Journal of Engineering Science and Technology
Vol. 11, No. 11 (2016) 1629 – 1638

TOWARDS THE INVESTIGATION OF USING SOCIAL NETWORK ANALYSIS FOR COUNTER TERRORISM IN WEST AFRICA: CASE STUDY OF BOKO HARAM IN NIGERIA

F. OLAJIDE*, K. ADESHAKIN

Department of Computer and Information Sciences,
Covenant University, Ota, Ogun State, Nigeria
*Corresponding Author: funminiyi.olajide@cu.edu.ng

Abstract

In this paper, an investigative review of social network analysis (SNA) to counter terrorism is presented. Various measures used for predicting key players of terrorist networks are discussed. The methods used for the survey is based on the existing research work that was carried out on counter terrorism of insurgency, for example, 9/11 (2001) attack in the United States. The research papers have shown that the SNA is one of the most efficient and effective methods for understanding terrorist networks. For example, the National security agency has been mapping phone calls ever since the 9/11 event and through this research work, United States have been able to uncover so many hidden terrorist and criminal groups. This paper provides an avenue for a suggestive idea that the Nigerian government can make use of SNA technique by phone mapping. This is based on the fact that Nigeria can combat terrorism in the nation. The Nigerian government can emulate phone mapping technique as Boko Haram terrorists are within the country and they actually make use of phone calls. The government only needs to collaborate with the telecommunication and network providers companies in Nigeria to track down these terrorists. Using SNA to understand/discover terrorist networks in the region is novel.

Keywords: Social network analysis, Counter terrorism, Covert networks, Boko Haram.

1. Introduction

Over the years, one of the challenges faced by government of different nations has been the rise of the Islamic extremist groups. In recent years, Nigeria has been experiencing a serious time of insecurity and violence orchestrated by an Islamic

Nomenclatures

A_{ij}	Element in the adjacency matrix A at ij^{th} position
d_{ij}	Distance or path length between two nodes *i* and *j*
g_{jk}	Total shortest part between two nodes j and k
$g_{jk}(i)$	Total shortest path between *j* and *k* which passes through node *i*
$L(b)$	Links outgoing to node *b*
$n(n - 1)$	Maximum possible number of ties that can exist in the network.
N	Number of nodes in the network and (N-1) is the factor for normalization
Nb_a	Nodes that are connected to the node *a*
Nb_i	Neighbouring nodes of *i*
(N-1)	Normalization
(N-2)	
PR	Page rank
$PR(b)$	Page rank of node *b*.
X_j	Eigenvector centrality of node *j*

Greek Symbols

$\lambda\lambda$	Eigenvalue
ϵ	Element

Abbreviations

API	Application Program Interface
BH	Boko Haram
GTD	Global Terrorism Database
HTTP	Hypertext Transfer Protocol
NSA	National Security Agency
SNA	Social Network Analysis

extremist group known as Boko Haram (BH). Akinfala [1] gave a brief history of this Islamic extremist group, a group founded by Mohammed Yusuf (a Kanuri) which had the name YusufiyaIslamiya group between 2001 and 2002. The group became known internationally in 2009 when members of the Islamic sectarian apprehended and killed member of the Nigerian Police Force, led the leader of the group, Mohammed Yusuf. However, a research by Jon [2], revealed a research reports which showed that there is a possible link between the Boko Haram and other International Terrorist Group or organizations, particularly the Al-Qaeda terror groups [2].

Boko Haram sect is largely based in the North-eastern part of Nigeria, which is made up of six states. Her aim is to achieve a pure Islamic state based on sharia law which promotes eradication of western ideology in Nigeria. Akinfala [1], in his research made a statistical analysis that showed that this group have killed over seven thousand Nigerians, mostly, in the Northern region. They are attacking public and International buildings and in recent times, the kidnapping of 276 female students in the town of Chibok in Borno State, Nigeria. Prior to the year 2009, the Nigerian Government paid less attention to the Boko-Haram sect, despite the security reports due to the assumption that the sects are largely

present at a particular location, leading to wide attack, killings and kidnapping of innocent Nigerian.

Teaching focused on purification of Islam and was not the only sect as at that time who had this motif. The rise of different sects became an issue to the government but was not treated seriously because of the need to avoid religious or ethnic conflict. Efforts were made by the National Security Adviser to fight against the Boko-Haram sect, by working with governments of other African nations, the U.S. government and Middle Eastern governments based on the assumption that the sect recruited members from different part of Africa. With this alliance formed, concrete results are still yet to be reported on the impact of the collaboration in reducing the activities of the sect. The inability of the government to predict possible conflict, due to its dynamic nature is also an issue yet to be addressed, not only in the issue of the Boko-Haram sect but other conflicts that can affect peace in Nigeria.

After the attacks of 9/11, according to Ressler [3], Social network analysis (SNA) became an important topic in the circle of academia, government and mainstream media. The importance of using SNA as a tool is interesting in the understanding of countering terrorism. After the occurrence of 9/11, researchers began to use SNA as a tool for solving the puzzle of terrorist networks. Valdis Krebs in 2001 mapped the Al-Qaeda network by extracting reports on the Al-Qaeda hijackers [4], and used computer software to process the data based on basic network principles. Other researchers Carley et al. [5] also worked on the potential uses of SNA and with other multi-agent modelling techniques to destabilize terrorist networks.

Rothenberg [6] predicted the structure of the Al-Qaeda terrorist network in his articles and also, in the daily newspapers and radio commentary. Thus, terrorist activities have been on the rise, and researchers globally have been using SNA to understand terrorist networks. In this paper, researcher focuses on the review of how SNA can be used to map terrorist networks. The prospects of using SNA are considered as important tools with formulated metrics, in order to uncover terrorist networks in West Africa (Nigeria). A review of related research work using various SNA measures in the field of counter-terrorism analysis is summarized. In addition, the researcher focused on detailed comparison of various measures and techniques for SNA and also, methods for collecting social network data.

The research works in the area of counter terrorism using SNA is not new in the developed countries of the world. Krebs [4] in his research work, mapped the terrorist network of the 9/11 attack by gathering data and provided statistical data to the public based on the available information gathered about the 19 hijackers that were involved in the attack [4]. Using social network centrality measures and tools, the research work of Krebs was able to identify the important actors (key players) in the network which allowed him to understand how the terrorist network is structured and how this structure can help in prosecution and not prevention of criminals. Kathleen et al; presented a paper on destabilizing dynamic covert network and in the research work, appropriate approach was proposed to assess destabilization tactics for covert networks which can be applied to dynamic networks so as to destabilize them by identifying individuals whose roles are dynamic and can disrupt the structure of the network [7]. One of

the proposed approach, being collection of data are referred to data collection in publicly available archives which could form part of the information needed to understand covert networks and identifying potential members of the network which would form a basis for analysis.

Jennifer et al. [8] analysed and visualized criminal networks by using several SNA measures based on facts to describe the dynamism of terrorist networks. The result of this research showed that SNA measures could help in detecting and describing changes in criminal organizations through the use of centrality measures for individuals and cohesion, stability and density for groups [8]. Domain experts in the field of study commended the approach as being useful and applicable in crime investigation and criminal prosecution. Klausen et al. [9] built on existing research work and applied various SNA measures to study the social network of YouTube account holders linked with al-Muhajiroun's jihadist post on YouTube and this study revealed that SNA can serve as a diagnostic tool when trying to convince people about terrorism on social media platforms. The study also showed how SNA can be used to map communication structures and give an understanding of communication networks. Wu et al. 10] used SNA to find the likely replacement of Bin Laden as leader of Al-Qaeda by examining the Al-Qaeda terrorist network and important criteria's for selecting the next leader of the Al-Qaeda Terrorist group. Using a media based sample alongside SNA, the research was able to predict the most likely successor of Bin Laden considering the dynamics in the Al-Qaeda structure which in turn provided an insight of leadership potential which could be used to predict the next leader. Sarvari et al. [11] used publicly leaked email addresses of criminals to create a large scale social network graph and to find out the Facebook pages that are linked to various email addresses. It was proved that SNA measure were also applied and thus, resulted in the discovery of higher ranked criminals and criminal communities and a manual analysis to discover criminal groups on Facebook. This research shows how much information can be derived from having access to criminal emails which holds a great potential of uncovering covert criminal networks.

In time past, Nasrullah and Henrik [12] used SNA centrality measures to investigate complex networks. Explained how terrorist networks can be destabilized and hence, proposed an algorithm that can be used to structure covert networks. The algorithm was tested with Krebs research of the 19 hijackers which showed the possibility of disrupting covert networks and Everton [13] built his research work and considered the entire social network topography by using SNA measures for identifying the important nodes in the social network and argued that nodes within a network of criminals could best disrupt the network other nodes and more importantly, overall network topography should be considered before planning strategies to disrupt a network. The research paper of Roberts and Everton 14] argued on the fact that two different approaches can be used to combat dark networks which are kinetic and non-kinetic However, the kinetic approach uses brute force but the non-kinetic approach emphasizes on the use of SNA in uncovering dark networks. In this research, data from Noordin top terrorist network was used to explain the two approaches. In 2013, Everton and Cunnigham [15], presented paper that can detect changes over time in networks structure and the effectiveness of the research was presented while studying the Noordin top's terrorist network from 2001-2010. The research indicated that decentralized terrorist networks are able to operate effectively and are hard to overcome.

2. Tools and techniques for counter terrorism using SNA

Social network analysis (SNA) applies network theory to analyse social networks in terms of social relationships. It was noted that networks are made up of nodes (individuals, groups, organizations) connected by edges (relationships, friendship, kinship, financial transactions). This network can either be an online network or an offline network. Online networks refer to online social networks such as Facebook and Twitter, where information is exchanged in real time period, with different forms of messages that are passing on the network. However, offline networks on the other hand are formed by relationships among individuals such as kinship, friendship, groups or organizations and also network of individuals in the group or the organization.

The method of collection of data is one of the major challenges facing SNA for counter terrorism, which makes it difficult to have a complete network. To gain information concerning terrorists or terrorist organization is not an easy task, and therefore, information concerning members of terrorist groups is not made known by these groups, to the public and the government rarely makes this data available to researchers due to security reasons. But, the recent research work using SNA for counter terrorism according to Choudhary and Singh [16], has made it possible to make use of both online and offline social networks as means of collecting data to build networks of analysis for counter-terrorism. However, researchers over the years have collected data from online social network for analysis and this has made it possible to understand the behavior in such network but unable to also uncover hidden details and activities of the network. Most of the popular social networks such as Facebook, Twitter are commercial entities and as a result, it is not easy to get data due to user privacy. Therefore researchers collect data directly from these online networks or by sniffing the network traffic and passing the data to and from the online social network [17].

Some online social network providers such as Facebook and Twitter have API (Application Program Interface) that can be used to elicit certain data and this is commonly used by researchers in the field of SNA. But, in situations where data are available on the website but may not be available on the API, some researchers make use of other alternative means of eliciting data through web crawling. This is the online social network with an automated script that explores the website and collects needed data using HTTP requests and responses [17]. Researchers in the field of SNA use either of these methods to elicit data from online social networks and can be used to actualize many other research purposes.

It is clear that offline SNA involves collecting data from publicly available reports such as news articles, call records and other publicly available information that might be relevant for the research work. Valdis Krebs supported the research idea and was one of the first researchers to make use of publicly available reports on terrorist using SNA to map a terrorist network, for example, the research presented in 2001 after the 9/11 attack [4]. Rodriguez [18] came up with a similar work to that of Krebs after the Madrid bombing in 2004. He also used public sources to map the terrorist network in his research.

There are also database repositories like GTD (Global Terrorism Database) that contain statistical data on terrorist activities which can be used for offline analysis however, method for analysis is paramount for the case of Boko Haram in Nigeria. This research considered some methods of SNA that can be applied

on the Islamic insurgence issues in the Northern part of Nigeria suck like Degree centrality, *Betweeness* centrality, Closeness centrality and Eigenvector centrality. These four analysis metrics of the commonly used centrality measures can be applied to analyse terrorist networks. This is because the centrality of a node can define its importance in the network, and this can show how powerful is connected in a node within the network, This can also be used to support how information flows within the network and with the different groups in the network.

2.1. Degree centrality

In SNA, centrality measures are important for the analysis of degree centrality. According to Opsahl et al. [19] a node centrality can be used to define its importance or prominence of personality in a network as this may be linked to its influence, control and power within the network. Clearly, degree centrality of a node is the number of direct links or connections to the node in a network. A node with high degree centrality in a network is considered to be a very important node in that network. In a directed network, two measures of degree centrality can be defined: in-degree and out-degree.

In-degree, involves several nodes being directed to a single node which represents the importance of that node in the network. This type of nodes are often said to be prominent or thus have high prestige in the network. Out-degree on the other hand involves a single node being directed to many other nodes. Nodes with high out-degree centrality are often referred to as influential nodes. In terrorist networks, an actor with high degree centrality shows how many actors have direct connection to that actor which can be used to deduce facts about the network but this are dependent on the research goal. Degree centrality of a node in a network can be mathematical represented in equation 1.

$$Gi = \frac{\Sigma j \epsilon G A i j}{N-1} \quad (1)$$

N.B social networks are generally represented as adjacency matrix A Where A_{ij} refers to the element in the adjacency matrix A at ijth position, N refers to the number of nodes in the network and (N-1) is the factor for normalization. In a terrorist group, this centrality measure can help to discover individuals that are likely to hold vital information in the network. It can be used to analyse a node connection to other nodes in a network which can either be directed to the node or directed from the node or both. Nodes with the highest degree centrality are those with the most direct connection to other nodes. This centrality measure can help to discover individuals that are likely to hold vital information in the network or individuals that are involved in most activities. The centrality measure can rates the importance of a node to the network which gives a form of ranking of each node in the network, that is, from the least important to the most important.

2.2. Betweeness centrality

Betweeness centrality is a measure used for identifying nodes that are bridges in a network; these are nodes that other nodes must pass through for information from one node to another node. A node with high *Betweeness* centrality is considered

an important and influential node in a network. In terrorist networks, *Betweeness* centrality shows the actor that acts as a link between two groups or a liaison, which is important to a terrorist network. *Betweeness* centrality of a node in a network can be mathematically represented in equation 2.

$$Bi = \frac{\Sigma j,k=G \frac{gjk(i)}{gjk}}{(N-1)(N-2)} \quad (2)$$

where g_{jk} represents the total shortest part between two nodes *j* and k and $g_{jk}(i)$ refers to the total shortest path between *j* and *k* which passes through node *i*. (*N*-1) (*N*-2) represents normalization. This illustration helps to identify individuals who control information flow in the network and in that case, removal of node within a network of other nodes could disrupt the flow of information in the network.

2.3. Closeness centrality

Closeness centrality emphasizes distance between a node and other nodes in a network. It shows how fast other nodes can be reached from a node. It also refers to the average of all the shortest paths between one node and another in a network. In terrorist networks, closeness centrality shows those actors that have easy access to each. Closeness centrality of a node can be mathematically represented in Eq. (3)

$$Ci = \frac{n-1}{\Sigma j \epsilon dij} \quad (3)$$

where d_{ij} represents distance or path length between two nodes *i* and *j*.

Closeness centrality measures the distance between nodes by calculating the combined weight of traversed links or counting the number of hops. There is shortest path that can find the shortest route between two nodes in a network. This applies when we have multiple paths that are connecting the two nodes. This can help to find suspected connections between these nodes in such a network density are an important tool to be considered in a network with *n* number of nodes. The density can thus be calculated as in: *n*(*n* - 1), which gives the maximum possible number of ties that can exist in the network.

2.4. Eigenvector centrality

Eigenvector centrality tends to find the most central nodes in terms of the overall structure of the terrorist network. A node with a high eigenvector centrality is considered a terrorist leader node in the network because it is more central and has influence over other nodes in the network. Therefore, in terrorist networks, Eigen vector centrality shows that connection between individuals with a group can be well connected in the network. We can assume them to be heads of department in a terrorist network and hence, Eigenvector centrality can be represented in Eq. (4)

$$X_i = \frac{1}{\lambda} \sum_{j \epsilon N b_i} A_{ij} . X_j \quad (4)$$

where Nb_i represents neighboring nodes of i and $\lambda\lambda$ is eigenvalue. X_j is the eigenvector centrality of node j and A_{ij} refers to the element in the adjacency matrix A at ij^{th} position.

2.5. Page rank

Page rank, just as the name implies is used in ranking and knowing the importance of nodes in a social network. Applying this to a terrorist network, shows the importance or the position an actor holds in the network. Page rank of a node **a** in a network can be represented in equation 5.

$$PR(a) = \sum_{b \in Nb_a} \frac{PR(b)}{L(b)} \quad (5)$$

where Nb_a represents nodes that are connected to the node a and $L(b)$ represents the links outgoing to node b. *PR* stands for page rank, therefore $PR(b)$ is the page rank of node b.

3. Summary and Conclusion

Due to the recent emergence of Islamic extremist group that poses threat to the Nigerian government and its citizens, this research presented the investigative study of metrics that can be used to carry out research work in the field of SNA. The methods used for the survey is based on the existing research work that was carried out on counter terrorism of insurgency, for example, 9/11 (2001) attack in the United States. The researchers are interested in the investigation of how these different approaches can be applied on the recent but on-going Boko Haram attacks in Nigeria. In this paper, the researches have shown that the SNA is one of the most efficient and effective methods for understanding terrorist networks. This is a suggestive research ideas that the Nigerian government can make use of to combat terrorism in the nation. For example, the NSA, has been mapping phone calls ever since the 9/11 event and through this mapping technique, United States have been able to uncover so many hidden terrorist and criminal groups.

The Nigerian government can also do the same because these terrorists are within the country and they actually make use of phone calls. This means that the government can collaborate with the telecommunication and network providers companies in Nigeria to track down these terrorists. For example, a research work, presented a SNA measures of YouTube account holders that are linked with Al-Muhajiroun's Jihadist post on YouTube by applying various SNA measures. The terrorist sect of Boko Haram in Nigeria releases videos but there are no proper research conducted to analyse how their messages are published online. The question of who posted the message has not been answered, including the individuals who are linked to the uploading of such materials. However, the use of data mining techniques can be described as an analytical process designed to explore data for example; large amount of data, typically in business and market related such like Big Data. Therefore, this paper is in support of the research carried out by Vedanayaki, as it was concluded that data mining techniques can be used to elicit needed data from a large set of data using SNA. Henceforth, this research has uncovered the important of SNA for tracing and investigating the

acts of terrorism in Nigeria. This research is pointing towards these question of who, how and when using temporal, functional, relational and correlation analysis of event reconstruction of activities carried out by Boko Haram on the Internet This is a direction toward further research work, because no dark network has been fully uncovered and these can be uncovered to an extent that this research will make public to understand how this terrorist groups function within a network of nodes.

4. Further work

One of the major issues with dark networks is having adequate data to map the network. Further research will gather data using SNA of a robust network that can uncover hidden facts about terrorist networks. Mapping of terrorist network in Nigeria through media reports and terrorist databases will also be carried out to have a better understanding of how the networks of Boko Haram are structured in Nigeria.

Acknowledgement

The authors sincerely appreciate the Covenant University who fully sponsored the project training aspect and financial support through the cause of writing this paper.

References

1. Akinfala, F.F.; Akinbode, G.A.; and Kemmer, I.A. (2014). Boko Haram and terrorism in Northern Nigeria: (A psychological analysis). *British Journal of Arts and Social Sciences*, 17(1), 115-136.
2. Jon, O.D. (2013). Terrorism and counter terrorism in Nigeria: Theoretical paradigms and lessons for public policy. *Canadian Social Science*, 9(3), 96-103.
3. Ressler, S. (2006). Social network analysis as an approach to combat terrorism: Past, present, and future research. *Homeland Security Affairs*, 2(2), 1-10.
4. Krebs, V. (2001). Mapping networks of terrorist cells. *Connections*, 24(3), 43-52.
5. Carley, K.; Lee, J.S.; and Krackhardt, D. (2001). Destabilizing terrorist networks. *Connections*, 24(3), 79-92.
6. Rothenberg, R. (2001). From whole cloth: making up the terrorist network. *Connections*, 24(3), 36-42.
7. Kathleen, C.; Matthew, D.; Max, T.; Jeffrey, R.; and Natasha, K. (2003). Destabilizing dynamic covert networks. *Proceedings of the 8th International Command and Control Research and Technology*.
8. Jennifer, X.; Byron, M.; Siddharth, K.; and Hsinchun, C. (2004). Analyzing and visualizing criminal network dynamics: A case study. *Intelligence and Security Informatics*, 3073, Springer Berlin Heidelberg, 359-377.
9. Klausen, J.; Barbieri, E.T.; Reichlin-Melnick, A.; and Zelin, A.Y. (2012). The YouTube Jihadists: A social network analysis of Al-Muhajiroun's propaganda campaign. *Perspectives on Terrorism*, 6(1).

10. Wu, E.; Rebecca, C.; and Garth, D. (2014). Discovering bin-Laden's replacement in al-Qaeda, using social network analysis: A methodological investigation. *Perspectives on Terrorism*, 8(1).
11. Sarvari, H.; Mbaziira, A.; Abozinadah, E.; and McCoy, D. (2014). Constructing and analyzing criminal networks. *IEEE Security and Privacy Workshop*.
12. Nasrullah, M.; and Henrik, L.L. (2006). Practical algorithms for destabilizing terrorist networks. *Intelligence and Security Informatics, IEEE International Conference on Intelligence and Security Informatics*.
13. Everton, S. (2012). Network topography, key players and terrorist networks. *Connections*, 32(1), 12-19.
14. Roberts, N.; and Everton, S. (2011). Strategies for combating dark networks. *Journal of Social Structure*, 12(2).
15. Everton, S.; and Cunningham, D. (2013). Terrorist network adaptation to a changing environment. *Crime and Networks*, 287-308.
16. Choudhary, P.; and Singh, U. (2015). A survey of social network analysis for counter-terrorism. *International Journal of Computer Applications*, 112(9), 24-29.
17. Fehmi, B.A.; Iain, P.; and Tristan, H. (2012). Reliable online social network data collection. *Computational Social Networks*. Springer London, 183-210.
18. Rodriguez, J.A. (2005). The March 11th terrorist network: In its weakness lies its strength, Department of sociology and analysis of organisations. *Working Paper EPP-LEA:03*, Barcelona.
19. Opsahl, T.; Agneessens, F.; and Skvoretz, J. (2010) Node centrality in weighted networks: Generalizing degree and shortest paths. *Social Networks*, 32(3), 245-25.