A New Model for Predicting and Dismantling a Complex Terrorist Network

BOTAMBU COLLINS1,2, DINH TUYEN HOANG3, NGOC THANH NGUYEN4,5, (Senior Member, IEEE), AND DOSAM HWANG1

1Department of Computer Engineering, Yeungnam University, Gyeongsan 38514, South Korea
2MX Company Ltd. Group, Daegu 427-34, South Korea
3Faculty of Engineering and Information Technology, Quang Binh University, Đông Hới, Quảng Bình 510000, Vietnam
4Faculty of Information Technology, Nguyễn Tất Thành University, Hồ Chí Minh City 70000, Vietnam
5Faculty of Computer Science and Management, Wrocław University of Science and Technology, 50-370 Wrocław, Poland

Corresponding author: Dosam Hwang (dosamhwang@gmail.com)

ABSTRACT The perennial nature of terrorist attacks in recent times has ushered in a new wave of study in the field of terrorism known as social network analysis (SNA). Terrorist groups operate as a social network stealthily to enhance their efficacy rate, thereby making sure their activities are cloaked. This study proposes a new method to uncover and dismantle a terror network by applying a 4-centrality measure. After establishing link prediction using centrality measures, we dismantle the network based on Galton-Watson extinction probability. This study examines the 9/11 incident and measures the link prediction of the M-19 network. In curbing terrorist network activities, the elimination of a highly ranked node in the network is a condition sine qua non. We further examine the lethality of the network as well as network bonding to obtain the degree of cohesiveness, which is a crucial determinant for network survival. Our experimental results indicate that link prediction is vital in uncloaking a terror network, which is the core of counterterrorism.

INDEX TERMS Modeling terrorist network, network bonding, modeling lethality, terrorist network cohesiveness, M-19 network, 4-centrality measures, Galton-Watson extinction.

I. INTRODUCTION

Recently, terrorist activities have increased globally with terrorist groups and networks found guilty of causing chaos to humanity. The abhorrent nature of terrorism attacks has destroyed countless lives and property. Counterterrorism measures are necessary to curb terrorist activities, and understanding their operational model is a stepping stone. The literature on how to uncloak a terror network has increased drastically in recent years. [1], [2], [3], [4]. However, there has been much adversity in the formal approach of counterterrorism deployed by stakeholders, which is backed by the resilient nature of the modern-day terrorist group as their actions recorded over 180,000 cases from 1970 to 2019 according to data from the Global Terrorism Database (GTD). Consequently, many studies have been conducted to find a suitable solution.

The associate editor coordinating the review of this manuscript and approving it for publication was Leandros Maglaras3.

Terrorism is a nonstatic and dynamic process [5]. Research has shown that terror groups both new and experienced exchange and share intelligence on operational tactics, especially in a situation where the transactions of the latter are successful. Hence, for us to dismantle a terror network, our operational models need to be dynamic. The application of a social network model with link analysis (SNA) has been useful in curbing terrorist activities [3], [6], [7]. Contrary to a social network, a terror network has a subcell (periphery) out of its main network (core). In this study, we considered the core to be the command and control center (see the terror network command center). The core directs and oversees the operation of the periphery. The terror network operates a pecking order structure with every vertex having a defined function in the network [6], [8], [9], [10].

Gaining insight into a terrorist operational model is a stepping stone toward curbing terrorist action [8]. Scholars involved in this approach have often argued that the modeling of the terrorist network is an NP-complete problem [4].
The tragic event of 9/11 paved the way for the first mapping of the terror network by Valdis Krebs [7], and his work became the baseline for the study of the 9/11 terror network [6], [10]. Krebs mapped out the network based on information from security experts and the press. The author included other conduits of the network that operated outside of the cells that we did not include in this study. Scholars involved in graphical modeling of terrorist networks citing 9/11 as a case study should consider the baseline provided by Krebs in [7].

A terror network is a surreptitious social network [8] having a stratified system that resembles an organizational network in its operation [1], [9]. Terror network operations are enshrouded in secrecy, making it difficult to track their transactions. More concretely, the obscure manner of terrorist operations makes surveillance challenging for security forces. In addition, the ambiguous nature of terrorist data makes it a difficult task [4], hence, scholars termed it an NP-complete problem. Consequently, a graph system is required to unmask their secretive nature [7]. There is no known clear approach to perturbing terrorist activities [3], [7]. Therefore, it is necessary to employ brute force and a heuristic approach in unmasking terrorist networks.

Conventional terrorist operations are stealth [7] thereby ensuring that their actions are unperturbed; this process necessitates the skills required to be maximally lethal. The theory of functionalism opined by David Mitrany [11], he posits that cooperation among a network of entities will necessitate conditions necessary for further cooperation leading to spillover effects or ramification processes. Where certain conditions change states’ interest from areas of low cooperation to areas of high cooperation, we assume that the terrorist action takes the process of ramification as well with a cascading effect (see network lethality section). The prevalence of maximal lethal attacks is a result of a conducive environment [4]. Terrorist only operate in a neighborhood that it sees as a safe haven with conducive environmental features capable of concealing their operations as well as enhancing its efficacy. We see a terrorist network (TN) to be a surreptitious network graph \( TN = G \). With a set of actors \( V \) (nodes) sharing information within them (edges \( E \)) such that \( TN = G(V, E) \) indicates the interaction within the network such that \( V, E \) shows there exists a relationship. For the convenience of this study, we applied the concept of vertices and nodes interchangeably.

The justification of this work rests on the supposition that terrorism is a vigorous affair in which a group with a similar ideology will mimic the same tactics employed by other groups to make their transactions successful. As a result, we surmised that since the transaction of the M-19 was a success, other terrorist organizations will use the same pattern of operation. Thus, a vivid study of the M-19 network and operational model will act as a useful tool in countering terrorism in the future.

This study seeks to answer the following research questions:

- How can a terrorist network be unmasked?
- Can link prediction act as a counterterrorism measure?
- How can a terrorist network be dismantled?

This paper is a revised and expanded version of an earlier work by B.Collins et al. [33] which was presented at the International Conference on Industrial, Engineering & Other Applications of Applied Intelligent Systems IEA/AIE 2020.

The contribution of this paper is as follows:

1. To the best of our knowledge we are the first to examine the M-19 network by predicting missing links in the network. We build a heuristic algorithm based on 4-centrality measures that we use to predict and rank nodes in the network.
2. The algorithm proposed here outperforms other studies as the result put Mohammed Atta as the central figure, which is in line with the 9/11 commission report.
3. We proposed a unique model to measure network lethality and cohesiveness.
4. We build a mathematical model for dismantling a terrorist network using the Galton-Watson tree extinction process.

Finally, we prove that terrorist activities are enhanced as a result of conducive environmental features.

The rest of this paper is organized as follows: Section 2 examines related work, while Section 3 is the methodology. Section 4 is our case study, where we succinctly give an account of the M-19 network that was responsible for the 9/11 event. We measure the lethality of the M-19 network and show the network bonding, also referred to as network cohesiveness. We also propose a new method for dismantling a terror network. We discuss our results in Section 5, while the conclusion and future directions are presented in Section 6.

II. RELATED WORK

The scholarship on a terrorist network has witnessed a manifold increase in recent times, especially concerning gaining insight into a terrorist network. Diverse approaches to understanding terrorism such as the use of AI [24], including the CNN model [29], machines learning [25], [26], [27], [31], and natural language processing [28] have all been applied. The work in [20] suggests the aggregation of knowledge from diverse sources in solving complex issues collectively. Concerning graph theory, many authors have applied graphs to explain certain phenomena [30], such as recommendation systems in graph networks [18]. The application of multilanguage semantic behavioral algorithms to aid in intelligence gathering was examined in [23], and the study provides insight into jihadist activities online. In [5], the scholar examined the rationale behind the disappearance of some terror networks and contends that splintering accounts for the extinction of some terrorist groups. Some terrorists splint from the core network to integrate with another network, leading to the extinction of such a group. Furthermore, terrorist seek to foster an ideology, and terrorist groups with identical doctrines will usually join forces to boost their vitality. Ideological differences and failure to come to a common consensus may facilitate a node splinting from one network
to another. Smaller networks facing the threat of extinction will be gained by a larger network with a higher life span [5].

The application of the self-exciting point process model also known as the Hawkes process [19] to curb terrorism was coined in [12]. The author developed the point process model and observed that events themselves are self-exciting and that terrorism follows a series of attack patterns within a given space and time. The Hawkes process, although originally modeled to predict the likely occurrences of natural disasters such as tsunamis, and earthquakes, has been a success in predicting the likelihood of a terrorist attack. The point process has a preliminary model known as the Poisson process, which stipulates that event occurrences are statistically independent of each other. The Hawkes process is a simplified self-exciting point process whose parameter functions depend on the previous history of events [19]. The Hawkes process holds the premise that the occurrences of a chain of events will create conditions that necessitate future events to occur. viewed from this perspective, the successful operation of a terrorist will trigger a future attack, and hence, necessary steps must be taken to prevent future event occurrences or attacks. The use of probabilistic models to forecast terrorist threats using a combination of the Hidden Markov Model (HMM) and Bayesian Networks (BN) was examined in [4]. The scholar examined the events that unfolded before an attack such as forethought, designing target, personnel mobilization, resource mobilization, and execution. For instance, for an attack to be successful, the author contended that “a terrorist withdraws money from a bank, buys chemical which can be used to make a bomb, purchase a flight ticket into the USA, and carry out an attack in the USA such as the 9/11.” It took nearly four years to plan the 9/11 bombing and approximately one year to plan the bombing of Bali and Madrid [4]. Thus, predicting this scenario will act as a prevention mechanism for future attacks.

For instance, in [6], the author used a heuristic approach in examining a terror network, including SNA, agent-based, and NK-Boolean fitness landscapes, to measure the complex and dynamic nature of a covert terror network. The author argued that a terrorist network consists of a stratified structure with deceit being a noticeable scheme adopted by the terror group. Additionally, some authors investigated the set of norms and customs governing deportment within a terror network to understand the cohesive nature of agents in the network [13]. The author studied the role of key players in a terror network and contended that the finance operator holds an important function on the success of the network. Although the terrorist network appeared obscure, its operations take a pecking order with decisions and task distribution made at the top, thereby mimicking real organization in its performance [13]. Hidden features in the network can be unclad through link prediction, such as actors’ interactions, which is an important element to consider when simulating a terror network. In contrast to our work, the authors used centrality measures but failed to calculate these measures in terms of index and performance. More to the contrasting nature of this study is that no real case study was employed; rather, the work used 3-centrality measures, whereas we used 4-centrality measures; eigenvector, degree, betweenness, and closeness centrality. As a close cognate to our study is the work of Bo Li and collaborators in [9], the authors propounded the agent-based terrorist network simulations and looked at the functions of different agents in the network. They further posited that the actions of the agents are not mutually exclusive to the network output.

Francesca Spezzano and colleagues [14] investigated the terrorist network to solve the person’s successor problem. The person successor problem here refers to who will restore leadership and maintain network functionality and efficiency in case an important node is removed from the network. This work brings to the limelight how a terrorist network...
restructures itself after the removal of a key node. The removal of a core node in the network will prone the network to fail and limit its lethality. For instance, the deletion of Osama Bin Laden led to the Al-Qaeda network being less lethal and limited in its transactions. A number of factors are adduced to explain this scenario; for example, when a core node is deleted from the network, there is the danger of network extinction. Furthermore, there is pressure to reshape itself and gain normality or restore itself to default. For this to happen, it will require a new vertex that has the same features as the removed node which is a challenging task for the network. Forecasting a core vertex whose removal will render the network inactive is crucial in restraining the severity of the network’s actions [14]. This study varies in that the focus is on the M-19 network responsible for the devastating incident of 9/11. Instead of foretelling the outcome of a node’s removal from the network, our focal point is unveiling the whole network, which is an indispensable step in terrorism prevention.

A study closer to ours is that of Zhendong Su et al. [15], who applied the 9/11 event as a case study to predict missing vertices in the network. The study was driven by the fact that most studies on terrorist network modeling are based on known information, which is usually erroneous, and hence, previous studies constructed terrorist networks by leaving out some key nodes. Using link prediction, the author could solve the disintegration problem in terrorist networks. Contrary to our research, the author used 62 vertices in the 9/11 event which indicates the inclusion of vertices that were not physically involved in the hijacking of the planes. By contrast, we focused on the 19 vertices that were involved in the action. We then measure the lethality of the network and show its resilient nature.

Last, feminist models have been examined to show the actions of women in a terror network. A solid case in point is Pedro Manrique and collaborators [32], who proposed a mathematical model to show the importance of women in a terror network. Although viewed as a feminist approach, the authors shed light on the pivotal role of women by identifying their key roles. Using ISIS as a case study, they observed that although men appear to dominate the network numerically, women hold a central role in terms of connectivity and can easily conceal network activities.

III. METHODOLOGY
The application of social network analysis (SNA) in modeling a terrorist network appeared nebulous with the use of simulated graph networks built upon the intelligence unveiled after the occurrence of an incursion by the terrorist. Concerning the M-19, the 19 nodes accountable for the tragic incident were unravelled after the incident, and intelligence gathering uncovered an associated network covering a fragment of the world. For our dataset, we utilized the dataset from [16] and a revised version of the M-19 graph modeled by [7]. We affixed a code (M-01 to M-19) to the 19 individuals who were liable for the 9/11 incursion, as seen in Table 1.1.

We then applied breadth-first search to traverse the graph to uncover geodesics, which is a stepping stone in computing centrality measures. Link prediction was modeled with the application of 4-centrality measures, where we ranked the nodes using the PageRank technique to determine the key node in the graph. We represented the various nodes on a matrix and iterated them up to $m$ times where $M = 200$. The iteration process ended when the results remain perpetually fixed; hence, at $M = 200$ our iteration process stopped. To obtain the betweenness centrality, the Girvan–Newman algorithm was computed [21], [22]. Note that each centrality measure was computed using various algorithms. Our algorithms revealed that M-01 is the most linked node in the network, suggesting that his deletion will render the network inactive, as seen in FIGURE 1. We calculated the lethality of the network as well as network cohesiveness. Furthermore, we compared the lethality of the M-19 network with other global terrorist networks, and our results showed that the M-19 network has the highest casualty rate ever recorded by a terrorist network in the last 10 years. Finally, we proposed a new model for dismantling a terror network by applying the Galton-Watson extinction probability.

A. THE M-19 NETWORK
The M-19 network is composed of 19 members of the al Qaeda terrorist group that were accountable for the deadly incident of September 11, 2001. With Osama Bin Laden at the helm of the terror network, the hijacking of 4 US commercial planes led to one of the deadliest terror attacks in history. FIGURE 3 depicts the entire M-19 network with colors representing the different flights.

![FIGURE 3. M-19 network.](image-url)

M-19 involves a network of 19 nodes (terrorists) whose actions construct a cell of 5 vertices each based on a target mission, as seen in FIGURE 3. The other 4 subcells are shown in FIGURE 4.

The security protocol allows for the shootdown of an enemy plane entering United States’ territory [16], Contrary
FIGURE 4. Four cells of M-19 network.

to 9/11, the US never envisages a situation whereby a civilian plane could be turned into a missile [16]. The terrorist split itself into subcells, where each plane contains 5 members of a cell and 4 members in the 4th plane. Based on the report in [16], it is not clear whether flight 93 was shot down because, by the time of the crash, an order had already been given for it to be shot down. FIGURE 4 shows the different 4 subnetworks or cells. We split the M-19 network into cells of 4 based on the 4 hijacked planes.

B. TERROR NETWORK CONTROL CENTER

Every terror network has a command or control center that directs its activities, monitors performance, seeks the necessary funding, and sets a finite target to be met. The work of Brian Jackon in [17] gives insight into the command and control center of a terrorist network. Jackson identified 3 types of controls exerted by the network leader to be strategic i.e., the ability to set and define the goals and objectives of the network. Operational control i.e., the ability to monitor and engage in furtherance of the network’s principal objective. Finally, tactical control indicates influencing other vertices in the network to oversee the day-to-day running of the organizational business. The work in [17] also describes a format in which a terrorist network is constructed: the author maintained that terror networks or organizations are bound by connections that exist within the community of the network. In constructing a terrorist network that can function and yield the necessary output, the author surmised that “a group of individuals (vertices) is required with the necessary connections among them, with strong communications skills, and the authority to establish relationships necessary to shape a coherent agenda for the network’s activities” [17].

FIGURE 5 shows the M-19 control center linked to the Al Qaeda base in the Middle East. C1, C2, C3, and C4 depict the 4 different conduit subcells that hijacked the 4 airplanes. G1, G2, and G3 are gatekeepers, necessary to enhance the efficacy of the network and improve its stealthy nature.

The gatekeepers prevent direct communication with the main Al Qaeda network, making it difficult to be uncoiled. The Middle East is already listed as a haven for most terrorist organizations, and hence frequent communication from the Middle East with the different conduit units may be suspicious. Hence, the need for gatekeepers becomes inevitable. These gatekeepers are believed to be those vertices that were in other parts of the world especially in Europe to monitor the progress of the mission. To further elucidate the stealthy nature of the M-19 network, Osama Bin Laden in an audio message alluded that some conduit members did not know the identity of others even if they communicated. They perform different functions, meaning that some conduits could engage in the act of terrorism not necessarily knowing that he or she is aiding terrorism.

C. LETHALITY AND COHESIVENESS OF THE M-19 NETWORK

The lethality of a terrorist network is considered the extent to which a terrorist network can cause severe casualties on a given target. It is calculated based on the severity of the network [10], [14], and previous records are considered when denoting its formula. FIGURE 6 below indicates the lethality of the M-19 network. The terrorist actions take the process of ramification catalyzed by an enabling environmental feature (ConE) [4] consequently, ramifying itself from areas of low action LA (soft Target denoted as $SiTi$) to the areas of high action $Ha_i$ (Maximally Lethal Target denoted as $(Max_{Li\in Ti})$). The ramification process is denoted as;

$$Ram = ConE(LA..SiTi \rightarrow Max_{Li\in Ti} Ta(\text{HA}))$$

$Ram$ is the ramification process from areas of low action. $ConE$ is the conducive environment that enhances the process. $SiTi$ is the soft target when the environment is unconducive for the terrorist to be lethal. $(Max_{Li\in Ti})$ is the maximally lethal target which is triggered by enabling environmental features. $Ha_i$ is the area of high taction.
In this light, we assume that the M-19 enjoys a conducive environment in the United States (USA), which maximizes its lethality. Equation (1) above shows the process for the network to be lethal. For the lethality itself, the formula is as follows:

\[ LT(\text{Severity})PT_i = \frac{1}{n} \sum_{CaS+n\in T_1,\ldots, T_n} \frac{\text{TotalAction}(TA_i)}{\text{numberofplannedTarget}(PT_i)} + Target(T_i) \]  

(2)

Let \( LT \) be lethality which represents the severity and all planned targets of the network.

\( PT_i \) is the planned target or desired target, we hypothesized that terrorists set out a finite target to be met. Therefore, the probability for all desired \( PT_i \) to be met is \( \frac{1}{R_i} \) or \( \frac{1}{n} \). \( CaS+n \in T_1, T_2, \ldots, T_n \) denotes the casualty representing the summation of different targets such as \( T_1, T_2, \ldots, T_n \), which depicts the 4 hijacked planes by the M-19 network.

Finally, the lethality will be derived simply by the summation of all the casualties reached from all given targets, plus the percentage of all actions carried out plus the target met. We assume that a terrorist can still cause damage without meeting its desired target. Hence, one must consider the extent of network cohesiveness (NC) or group bonding.

We hypothesize that the efficacy of the network is backed by the level of network cohesiveness. The higher the network bonding is, the more lethal the network.

Given a terrorist network \( TN = G(V_i \in NC) \) For \( V_i \in NC \): Let \( R_i \) be a set of requirements for a vertex to join the network;

Let \( TiTi \) be the training time requirements for a vertex to be sent on a mission;

Let \( \text{fb}(g, b) \) be a set of factor binding \( V_i \) with \( G \);

Let \( \text{LP}(g, b) \) be the level of punishment that \( V_i \) will receive for disconnecting from \( G \);

Let \( dp \) be the probability for the vertex to disconnect from the network;

Let \( w_i \) be the probability that \( V_i \) will disconnect at will \( w_i = 1 \);

Let \( S_i \) be the probability that \( V_i \) will disconnect but not at will (possible arrest by police) \( S_i = 0 \).

The degree of network cohesiveness is derived as follows:

\[ NC(g, b) = d \frac{T_iT_i}{R_i} \sum \text{fb}(sn) \]  

(3)

In calculating the \( NC \), we made 4 assumptions that guide our formulation.

Assumption 1: Given a Terrorist Network \( TN = G \) with a network cohesiveness (NC) such that the NC prevents a certain vertex \( V_i \) from disconnecting from the network. The damages to be incurred by the vertex as a result of disconnecting from the network outweigh the benefits. If \( NC > g = 1 \) otherwise if \( NC < g = 0 \). In other words, to guarantee group loyalty herein referred to as network cohesiveness, a given vertex is held of something more precious than his life such as immediate family members to guarantee that the vertex does not disconnect from the network (betray the network).

The formula for this is outlined as follows:

\[ NC(\text{betrayal}) = \frac{T_iT_i}{R_i} \sum \text{fb}(n(LP)) \]  

(4)

Let \( ai_1, ai_2, \ldots, ai_n \) be a set of binding factors that guarantees loyalty.

Assumption 2: Suppose a vertex \( V_i \) is a suicide bomber and is tasked to carry out a target \( T_i \). Once the task is carried out the vertex is automatically deleted from the network. Hence, compensation to family members or nodes connected to the vertex is performed to enhance network bonding and network cohesiveness. Let \( mb_w \) be a set of family relations binding \( V_i \) to \( G \); Let \( V_{id} \) be the disconnected vertex; Let \( V_{ir} \) be a replacement vertex such that \( V_{ir} \) must match the features of \( V_{id} \).

\[ mb_w \begin{cases} \text{if } V_{id} \notin G, \\ \text{input}(V_{ir}), \text{if } V_{id} \in V_{ir}, \\ 1, \text{if } w \in N, \\ \text{else : train new node} \end{cases} \]  

(5)

We hypothesized that compensation is accomplished before a vertex is deployed on a mission. Once the above conditions are set, a replacing vertex is prepared for future targets.

Assumption 3: Suppose a vertex \( V_i \) is a suicide bomber who is tasked with target \( Ti \) and the vertex disconnects from the network without completing the task. The vertex is deleted from the network, including nodes connected to it, which guarantees network bonding and cohesion.

\[ Ti(0, 1) = dp(w_iS_i) => V_{ir} = V_{ir}(\text{disconnect}) \]  

(6)

In equation (6) we believe that once a vertex disconnects from \( G \) whether at will \( w_i \) or not \( S_i \), such a vertex is deleted from the network, and every \( E \) relating to the node is blocked. We give \( T_i = 0 \) if he is not and \( T_i = 1 \) if he is disconnected. Therefore a replacing vertex is prepared for future targets.

Assumption 4: Suppose a vertex \( V \) is a suicide bomber who is tasked to target \( T_i \), and the vertex is disconnected from...
the network without it participation (such as being arrested or killed by the FBI). The nodes connected to the vertex are not removed from the network. Rather, the nodes are maintained, and compensation, as well as more roles, are given to them. Hence, a replacement vertex is prepared. The outcome of this assumption is the same as equation (6) above. The duration that a vertex has been in the network is crucial.

D. 4-CENTRALITY MEASURES

Centrality measures have been used to detect useful links in different networks. For example, the survey in [36] shows that centrality measures were applied to protein networks, which indicates that proteins with high centrality measures are essential protein, the view was also reflected in the work in [37] where the author maintained that some protein nodes become more important in terms of their centrality measures. Centrality measures are essential factors in the modeling and simulation of a terror network. In [8], the author argued that a suitable method to dismantle a terror network is the complete deletion of nodes having high centrality measures.

1) CLOSENESS CENTRALITY

The mean of the shortest path to all other vertices in the network is known as closeness centrality. Closeness centrality depicts how a vertex can quickly access information in the network. The formula is given as follows:

\[
\text{Closeness Centrality}(J) = \frac{1}{\sum_{i} d(i, j)}
\]

where \(d(i, j)\) is the distance between vertices \(i\) and \(j\). The normalized form of the equation is denoted as:

\[
\text{Closeness Centrality}(J) = \frac{N - 1}{\sum_{i} d(i, j)}
\]

where \(N\) is the number of vertices.

2) DEGREE OF CENTRALITY

This is the number of edges connected to a vertex such that it indicates the usefulness of the vertex. With the eigenvector centrality, the number of edges connected to a vertex does not imply that such a vertex is useful in the network; rather, the number of important edges connected to a given vertex gives it a meaningful position in the network. The formula is given as:

\[
\text{Degree Centrality}(G) = \sum_{j=1}^{n} x_{ij}(i \neq j)
\]

The normalized version is denoted as:

\[
\text{Degree Centrality}(G) = \frac{\sum_{j=1}^{n} x_{ij}}{(n - 1)(n - 2)(i \neq j)}
\]

3) BETWEENNESS CENTRALITY

The betweenness centrality here is the extent to which a vertex lies on the geodesics path between other vertices. The betweenness of edges is calculated based on the number of shortest paths. Here, we used the Brandes algorithm, which starts with a BFS search, visits every vertex once, and computes the number of shortest paths from M-01 to M-19 that go through each of the edges within the M-19 network. We denote the formula as follows:

\[
\text{Betweenness Centrality}(G(u)) = \sum_{i \neq u \neq j} \frac{\sigma_{ij}(u)}{\sigma_{ij}}
\]

\(\sigma_{ij}\) is the number of shortest paths from vertex \(i\) to vertex \(j\) and \(\sigma_{ij}(u)\) is the number of geodesics that pass through \(u\).

4) EIGENVECTOR CENTRALITY

Eigenvector centrality indicates the extent to which a vertex is connected to influence other vertices in the network. The computation for these centrality measures is quite complicated. A connection to an important individual in a network is more crucial than connecting with so many less important individuals.

We consider our terrorist network graph to be \(TN = G(V, E)\) with vertices \(V\), Let \(A = av, t\) be the adjacency matrix, that is \(av, t = 1\) if vertex \(v\) has a relationship with vertex \(t\) and \(av, t = 0\) otherwise if there is no relationship. Hence, we can denote this formula as:

\[
x_v = \frac{1}{\lambda} \sum_{t \in MG} x_t = \frac{1}{\lambda} \sum_{t \in MG} d_{t, v}
\]

where \(\lambda\) is a constant and \(MG(v)\) is a set of neighbors of \(V\).

![FIGURE 7. Showing 4-centrality measures.](image)

5) PageRank CENTRALITY

PageRank is analogous to the eigenvector centrality measure and it works by counting the number and quality of links to a node in a given network and estimating the usefulness of the node. Thus, there is the supposition that more important nodes are likely to receive more links from other nodes. PageRank although having a close link to eigenvector centrality assumes that a random walker in a network can start at an arbitrary node and follow the hyperlinks or edge and visit a given node. The probability of the random-walker visiting...
a given node is what defines this method. The simplified PageRank formula is denoted as:

\[ PR(t + 1) = MPR(t) \]

\[ PR(t1) = PR(t2) + PR(t3) + PR(t3) + PR(tn) \]

\[ PR(\mu) = \sum_{v \in M \mu} \frac{PR(v)}{L(v)} \]

The above equation shows the PageRank value for a vertex, which is dependent on the PageRank values for each node \( v \) contained in the set \( M \) (the set containing all nodes or vertices linking to node), divided by the number \( L(v) \) of links from node \( v \). The algorithm involves a damping factor for the calculation of the PageRank. The damping factor is introduced with a range of 0 and 1, and is denoted as:

\[ M = (1 - d)TM = dB \]

where: \( M \) is the Google-Matrix or PageRank matrix \( d \) being the damping factor \( TM \) is the transition matrix, and \( B \) is the identity matrix.

In a directed graph, we can use what is referred to as the steady state approach. We construct a transition matrix when the eigenvalue is 1, which is in the steady-state. We solve the eigenvalue-eigenvector problem by applying this formula:

\[ \overrightarrow{TM} = \overrightarrow{Pa} \]

where: \( \overrightarrow{TM} \) is the transition matrix of the hyperlinks. \( \overrightarrow{Pa} \) is the final page of the given nodes or vertices in the network. The sum of the column values is equal to 1 based on the probabilities. It is a Markov chain. The transition matrix defines the next steps or iteration when the stationary distribution becomes the final PageRank vector. A given matrix is considered positive column stochastic matrix if and only if: 1 is the largest eigenvalue, 1 is an eigenvalue with multiplicity 1, and for the eigenvalue 1; there exists a unique eigenvalue for which the summation of its entries equals 1. Following the Perron–Frobenius theorem, the sum of all nodes in PageRank is 1.

E. NEW MODEL FOR DISMANTLING A TERRORIST NETWORK

The method in STONE is about what will happen if a vertex is removed from the network, and how the network will reshape itself to be maximally lethal. Carley’s method is based on the premise that vertices with high centrality measures should be removed from the network to curb terrorist network activities and minimize the lethality of the network. Heuristically, our method involves the fusion of these novel methods. We begin by computing the different centrality measures (see 4-centrality measures), and we optimize our model using the Galton-Watson extinction process which explains the probability of a terrorist network (hereafter referred to as a tree) being extinct. However, our main goal is not to explain the Galton-Watson tree but to use it to trigger an extinction process of the M-19 network. The other part or function of the Galton-Watson tree is not explained in this work; only the branching process and extinction probability are explained. See FIGURE 10 for the M-19 tree with extinction probability.

Let \( BC_i \) be for the betweenness centrality such that \( BC_i = 1 \) indicates that such a vertex is highly ranked; otherwise \( BC_i = 0 \) is of low ranking.

Let \( DC_i \) be for degree centrality such where \( DC_i = 1 \) indicates that such a vertex is highly ranked, otherwise, \( DC_i = 0 \) is of low ranking.

Let \( CC_i \) be for closeness centrality such that \( CC_i = 1 \) indicates that such a vertex is highly ranked; otherwise, \( CC_i = 0 \).

Formally:

Denoted as

\[ |BC_i| + |DC_i| + |CC_i| + |EC_i| = TGR \]

If \( TGR = R_{Max} \), then remove node else: if \( TGR = 0 \), otherwise

For \( v \) in \( TGR \)

Let \( R_{Max} \) denote the highest-ranking node in the network; Let \( RV_i \) be the removed node; Let \( PR \) be the probability for the network to resize itself; The network will resize itself proportionally to the original size; \( L_i \) is the length of time the network resize itself.

The Watson Tree extinction model is then applied to give the probability of the terrorist node being extinct in the network.

Note that our goal is to remove the nodes according to the Galton-Watson tree such that the entire network becomes extinct.

1) BASIC NOTION OF GALTON-WATSON TREE

The Galton-Watson [34], [35] process is a stochastic method for network growth. In a real-life situation, it represents a population growth leading to their demise. The Galton-Watson tree is considered to be a random tree in which each vertex produces identical independent offspring. This is also known as the Galton-Watson branching process. Let \( T_k \) denote a discrete random tree in the branching process starting with a single parent (root or ancestor) having the probability \( P_k \) of producing an offspring up to the \( K^{th} \) generation.

We denote \( T_k \) as the set of all possible tree vertices.

\[ T_k = (i_1 = 1, i_2, \ldots, i_k) : k \geq 1, i_j \geq 1 \]

The Galton-Watson is a discrete tree \( t \) that is a subset of \( T_k \) satisfying the following condition:

\[ \delta = (1) \) is the root (\( \delta \in T_k \))

\[ \delta = (1, i_2, \ldots, i_k) \) is a vertex of generation \( k = |\delta| \), where \( |\delta| \) is the length \( \delta \)

All vertices \( (i_1, i_2, \ldots, i_k, i_{k+1} \geq 1) \) are offspring of \( \delta \) belonging to generation \( k + 1 \). Let \( N_1 : t \in T, i.r.v. \) accept values in 0, 1, \ldots with, \( N_3 = N \) having a generic of r.v. This is referred to as the law of offspring distribution.
a: OFFSPRING DISTRIBUTION
Let $P_k := PN = K$

$$m := E[N] = \sum_{k=0}^{\infty} kP_k$$

mean of the offspring.

$$\delta(T_s) := E[T_s^n] = \sum_{k=0}^{\infty} P_k T^k, T_s \in [0, 1]$$

b: FOR GENERATION RECURSION
Let $X_n := \delta \in T_s : |\delta| = n$ number of particles in the $k^{th}$ generation of $T_s$. 

$$X_1$$
$$X_2 = N(1)$$
$$\ldots$$
$$X_n = \sum_{i=1}^{\delta \in T_s} N_{\delta} \quad n \geq 2$$

For $n \geq 2$ let the recursion be:

$$X_n = \sum_{i=1}^{X_{n-1}} N_i \quad N_i = N, i.i.d$$

are independent of $X_n - 1$.

Denote

$$T_s := \sum_{n=1}^{\infty} X_n$$

number of the individual in $T_s$.

$T_s < \infty$ if and only if (iff) $X_n = 0$ for large $n$ : there exists an extinction of the process. If $T_s = \infty$ then $T_s$ is an infinite tree, hence; there is a nonextinction process (percolates).

c: EXTINCTION PROBABILITY
The extinction probability is done by applying the Horton’s law [35] stipulates that the number of $E[T_s]$ offspring of order $k$ in a discrete tree $T_s$ offspring of order $k$ in a discrete tree [34] leading to extinction.

We denote

$$P_{ex} := PT_s < \infty$$

extinction probability

Theorem 1: $P_{ex}$ is the least of the solutions in $T_s$ of the equation.

$$T_s = \delta(T_s) \quad \text{for} \quad T_s \in [1, 0]$$

Proof: Denoting $\delta_n(T_s) := E[T_s^n]$ by (22) above we have $n \geq 2$

$$\delta_n(T_s) = \sum_{k=0}^{\infty} P[X_{n-1} = k]E[T_s^{\sum_{i=1}^{k}N_i}|X_{n-1} = k]$$

(25)

Independence = $\sum_{k=0}^{\infty} P[X_{n-1} = k](E[T_s^{N_i}]^k$ 

Induction = $\frac{\delta(\delta(\ldots (\delta(T_s))\ldots))}{n^{th\text{time}}} = \delta_n(T_s)$

(26)

(27)

(28)
Moreover

\[ P_{ex} = P\left( \bigcup_{n \geq 1} \{X_n = 0\} \right) \]  

(29)

Increasing events \[ \lim_{n \to \infty} PX_n = 0 = \lim_{n \to \infty} \delta_n(0) \]  

(30)

since \[ \delta_n(T_s) = \delta^n(T_s) = \lim_{n \to \infty} \delta^n(0) \]  

(31)

Hence

\[ P_{ex} = \lim_{n \to \infty} \delta_n(0) \]  

(32)

\[ \text{continuity of } \delta(.) = \delta(\lim_{n \to \infty} \delta_{n-1}(0)) \]  

(33)

Proof that \( P_{ex} \) is the least solution in the equation (see Theorem 1). If we assume then for some \( \xi \), where \( 0 \leq \xi \leq 1 \), \( \xi = \delta(\xi) \). we obtain

\[ 0 \leq \xi \]  

(34)

\[ \delta(.) \text{ is increasing } \delta(0) \leq \delta(\xi) = \xi \]  

(35)

\[ \delta^n(0) \leq \xi \]  

(36)

\[ P_{ex} = \lim_{n \to \infty} \delta^n(0) \leq \xi \]  

(37)

Note that \( m = E[N] \) is the expected number of children of the offspring of a given vertex.

**Corollary 1:** If \( m \leq 1 \), \( P_{ex} = 1 \) (we consider it a subcritical case

if \( m > 1 \), \( P_{ex} = 1 \) is a supercritical case

if \( m = 1 \) (critical case)

Then If \( P_0 = 0 \) (hence \( P_1 = 1 \)) then \( P_{ex} = 0 \) if \( P_0 > 0 \) then \( P_{ex} = 1 \)

Proof: Recall \( \delta(0) = P_0 \), \( \delta(1) = 1 \) and \( \delta \text{ (is convex)} \) also

\[ m = E[N] = \frac{d}{ds} \delta(T_s) | T_s = 1 = \delta'(1) \]  

(38)

We achieved extinction.

\( M-1 \) is the founding father of \( 11 \text{ offspring} \) each having an independent probability of producing offspring. The deactivation of \( M-1 \) will activate the various offspring, as seen in FIGURE 11.

### IV. EVALUATION AND DISCUSSION OF THE RESULTS

This section aims to answer the following questions:

a) **How can a terrorist network be uncloaked?**

b) **Can link prediction act as a counterterrorism measure?**

c) **How can a terrorist network be dismantled?**

The results of our link prediction answer our research questions, proving that link prediction can help uncover terrorist activities, as seen in the ranking of vertices in the network. Furthermore, once their ranking has been established, dismantling them occurs in the form of counterterrorism measures that answer our second and third research questions. Indeed, the Galton-Watson extinction put the least vertex of our network as a critical case, thus, leading to an extinction of the network. FIGURE 9 shows the M-19 network based on the Galton-Watson trees, while FIGURE 10 shows the results of the M-19 network after extinction. Fig.1 shows the efficacy of the M-19 network and flow of information. A careful examination shows that Mohammed Atta, although being the key figure or network leader, at a certain point is almost not connected to other nodes. This is crucial in enhancing the efficacy of the network. Frequent communication makes the network vulnerable, and it could be uncloaked, so it is necessary to allow the key vertex to be dormant, and not connected to other vertices [6]. Table 2 shows the matrix representation of the M-19 network. This matrix is important in detecting the page rank of the different vertices in the network, and the summation of the column matrix will result in one indicating that the matrix representation is correct. In FIGURE 3, we unveil the entire M-19 network and predict the link importance using the 4-centrality measures. The 4-centrality measures as shown in FIGURE 7 indicate that M-01 (Mohammed Atta) is the central figure in the 9/11 case. He obtain the highest betweenness centrality, closeness, eigenvector and degree of centrality, which indicates that his removal could have dismantled the network. This also answers our third research question. In curbing terrorist network lethality, it is necessary to remove a vertex with high centrality measures [8].

In terms of network lethality, M-19 so far has the highest lethality rate ever recorded in the history of terrorism. Another salient feature uncovered in this study is...
Timing, which is a crucial factor for the lethality of the network. The flights were just a few minutes away from each other. This was a well-calculated game in the sense that, should a plane crash and one hour later another one follow, there is a high possibility that all flights will be grounded. Hence, before flights were grounded, all target flights were already up in the sky, and three hit the target. The 4th flight did not hit the target, although it did crash in a field. There was a delay in the fourth flight, thereby increasing the interval between the three cells and the fourth cell.

The entire network recorded 2996 fatalities which are the highest so far with a single strike from any terrorist network. Flight 11 had the highest fatality rate, at 56%, followed by flight 175 at 32%. Flight 77 had a 10% fatality rate, and flight 93 recorded just 1%. Since flight 93 did not meet its target, 1% came from the 44 casualties on board the plane. In terms of global lethality, M-19 still enjoys so far the highest in terms of any terrorist attack per single strike, as seen in Figure 2. We compute the lethality rate from 1990-2020, taking into account the highest number of casualties as well as geographical location and attack type.
and ensuring that the casualties occur from a single terror network. The results still show that the 9/11 incident remains outstanding.

V. CONCLUSION

The discourse on modeling terrorist network lethality has been a challenging and complex issue. A terror group operates in a covert network that is difficult to detect, and their transaction becomes unnoticeable. The opaque nature of some terrorist networks makes them difficult to trace. By applying graph theory and graph networks, their activities can be unclouaked through link predictions, as we showed in our methodology. Conventionally, terrorist networks have a unique style of operation that rest upon past actions or successful transactions from other terror networks in which they simply copy the tactics of the latter. To enhance its survival rate and fend off any potential threat of extinction, a terror group will confine itself in a stealth network; that is, a conducive environment or safe haven. Although terrorists are sets of individuals, they do not operate in isolation; rather, their modus operandi takes the form of an orderly hierarchical organizational network having a chain of command.

In this study, we examined the Al-Qaeda link network under the auspices of Osama Bin Laden that hijacked 4 civilian planes in the USA. This tragic incident led to a massive loss of lives and property, and studying this network as our case study opens an avenue for preventing future attacks. Our findings revealed that Mohammed Atta played a pivotal role in the network in which his removal could have caused network malfunction. This is in line with Carley et al., [8] who opined that an essential aspect in dismantling a terror network is the elimination of a node with the highest centrality measures that will disrupt the network’s functionality. Mohammed Atta enjoyed all these features, which makes our results more accurate. The removal was done by applying the Walton-Gatton extinction probability and branching process.

REFERENCES

[1] J. P. Keller, K. C. Desouza, and Y. Lin, “Dismantling terrorist networks: Evaluating strategic options using agent-based modeling,” Technol. Forecasting Social Change, vol. 77, no. 7, pp. 1014–1036, Sep. 2010.

[2] B. Collins, “Regional integration and regional security. Challenges in the ECCAS,” Int. J. Sci. Eng. Res., pp. 1–150, Aug. 2018.

[3] G. Li, J. Hu, Y. Song, Y. Yang, and H.-J. Li, “Analysis of the terrorist organization alliance network based on complex network theory,” IEEE Access, vol. 7, pp. 103854–103862, 2019.

[4] S. Singh, H. Tu, J. Allanach, J. Areta, P. Willett, and K. Pattipati, “Modeling threats,” IEEE Potentials, vol. 23, no. 3, pp. 18–21, Aug. 2004.

[5] D. M. Mehta, “The transformation and demise of terrorist organizations: Causes and categories,” Honors Undergraduate Theses, Univ. Central Florida, Orlando, FL, USA, 2016.

[6] P. V. Fellman, “The complexity of terrorist networks,” Int. J. Netw. Virtual Org., vol. 8, nos. 1–2, pp. 4–14, 2011.

[7] V. Krebs, “Unclouaking terrorist networks,” FM, vol. 7, no. 4, Apr. 2002.

[8] K. M. Carley and J. R. K. Kamneva, “Destabilizing terrorist networks,” in Proc. NAACSOS Conf., Pittsburgh, PA, USA, 2003, pp. 1–6.

[9] B. Li, D. Sun, R. Zhu, and Z. Li, “Agent based modeling on organizational dynamics of terrorist network,” Discrete Dyn. Nature Soc., vol. 2015, pp. 1–17, Nov. 2015.

[10] J. Alison, L. Deng, and Z. Zhu, “CS224W final project report: Uncovering the global terrorism network,” Stanford Univ., Stanford, CA, USA, 2017, p. 10.

[11] D. Mitra, “A working peace system,” in The European Union, B. F. Nelsen and A. C. G. Stubb, Eds. London, U.K.: Palgrave, 1994, doi: 10.1007/978-1-349-23984-9_12.

[12] Z. Khraibani and H. Khraibani, “Self-exciting point process to study the evolution of the attack terrorism,” Int. J. Statist. Appl., vol. 6, no. 6, pp. 361–367, 2016.

[13] A. Berzinji, L. Kauti, and A. Rezine, “Detecting key players in terrorist networks,” in Proc. Evol. Intell. Secur. Informat. Conf. (EISIC), Aug. 2012, pp. 297–302.

[14] F. Spezzano, V. S. Subrahmanian, and A. Mannes, “STONE: Shaping terrorist organizational network efficiency,” in Proc. IEEE/ACM Int. Conf. Adv. Social Netw. Anal. Mining (ASONAM), Aug. 2013, pp. 348–355.

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

[16] P. J. Moris and L. R. Michael, “The 9/11 commission report,” Amer. J. Nursing, vol. 70, no. 6, p. 1233, 2002.

[17] B. A. Jackson, “Groups, networks, or movements: A command-and-control-driven approach to classifying terrorist organizations and its application to al qaeda,” Stud. Conflict Terrorism, vol. 29, no. 3, pp. 241–262, May 2006.

[18] D. T. Hoang, N. T. Nguyen, V. C. Tran, and D. Hwang, “Research collaboration model in academic social networks,” Enterp. Int. Syst., vol. 13, nos. 7–8, pp. 1023–1045, Sep. 2019, doi: 10.1080/17517755.2018.1556812.

[19] P. J. Laub, T. Taimre, and P. K. Pollett, “Hawkes processes,” 2015, arXiv:1507.02822.

[20] D. T. Dang, N. T. Nguyen, and D. Hwang, “Multi-step consensus: An effective approach for determining consensus in large collectives,” Cybern. Syst., vol. 50, no. 2, pp. 208–229, Feb. 2019, doi: 10.1080/01969722.2019.1565117.

[21] J. C. Hurajová and T. Madaras, “Revising the Newman–Girvan algorithm,” in Proc. CEUR Workshop Proc., vol. 1649, 2016, pp. 200–205.

[22] L. Despalatovic, T. Vojkovic, and D. Vukicevic, “Community structure in networks: Girvan–Newman algorithm improvement,” in Proc. 37th Int. Conf. Inf. Commun. Technol., Electron. Microelectron. (MIPRO), May 2014, pp. 1–6, doi: 10.1109/MIPRO.2014.6859714.

[23] M. Mencarini and G. Sensidoni, “Multilingual semantic behavioural algorithms to discover terrorist related online contents,” in Proc. 1st Italian Conf. Cybersecurity (ITASEC), Venice, Italy, 2017, pp. 222–231.

[24] K. McKendrick, Artificial Intelligence Prediction and Counterterrorism, vol. 9. London, U.K.: The Royal Institute of International Affairs-Chatham House, 2019.

[25] F. Ding, Q. Ge, D. Jiang, J. Fu, and M. Hao, “Understanding the dynamics of terrorism events with multiple-discipline datasets and machine learning approach,” PLoS ONE, vol. 12, no. 6, pp. 1–11, 2017, doi: 10.1371/journal.pone.0179057.

[26] S. Kalakuzi, A. Mehta, and D. Bordia, “Using global terrorism database (GTD) and machine learning algorithms to predict terrorism and threat,” Int. J. Adv. Technol., vol. 9, no. 1, pp. 5995–6000, 2019, doi: 10.35940/ijat.A1768.109119.

[27] A. Basuchoudhary and J. T. Bang, “Predicting terrorism with machine learning: Lessons from ‘Predicting terrorism: A machine learning approach,’” Peace Econ., Peace Sci. Public Policy, vol. 24, no. 4, pp. 1–8, Dec. 2018, doi: 10.1515/peps-2018-0040.

[28] A. Afzal, K. B. Bajwa, T. Alghamdi, and H. Aldahawi, “Countering terrorism on social,” Comput. Sci. Technol., vol. 8, no. 99, pp. 35–42, 2018.

[29] S. J. Dixon et al., “A neural network for counter-terrorism,” in Proc. Int. Conf. Innov. Techn. Appl. Intell. London, U.K.: Springer, 2011.

[30] A. Chakraborty, T. Dutta, S. Mondal, and A. Nath, “Application of graph theory in social media,” Int. J. Comput. Sci. Eng., vol. 6, no. 10, pp. 722–729, Oct. 2018, doi: 10.26438/ijcse/v6i01072279.
X. He and J. Zhang, “A machine learning approach for enhancing defence against global terrorism,” in Proc. 12th Int. Conf. Contemp. Comput. (IC3), Aug. 2019, pp. 1–5.

P. Mannrique, Z. Cao, A. Gabriel, J. Horgan, P. Gill, H. Qi, E. M. Restrepo, D. Johnson, S. Wuchty, C. Song, and N. Johnson, “Women’s connectivity in extreme networks,” Sci. Adv., vol. 2, no. 6, pp. 1–7, Jun. 2016, doi: 10.1126/sciadv.1501742.

B. Collins, D. T. Hoang, and D. Hwang, “A model for predicting terrorist network lethality and cohesiveness,” in Trends in Artificial Intelligence Theory and Applications. Artificial Intelligence Practices (Lecture Notes in Computer Science), vol. 12144. Cham, Switzerland: Springer, 2020.

K. Singh, A. S. Chaudhary, and P. Kaur, “A machine learning approach for enhancing defence against global terrorism,” in Proc. 12th Int. Conf. Contemp. Comput. (IC3), Aug. 2019, pp. 1–5.

R. E. Horton, “Erosional development of streams and their drainage basins; hydrophysical approach to quantitative morphology,” Geol. Soc. Amer. Bull., vol. 56, pp. 275–370, 1945, doi: 10.1130/0016-7606(1945)56<275:EOSXT2.CO.2.

M. Ashtiani, A. Salehzadeh-Yazdi, Z. Razaghi-Moghadam, H. Hennig, O. Wolkenhauer, M. Mirzaie, and M. Jafari, “A systematic survey of centrality measures for protein-protein interaction networks,” BMC Syst. Biol., vol. 12, no. 1, pp. 1–17, Dec. 2018, doi: 10.1186/s12918-018-0598-2.

X. He and J. Zhang, “Why do hubs tend to be essential in protein networks?" PLoS Genet., vol. 2, no. 6, pp. 826–834, 2006, doi: 10.1371/journal.pgen.0020088.

K. Singh, A. S. Chaudhary, and P. Kaur, “A machine learning approach for enhancing defence against global terrorism,” in Proc. 12th Int. Conf. Contemp. Comput. (IC3), Aug. 2019, pp. 1–5.

B. Collins, D. T. Hoang, and D. Hwang, “A model for predicting terrorist network lethality and cohesiveness,” in Trends in Artificial Intelligence Theory and Applications. Artificial Intelligence Practices (Lecture Notes in Computer Science), vol. 12144. Cham, Switzerland: Springer, 2020.

K. Singh, A. S. Chaudhary, and P. Kaur, “A machine learning approach for enhancing defence against global terrorism,” in Proc. 12th Int. Conf. Contemp. Comput. (IC3), Aug. 2019, pp. 1–5.

K. Singh, A. S. Chaudhary, and P. Kaur, “A machine learning approach for enhancing defence against global terrorism,” in Proc. 12th Int. Conf. Contemp. Comput. (IC3), Aug. 2019, pp. 1–5.

R. E. Horton, “Erosional development of streams and their drainage basins; hydrophysical approach to quantitative morphology,” Geol. Soc. Amer. Bull., vol. 56, pp. 275–370, 1945, doi: 10.1130/0016-7606(1945)56<275:EOSXT2.CO.2.

M. Ashtiani, A. Salehzadeh-Yazdi, Z. Razaghi-Moghadam, H. Hennig, O. Wolkenhauer, M. Mirzaie, and M. Jafari, “A systematic survey of centrality measures for protein-protein interaction networks,” BMC Syst. Biol., vol. 12, no. 1, pp. 1–17, Dec. 2018, doi: 10.1186/s12918-018-0598-2.

X. He and J. Zhang, “Why do hubs tend to be essential in protein networks?" PLoS Genet., vol. 2, no. 6, pp. 826–834, 2006, doi: 10.1371/journal.pgen.0020088.

K. Singh, A. S. Chaudhary, and P. Kaur, “A machine learning approach for enhancing defence against global terrorism,” in Proc. 12th Int. Conf. Contemp. Comput. (IC3), Aug. 2019, pp. 1–5.

B. Collins, D. T. Hoang, and D. Hwang, “A model for predicting terrorist network lethality and cohesiveness,” in Trends in Artificial Intelligence Theory and Applications. Artificial Intelligence Practices (Lecture Notes in Computer Science), vol. 12144. Cham, Switzerland: Springer, 2020.

K. Singh, A. S. Chaudhary, and P. Kaur, “A machine learning approach for enhancing defence against global terrorism,” in Proc. 12th Int. Conf. Contemp. Comput. (IC3), Aug. 2019, pp. 1–5.

R. E. Horton, “Erosional development of streams and their drainage basins; hydrophysical approach to quantitative morphology,” Geol. Soc. Amer. Bull., vol. 56, pp. 275–370, 1945, doi: 10.1130/0016-7606(1945)56<275:EOSXT2.CO.2.

M. Ashtiani, A. Salehzadeh-Yazdi, Z. Razaghi-Moghadam, H. Hennig, O. Wolkenhauer, M. Mirzaie, and M. Jafari, “A systematic survey of centrality measures for protein-protein interaction networks,” BMC Syst. Biol., vol. 12, no. 1, pp. 1–17, Dec. 2018, doi: 10.1186/s12918-018-0598-2.

X. He and J. Zhang, “Why do hubs tend to be essential in protein networks?" PLoS Genet., vol. 2, no. 6, pp. 826–834, 2006, doi: 10.1371/journal.pgen.0020088.