



# Implicit Terrorist Networks: A Two-Mode Social Network Analysis of Terrorism in India

Rithvik Yarlagadda<sup>1</sup>, Diane Felmlee<sup>2</sup>, Dinesh Verma<sup>3</sup>, and Scott Gartner<sup>2(✉)</sup>

<sup>1</sup> University of Maryland, College Park, MD, USA  
ryarlag@terpmail.umd.edu

<sup>2</sup> Pennsylvania State University, University Park, PA, USA  
{dhf12, ssg13}@psu.edu

<sup>3</sup> IBM T.J. Watson Research Center, Yorktown Heights, NY, USA  
dverma@us.ibm.com

**Abstract.** Recent studies examine factors that lead to the emergence of terrorism and why some locations are more frequently targeted than others. However, much of the research assumes that terrorist incidents and groups are independent. We show that the assumption of independence is not always valid. Instead, we identify the conditions under which terrorist groups share choices over target locations, forming Implicit Terrorist Networks. We demonstrate the utility of this approach by examining Islamic terrorism in India (1990–2015). Using a two-mode network approach, we find that violent target locations are not independent of each other, but instead have a tendency to occur in clusters. The results highlight the patterns by which India has been targeted by a number of active, Islamic terrorist organizations over a 25-year period. More generally, our study: (1) demonstrates the utility of employing an Implicit Network approach to understanding terrorism, (2) shows that cluster analysis can assist in identifying terror group aliases, (3) identifies unexpected locations for violence that may indicate the involvement of external factors, providing leads for counter terrorism efforts, and (4) provides a tool for identifying the structures underlying patterns of global terrorism.

**Keywords:** Social network analysis · Terrorism · India

## 1 Introduction

Criminal groups, such as terrorists and organized crime, sometimes make formal agreements with each other [1], such as the 2015 alliance between Boko Haram and ISIS. There are, however, obvious deterrents to such agreements: they are unenforceable, generate evidence, and illegal organizations tend to be unstable and have rapidly changing alliances. Groups can collaborate in other, less formal but more observable ways, by operating in the same way or in similar locations, thus forming *Implicit Terrorist Networks* [2, 3]. An implicit terrorist network

represents a congruence of violent behavior from two or more terrorist groups that may or may not result from their decision to act together. In implicit networks, terrorist groups seemingly or actually cooperate together without mechanisms for direct collaboration. We examine implicit networks among Islamic terrorist groups in India between 1990 and 2015.

## 2 Theory

The locations of terrorism vary widely [4]. We examine three key factors motivating the selection of targets. First, terrorist groups favor targets that result in high civilian casualties [5]. Thus, those targets that likely lead to high casualties are more attractive and more likely to be selected by extremist groups for violence. The key here is crowds and cities versus individuals and rural countryside. Second, terrorism often remains the only option available for actors unable to project force through more conventional military means against a stronger foe [6]. Terror groups thus select less protected, soft targets given the tremendous asymmetry of power. A third factor concerns the symbolic importance of a state, city, or building. Symbolic targets are selected by terrorists to garner attention and spread their political message [7]. We explore these factors and the insights they provide on implicit networks with the use of two-mode social network analysis. We investigate both the network centrality of terrorist groups and their attack locations, and the subgroup formation of terrorist attacks within India.

## 3 Methods

### 3.1 Data

We employ the Global Terrorism Database/GTD [8], an open-source database maintained by the National Consortium for the Study of Terrorism and Responses to Terrorism (START); and South Asian Terrorism Portal/SATP [9]. SATP provides data on 15 Indian Islamist groups. GTD data consist of 51 locations and 154 events, representing all terrorist attacks, bombing or explosions in India conducted by groups between 1990 and 2015. We considered multiple strikes in a given location on the same day as one single attack. Also, an attack claimed by multiple terrorist groups at a specific location was coded as an incident for both groups. Despite the high level of activity (7th highest in the world, GTI 2016), terrorism within India using social network approaches has been rarely studied [10,11].

### 3.2 Two-Mode Network Analysis

Two-mode networks consist of two types of nodes: “actors” and “events,” where direct ties exist only between nodes belonging to different types [3,12–14]. We constructed a 51 by 15 two-mode, or bipartite, network, where rows represent the 51 locations that experienced terrorist incidents and the 15 columns represent the

extremist organizations. An entry in the  $m \times n$  matrix cell represents the number of attacks in location  $m$  by actor  $n$  (see Fig. 1). For the centrality analysis, this matrix was dichotomized to a binary matrix, with a *one* indicating the occurrence of any attack, and *zero* otherwise. In order to perform the analyses, the two-mode network is converted into two one-mode, symmetric networks, with one of them representing target locations and the other representing extremist organizations. The ties in the two resulting one-mode networks indicate at least one incident of an attack by common terrorist groups between any two pairs of locations, and at least one commonly attacked location between any two pairs of organizations. We focus on degree centrality (the most direct measure of groups’ connection to violence) and include three other common measures as a robustness check.

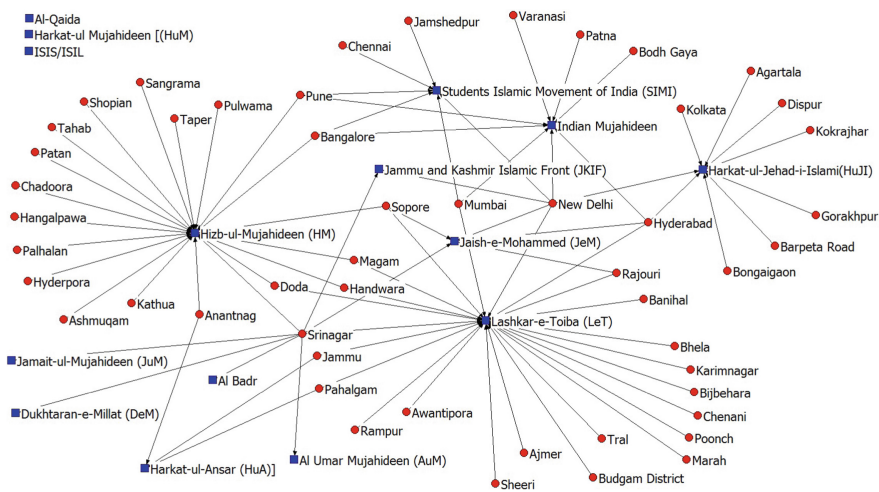


Fig. 1. Two-mode network (blue rectangles/groups; red ovals/locations attacked) (Color figure online)

## 4 Results

### 4.1 Centrality of Organizations and Locations [15, 16]

As seen in Table 1, Lashkar-e-Taiba (LeT) exhibits the highest normalized degree centrality of all the terrorist organizations, with a score of 0.471. This reflects the fact that LeT perpetrated the most number of attacks in the dataset. Following LeT in degree centrality is Hizb ul-Mujahidin (HM), which has a slightly lower score of 0.392. Each terrorist group is ranked according to their level of centrality (‘1’ = highest rank of centrality) on four different network centrality measures (Table 1). The extremist groups, LeT and HM, achieve the two highest ranks across all four centrality measures. The high level of centrality of these

two groups is evident in the two-mode network graph, as well, with numerous edges emanating from each of these groups towards multiple target locations (see Fig. 1). Note that there are three isolate organizations in the data set, with centrality scores of ‘0’, which likely operate at a distance.

The normalized two-mode degree centrality measure for geographical targets indicates that Srinagar, the capital of Jammu & Kashmir, is highly conflictual and violent (in analysis not shown here). With the highest level of degree centrality (0.533), Srinagar is also the most central and highly attacked location. It is followed in degree centrality by the capital of India, New Delhi (0.400). These findings mean that Srinagar was attacked by more than 50 percent of the Islamic terrorist organizations and New Delhi by 40 percent. Places such as Agartala (0.067) and Taper (0.067), on the other hand, exhibit the lowest degree centrality, indicating that they were struck by just one group. It is not the case, however, that all state capitals are highly central or particularly susceptible to violence.

**Table 1.** Two mode centrality for terrorist groups. (*Degree centrality* is the number of ties directly connected to an actor regardless of the direction of those ties, identifying the groups carrying out the most attacks and the locations targeted most frequently. *Eigenvector* measures the influence of a node in the overall network (Newman 2008), reflecting the groups sway over other terrorist groups. *Closeness centrality* is the average length of the shortest path between the node and all other nodes in the graph, indicating how close a specific group is to the sites or activities of other groups. *Betweenness centrality* measures how often a node lies in the shortest path between other nodes, capturing how a group affects the overall connections between nodes and locations.)

Group	Degree	Eigen	Between	Closeness	D-Rank	E-Rank	B-Rank	C-Rank
LeT	0.471	0.768	0.622	0.5	1	1	1	1
HM	0.392	0.493	0.523	0.381	2	2	2	2
HuJI	0.176	0.122	0.405	0.197	3	6	7	3
I Mujah	0.157	0.205	0.467	0.117	4	4	4	4
SIMI	0.118	0.152	0.457	0.075	5	5	5	5
JeM	0.098	0.234	0.473	0.039	6	3	3	6
JKIF	0.039	0.111	0.457	0.01	8	7	6	7
HuA	0.059	0.072	0.374	0.006	7	8	12	8
Al Badr	0.02	0.059	0.385	0	9	9	8	9
AUM	0.02	0.059	0.385	0	10	10	9	10
DeM	0.02	0.059	0.385	0	11	11	10	11
JuM	0.02	0.059	0.385	0	12	12	11	12

## 4.2 Subgroups

For cluster analysis we constructed two sets of edge lists and two one-mode networks derived from the two-mode matrix. These one-mode networks are dichotomized, but we use the number of attacks to inflate node sizes in the network graphs. We employed a Clauset-Newman-Moore hierarchical clustering algorithm based on modularity to uncover the clustering of actors and events [17].

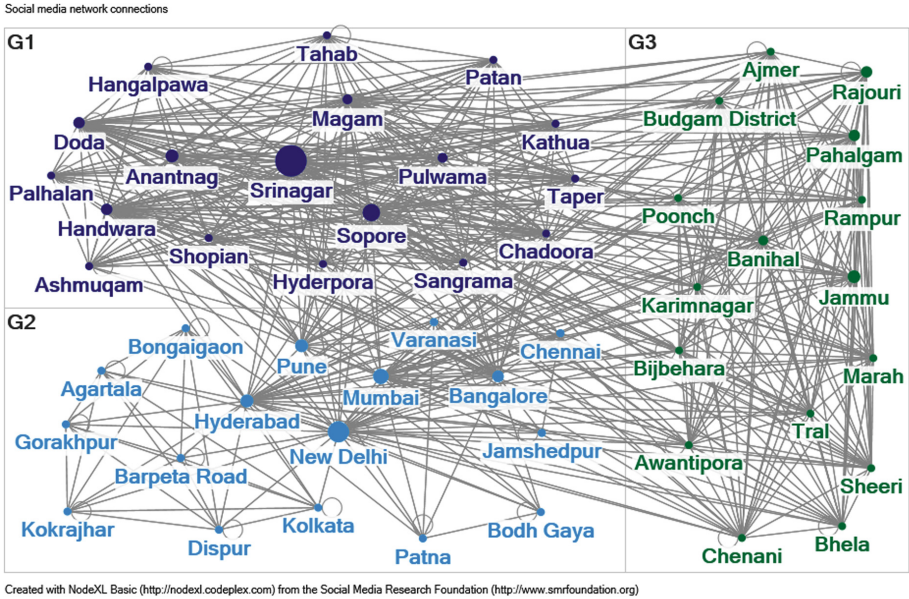
As depicted in Fig. 2, we identify three primary target subgroup clusters (G1, G2, G3). State capitals are clustered together in G2 (except for Srinagar), suggesting they represent a strategic target type. Locations outside of the conflicted state of Jammu & Kashmir (J&K) in India tend to be clustered in one of the subgroups. The geographic locations within J&K are clustered in G1 and G3. Two exceptions are Karimnagar and Ajmer, which are geographically located outside of J&K, but placed within G3, suggesting these cities act as transit points for terrorist groups active in J&K. An intervention strategy that increases state vigilance in Karimnagar and Ajmer may have an impact in reducing terrorism in J&K. The clustering of many cities within J&K together into subgroups underscores the notion that geographical location, as well as regional conflict, are critical for making an area attractive as a terrorist target. The findings also suggest that the two clusters, G1 and G3, are “in-effect” the same, forming an implicit network among themselves that may be analyzed as a single group.

Clustering also occurs among the terrorist groups (not shown). There were two main clusters, one consisting of the domestic organizations and the other international groups. The general clustering pattern for the non-isolates highlights the tendency of domestic groups and international entities to target similar locations within categories of organization (domestic/international), and to strike at locations that differ from those of the other category. Clustering can also indicate the presence of implicit terrorist networks.

Implicit terrorist networks have major theoretical and policy importance. Theoretically, they expand our notion of a terrorist network, connecting network-actors and behavior more closely together. Empirically, they allow us to measure networks through observable visible phenomena rather than employing questionable intelligence. There are also four critical counter-terrorism policy impacts.

## 4.3 Counter-Terrorism Policy

It is said that it takes a network to take down a network [18]. An addendum is that it takes an understanding of implicit networks to target and destroy terrorism networks. Terrorist groups often pick on specific locations that are referred to as hot spots, which tend to occur in clusters. Counter-terrorism resources should be focused on areas most likely to be targeted, such as state capitals, national capitals and other symbolic cities or areas. Extremist groups act in ways that are not independent, creating implicit networks. Counter-terrorists need to understand the interaction of groups and contexts [19] and recognize that violence does not inoculate an area but indicates the opposite - a high likelihood of more violence in the same area.



**Fig. 2.** Subgroups of locations (node size corresponds to the number of attacks experienced)

Subgroups in unexpected locations may indicate an external presence or additional support. For example, Karimnagar and Ajmer, shown in Fig. 2 are two cities geographically located outside of Jammu & Kashmir (J & K), but placed together as part of the two subgroups G1 and G3 comprising locations based in J & K. Sub-groups might actually be variants of the same group. As found in our network community analysis (Fig. 2), there is a strong likelihood that the two clusters G1 and G3 are “in-effect” the same, and thus represent an “implicit terrorist group.” Counter-terrorist practices may benefit from effectively treating those in clusters as a single group, recognizing implicit networks.

## 5 Conclusion

Social network analysis (SNA) represents a tool for understanding terrorist networks. Krebs [20] was among the first to use SNA to analyze 9/11. Scholars argue that networked structures facilitate terrorists’ use of violence [18] and networks influence terrorist acts’ impact [21]. Several studies use SNA to examine network links within [22] or between extremist groups [1]. We extend extant research by treating the links between terrorist groups and the geographic location of their

attacks as two-mode networks. To the best of our knowledge, this is the first work applying this approach to the study of terrorism and implicit terrorist networks.

**Acknowledgment.** This research was sponsored in part by the U.S. Army Research Laboratory and the U.K. Ministry of Defense under Agreement Number W911NF-16-3-0001. The views and conclusions contained in this document are those of the authors and should not be interpreted as representing the official policies, either expressed or implied, of the U.S. Army Research Laboratory, the U.S. Government, the U.K. Ministry of Defense or the U.K. Government. The U.S. and U.K. Governments are authorized to reproduce and distribute reprints for Government purposes notwithstanding any copy-right notation hereon.

## References

1. Asal, V.H., Park, H.H., Rethemeyer, R.K., Ackerman, G.: With friends like these... Why terrorist organizations ally. *Int. Public Manag. J.* **19**(1), 1–30 (2016)
2. Felmlee, D.H.: Interaction in social networks. In: Delamater, J. (ed.) *Handbook of Social Psychology. Handbooks of Sociology and Social Research*. Springer, Boston (2006). [https://doi.org/10.1007/0-387-36921-X\\_16](https://doi.org/10.1007/0-387-36921-X_16)
3. Felmlee, D.H., Lungeanu, A., Kreager, D.: Online Dating Preferences: Two-Mode versus One-Mode ERGM Network Analysis. Presented at the meetings of the Population Association of America, Chicago, IL (2017)
4. Berrebi, C., Lakdawalla, D.: How does terrorism risk vary across space and time? An analysis based on the Israeli experience. *Def. Peace Econ.* **18**(2), 113–131 (2007)
5. McCauley, C.: Jujitsu politics: Terrorism and response to terrorism. In: *Collateral Damage: The Psychological Consequences of America's War on Terrorism*. Greenwood Publishing Group (2006)
6. Crenshaw, M.: The logic of terrorism. *Terror. Perspect.* **24**, 24–33 (2007)
7. Drake, C.J.: The role of ideology in terrorists' target selection. *Terror. Polit. Violence* **10**(2), 53–85 (1998)
8. National Consortium for the Study of Terrorism and Responses to Terrorism (START) Homepage. <https://www.start.umd.edu/gtd>. Accessed 26 Apr 2018
9. South Asian Terrorism Portal. India: Terrorist, Insurgent, and Extremist Groups. <http://www.satp.org/satporgrp/countries/india/terroristoutfits/index.html>. Accessed 26 Apr 2018
10. Basu, A.: Social network analysis of terrorist organizations in India. In: *North American Association for Computational Social and Organizational Science (NAACSOS) Conference*, pp. 26–28 (2005)
11. Saxena, S., Santhanam, K., Basu, A.: Application of social network analysis (SNA) to terrorist networks in Jammu & Kashmir. *Strateg. Anal.* **28**(1), 84–101 (2004)
12. Wasserman, S., Faust, K.: *Social Network Analysis: Methods and Applications*, 1st edn. Cambridge University Press, Cambridge (1994)
13. Breiger, R.L.: The duality of persons and groups. *Soc. Forces* **53**(2), 181–190 (1974)
14. McPherson, J.M.: Hypernetwork sampling: Duality and differentiation among voluntary organizations. *Soc. Netw.* **3**(4), 225–249 (1982)
15. Freeman, L.C.: Centrality in social networks: Conceptual clarification. *Soc. Netw.* **1**, 215–239 (1979)
16. Newman, M.E.: The mathematics of networks. *New Palgrave Encycl. Econ.* **2**, 1–12 (2008)

17. Clauset, A., Newman, M.E.J., Moore, C.: Finding community structure in very large networks. *Phys. Rev.* **70**(6), 1–6 (2004)
18. Arquilla, J., Ronfeldt, D.: *Networks and Netwars: The Future of Terror, Crime, and Militancy*. Rand Corporation, Santa Monica (2001)
19. Gartner, S.S.: *An Introduction to Net Assessment 2.0: Special Issue on the Net Assessment of Violent Non-State Actors*. CTX: Conflict Terrorism Exchange (2015)
20. Krebs, V.E.: Mapping networks of terrorist cells. *Connections* **24**(3), 43–52 (2002)
21. Gartner, S.S.: Ties to the dead: Connections to Iraq War and 9/11 casualties and disapproval of the president. *Am. Sociol. Rev.* **73**(4), 690–695 (2008)
22. Everton, S.F.: *Disrupting Dark Networks*. Cambridge University Press, Cambridge (2012)