Critical Terrorist Organizations and Terrorist Organization Alliance Networks Based on Key Nodes Founding

Jun Hu1, Chengbin Chu1, Ling Xu1, Peng Wu1* and Hui-jia Lia2*

1School of Economics and Management, Fuzhou University, Fuzhou, China, 2School of Science, Beijing University of Posts and Telecommunications, Beijing, China

The past years have witnessed increasingly widespread terrorism, violently destroying world peace and regional prosperity. Therefore, uncovering terrorist plots has become the most crucial step for eliminating terrorist attacks. However, with the terrorist scheme being disguised under the huge amount of data flow on the internet, identifying terrorist organizations still remains challenging. Since many terrorist organizations are prone to launch terrorist attacks together, here, we model their relationships as a Terrorist Organization Alliance (TOA) network and propose a novel method to identify the key terrorist organizations in the TOA network. The TOA network utilizes existing key nodes in order to extract useful information, and, with the help of the entropy weight method, the new solution to the TOA network is effective and precise. The experiments are performed on the dataset from the Global Terrorism Database, and the results are statistically validated through t-tests and convergence analysis. Compared with the traditional methods, our method is proven to be superior in terms of measure the harm of terrorist attack organizations and find the key terrorist organizations.

Keywords: terrorist organization alliance, key terrorist, complex network, centrality, social network

1 INTRODUCTION

In recent years, terrorist attacks have happened frequently around the world. With the rapid and widespread data flow on the internet and media contents, terrorist attacks are becoming increasingly serious. Terrorism has a significant and lasting impact on the social security, political process, and social ecology of all countries [1, 2]. The task of counter-terrorism and terrorism prevention is urgent and arduous; however, the cost is extremely expensive.

Globally, with terrorist organizations such as Al-Qaeda (and the extremist group Islamic State in 2017) suffering heavy blows, terrorist organizations have begun to change their operational strategies. Their activity areas have begun to show a diffuse expansion from the center to periphery, illustrating a new trend of organizational terrorism to individual terrorism, cyber terrorism, and so on. Compared with the government, terrorist organizations are generally relatively weak, and they often cooperate with each other in order to enhance their strength. This is becoming a new trend in the current development of terrorism, manifesting in international cooperation.

In the research of terrorist activity, the traditional studies mostly focus on the forecast of the terrorist attack event based on the terrorist activity characteristic. Xue A. et al (2011) proposed a
prediction algorithm PBCS based on context subspace, and it aims to predict terrorist behavior [3]. Nurudeen M et al. (2018) proposed a hybrid neural fuzzy model in order to predict criminal behavior in a wide range of areas through simulating crime indication events extracted from wide-area surveillance networks [4]. Li Z. et al. (2018) proposed a comprehensive framework that combines social network analysis, wavelet transform, and the pattern recognition approach to investigate the dynamics and eventually predict the attack behavior of terrorist group [5]. According to the new characteristics of terrorist organization cooperation, scholars introduce network analysis methods to the investigation of terrorist organizations and terrorist attacks. Carly et al (2002) analyzed the terrorist network and suggested that the corresponding terrorist attack prevention strategy should be formulated according to the time of the terrorist attack [6]. Li G. et al. (2019) analyzed the construction process of the terrorist attack alliance network and adopted a new dynamic interactive clustering algorithm to analyze the subgroups of tourist organizations [7, 8]. Hakim et al. (2020) studied the role social contexts played in the link between interpersonal networks and social identity dynamics of a mujahid, found that constraints for the participation in different interpersonal networks. The constraints influenced the process of identity negotiation as a mujahid versus alternative identities of a family member and belonging to a neighborhood [9].

There exist various methods to evaluate the importance of nodes in networks, and many are essentially derived from graph theory [10–11] and graph-based data mining [13, 14]. The research on the importance of nodes in complex networks originates from the field of sociological network analysis [15–18]. Freeman and other scholars have done a lot of research on sociological networks in the early stage. Since then, the fields of system science research, information search, and document retrieval have raised similar problems independently and explored the important sections in networks. The importance of nodes in networks has become a basic problem in various research fields of complex networks.

In this paper, we proposed a new way to analyze the key terrorist organizations. In section 2, a definition of the TOA network is provided, and a figure is given to explain the construction process of this network. In section 3, some traditional methods are given to find the key terrorist organizations, and an entropy method to find critical organizations is also given based on these traditional methods. In section 4, we calculate the importance of nodes by using the traditional method and our method, respectively; In section 5, we use the t-test and convergence analysis to test the results, which found that the accuracy of our method is better than that of traditional methods.

2. MODEL

Up to now, various countries have been attacked by terrorist organizations, as shown in Figure 1. The frequencies of attacks occurring in South Asia, the Middle East, North Africa, and Sub-Saharan Africa amount to 81%, which means that these places are frequently affected by terrorist attacks. In the future, some countries might also be attacked, and it is thus of great significance to analyze the regular pattern of the terrorist attack is very meaningful. In this section, we first propose a Critical Nodes Finding Model for Terrorist Organization Alliance Networks and present a solution.

2.1 Problem Definition

We know that there exist certain social relationships between terrorist groups, including but not limited to sectarian, blood relatives, ethnic relations, etc. At the same time, within the same regions and similar terrorist organizations of related skill fields, resources, and tasks, there is often cooperation. In terms of terrorist attacks, there will be the phenomenon of coalition, and these coalitions will often make some terrorist attacks escalate.

Figure 2 illustrates the construction process of the terrorist groups network. When a terrorist attack event occurs, some groups usually claim that this attack was launched by them. Based on this fact, we suppose there is a relationship between these groups, and these groups will be linked. Thus, a complex network $G = (V, E)$ of terrorist organizations is built. The point set $V(G)$ is the terrorist groups, and the link in $E$ indicates that they make the same attacks at the same time.

3 PRELIMINARIES

3.1 Centrality Measures of the Terrorist Organizations Graph

This is a terrorist organizations graph $G = (V, E)$ with $n = |V|$ nodes and $m = |E|$ edges. Various methods are proposed to measure the importance of nodes, such as Degree centrality (DC), closeness centrality (CC), and betweenness centrality (BC) [19]. The TOA network as shown in the Figure 3.

3.1.1 Degree Centrality

The degree centrality (short for DC) of terrorist organization alliance network’s node $i$, being denoted as $CD(i)$, is defined as

$$CD(i) = \sum_{j} x_{ij},$$  \hspace{1cm} (1)

where $i$ is the focal node, $j$ represents certain node, $N$ is the total number of nodes, and $x_{ij}$ represents the connection between node $i$ and node $j$. The value of $x_{ij}$ is defined as 1 if node $i$ is connected to node $j$, and 0 otherwise.

3.1.2 Betweenness Centrality

The betweenness centrality (short for BC) of terrorist organization alliance network’s node $i$, being denoted as $CB(i)$, is defined as

$$CB(i) = \sum_{j\neq k \neq i} \frac{g_{jk}(i)}{g_{jk}},$$  \hspace{1cm} (2)

where $g_{jk}$ equals $(\sum_{x \in E} x_{ij} x_{kj})/equals (\sum_{x \in E} x_{ij} x_{kj})/equals (\sum_{x \in E} x_{ij} x_{kj})/equals (\sum_{x \in E} x_{ij} x_{kj})/equals (\sum_{x \in E} x_{ij} x_{kj})$.
where $g_{jk}$ denotes the number of the shortest paths between nodes $j$ and $k$, and $g_{jk}(i)$ means the number of the shortest paths between nodes $j$ and $k$ that go through node $i$.

3.1.3 Closeness Centrality

The closeness centrality of terrorist organization alliance network’s node $i$, being denoted as $CC(i)$, is defined as
where $d_{ij}$ denotes the distance between node $i$ and node $j$.

### 3.1.4 Eigenvector Centrality

Let $A$ be an $n \times n$ similarity matrix. The eigenvector centrality $x_i$ of terrorist organization alliance network’s node $i$ is the $i$th entry in the normalized eigenvector, which belongs to the largest eigenvalue of $A$. In the matrix $A$, $\lambda$ is the largest eigenvalue and $n$ is the number of vertices.

$$Ax = \lambda x, \quad x_i = u \sum_{j=1}^{n} a_{ij} x_j, \quad i = 1, 2, \ldots, n,$$

with proportionality factor $u = \frac{1}{\lambda}$ so that $x_i$ is proportional to the sum of similarity scores of all nodes connected to it.

### 3.1.5 PageRank

The PageRank is an eigenvector centrality which is used to rank the websites, PageRank is one of these key nodes fingding ways for the key nodes. Mathematically, the PR value of terrorist organization alliance network’s node $v_i$ at $t$ step is

$$PR_i(t) = \sum_{j=1}^{n} a_{ij} \frac{PR_j(t-1)}{k_{out}^j},$$

where $n$ is the total number of nodes in the network, and $k_{out}^j$ is the out-degree of node $v_j$. The above iteration will stop if the PR values of all nodes reach the steady state.

### 3.2 Information Entropy

In information theory, entropy is defined as measuring the level of uncertainty. The order of the data determines the degree of entropy, i.e., according to the definition of information entropy, we know that the information entropy of this group of data will be greater when a group of data contains more information. Therefore, the larger the entropy of the data, the greater its weight.

Whether people can get high-quality decision-making information is determined by the quality of data. Therefore, it is particularly important to find high-quality data in multiple

| Table 1: The statistical features of terrorist organization alliance network. |
|----------------------------------|----------------------------------|
| **Name**                     | **Terrorist organization alliance network** |
| Node                          | 567                              |
| Edge                          | 663                              |
| Average degree                | 2.339                           |
| Network diameter              | 15                              |
| Weighted average degree       | 6.688                           |

**Figure 3**: Terrorist organization alliance network.

**Figure 4**: The degree of TOA Network: Plot the number of the degree on the vertical Y-axis to logarithmic against weight degree on the horizontal x-axis to logarithmic.

**Figure 5**: The weight degree distribution of the TOA Network: Plot the number of the weight degree on the vertical Y-axis to logarithmic against weight degree on the horizontal x-axis to logarithmic.
data. Entropy is utilized to measure the data’s order, which can reflect the importance of data. Thus, based on the information theory, we can find the important factors, which are the high-weight data. In the multi-index decision-making problem, the greater the variability of the index is, the smaller the information entropy is, thus we can more information from this index. Therefore, the weight of this index is bigger than other indexes [20–22].

Definition 1. Among the problems of evaluating $n$ objects and $M$ evaluation indicators, the entropy of the $i$-th evaluation indicator is
\[ H_i = -K \sum_{j=1}^{n} f_{ij} \ln f_{ij}, \quad i = 1, 2, \ldots, n, \]  
\[ \text{where } K = (\ln n)^{-1}, f_{ij} = \sum_{j=1}^{m} f_{ij}, \text{ assume that, } f_{ij} = 0, f_{ij} \ln f_{ij} = 0. \]

Because \( 0 \leq f_{ij} \leq 1 \), we can get \( 0 \leq -\sum_{j=1}^{n} f_{ij} \ln f_{ij} \leq 1 \) and \( 0 \leq H_i \leq 1 \).

Definition 2 In the problem of \((m, n)\) evaluation, the entropy weight of the first evaluation index is defined as

\[ w_i = \frac{1 - H_i}{m - \sum_{i=1}^{m} H_i} \]  

From the above definition and the properties of the entropy function, the following properties of the entropy weight can be obtained:

Remark 1.

1) When the values of each evaluated object on index i are identical, the maximum value of entropy is 1 and the weight of entropy 0. This also means that the indicator does not provide any useful information to decision makers, and the indicator can be considered to be canceled.

2) When the values of each evaluated object on index i are quite different, the entropy value is small, and the entropy weight is large, it shows that the index provides useful information for decision makers. At the same time, it is pointed out that in this problem, there are obvious differences among the objects in this index, which should be investigated emphatically.

3) The bigger the index’s entropy is, the smaller its entropy weight is. The less important the index is, the more satisfied it is.

Algorithm 1 Calculating entropy weight.

1) Case 1 the Large Value of the indicator, the Better indicator

\[ r_{ij} = \frac{x_{ij} - x_{ij}^{\min}}{x_{ij}^{\max} - x_{ij}^{\min}} + 1 \]

2) For \( i \leftarrow n \) for \( j \leftarrow 1: m \)

\[ f_{ij} = \frac{r_{ij}}{\sum_{j=1}^{m} r_{ij}} \]

end end

3) For \( i \leftarrow 1: n \)
TABLE 3 | The top-20 ranked Terrorist Organizations.

| Rank | Closenesscentrality | Harmonicclosenesscentrality | Betweennesscentrality | Eigencentrality | Pageranks | Degreecentrality | Score | Rank |
|------|----------------------|-----------------------------|-----------------------|-----------------|------------|------------------|-------|------|
| 1    | 0.018,499,169        | 0.02,617,749                | 0.399,236,595         | 0.289,086,571   | 0.367,830,974 | 0.356,905,192   | 1    |
| 2    | 0.020,097,098        | 0.023,554,514               | 0.078,136,989         | 0.120,363,525   | 0.129,822,697 | 0.293,586,168   | 2    |
| 3    | 0.018,754,365        | 0.028,691,403               | 0.194,583,999         | 0.259,047,325   | 0.219,371,161 | 0.21,420,798    | 3    |
| 4    | 0.019,549,456        | 0.022,610,798               | 0.080,022,983         | 0.100,945,885   | 0.129,822,697 | 0.180,368,367   | 4    |
| 5    | 0.017,081,169        | 0.022,888,531               | 0.337,380,474         | 0.191,149,312   | 0.28,128,251  | 0.17,081,775    | 5    |
| 6    | 0.016,344,832        | 0.022,758,058               | 0.192,874,792         | 0.25,290,922    | 0.292,101,068 | 0.149,096,878   | 6    |
| 7    | 0.016,890,467        | 0.020,896,569               | 0.087,099,295         | 0.068,940,004   | 0.075,729,906 | 0.132,724,445   | 8    |
| 8    | 0.016,834,956        | 0.020,520,250               | 0.056,055,613         | 0.068,7923,14   | 0.075,729,906 | 0.129,633,559   | 9    |
| 9    | 0.017,555,938        | 0.021,712,772               | 0.114,142,541         | 0.109,953,308   | 0.129,822,697 | 0.108,712,052   | 10   |
| 10   | 0.014,944,893        | 0.018,394,179               | 0.041,950,184         | 0.109,067,332   | 0.129,822,697 | 0.104,964,168   | 11   |
| 11   | 0.016,020,379        | 0.020,868,619               | 0.113,598,381         | 0.164,053,214   | 0.183,915,487 | 0.101,417,827   | 12   |
| 12   | 0.015,382,509        | 0.021,748,358               | 0.066,762,743         | 0.155,836,443   | 0.129,822,697 | 0.100,306,514   | 13   |
| 13   | 0.018,680,749        | 0.020,398,491               | 0.043,668,888         | 0.078,606,559   | 0.086,548,464 | 0.09,670,911    | 14   |
| 14   | 0.017,810,194        | 0.020,816,329               | 0.071,575,316         | 0.078,606,559   | 0.086,548,464 | 0.09,670,911    | 15   |
| 15   | 0.015,344,473        | 0.020,303,818               | 0.255,806,856         | 0.114,586,224   | 0.173,096,929 | 0.096,050,992   | 16   |
| 16   | 0.011,888,741        | 0.021,174,216               | 0.103,211,842         | 0.092,717,815   | 0.108,185,581 | 0.088,000,809   | 17   |
| 17   | 0.018,781,677        | 0.022,174,791               | 0.093,768,699         | 0.084,629,162   | 0.108,185,581 | 0.088,000,809   | 18   |
| 18   | 0.015,931,401        | 0.020,317,442               | 0.123,114,186         | 0.101,618,791   | 0.129,822,697 | 0.082,627,129   | 19   |

TABLE 2 | The top-20 ranked Terrorist Organizations base on degree centrality (DC), betweenness centrality (BC), eigenvector centrality (EC), and PageRank (PR) in TOA network.

| Rank | DC          | BC          | EC          | RageRank     |
|------|-------------|-------------|-------------|--------------|
| 1    | Islamic state of Iraq and the levant (ISIL) | Al-qaida    | Islamic state of Iraq and the levant (ISIL) | Tehrik-i-Taliban Pakistan (TTP) |
| 2    | Tehrik-i-Taliban Pakistan (TTP) | Lashkari-e-Jangvi | Al-Nusrah front | Lashkari-e-Jangvi |
| 3    | Al-Nusrah front | Ansar al-sharia (Libya) | Al-Nusrah front | Ansar al-sharia (Libya) |
| 4    | Lashkari-e-Jangvi | Hammar Islamic resistance movement | Free syrian army | Lashkari-e-Taiba (LeT) |
| 5    | Lashkari-e-Taiba (LeT) | United liberation front of Assam (ULFA) | Jaysh al-Islam (Syria) | Tehrik-i-Taliban Pakistan (TTP) |
| 6    | Ansar al-sharia (Syria) | Harkatul Jihad-e-Islami | Shamia front | Kurdistan workers’ party (PKK) |
| 7    | Al-Sham legion | Jemaah Islamiya (JI) | Southerm front | Al-qaida in the arabian peninsula (AQAP) |
| 8    | Free syrian army | Harkatul Jihad-e-Islami | United liberation front of Assam (ULFA) | Al-qaida in the islamic maghreb (AQIM) |
| 9    | Al-sham Obsidian army | Jemaah Islamiya (JI) | Al-Shabaab | Al-qaida in the islamic maghreb (AQIM) |
| 10   | Al-Sham legion | Hammar Islamic resistance movement | Al-Nusrah front | Al-Shabaab |
| 11   | Al-Nusrah front | Jemaah Islamiya (JI) | Al-Shabaab | Al-qaida in the islamic maghreb (AQIM) |
| 12   | Al-Sham legion | Al-Nusrah front | Al-Shabaab | Al-qaida in the islamic maghreb (AQIM) |
| 13   | Al-Sham legion | Al-Nusrah front | Al-Shabaab | Al-qaida in the islamic maghreb (AQIM) |
| 14   | Lashkari-e-Taiba (LeT) | Lashkari-e-Taiba (LeT) | Al-Nusrah front | Al-Shabaab |
| 15   | Al-Nusrah front | Al-Nusrah front | Al-Shabaab | Al-qaida in the islamic maghreb (AQIM) |
| 16   | Al-Sham legion | Al-Nusrah front | Al-Shabaab | Al-qaida in the islamic maghreb (AQIM) |
| 17   | Al-Sham legion | Al-Nusrah front | Al-Shabaab | Al-qaida in the islamic maghreb (AQIM) |
| 18   | Al-Sham legion | Al-Nusrah front | Al-Shabaab | Al-qaida in the islamic maghreb (AQIM) |
| 19   | Al-Sham legion | Al-Nusrah front | Al-Shabaab | Al-qaida in the islamic maghreb (AQIM) |
| 20   | Al-Sham legion | Al-Nusrah front | Al-Shabaab | Al-qaida in the islamic maghreb (AQIM) |
The weight average degree of this network means that the number of other organizations joined by each organization is two. The weight average degree of this network is 2.399, which is calculated as follows:

\[ W = \frac{\sum_{i=1}^{n} w_i}{n} \]

where \( w_i \) is the weight of the node, and \( n \) is the total number of nodes.

There are 567 terrorist organizations with a joint attack on the same area. The average degree of this network is 2.115. The Statistical characteristics of nodes in the network are not entirely determined by a high degree or good robustness. The Terrorist Organization Alliance Network to demonstrate that the proposed method does a lot better than other centrality approaches when the in-degree and out-degree of nodes are different; thus, a global way to measure the key nodes is very necessary. Various community detection algorithms can be applied [24].

As shown in the Figures 4, 5, 6, the double-logarithmic relationship between cumulative node degree function \( P(k) \) and degree \( k \), node weight degree function \( P(k) \), and weight degree \( k \) is described. First of all, we used the power law fitting for the degree distribution and weight distribution and found that all R2 are greater than 0.9, which means that the TOA network is a scale-free network. Thus the TOA network is a social network. And in the TOA network, we find that there are a large number of nodes with degree 1. According to analysis of the source data, most of the organizations carry out the attack once or the event is only between the two organizations creating terrorist attacks. However, such organizations are not rare. It is very likely that these organizations are temporarily organized to launch an attack and then disband or change their names.

As shown in the Figures 7–8, we find that the distribution of the eigencentrality of the TOA network is a power law.

The Figure 9 to Figure 10 display the distribution of CC, BC, EC, and RR, respectively. The distribution of the BC, EC, and RangeRank are the same; however, the distribution of CC is different from the three, which is very interesting.

The top-20 ranked groups by betweenness centrality (BC), degree centrality (DC), eigenvector centrality (EC), and PageRank (PR) in TOA network as shown in the Table 2. Table 2 compares four identity nodes finding ways in the TOA network and gives the top 20 critical terrorist organizations in different ways. The terrorist organization ISIL always occupies the top one in the DC, EC, and RR ways, and in the BC, the ISLT is the second critical organization. Due to the closeness of the 130 Terrorist Organizations (centrality of 1), it is not possible to display these Terrorist Organizations. Comparison of the proposed method ranks ISIL, TTP, Al-Musrah Front, Lashkar-e-Jhangvi, LeT, BIFM, and ASG all as being in the top 20; others are not all in the top 20, as some are in three methods like the Taliban only note in the RangRank and PKK only in the DC and BC, some are in two methods like the Free Syrian Army in the DC and RangRank, some are in one method like the Garo National Liberation Army only in the DC.

In this part, we compare the traditional methods with the results obtained in the DC, BC, CC, EC, and RR. At the same time, from Table 2 and Table 3, we can find the results of these traditional ways are different; thus, a global way to measure the key nodes is very necessary.
5 SIGNIFICANT ANALYSIS

In this section, we used the two-tail test to find the significant among these ways. The t-text is shown below.

\[ t = \frac{X_1 \bar{X} - X_2 \bar{X}}{\sqrt{\frac{(n-1)\sigma_1^2 + (n-1)\sigma_2^2}{n-2}}} \]  

(9)

Where \( X_1 \) and \( X_2 \) are the mean of the two samples, respectively; \( \sigma_1^2 \) and \( \sigma_2^2 \) are the variance of the two samples, respectively.

As shown in Tables 3, 4 and Table 6, \( H = 0 \) indicates that the zero hypothesis is not rejected under 5% confidence; \( H = 1 \) indicates that the zero hypothesis is rejected, that is, that there is discrimination.

6 CONCLUSION

At present, the research on terrorist attacks is mainly based on multi-agents, such as Refs. reference [25, 26]. These two articles analyze terrorist organizations through multi-agent simulation and study their change rules. In this paper, the complex network method is used to find the key terrorist organizations. The entropy method is used to measure the harm of terrorist attack organizations and find the key terrorist organizations. Compared with other models, it is relatively novel.

In this paper, we sort the terrorist organizations by using the calculation model of the key nodes in the complex network and find the key terrorist organizations. Through the previous calculation, we find that the terrorist attacks made by terrorist organizations are very harmful, and their concentration will obviously concentrate some weapon resources together, and attack at different locations at the same time. These researches seriously endanger the security of today’s society. The purpose of this paper is to better prepare for the fight against terrorist organizations and the maintenance of world peace. And we observe some characteristics of the TOA network. Based on the traditional methods, a new method is given to find the key nodes as soon as critical organizations. We find that there are significant differences among these traditional methods; comparing these ways, we found that there is no significant difference among CC, HC, and Pageranks, and there is no significant difference between EC and our way. There are

TABLE 6 | T-test results of these ways.

|     | CC | HC | BC | EC | Pageranks | DC | Ourway |
|-----|----|----|----|----|-----------|----|--------|
| CC  | 0  | 0  | 1  | 1  | 0         | 1  | 1      |
| HC  | 0  | 0  | 1  | 1  | 0         | 1  | 1      |
| BC  | 1  | 1  | 0  | 1  | 1         | 1  | 1      |
| EC  | 1  | 1  | 1  | 0  | 1         | 1  | 0      |
| Pageranks | 0  | 0  | 1  | 1  | 0         | 1  | 1      |
| DC  | 1  | 1  | 1  | 1  | 1         | 0  | 1      |
| Ourway | 1  | 1  | 1  | 0  | 1         | 1  | 0      |

FIGURE 11 | The relationship between node strength and different centrality values.
significant differences between other indicators. Therefore, through t-tests and Figure 11, we found that there are differences between the integrated score and each centrality, which also shows that the information obtained by traditional methods is local information and cannot fully reflect the importance of nodes. Therefore, the weighted method can better integrate all the information, and we can get the more accurate and important nodes.

DATA AVAILABILITY STATEMENT

Publicly available datasets were analyzed in this study. This data can be found here: https://www.start.umd.edu/gtd/.

REFERENCES

1. Balcells L, and Torrats-Espinosa G. Using a Natural experiment to Estimate the Electoral Consequences of Terrorist Attacks, Proc Natl Acad Sci USA 115 (2018) 10624–9. doi:10.1073/pnas.1803021115
2. Mitts T. Terrorism and the Rise of Right-Wing Content in Israeli Books. Int Org (2019) 73:203–24. doi:10.1177/002081318003083
3. Xue A, Wang W, and Zhang M. “Terrorist Organization Behavior Prediction Algorithm Based on Context Subspace [C]” in International Conference on Advanced Data Mining and Applications. Berlin, Heidelberg: Springer, 2012 (2011) 332–45. doi:10.1007/978-3-642-25886-3_25
4. Nurudeen M, Zou B, and Zhu C. A Neuro-Fuzzy Crime Prediction Model Based on Video Analysis[J]. Chin J Electro, 27 (2018) 968–75. doi:10.1049/cej.2018.02.019
5. Li Z, Sun D, Li B, Li Z, and Li A. Terrorist Group Behavior Prediction by Wavelet Transform-Based Pattern Recognition, Discrete Dyn Nat Soc 2018, (2018) 1–16. doi:10.1155/2018/5676712
6. Carley K, Lee J-S, and Krakhardt D. Destabilizing Networks[J]. Connections (2002) 24:79–92.
7. Li G, Hu J, Song Y, Yang Y, and Li H-J, Analysis of the Terrorist Organization Alliance Network Based on Complex Network Theory, IEEE Access 7 (2019) 105854–62. doi:10.1109/access.2019.2929798
8. Fang L, Fang H, Tian Y, Yang T, and Zhu J. The alliance Relationship Analysis of International Terrorist Organizations with Link Prediction. Physica A: Stat Mech its Appl (2017) 482:573–84. doi:10.1016/j.physa.2017.04.068
9. Hakim MA, and Mujahidah DR. Social Context, Interpersonal Network, and Identity Dynamics: A Social Psychological Case Study of Terrorist Recidivism, Asian J Soc Psychol 23 (2020) 3–14. doi:10.1111/ajsp.12349
10. Li S, Zhao D, Wu X, Tian Z, Li A, and Wang Z. Functional Immunization of Networks Based on Message Passing, Appl Math Comput (2020) 366:124728. doi:10.1016/j.amc.2019.124728
11. Zhu P, Han J, Guo Y, and Lombardi F, Reliability and Criticality Analysis of Communication Networks by Stochastic Computation, IEEE Netw 30 (2016) 70–6. doi:10.1109/mnet.2016.1500211
12. West DB. Introduction to Graph Theory[M]. Upper Saddle Rive: Prentice hall (2001) 2.
13. Gao C, Fan Y, Jiang S, Deng Y, and Liu J, Dynamic Robustness Analysis of a Two-Layer Rail Transit Network Model, IEEE Trans Intell Transport Syst (2021) 1–16. doi:10.1109/tits.2021.3058185
14. Washio T, and Motoda H. State of the Art of Graph-Based Data Mining, SIGKDD Explor Newsl 5 (2003) 59–68. doi:10.1145/959242.959249
15. Gao C, Su Z, Liu J, and Kurths J, Even central users Do Not Always Drive Information Diffusion, Commun ACM 62 (2019) 61–7. doi:10.1145/3224203
16. Zhu P, Guo H, Zhang H, Han Y, and Chu C, The Role of Punishment in the Spatial Public Goods Game[J], Nonlinear Dyn 102 (2020) 1–10. doi:10.1007/s11071-020-05965-0

AUTHOR CONTRIBUTIONS

JH: Visualization, Software, Computation, Drawing and Writing CC: Writing-Reviewing and Editing LX: Conceptualization, PW: Investigation, Visualization, Software HL: Methodology, Validation.

FUNDING

This work is supported by the National Natural Science Foundation of China (Nos. 71871233, 71701049, and 717871159), the Fujian Science and Technology Economic Integration Service Platform, Fundamental Research Funds for the Central Universities of China (Nos.2020XD-A01-1).

16. Zhu P, Hui X, Guo Y, Xue J, and Liu J. Investigating the Effects of Updating Rules on Cooperation by Incorporating Interactive Diversity[J]. The Eur Phys J B (2020) 94:58. doi:10.1140/epjb/e2020-100059-1
10. Pappi PU, and Scott J. Social Network Analysis: A Handbook. Contemp Sociol (1993) 22:128. doi:10.2307/2075047
12. Du Y, Gao C, Hu Y, Mahadevan S, and Deng Y. A New Method of Identifying Influential Nodes in Complex Networks Based on TOPSIS. Physica A (2014) 399:5769. doi:10.1016/j.physa.2013.12.031
16. Bialynicki-Birula I, and Mycielski J. Uncertainty Relations for Information Entropy in Wave Mechanics], Commun Math Phys 44 (1975) 129.
15. Campbell J. Grammatical Man: Information, Entropy, Language, and life[M]. New York: Simon & Schuster (1982).
10. Devroye L, Györfi L, and Lugosi G. A probabilistic Theory of Pattern Recognition. Berlin, Heidelberg: Springer Science and Business Media. (1996) 31.
10. Li H-J, Bu Z, Wang Z, and Cao J. Dynamical Clustering in Electronic Commerce Systems via Optimization and Leadership Expansion, IEEE Trans Ind Inf, 16 (2020) 5327–34. doi:10.1109/tii.2019.2960835
11. Zhu P, Wang X, Zhi Q, Ma J, and Guo Y. Analysis of Epidemic Spreading Process in Multi-Communities. Chaos, Solitons Fractals (2018) 109:231–7. doi:10.1016/j.chaos.2018.02.007
11. Lu P, Yang H, Li H, Li M, and Zhang Z. Swarm Intelligence, Social Force and Multi-Agent Modeling of Heroic Altruism Behaviors under Collective Rules[J]. Knowledge-Based Syst 214 (2021) 106–725. doi:10.1016/j.knosys.2020.106725
13. Moya I, Chica M, Sáez-Lozano JL, and Cordón Ó. An Agent-Based Model for Understanding the Influence of the 11-M Terrorist Attacks on the 2004 Spanish Elections, Knowledge-Based Syst 123 (2017) 200–16. doi:10.1016/j.knosys.2017.02.015

Conflict of Interest: The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Publisher’s Note: All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.

Copyright © 2021 Hu, Chu, Xu, Wu and Lia. This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY). The use, distribution or reproduction in other forums is permitted, provided the original author(s) and the copyright owner(s) are credited and that the original publication in this journal is cited, in accordance with accepted academic practice. No use, distribution or reproduction is permitted which does not comply with these terms.