate to the sum of the degree centrality scores of its neighbors* [12].
>
> 2) ***Closeness Centrality****: measures the mean distance from a vertex to other vertices connected to it* [13].
>
> 3) ***Betweenness Centrality****: measurement of how well a vertex lies on the shortest paths connecting other vertices* [13].

In this research, we will compare our methodology with the centrality measures described above. Betweenness centrality will be of particular interest, since these vertices act as hubs and are in an excellent position to promulgate influence to the others with the shortest path.

When considering the influence strength or relative power of a node, another useful metric we will use is the average path length of the network. A smaller average path length would usually imply that there are many redundant short paths to other vertices in the network. This has effects when looking at the process of influence. Influence and information can spread easier and quicker in a network with a small average path length than a network with a large average path length, as it takes a fewer number of edges to traverse between two vertices. More often than not, a network usually contains more than one connected component. For the purpose of this research, if more than one component exists in the network, we will only consider the largest component of the network.

Definition 8 (Component)

> ***Component*** *is a subset of the vertices of a network such that there exists at least one path from each member of that subset to each other member* [9].

Another important metric which is used to describe the relative size of a network is the network diameter. Newman defines network diameter as:

Definition 9 (Diameter)

> ***Diameter*** *of a network is the length of the longest geodesic path in the network* [9].

The network diameter would give an approximate measure of the size of the network. It is useful to consider the longest geodesic path when we want to look at what is the maximum number of edges needed to traverse across the network. That would give us the highest latency at which information would spread across the entire network.

Another research area in network science detects hidden communities which are formed in a network. In social networks, these communities could be perceived as circles of friends which either interact more with each other or have a common interest. In this sense, vertices in a community tend to be strongly connected together, comprising a dense subgraph. Defined by Radicchi, communities are:

Definition 10 (Community)

> *A* ***community*** *is a subset of vertices within the graph such that connections between vertices within a community are denser than connections with the other communities in the rest of the network* [14].

In addition to developing algorithms to detect communities within a network, there is also a need to find a function which measures the strength of the communities in the network. Network modularity becomes the measure which describes the strength of division of any network into modules or communities. A high value of modularity describes a graph where nodes within a community are densely connected while, connection to other nodes in other communities are sparse. Newman uses the concepts of modularity to partition the network into modules or communities. He defines network modularity as:

Definition 11 (Network Modularity)

> ***Network modularity*** *is the difference between the edges in the network that connect vertices within the community, and the expected value with the same community divisions but with random generated connections between the vertices* [15].

2.3 Measure of Influence

Understanding how influence spreads in social networks is a growing research area. For example: How does a virus spread? How is information passed from one location to another? How can a group or individual influence the decisions of other individuals? Understanding the spreading process can help us in many ways such as limiting and containing the virus, or increasing the speed at which information can be spread, or allowing us to target specific groups of interest so that we can influence their decision.

In terms of social influence, the relationship between actors is linked by their behaviors and attitudes, which ultimately determines the structure of such networks. Research has shown that influence tends to spread among actors with similar interest, allowing attitudes of actors to be reinforced [4]. Yet we may also observe competition in influence strength in a network. Two actors who are highly influential at close proximity with each other in a network may be competitors of each other [16]. For this study, we will determine the influence strength of each actor (perpetrator group) based on their behaviors and attitudes.

Existing centralities, such as degree centrality [17], semi-local centrality [18], closeness centrality [13], betweenness centrality [19], eigenvector centrality [12], Katz centrality [20], and PageRank [21], can be applied in a network to identify nodes which are important, significant, and crucial [22]. Most of these centralities were introduced on a static network structure, and later extended to dynamic networks [23], large networks [24] and more recently to multi-layer networks [25] to better represent the real-world, such as [26], [27].

We measure influence in a network by considering the dynamic interaction between nodes. In addition, even if the structure of these networks is static, these centralities can only identify highly influential nodes due to their position in the network, and these measures

may not reflect their true influence strength [5]. Moreover, we search for a method to determine and track the actual influence strength of a perpetrator group, which is different than influence in standard social networks [28]–[31].

Environment factors play a critical role in providing opportunities for influence to spread. Terrorist activities seem to bloom in regions of conflict and instability. Research has also shown that geographical proximity is an indicator of influence opportunities [32]. In a related work by [33], geographical location is used to identify crime patterns to aid investigators in their analysis. In this study, we consider the location of a terror incident as a source and opportunity for a perpetrator group to influence others by identifying locations vulnerable to a terrorist operation. Therefore, we relate one perpetrator group to another if they have conducted an incident in the same location.

There are existing algorithms which calculate the influence metrics of a node, in a manner that is a little different from centrality algorithms. These metrics quantify and rank the influence of each vertex in a network and are usually used to analyze social networks. The common algorithms are 1) accessibility and 2) expected force.

There are ongoing research efforts that describe another way to determine the influence power of a node – by ranking each node and giving it a score [34], [35]. Influence can be quantified by observable reactions to stimuli, and if an entity performs a reaction favorable to the stimuli, we can consider the entity as being influenced. Therefore, we can determine the influence of a node by simply observing the actions and reactions of other nodes. This method is more accurate in measuring influence as it accounts for actual actions rather than the structural position of a node inside a network. For this research, we use this scoring system as basis and rank each node's influence based on the actions of neighboring nodes.

2.4 Terrorist Networks

With the increase in global terrorism activity in recent years, the academic world has seen a surge in research pertaining to terrorism. Threatening economic and social stability, terrorism poses a serious scourge to the international community. Academic programs in military and homeland security began focusing on studying terrorism, and took a deep dive into analyzing ways to counter terrorism. Researchers apply network science to analyze and understand the structure of terrorist organizations or perpetrator groups.

Network science is useful in studying the links between terrorist networks. Researchers can study the behavior of these networks, as well as track and uncover hidden collaborations between the perpetrator groups. In this section, we define terrorism and discuss past research on the structure of terrorism, as well as network analysis tools that have been used to uncover some of the hidden information within the terrorist network structures.

2.4.1 Definition of Terrorism

While terrorism is not new, the world has not agreed upon the most fundamental question: What is terrorism? [36]. A definition is important for the academic field as it facilitates a common understanding and boundaries for the scope of the problem. It allows a shared effort for data collection. For the purpose of this research, we define terrorism according to the data collection agency which published the Global Terrorism Database (GTD) on the open source platform. The National Consortium for the Study of Terrorism and Responses to Terrorism (START) defines terrorism as:

Definition 12 (Terrorism)

> ***Terrorism*** *is the threatened or actual use of illegal force and violence by a non-state actor to attain a political, economic, religious, or social goal through fear, coercion, or intimidation* [37].

The definition given by START appears to be as general and inclusive as possible so that the data collection would be broad and cover many incidents. Users can truncate and filter the data set according to the definition suitable for their area of research. For this research, we adopt the definition by START and use the dataset as a whole. There will be occasions where we omit certain data, which will be described in Chapter 3.

2.4.2 Terrorist Network Structure

Many researchers have applied network science to study terrorist networks. According to Sam, social network analysis tools such as centrality can help identify key terrorist roles, which can be targeted to disrupt the stability of the terrorist organization [38]. However,

there are limitations to using standard social network analysis tools. These tools may not be able to correctly identify key player roles if the networks are small and sparsely connected.

Many other researchers have analyzed the structural properties of a terrorist network. Lindelauf observed that terrorist networks are not randomly constructed. Instead, they are built in a constructive and systematic manner which finds an optimal balance between secrecy and information flow, thereby not following a small world topology structure [39]. According to Lindelauf, counter-terrorism efforts focus on identifying, capturing and isolating key personnel. This is essential in disrupting the terrorism process, by breaking the structure of a terrorist network.

Although several researchers' efforts have been focused on identifying individuals of certain perpetrator groups, little has been done to look at the interactions and possible collaborations between perpetrator groups. With the rise of digital technology, perpetrator groups may exchange information, and be influenced with the best practices by other groups to conduct their operations more effectively.

CHAPTER 3:
Data

The GTD is maintained by researchers at the National Consortium for START, which is led by the University of Maryland. The data can be found online at "https://www.start.umd.edu/gtd" [37]. The program is funded by the U.S. Department of State Bureau of Counterterrorism and Countering Violent Extremism and the U.S. Department of Homeland Security Science and Technology Directorate's Office of University Programs. Boasting a compilation of more than 170,000 terrorist attacks from 1970 to 2016 around the world, the database provides an opportunity to examine the temporal evolution of terrorism.

Published in the 2003 National Strategy for Combating Terrorism, the Bush administration defined terrorism activities as "premeditated, politically motivated violence perpetrated against noncombatant targets by subnational groups or clandestine agents." Additionally, the Bush administration identified the evolutionary nature of terrorism: "While terrorism is not new, today's terrorist threat is different from that of the past. Modern technology has enabled terrorists to plan and operate worldwide as never before" [40]. Fifteen years later, we believe that terrorist groups are even more structured, organized, and transformative, capable of carrying out terror activities across the globe.

Since the September 11, 2001 terror attacks on the United States, terrorism has become a top agenda item, not only in the U.S., but in the international community as well. Committees look for ways to address the growing threat and lethality from terrorism. To combat terrorism, academic researchers have been actively studying the behaviors of terrorist groups and the evolution of terrorism. In this chapter, we provide detailed analysis on terrorism as recorded in the GTD, which we hope can provide new insights to researchers.

3.1 Data Description

The data is obtained from "https://www.start.umd.edu/gtd". At the time of this analysis, it contained more than 170,000 entries of terrorist activities recorded around the world from 1970 to 2016. Each activity contains details of the terror event such as date of the incident;

name of the perpetrator group responsible for the attack; location of the incident; target type; attack type; value of property damaged; and number of victims killed. Due to the differing definitions of terrorism, the data was collected in a manner meant to be as inclusive as possible, therefore allowing researchers to filter through the data for their own purpose.

3.2 Limitations of the Data

There are a few limitations to the GTD. Since the database contains incidents from 1970 to 2016, there may exist some inconsistencies in the data collection. The lack of digital technology in the past may have limited data collection in the early years; many incidents, which would be seen as terrorism today, may not have been reported in the past. In addition, as the database became more inclusive and progressively updated throughout the years, some of the new variables of interest added to the database in recent years may not be reflected in past incidents. This results in an incomplete collection, where data is often missing or not available for incidents occurring in the earlier years.

While the database tries to provide information that is comprehensive and detailed as possible, there are many generic entries in the database. For example, the name of perpetrator can be labeled as "Gunmen," "Muslim Extremists," or even "Tribesmen." In addition, an "unknown" value is given to any variable where the true value cannot be determined. Unknown values are found in many areas such as the name of perpetrator, value of property damaged, etc. For the purpose of our analysis, observations with "unknown" information were omitted.

It is also important to note that all incidents which occurred in 1993 were lost and are omitted from the GTD. Even though efforts were made by START to recover the data, only an estimated 15% of the attacks were recovered. This means that our analysis was completed without any data from 1993, which may impact the outcome of our analysis especially in cases where the analysis approaches the years before and after 1993.

3.3 Data Analysis

This section provides a detailed analysis of changing trends in terrorism since 1970 for all of the recorded incidents in the GTD. It examines the terrorism trends based on geographic location of incident, perpetrators involved, and target types.

3.3.1 Scale and Spread of Terrorism

Figure 3.1 shows the total number of worldwide terror incidents that occurred annually from 1970 to 2016. As mentioned earlier, the 1993 data was missing from the database, hence it is not represented in the graph.

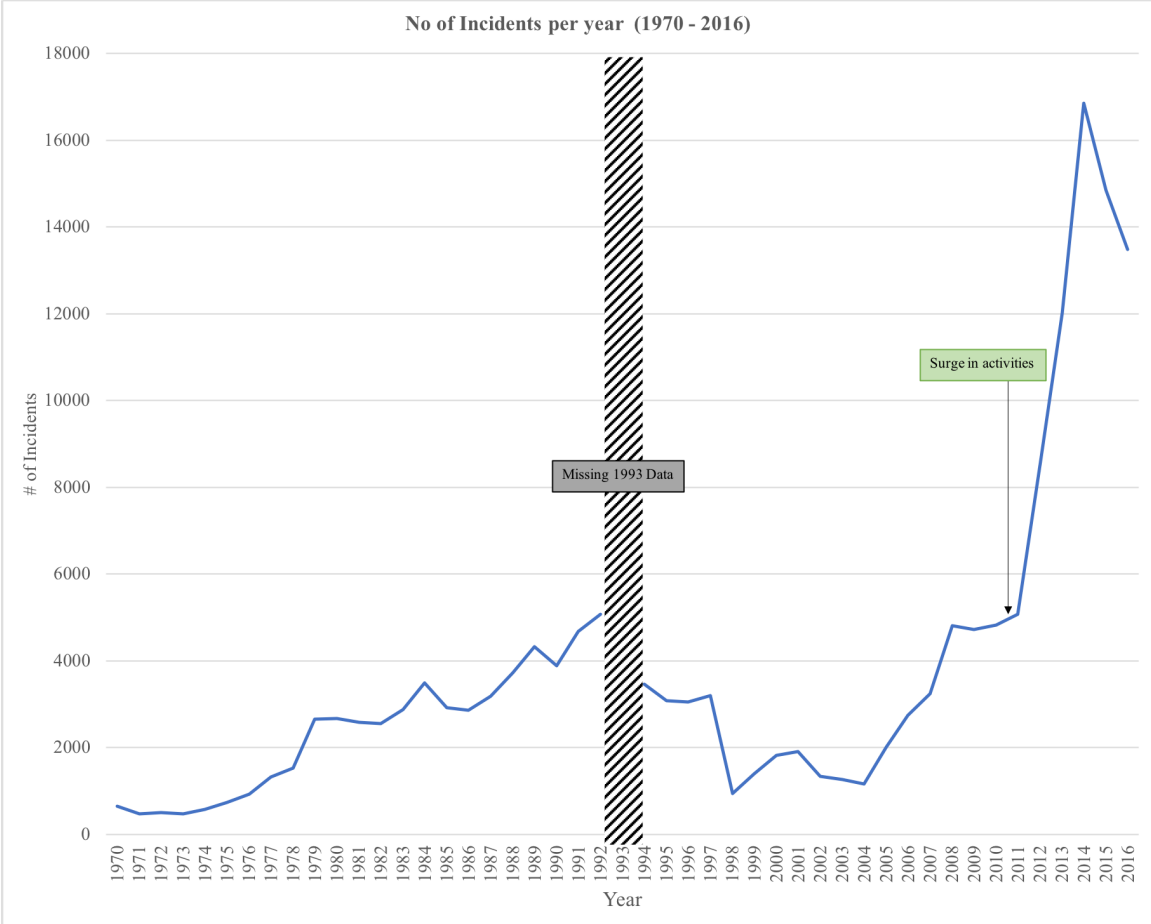

Figure 3.1. Number of Terror Incidents from 1970 to 2016

From Figure 3.1, it is notable that the number of terror incidents in the world surged after 2011. The total number of terror incidents that occurred from 2011 to 2016 make up almost 40% of all the incidents from 1970 to 2016. Additionally, the total number of terror incidents in Iraq, Pakistan, and Afghanistan make up 47% of all terror incidents from 2011 to 2016.

We postulate that the surge in activities may be caused by two reasons: 1) the increase in the number of perpetrator groups that occurs after 2011, causing the number of incidents to

increase; or 2) perpetrator groups become more capable of carrying out more attacks in a single year. In fact, we observe from Figure 3.2 that the number of perpetrator groups per year has nearly doubled since 2011, but this increase is not as dramatic as the increase in activities we saw in Figure 3.1.

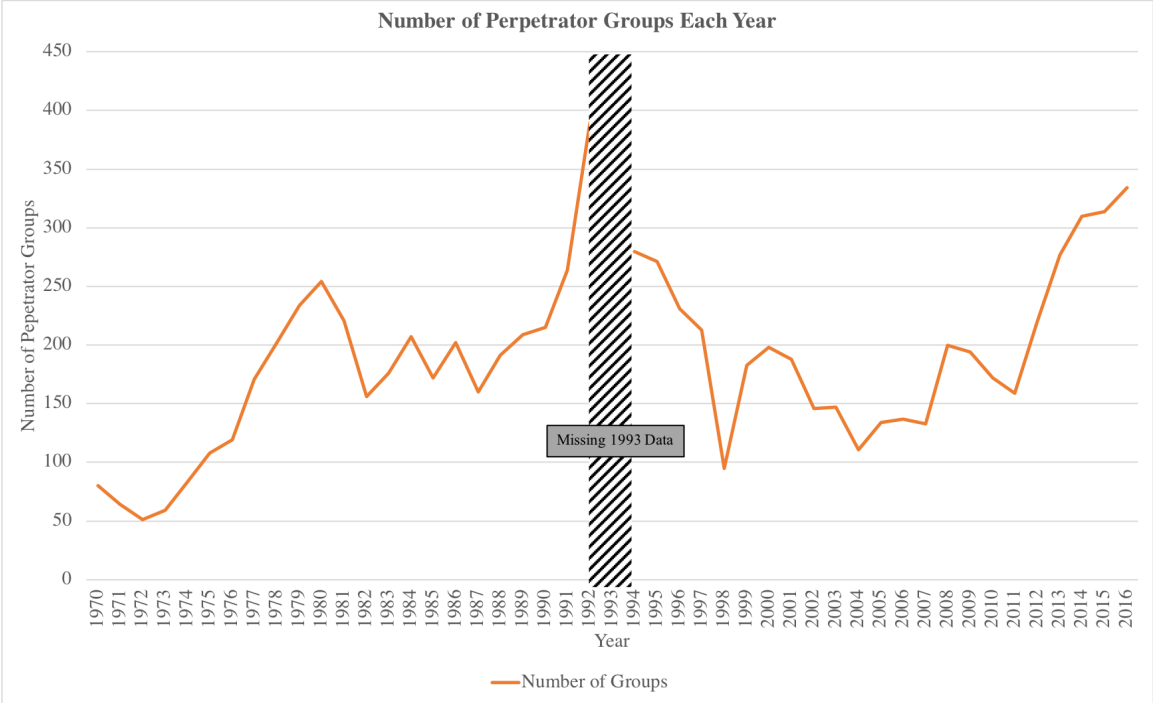

Figure 3.2. Number of Perpetrator Groups in Each Year

The highest number of perpetrator groups recorded is 390 in 1992, which is more than the 334 groups recorded in 2016. However, the number of terror incidents in 1992 is less than half of the number incidents in 2016. This could mean that perpetrator groups have become more capable of carrying out more attacks. One reason for such an increase in capability could be an increase in individual membership for some of the perpetrator groups, which would allow the perpetrator groups to sustain or increase their activities over the years.

We also examine how terrorism spreads based on geographical location. Figure 3.3 shows a heat map in five different non-overlapping timestamps: 1) 1970 – 1980; 2) 1981 – 1990; 3) 1991 – 2000; 4) 2001 – 2010; and 5) 2010 – 2016. The heat map represents the number of incidents within the city recorded during each timestamp. The size and the color represents the amount of activities in a city recorded within the given years.

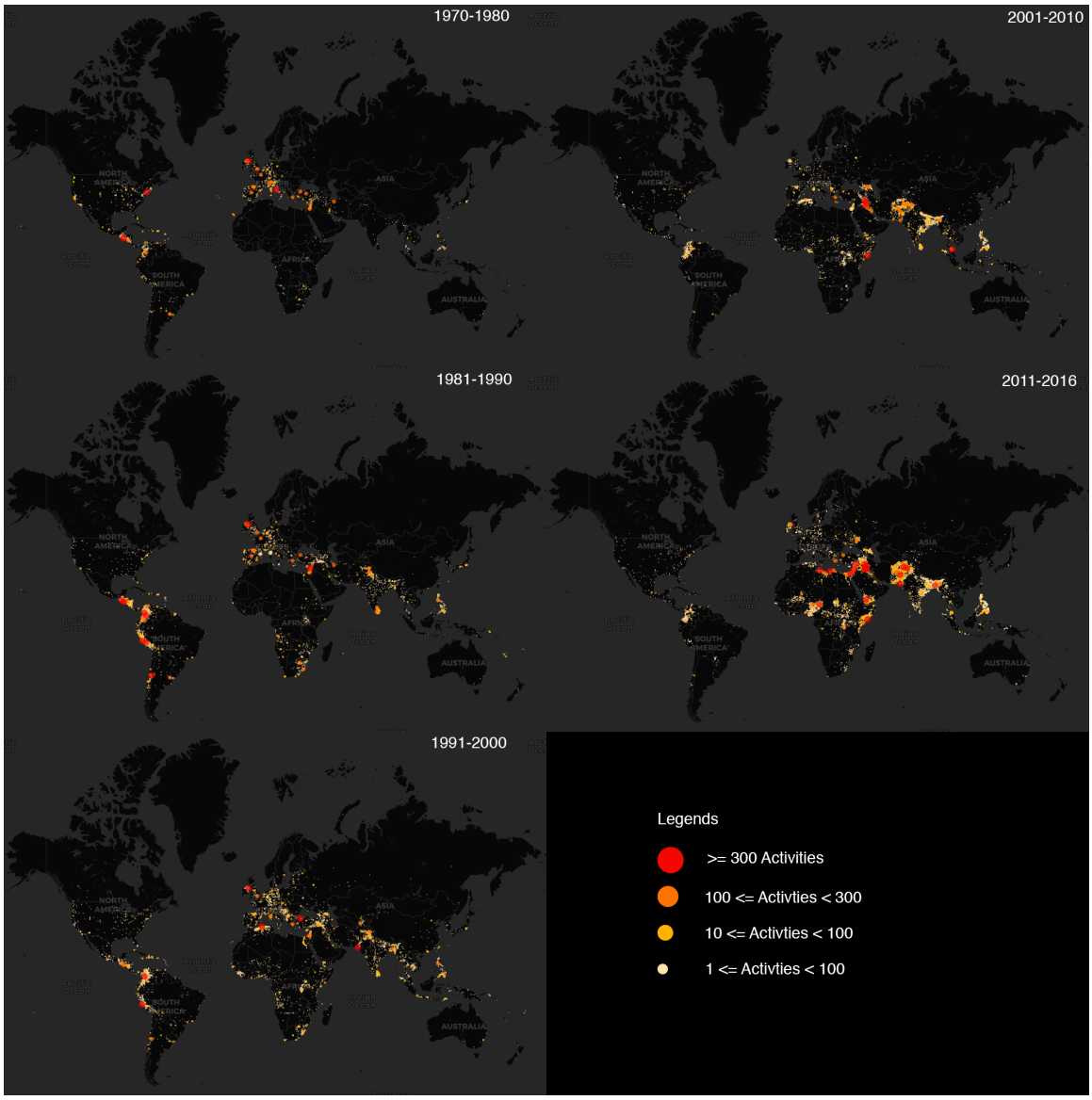

Figure 3.3. Spread of Terrorism (Geographical location)

We observe that the number of activities appear to not only intensify within an area but also increase across the entire globe. We observe that terror activities have also shifted eastward to South Asia (Afghanistan, Pakistan, India and Bangladesh) and South-East Asia (Southern Thailand and Philippines) from 1970 to 2016. Many of the terror activities occur near regions close to the coast. For example, many occurrences of terrorism activities are observed in regions around the western coast of South America, on both the east and west coast of Africa, and on the east coast of India, with some regions showing activities that

persist for many years.

Baghdad is the city with the largest number of recorded terror activities from 2015 to 2016. Almost 2,000 terror incidents were recorded in Baghdad over this two-year time period. This number is approximately seven times greater than the number of occurrences in Aleppo, Syria, the city with the second largest number of terror incidents during this time period. ISIL was the main perpetrator group in Baghdad, carrying out approximately 200 attacks in Baghdad during 2015 to 2016. An interesting observation is that around 1700 attacks cannot be attributed to any specific perpetrator group and are recorded as "unknown" in the data set. Such observations are not unique to Baghdad. The data set has a large number of terror incidents which cannot be attributed to any specific perpetrator group. It would be interesting to examine the data and investigate if there is any perpetrator organization which wants to remain as "unnamed" so that they do not appear as a group of interest. However, this will not be covered in the scope of this thesis.

3.3.2 Terrorism Target Type

The GTD categorizes the terror incidents into twenty-two different target types as shown in Table 3.1.

Table 3.1. Target Types Performed by Perpetrator Groups

ID	Target Type	ID	Target Type
1	Private Citizens and Property	12	Non-Government Organization
2	Military	13	Religious Figures / Institutions
3	Police	14	Telecommunications
4	Government (General)	15	Terrorists / Non-State Militia
5	Business	16	Tourists
6	Abortion Related	17	Transportation (Other than Aviation)
7	Airport and Aircraft	18	Utilities
8	Government (Diplomatic)	19	Violent Political Parties
9	Food or Water Supply	20	Educations Institutions
10	Journalists and Media	21	Other
11	Maritime (Includes Ports and Maritime Facilities)	22	Unknown

For better visualization, we select the top five target types from 2016 and illustrate the

popularity of these target types, in comparison to all "Others," from 1970 to 2016 in Figure 3.4.

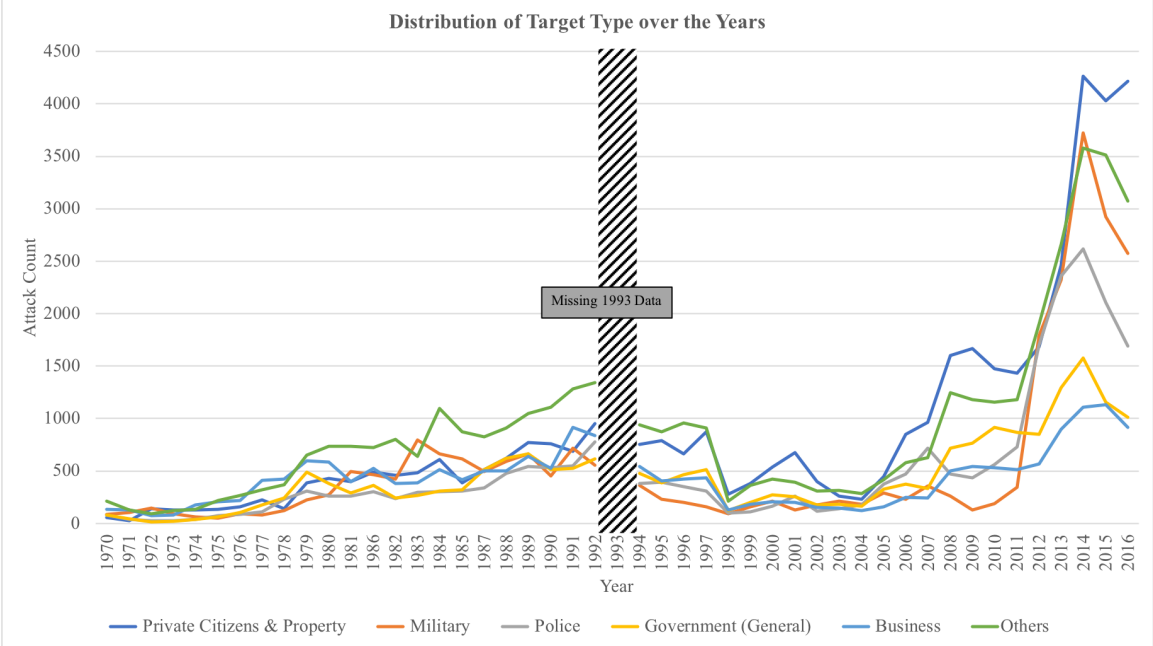

Figure 3.4. Target Type over the Years

From Figure 3.4, we observe that "Private Citizens and Property" remains as the top target type by perpetrator groups from 2014 to 2016, followed by "Military", "Police", "Government(General)" and "Business". However, "Private Citizens and Property" is not always the most important target type coveted by perpetrator groups. For example, from 1983 to 1987, the target type most attacked by terrorists was "Military".

Looking at the type of terror operations conducted by some of the individual perpetrator groups, we found that "Private Citizens and Property" is not the top target type for some perpetrator groups. For example, Figure 3.5 shows that the main target type of the Taliban from 2011 to 2016 was "Police". An interesting observation occurs during 2008 to 2011. During these years, the Taliban seems to be in a transition, as the top target type from 2008 to 2011 was "Private Citizens and Property", which is different from the rest of the years. Such a transition may reflect a change in direction for the perpetrator group, which could be as a result of a change in leadership.

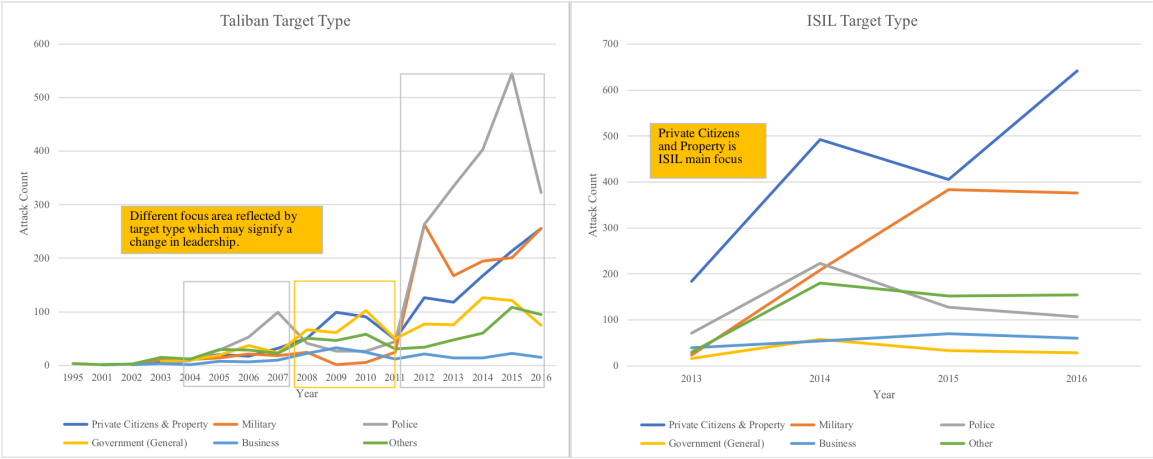

Figure 3.5. Taliban and ISIL Target Type over the Years

However, if we look into the operations performed by ISIL, the target type shown in Figure 3.5 shows that "Private Citizens and Property" was their focus area since 2013, and it remains as the their top target type. "Military" was their secondary target, and could be due to the fact that heavy military operations were being employed to defeat ISIL operations.

3.3.3 Lifespan of a Terrorist Group

With 3,453 different perpetrator groups recorded from 1970 to 2016, it is also interesting to analyze how long a perpetrator group exists and/or remains active. Figure 3.6 shows the distribution of terror activities for all of the terrorist groups recorded in the GTD.

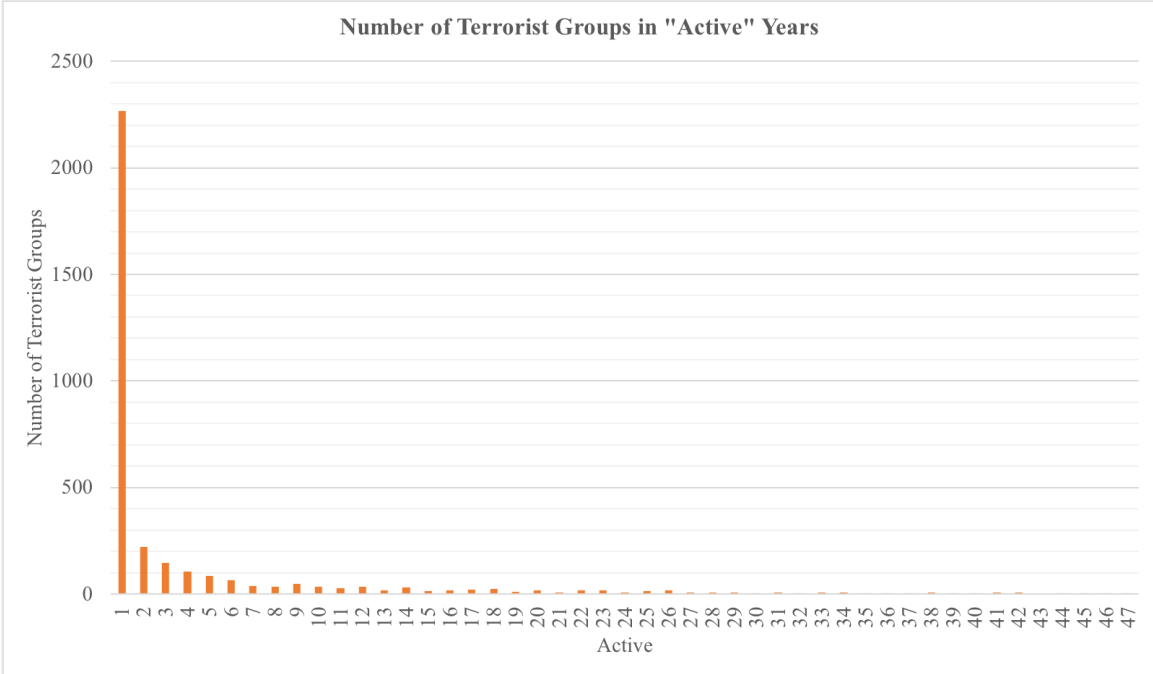

Figure 3.6. Lifespan of Terrorist Group

Figure 3.6 shows a wide distribution in the number of active years. The mean active lifespan of a terrorist group is 4.2 years, with a large standard deviation of 7.4 years. Almost 65% of the perpetrator groups are only active for a year, while others such as "New People Army" and "Population Front for the Liberation" have recorded at least one activity during every year from 1970 to 2016.

In this chapter, we presented a summary of the analysis of the data we obtained from the GTD. Based on the data, terrorism has surged since 2011. However, the number of perpetrator groups has not increased in a proportionate manner which may suggest that capabilities of the perpetrator groups have increased. In the next chapter, we will present the methodology we use to analyze the data using network science.

THIS PAGE INTENTIONALLY LEFT BLANK

CHAPTER 4:
Methodology

We create two separate experiments to analyze the GTD using network science. In Experiment 1, we analyze the data from 2011 – 2016 as a static network. In Experiment 2, we analyze the data from 1970 – 2016 temporally as a multi-layered network, where each layer is a temporal snapshot of the network. The results from each of the experiments are presented in Chapter 5.

4.1 Network Creation

For Experiment 1, we start with a bipartite (two mode) network: in which the nodes are perpetrators (x) and countries (y), and two nodes x and y are adjacent if perpetrator x performed a terrorist act in country y. This network allows us to analyze the extent of terrorism by looking at locations in which perpetrator groups operate around the world. We then create two projections of this two mode network: the first projection is the "country network" and the second projection is of the "perpetrator network".

For Experiment 2, we investigate the perpetrator network temporally, by dividing the network into two year segments each with one year of overlap, producing a two-year sliding window. For example: Layer 1 of the network contains data from $[1970, 1971]$ and Layer 2 of the network includes data in $[1971, 1972]$. In this network, we examine how the perpetrator network evolves with time and display some interesting evolutionary characteristics of the network.

4.2 Country Network

In the country network, we investigate the nature of international trans-border terrorist operations. To create this network, we represent the countries as nodes and two nodes x and y are adjacent if there exists a perpetrator group which acted in both countries (nodes). In Experiment 1, we present the topological characteristics of the country network.

4.3 Perpetrator Network

In the perpetrator network, we examine the extent of influence of a perpetrator group on the other perpetrator groups, based on location. We assume that perpetrator groups are heavily influenced by one another if they conduct at least one terror operation in the same location. For our analysis, we define the location as a city. We establish relationships between perpetrator groups x and y, based on the location in which x and y conducted at least one terror act. We design a weighted network with each node representing a different perpetrator group and weighted edges representing a common act of terrorism in a certain city. The formula of the weights is given as:

$$\frac{\text{Sum of number of times perpetrators } x \text{ and } y \text{ conduct terror activities in common cities}}{\text{Total number of times by } x \text{ and } y \text{ conduct terror activities in all cities}}$$

The weights will range from 0 to 1. Higher weights between an x and y perpetrator would mean that x and y are more related to each other based on the locations where they conduct terror activities.

4.3.1 Measure of Influence

For the perpetrator networks in both experiments, we analyze the influence strength for each of the perpetrator groups. Influence is the ability to sway the actions of others in carrying out the intended actions. There are two factors we consider when determining the strength of influence of an entity. One factor is the amount of followers the entity has, and the other is the ability to elicit a desired response in others. In this analysis, we choose the response to be the similarity in the type of operations the followers carry out.

In this section, we discuss how we determine the strength of influence for a specific perpetrator group. Following a method similar to the method proposed by Adithya Rao [34], we propose a scoring system, which incorporates the two aforementioned factors. First we define an influenced set of nodes as $I(a)$ such that $I(a) \subseteq N_G(a)$ is a set of neighboring nodes influenced by node a.

Definition 13 *We define the* ***influence score*** *of node a as*

$$\textit{Influence Score } (a) = \frac{|I(a)|}{|N_G(a)|} \times \frac{|N_G(a)|}{|V(G)|},$$

where $I(a)$ is the set neighboring nodes around node a which are being influenced by node a , $N_G(a)$ is the neighborhood of a, and $V(G)$ is set of all nodes in the graph.

The first fraction is a measurement of similar operations carried out by influenced neighbors, while the number of neighbor nodes to total number of nodes in the network ratio measures the number of followers a node has and normalizes it to the whole network. The normalization is important to give higher weights to nodes with more neighbors.

To determine the fraction of influenced perpetrator groups, we first find all the neighboring groups for each perpetrator group (influencing node) and then we determine the number of neighbors which carry out similar operations. Figure 4.1 illustrates how to determine the influence score for perpetrator group 1:

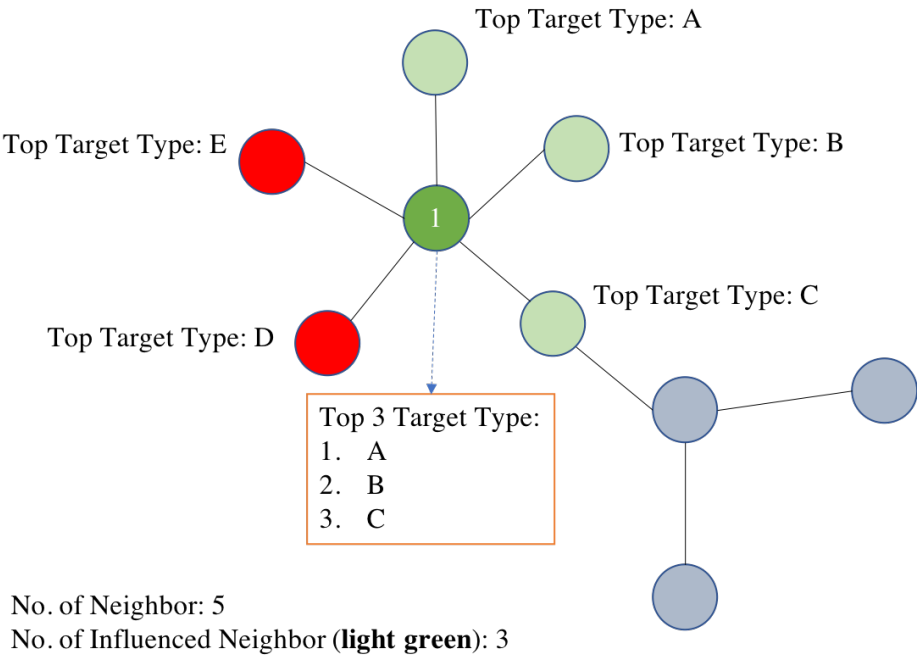

Figure 4.1. Example: Influence Score of Perpetrator Group 1

Based on the terror incidents that the influencing perpetrator group (dark green node) executed within each layer of the network, we identify the top three target types associated with the incidents conducted by this perpetrator group. We then examine the target types based on the terror incidents executed by the neighbors of the influencing group. If the top target type of the neighboring groups is one of the top three target types of influencing group, we mark the neighboring group as influenced (light green nodes). We then compute the ratio of influenced neighbors and normalize it to the total number of perpetrator groups in the layer. We repeat the process and obtain the influence strength for every perpetrator group in each layer. The top three perpetrator groups with the highest influence score from 2011 to 2016 is presented in Chapter 5.

Influence strength also has a temporal aspect to it as strength of influence may change over time. With the aforementioned method to tabulate influence score for each perpetrator group, we can examine how influence of a particular group changes over time by applying the metric to the temporal perpetrator network. We are particularly interested in perpetrator groups with an increasing influence strength over the years.

As the lifespan for most terrorist groups is only $1-2$ years, we select perpetrator groups who are active in 2015 - 2016 and analyze their influence trend. To detect an increasing trend of influence strength, we collect the data points for each perpetrator group's influence score from 2011 to 2016 and apply a linear regression algorithm to obtain a best fit polynomial line of degree 1. To plot the best fit polynomial line, only perpetrator groups with four or more influence scores were selected. The best fit polynomial line of degree 1 is obtained by applying the *numpy.polyfit* function in a Python program on the data set [41]. A positive slope from the best fit line would be indicative of an increasing trend in influence strength. The results will be shown in the next chapter.

CHAPTER 5:
Results and Analysis

In this chapter, we present the results of our two separate experiments. In Experiment 1, we use network science to analyze the GTD data from 2011 – 2016 in the form of two different static network projections. In Experiment 2, we analyze the evolution of perpetrator groups from 1970 – 2016 temporally as a multi-layered network, where each layer is a temporal snapshot of the network.

5.1 Network Analysis for Static Terrorist Network: 2011-2016

5.1.1 Bipartite Terrorist Network

In this section, we present the analysis on the static network from 2011 to 2016. We create a bipartite (two mode) network by letting the nodes represent either the perpetrators or the countries, and two nodes x and y are adjacent if a perpetrator x acted in a country y. Figure 5.1 shows the bipartite network, where the nodes are colored by type. A red node represents a perpetrator, and a gray node represents a country.

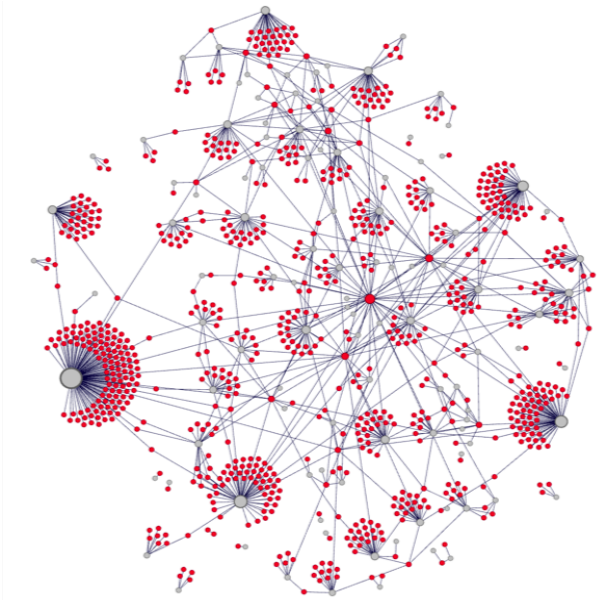

Figure 5.1. Bipartite Graph: Countries and Perpetrator Groups

In analyzing the countries, Figure 5.1 shows that the node with the highest degree is India. This means that, during the 2011 – 2016 time frame, India was targeted by the highest number of different perpetrator groups. However, the countries with the most number of incidents recorded between 2011 – 2016 are Iraq, Pakistan, and Afghanistan.

We now turn our attention to the individual perpetrator groups. In our work, we seek to identify perpetrator groups that have the ability to extend their operations across borders and target multiple countries. We determine the capability of these groups through an analysis of their ability to conduct terror operations worldwide.

Table 5.1 shows the top 10 trans-boundary terrorist groups ordered by degree, where the degree represents the number of countries attacked by that perpetrator group.

Table 5.1. Top 10 Perpetrator Groups that Attack the Most Number of Countries (bold font depicts groups that have non-generic group names)

Rank	Perpetrator Group Name	Degree
1	Muslim extremists	41
2	**Islamic State of Iraq and the Levant (ISIL)**	**22**
3	Gunmen	19
4	Jihadi-inspired extremists	13
5	Separatists	12
6	**Al-Qaida in the Islamic Maghreb (AQIM)**	**10**
7	Anarchists	9
8	**Animal Liberation Front (ALF)**	**9**
9	Tribesmen	9
10	**Informal Anarchist Federation**	**8**

During 2011 – 2016, ISIL conducted operations in 22 countries, the highest number among the non-generic perpetrator groups. The regions in which ISIL operated include Asia, Europe, Africa and Middle East Countries. Terror activities conducted by ISIL only surfaced in 2013, and ISIL's operations quickly expanded around the world.

5.1.2 First Network Projection: Terrorism Network by Country

Figure 5.2 shows the first projection of the bipartite (two mode) network, where the nodes represent countries, and nodes x and y are adjacent if there exists a terrorist group that attacks both countries within the same period of time. The projection shown in Figure 5.2 is laid out geographically.

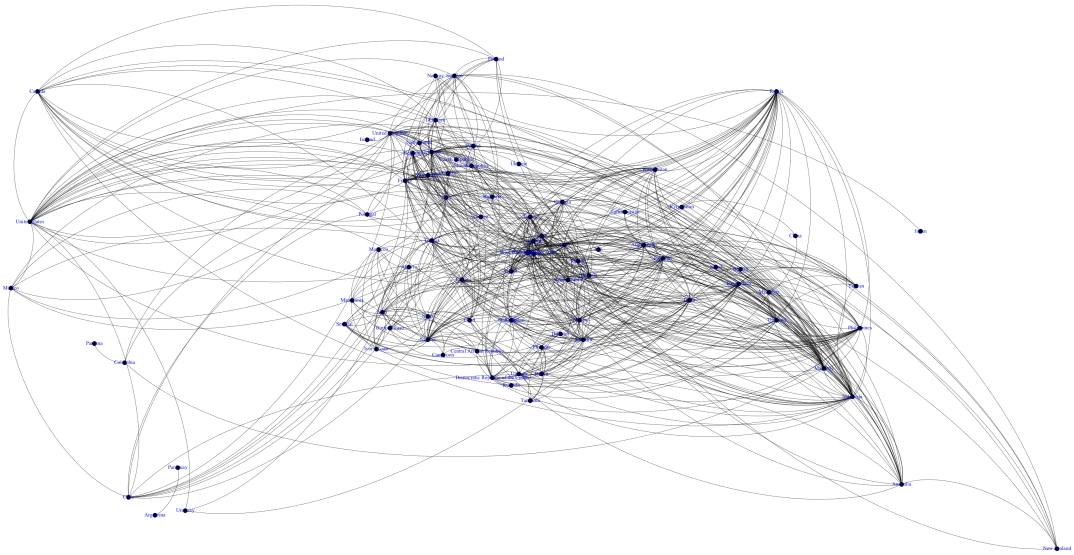

Figure 5.2. Geographical Representation of the Terrorism Network by Country

It is astonishing to see the widespread distribution of terrorism. There are many perpetrator groups that have expanded their operations worldwide. The network has two components, with the smaller component comprising only two countries (Argentina and Paraguay), and the larger component containing 85 countries. The network's characteristics are presented in the Table 5.2:

Table 5.2. Network Characteristics for the Terrorism Network by Country

Characteristic	**Values**
Number of Nodes	87
Number of Edges	698
Average Degree	16
Network Diameter	6
Modularity	0.347
Number of Communities	5
Number of Components	2
Average Path	2.168

The network has a relatively low modularity value which suggests that communities formed

in this network are not distinct. This implies that some perpetrator groups conduct operations at a global scale, instead of focusing their operations regionally.

5.1.3 Second Network Projection: Terrorism Network by Perpetrator Group

As described in Chapter 4, we create the perpetrator network as a second projection of the two mode network. Figure 5.3 shows the perpetrator network with nodes representing the perpetrator groups, where nodes x and y are adjacent if perpetrator groups x and y attack the same country at least once. We apply the measure of influence metrics as described in subsection 4.3.1, and attribute an influence score to each perpetrator group in the network.

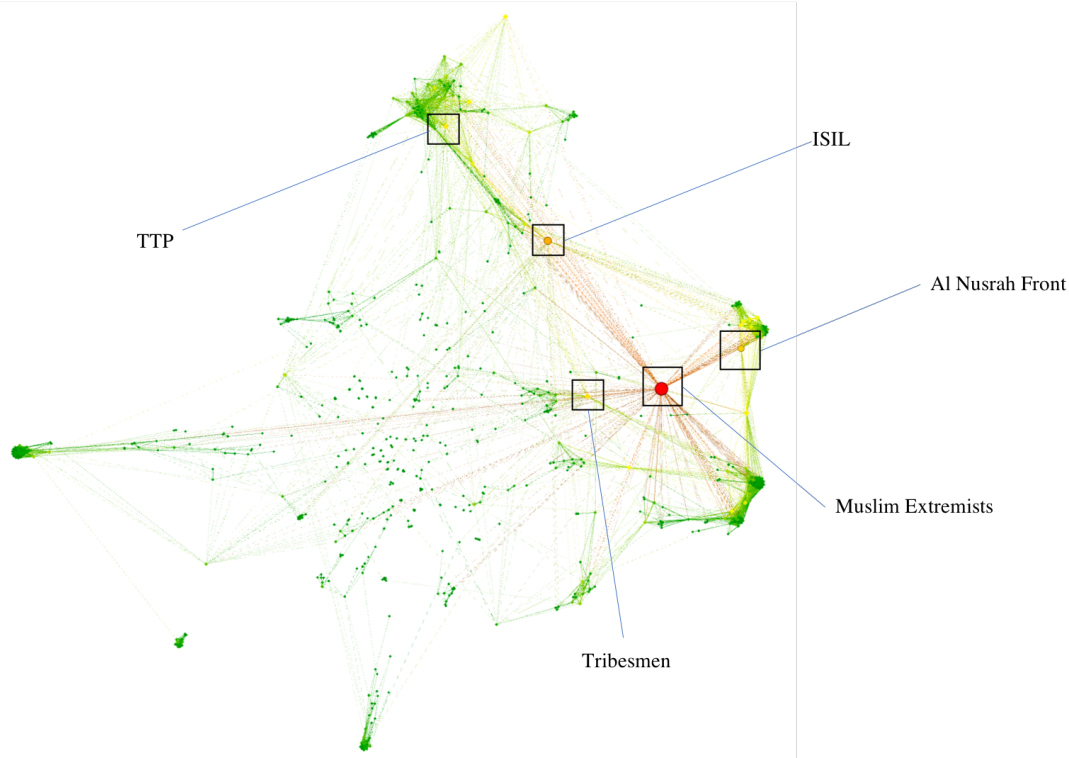

Figure 5.3. Perpetrator Group Influence Strength: 2015 – 2016

The colors of the nodes form a heat map representing the distribution of influence strength in this network, where red represents the most influential perpetrator groups and green is the least influential. The location of the top five most influential perpetrator groups are

identified in Figure 5.3. The Louvain community detection algorithm [42] shows that ISIL, Tehrik-i-Taliban Pakistan (TTP) and Al-Nusrah Front reside in different communities.

We also use the highest weighted edge to identify the top three neighbors of ISIL, TTP, and Al-Nusrah Front. A high weighted edge between two perpetrator groups suggests that the two groups have strong relationships with each other as they have a common attacking location. Table 5.3 shows the perpetrator groups with the highest weighted edge adjacent to ISIL, TTP, and Al-Nusrah Front, respectively.

Table 5.3. Most Influential Perpetrator Groups and Adjacent Groups with Highest Weighted Edge

Most Influential Groups	**Neighboring Groups**	**Weighted Edges**
ISIL	Al-Qaida in Iraq	0.52
	Gunmen	0.34
	Al-Naqshabandiya Army	0.27
TTP	Baloch Republican Army	0.22
	Gunmen	0.20
	Sunni Muslim Extremists	0.17
Al Nusrah Front	Free Syrian Army	0.45
	Southern Front	0.39
	Islamic Front Syria	0.38

The weighted edge can be seen as a measurement of common interest between two perpetrator groups based on the location of their attacks. Table 5.3 shows that perpetrator groups, like ISIL and Al-Qaida in Iraq, have a high weighted average because both of them share similar territorial interests, as they both perform a large number of terror operations in Baghdad. This is also observed between groups like Al-Nusrah Front and Free Syrian Army, where both have a common interest in Aleppo, Syria.

For each perpetrator group, we plot a distribution of the perpetrator group's influence strength against the group's number of edges (neighboring groups) as shown in Figure 5.4.

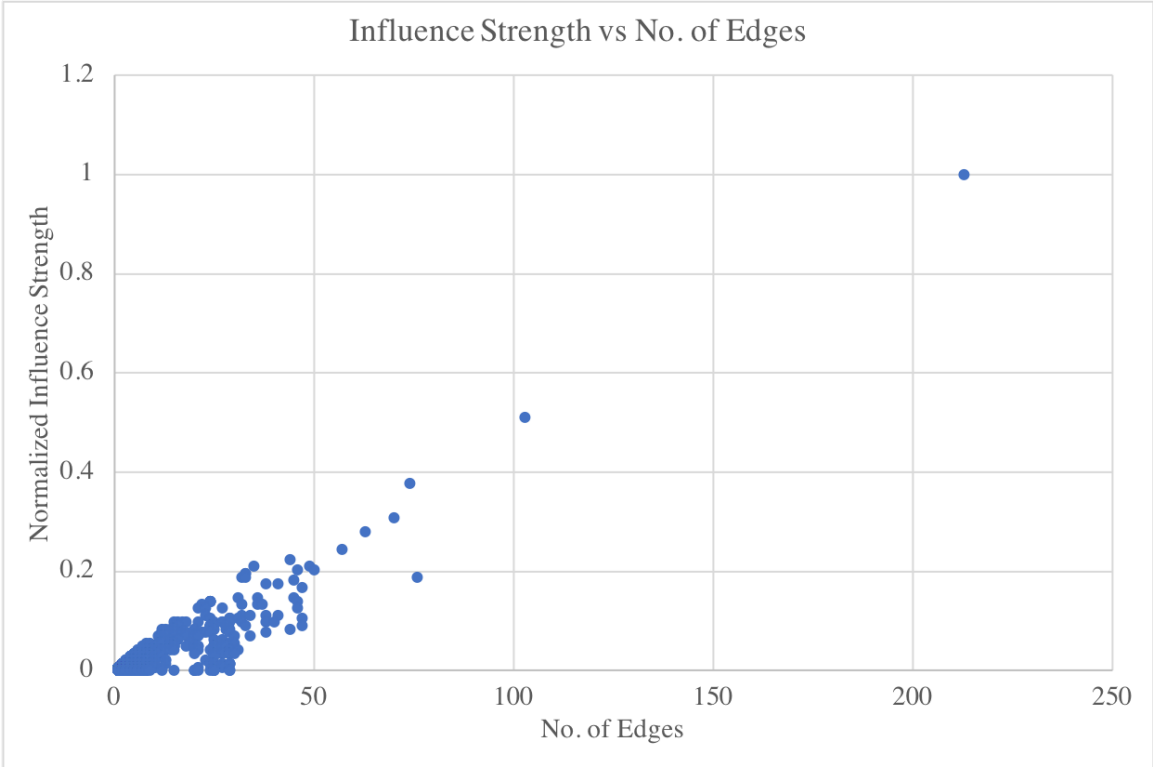

Figure 5.4. Distribution of Influence Score with Number of Edges

It is interesting to note that there exist some perpetrator groups with a relatively high degree (for example 29 edges incident to a single node), but the groups have an influence score of zero. This means that while these perpetrator groups conduct terrorist activities with 29 other perpetrator groups based on location, they are not able to influence these groups to conduct similar operations. These groups have unique target type operations which other perpetrator groups may not subscribe to. Such behavior cannot be observed by only analyzing the position of the perpetrator groups in the network.

5.2 Temporal Terrorist Networks

There are a total of forty-six layers in the multi-layered terrorist network, with each layer representing a 2-year window of data. A sliding window is created so that each layer has a year of overlap with the previous layer and a year of overlap with the next layer. We then carry out analysis on this temporal network. Figure 5.5 shows the average degree of the network graph for each layer. The x-axis shows the starting year of the layer, and the y-axis

shows the average degree.

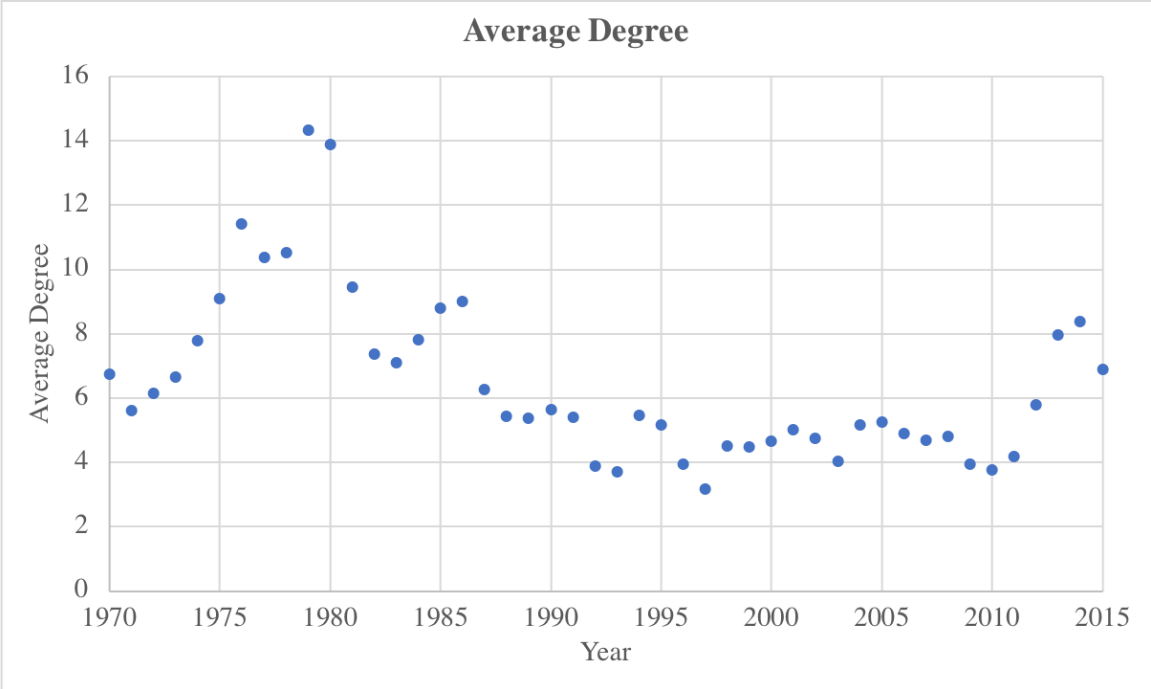

Figure 5.5. Average Degree in Each Layer of the Multi-layered Temporal Terrorist Network

While the frequency of the terror attacks has increased over the years, the average degree of the network graph has not dramatically increased. Even though the average degree increases from 2011 – 2015, it is still lower when compared to 1976 – 1981. One possible reason is that, unlike in the past where terrorism was localized to certain regions, terrorism today has become more worldwide. With more terror incidents occurring at more locations, the probability of two nodes having a common edge decreases.

We also examine the temporal pattern of perpetrator groups within each layer over time. Figure 5.6 depicts the number of perpetrator groups represented by the number of nodes in each layer of the network. The x-axis again represents the starting year for each layer, and the y-axis represents the total number nodes present in that layer.

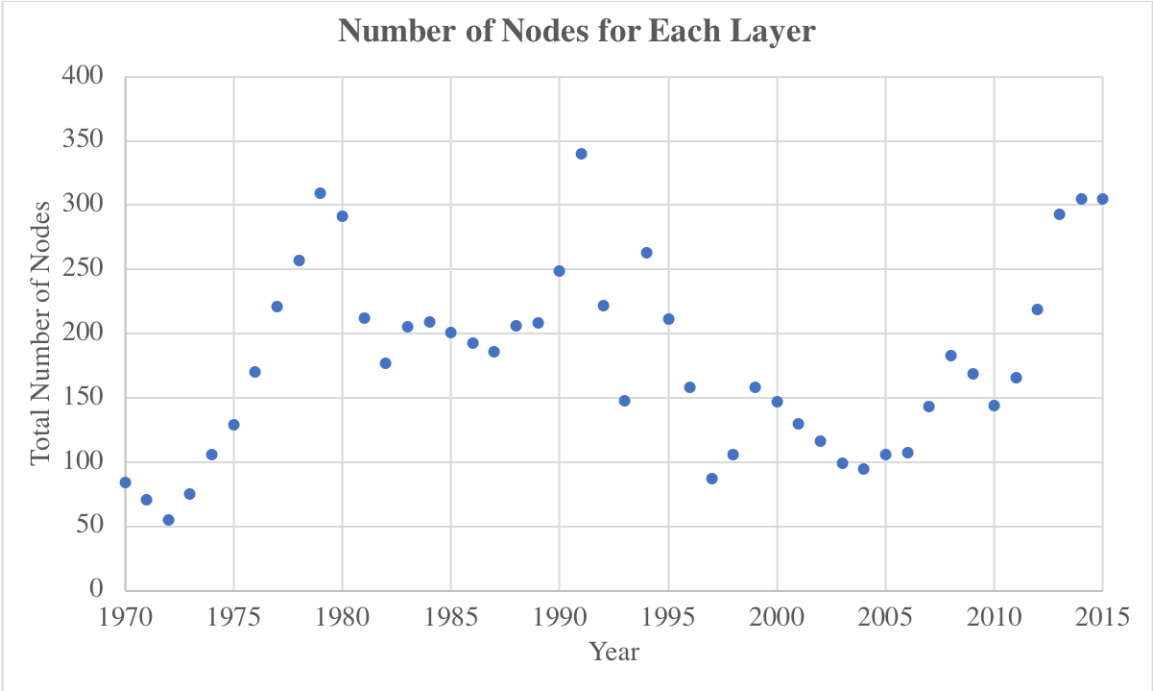

Figure 5.6. Number of Nodes in Each layer of the Temporal Terrorist Network

While the number of incidents recorded each year has increased significantly since 2011, we observe that the number of perpetrator groups has not increased in a proportionate manner. In fact, the highest number of perpetrator groups was recorded in 1991 – 1992. This means that existing perpetrator groups have grown more capable of conducting more operations each year. It may also imply that their membership has increased enabling the groups to sustain a higher number of operations per year.

We also run community detection on each layer of the network to observe the terrorist community evolution in time. Figure 5.7 shows the number of communities and the modularity of the network for each layer in the network.

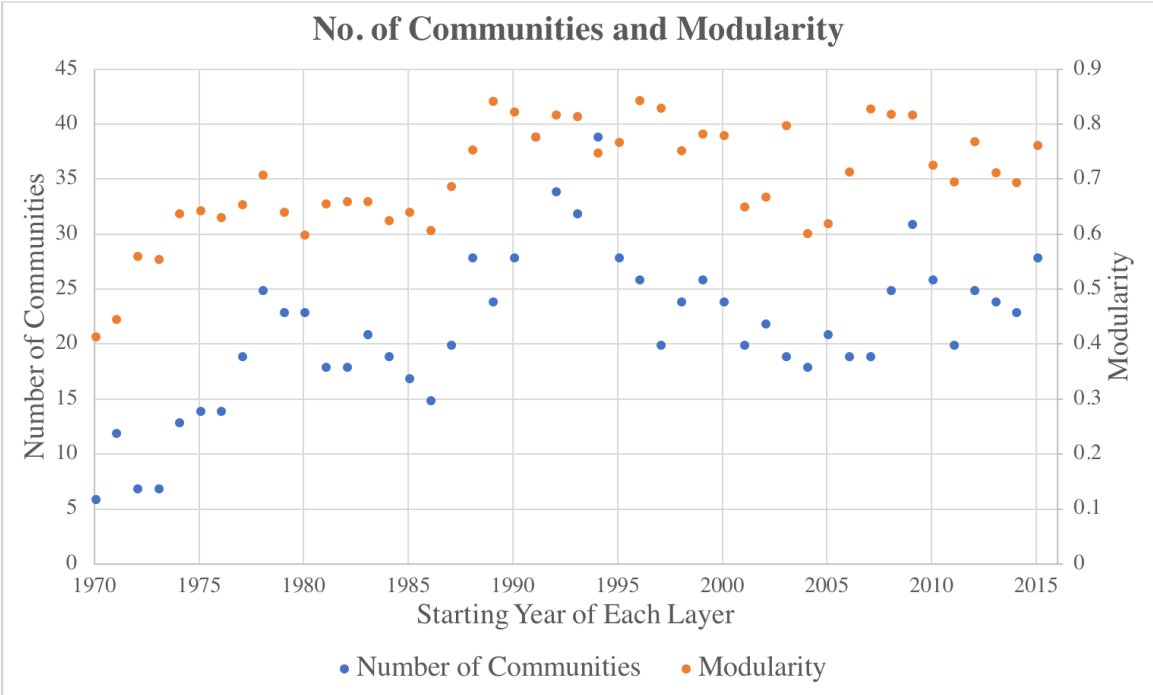

Figure 5.7. Number of Communities and Modularity Trend

On average, the number of communities has increased over the years. Modularity, which is a measure of how well a network can be partitioned into different modules, has also increased, on average, since 1970. Another observation is that the modularity of the layer appears to rise and fall with the number of communities detected which is what we expect. Over the years, perpetrator groups seem to have formed more distinct communities. This may be advantageous to researchers who can narrow their focus and study the network structure in each community instead of examining the network as a whole.

5.2.1 Influence Score Analysis

As described in Chapter 4, within each network layer, each node is given an influence score. We examine the distribution of influence scores using a histogram. Examples from several of the layers are shown in Figure 5.8

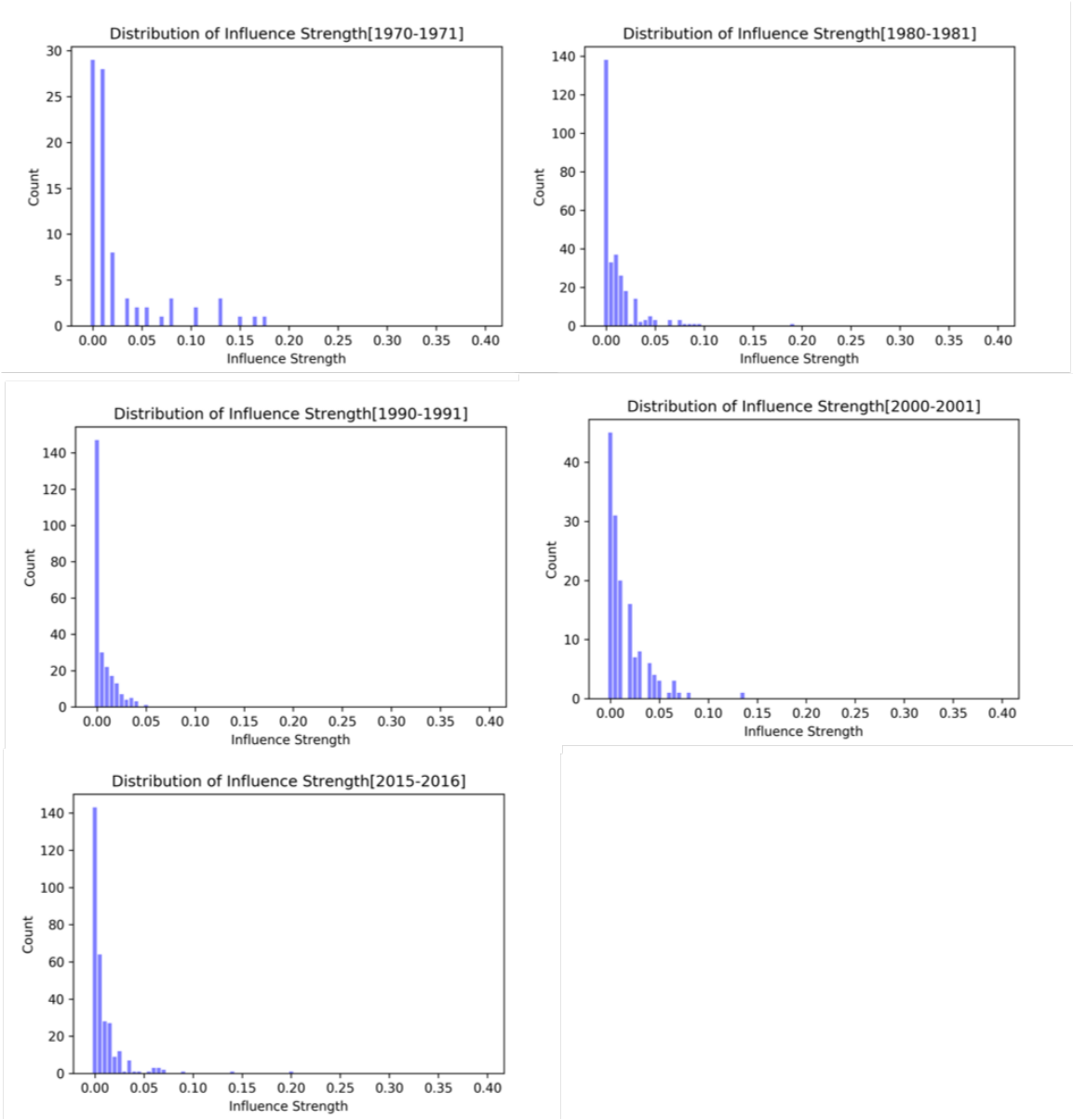

Figure 5.8. Influence Distribution

The shape of the distributions appear to follow a power law distribution with the largest count in low influence score and smallest count in high influence score. As can be seen from Figure 5.8, this general histogram shape remains fairly consistent over each of the two-year layers. Such power law distributions are also found in social networks, where there exist a few hubs and a long tail of peripherals [43].

Based on the proposed influence score methodology, the top three most influential perpetrator groups are presented in Table 5.4 for each of the five layers from 2011 to 2016. As some of the incidents that occurred cannot be attributed to one specific group, the researchers of the GTD classified these incidents under generic names, such as "Gunmen," "Muslim Extremists," and "Tribesmen". These generic names appear very frequently as nodes of interest; however, we remove these generic names from our analysis and present the rest of the results in Table 5.4.

Table 5.4. Influence Score

Rank	**Perpetrator Group Name**	**Influence Score**
	2011-2012	
1	Tehrik-i-Taliban Pakistan (TTP)	0.0964
2	Taliban	0.0843
3	Al-Qaida in Iraq	0.0663
	2012-2013	
1	Tehrik-i-Taliban Pakistan (TTP)	0.0913
2	Al-Nursah Front	0.0457
3	Free Syrian Army	0.0457
	2013-2014	
1	Tehrik-i-Taliban Pakistan (TTP)	0.0956
2	Al-Nusrah Front	0.0853
3	Islamic State of Iraq and the Levant (ISIL)	0.0520
	2014-2015	
1	Islamic State of Iraq and the Levant (ISIL)	0.1213
2	Al-Nusrah Front	0.0918
3	Tehrik-i-Taliban Pakistan (TTP)	0.0852
	2015-2016	
1	Islamic State of Iraq and the Levant (ISIL)	0.1443
2	Al-Nusrah Front	0.0918
3	Jaysh al-Islam (Syria)	0.0721

Beginning in 2014, we find that ISIL was the most influential perpetrator group. TTP, on the other hand, appears to have become less influential over the years. We also observe that

Al-Nusrah Front continues to be among the top three influential groups. In the most recent network layer (2014 – 2016), we see perpetrator groups, such as "Jaysh al-Islam (Syria)" and "Southern Front", which is ranked in 4th position after "Jaysh al-Islam (Syria)", appear for the first time as one of the most influential perpetrator groups. Both of these groups have carried out most of their operations in Syria. It may be important to pay attention to these groups by monitoring their activity in the future.

Figure 5.9 represents the network layer for 2015 – 2016. It shows the heat map representing influence strength for this layer, where red represents the most influential nodes and green is the least influential. The top five perpetrator groups whose influence strength was the highest and their respective locations in the network are identified.

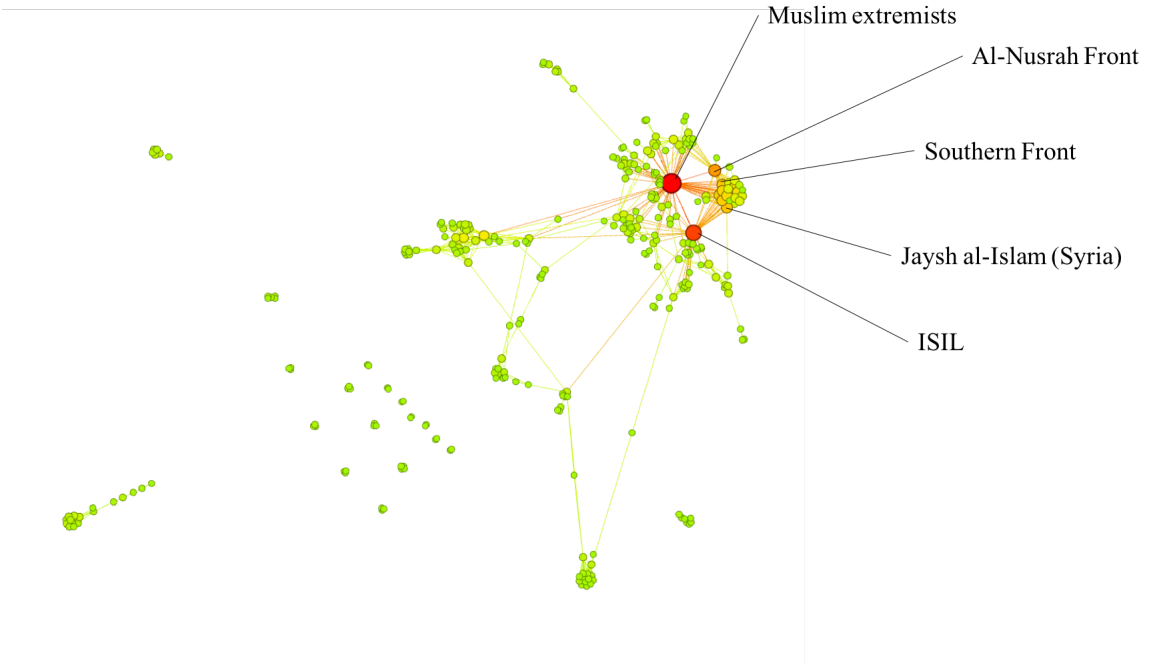

Figure 5.9. Influence Strength at Network Layer 2015 – 2016

We also run the Louvain community detection algorithm on the 2015 – 2016 network layer. We find that, with the exception of "Muslim extremists" which is a generic perpetrator group name, the other four most influential perpetrator groups reside within the same community. Further investigation shows that these nodes, ISIL, Al-Nusrah Front, Jaysh al-Islam(Syria), and Southern Front, are also neighbors of each other. When two highly influential nodes are at close proximity, there may exist a competition [16]. Therefore, we may be able to use

our analysis to anticipate a power struggle between these groups.

Using the 2014 – 2015 network layer, which consists of the highest number of terror activities, we compare the results produced by our method against the ranks produced by existing network algorithms (eigenvalue centrality, betweenness centrality, and closeness centrality). Table 5.5 shows perpetrator group rankings using our influence strength metric and the ranks computed from the existing network centrality algorithms.

Table 5.5. Comparison of Ranking between Influence Strength and Existing Network Algorithms

Rank	**Influence Strength**	**Eigenvalue Centrality**	**Betweenness Centrality**	**Closeness Centrality**
1	Muslim Extremists	Muslim Extremists	Muslim Extremists	Muslim Extremists
2	ISIL	Ansar Al-sharia (Libya)	ISIL	ISIL
3	Tribesmen	Haftar Militia	Tribesmen	Tribesmen
4	Al-Nusrah Front	Libya Revolutionaries Operations Room	TTP	TTP
5	TTP	Libyan Militia	Anarchists	Al-Nusrah Front

Table 5.5 shows some similarities and differences when comparing with different existing network algorithms. When compared with our influence strength metric, closeness centrality appears to produce the most similar results. However, this result may not be the same for the other network layers. When we run a similar comparison on the 2015 – 2016 network layer, the results show that the ranks produced by closeness centrality are no longer similar to those produced by our influence metric. This shows that our influence metric is unique and does not necessarily follow the ranking produced by the centrality measures.

As mentioned in Chapter 4, we are also interested in identifying perpetrator groups who show indicators of increasing influence. Table 5.6 shows the top five perpetrator groups with the highest indicators of increasing influence.

Table 5.6. Top 5 Perpetrator Group with Increasing Influence Strength Trend (sorted from the largest number increasing influence strength, to the smallest at the bottom)

Rank	Perpetrator Group	Community
1	Islamic State of Iraq and the Levant (ISIL)	1
2	Ahrar al-Sham	1
3	Al-Nusrah Front	1
4	Ansar al-Sharia (Libya)	2
5	Muslim extremists	2

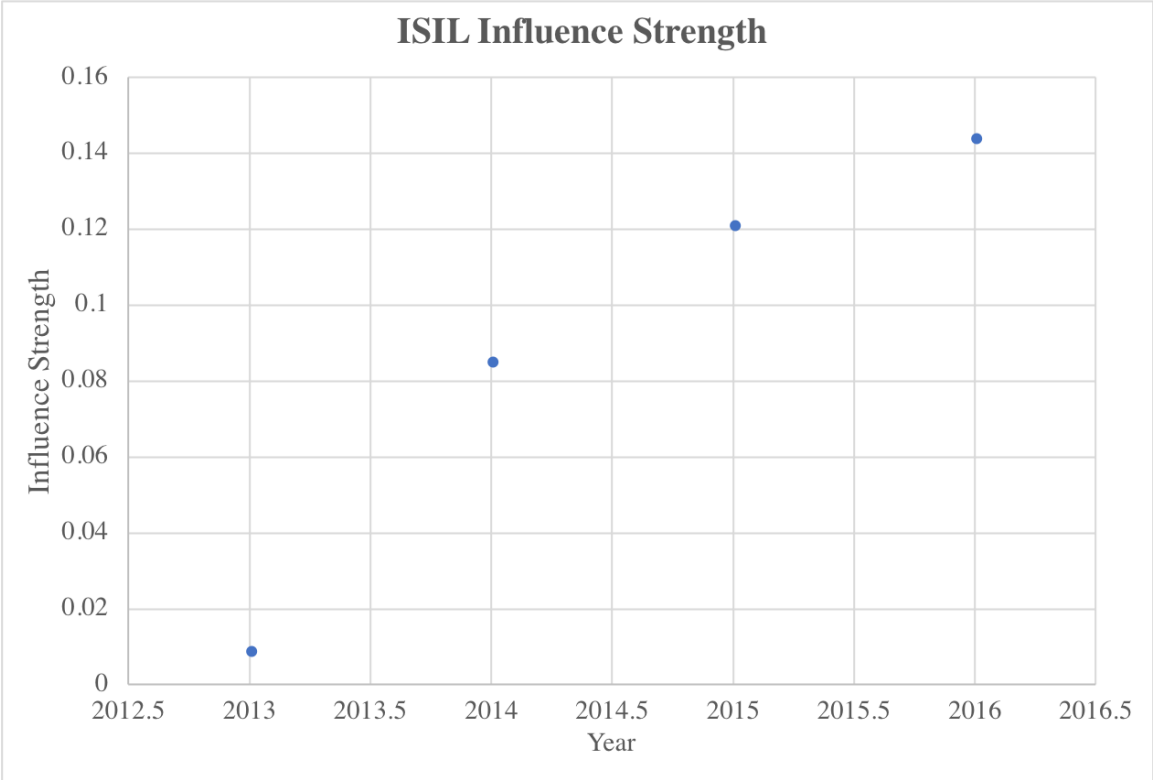

Figure 5.10. ISIL Influence Strength: 2013 – 2016

ISIL, Ahrar al-Sham, and Al-Nusrah Front are the top three perpetrator groups in terms of growing influence strength. The increasing influence of these groups may indicate that a growing number of other perpetrator groups want to conduct operations with similar target types and locations. These three perpetrator groups may have the potential to grow and influence many other groups in the future. Currently, ISIL remains the most dangerous

perpetrator group with the highest influence score and the highest growth in influence strength. Figure 5.10 illustrates ISIL's increase in influence strength since 2013. Lastly, as seen in Table 5.6, the Louvain algorithm shows that all three of the top perpetrator groups with increasing influence strength are located in the same community.

CHAPTER 6:
Conclusion and Future Work

In this thesis, we use network science to demonstrate the evolution of terrorism from 1970 to 2016. Using data available from the GTD, we provide analysis on the data from a global perspective, and adopt a novel network science approach to evaluate the influence strength of terrorist groups. In this chapter, we summarize our key findings from this thesis and then conclude by highlighting the corresponding potential for further research.

6.1 Conclusion

In the first part of the thesis, we present a summary of the GTD data. Based on the data, the number of terror activities has surged since 2011. We also observe that the number of perpetrator groups recorded in each year has nearly doubled since 2011, but this increase is not a dramatic as the increase in the number of activities. The largest number of perpetrator groups ever recorded was in 1992, when 390 perpetrator groups were recorded in that single year, which is still more than the number of perpetrator groups in 2016. Another interesting observation is that terrorism appears to be shifting eastward, with more recent terror activities recorded in central Asia. Some of the recent terror activities also occurred and intensified on lands near the coastal regions.

Influence plays an important role in a network, as nodes which are highly influential can induce a response from neighboring nodes. In areas of terrorism, perpetrator groups which are highly influential may influence the conduct of similar terror operations by other groups. These highly influential groups may be the main drivers as they lead to faster and wider spreading of terrorist ideologies. By focusing resources to identify and isolate these influential groups we hope to disrupt information spreading, thus breaking the network apart.

In this thesis, we adopt the idea from Adithya Rao [34], and formulate a method to measure and rank the influence strength of a terrorist group based on a set of responses from neighboring groups. The influence score metric allows us to measure a perpetrator group's actual influence score based on the terror activities of neighboring groups, as compared to

existing measures, which determines the group's influential strength by its relative position in the network. We highlight some of the more recent highly influential perpetrator groups and identify those perpetrator groups who show positive growth in influence strength. We believe groups like ISIL, Ahrar al-Sham, and Al-Nusrah Frontmay show the greatest potential to influence others in the near future.

6.2 Future Work

6.2.1 Alternative Computation of Influence Score

Our calculation of the influence score (Definition 13) depends on the number of neighboring nodes, the number of neighboring nodes being influenced, and the total number of nodes in the network. However, during computation, the number of neighbors is subjected to cross-cancellation and disappears from the final result. In the future, we recommend looking at how to provide an extension or alternative to this formula so that the final influence score for a node in the network is also quantified by the number of neighbors the node has.

6.2.2 Indirect Influence Measure

Our work focuses on an individual perpetrator group's direct strength of influence by observing the actions of the group's immediate neighbors. However, influence may spread beyond the immediate set of neighbors. In the terrorist network, it is possible that perpetrator groups may be indirectly influenced by other groups which are more than 1 degree of separation away. A group's influence score should also incorporate measures of indirect influence. Additionally, our study of influence was based on similarities between target types and locations. There are other attributes which could indicate a positive response to influence. For example, the use of similar weapon types or methods of attack by the perpetrator groups could indicate influence. However, determining the exact weights for each of these contributing factors, as well as validating the model, will be extremely challenging.

6.2.3 Influence Susceptibility

This work focuses on a way to identify the most influential perpetrator groups based on the groups they appear to have influenced. We did not look at what makes perpetrator groups

susceptible to influence. An interesting question to ask is: How do we detect if a terrorist group is susceptible to influence? And, assuming we could identify susceptible groups, how do we quantify their susceptibility? Is there a position in the terrorist network which can correlate to this influence susceptibility? The purpose of this future research would be to 1) identify the perpetrator groups which are highly susceptible to influence and 2) isolate them from groups which we determine to be highly influential. We believe that the isolation of perpetrator groups which are more susceptible to influence from the strongly influential groups would reduce the influence strength of these highly influential groups.

6.2.4 Analysis of Generic Perpetrator Groups

We mentioned in Chapter 3 that there is a very large number of perpetrator groups in the data set with generic group names. Almost 46% of the terror incidents recorded in the GTD cannot be attributed to a known perpetrator group. Another potential area of future research would be to examine the similarities and differences among these attacks in order to determine if there exists one or more perpetrator groups who are responsible for some of these attacks. We believe that it is possible that there may be groups who are attempting to remain anonymous so that they can continue to operate in the shadows, avoiding formal identification as a group of interest.

THIS PAGE INTENTIONALLY LEFT BLANK

List of References

[1] L. Euler, "Solutio problematis ad geometriam situs pertinentis," vol. 8, pp. 128–140, 01 1736.

[2] United States. White House Office, "National Security Strategy of United States of America," December 2017.

[3] J. G. March, "An introduction to the theory and measurement of influence," *American Political Science Review*, vol. 49, no. 2, p. 431–451, 1955.

[4] R. Lippitt, N. Polansky, and S. Rosen, "The dynamics of power: A field study of social influence in groups of children," *Human Relations*, vol. 5, no. 1, pp. 37–64, 1952. Available: https://doi.org/10.1177/001872675200500102

[5] R. Amato, A. Díaz-Guilera, and K.-K. Kleineberg, "Interplay between social influence and competitive strategical games in multiplex networks," *Scientific Reports*, vol. 7, p. 7087, Aug. 2017.

[6] B. Bollobás, *Modern Graph Theory*. New York, New York: Springer Science & Business Media, 1998, vol. 184.

[7] S. S. Ray, *Graph Theory with Algorithms and Its Applications: In Applied Science and Technology*. New Delhi, India: Springer Publishing Company, Incorporated, 2014.

[8] G. Chartrand and P. Zhang, *A First Course in Graph Theory* (Dover books on mathematics). Dover Publications, 2012. Available: https://books.google.com/books?id=ocIr0RHyI8oC

[9] M. Newman, *Networks: An introduction*. Oxford, England: Oxford University Press, 2010.

[10] S. Borgatti and M. Everett, "Network analysis of two mode data," vol. 19, pp. 243–269, 08 1997.

[11] A. Casteigts, P. Flocchini, W. Quattrociocchi, and N. Santoro, "Time-varying graphs and dynamic networks," *CoRR*, vol. abs/1012.0009, 2010. Available: http://arxiv.org/abs/1012.0009

[12] K. Stephenson and M. Zelen, "Rethinking centrality: Methods and examples," *Social Networks*, vol. 11, no. 1, pp. 1–37, 1989.

[13] G. Sabidussi, "The centrality index of a graph," *Psychometrika*, vol. 31, no. 4, pp. 581–603, 1966.

[14] F. Radicchi, C. Castellano, F. Cecconi, V. Loreto, and D. Parisi, "Defining and identifying communities in networks," *Proceedings of the National Academy of Sciences of the United States of America*, vol. 101, no. 9, pp. 2658–2663, 2004.

[15] M. E. J. Newman and M. Girvan, "Finding and evaluating community structure in networks," *Physical Review*, vol. E 69, no. 026113, 2004.

[16] P. V. MARSDEN and N. E. FRIEDKIN, "Network studies of social influence," *Sociological Methods & Research*, vol. 22, no. 1, pp. 127–151, 1993. Available: https://doi.org/10.1177/0049124193022001006

[17] M. E. Shaw, "Some effects of unequal distribution of information upon group performance in various communication nets," *Journal of Abnormal and Social Psychology*, vol. 49, no. 4, pp. 547–553, 1954.

[18] D. Chen, L. Lü, M.-S. Shang, Y.-C. Zhang, and T. Zhou, "Identifying influential nodes in complex networks," *Physica a: Statistical mechanics and its applications*, vol. 391, no. 4, pp. 1777–1787, 2012.

[19] L. C. Freeman, "A set of measures of centrality based on betweenness," *Sociometry*, pp. 35–41, 1977.

[20] L. Katz, "A new status index derived from sociometric analysis," *Psychometrika*, vol. 18, no. 1, pp. 39–43, 1953.

[21] S. Brin and L. Page, "The Anatomy of a Large-Scale Hypertextual Web Search Engine In: Seventh International World-Wide Web Conference (WWW 1998), April 14-18, 1998, Brisbane, Australia," *Brisbane, Australia*, 1998.

[22] M.Newman, *Networks: An Introduction.* Oxford University Press, Inc., New York, NY, USA, 2010.

[23] Y. Bar-Yam, *Dynamics of Complex Systems*. Reading, MA Addison-Wesley, 1997, vol. 213.

[24] U. Kang, S. Papadimitriou, J. Sun, and H. Tong, "Centralities in large networks: Algorithms and observations," in *Proceedings of the 2011 SIAM International Conference on Data Mining*. SIAM, 2011, pp. 119–130.

[25] S. Boccaletti, G. Bianconi, R. Criado, C. I. Del Genio, J. Gómez-Gardenes, M. Romance, I. Sendina-Nadal, Z. Wang, and M. Zanin, "The structure and dynamics of multilayer networks," *Physics Reports*, vol. 544, no. 1, pp. 1–122, 2014.

[26] M. Kas, M. Wachs, K. M. Carley, and L. R. Carley, "Incremental algorithm for updating betweenness centrality in dynamically growing networks," in *Proceedings of the 2013 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining*. ACM, 2013, pp. 33–40.

[27] C.-C. Yen, M.-Y. Yeh, and M.-S. Chen, "An efficient approach to updating closeness centrality and average path length in dynamic networks," in *Data Mining (ICDM), 2013 IEEE 13th International Conference on*. IEEE, 2013, pp. 867–876.

[28] S. J. Brams, H. Mutlu, and S. L. Ramirez, "Influence in terrorist networks: From undirected to directed graphs," *Studies in Conflict & Terrorism*, vol. 29, no. 7, pp. 703–718, 2006.

[29] J. Arquilla and D. Ronfeldt, *Networks and Netwars: The Future of Terror, Crime, and Militancy*. Santa Monica, CA: Rand Corporation, 2001.

[30] R. Lindelauf, P. Borm, and H. Hamers, "The influence of secrecy on the communication structure of covert networks," *Social Networks*, vol. 31, no. 2, pp. 126–137, 2009.

[31] I.-C. Moon and K. M. Carley, "Modeling and simulating terrorist networks in social and geospatial dimensions," *IEEE Intelligent Systems*, vol. 22, no. 5, 2007.

[32] L. Festinger, K. Back, and S. Schachter, *Social Pressures in Informal Groups: A Study of Human Factors in Housing* (Research Center for Group Dynamics series). Stanford University Press, 1950. Available: https://books.google.com/books?id=1zSsAAAAIAAJ

[33] S. V. Nath, "Crime pattern detection using data mining," in *Proceedings of the 2006 IEEE/WIC/ACM International Conference on Web Intelligence and Intelligent Agent Technology* (WI-IATW '06). Washington, DC, USA: IEEE Computer Society, 2006, pp. 41–44. Available: http://dx.doi.org/10.1109/WI-IATW.2006.55

[34] A. Rao, N. Spasojevic, Z. Li, and T. DSouza, "Klout score: Measuring influence across multiple social networks," *CoRR*, vol. abs/1510.08487, 2015. Available: http://arxiv.org/abs/1510.08487

[35] N. Agarwal, H. Liu, L. Tang, and P. S. Yu, "Identifying the influential bloggers in a community," in *Proceedings of the 2008 International Conference on Web Search and Data Mining* (WSDM '08). New York, NY, USA: ACM, 2008, pp. 207–218. Available: http://doi.acm.org/10.1145/1341531.1341559

[36] B. Ganor, *Trends in Modern International Terrorism*. New York, NY: Springer New York, 2011, pp. 11–42. Available: https://doi.org/10.1007/978-0-387-73685-3_2

[37] National Consortium for the Study of Terrorism and Responses to Terrorism (START). (2016). Global Terrorism Database [Data file]. [Online]. Available: https://www.start.umd.edu/gtd

[38] S. Mullins, "Social network analysis and counter-terrorism: measures of centrality as an investigative tool," *Behavioral Sciences of Terrorism and Political Aggression*, vol. 5, no. 2, pp. 115–136, 2013. Available: https://doi.org/10.1080/19434472.2012.718792

[39] R. Lindelauf, P. Borm, and H. Hamers, *Understanding Terrorist Network Topologies and Their Resilience Against Disruption*. Vienna: Springer Vienna, 2011, pp. 61–72. Available: https://doi.org/10.1007/978-3-7091-0388-3_5

[40] The White House, "National Strategy for Combating Terrorism," February 2003.

[41] T. Oliphant, "Python for scientific computing," vol. 9, pp. 10–20, 06 2007.

[42] R. L. E. L. Vincent D. Blondel, Jean-Loup Guillaume, "Fast unfolding of communities in large networks," *J. Stat. Mech. (2008) P10008*, 2008.

[43] C. Francalanci and A. Hussain, "Social influence and influencers analysis: A visual perspective," in *Data Management Technologies and Applications*, M. Helfert, A. Holzinger, O. Belo, and C. Francalanci, Eds. Cham: Springer International Publishing, 2015, pp. 81–98.

Initial Distribution List

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California