HIERARCHY EXTRACTION FOR COVERT NETWORK DESTABILIZATION AND COUNTERTERRORISM MECHANISM

Ismail A. A.[1], Ganiyu, S. O[2]., Alabi, I. O[2]., Abdulrazaq, A. A.[1], Muritala S.[3]
[1]Department of Computer Engineering, University of Maiduguri, Maiduguri, Borno State, Nigeria.
[2]Information and Media Technology Department, Federal University of Technology, FUT Minna, Minna, Niger State, Nigeria.

dekunleismail@unimaid.edu.ng, dekunleismail.aaazi@gmail.com

ABSTRACT

Reduction of incessant crimes is the utmost priority of security agencies. Use of intelligence has potential to bring crime rate under minimal control but, organizational structure imbibes by criminal groups has been keeping and protecting covert members. However, extraction of covert members from flat organization structure has some challenges especially in identifying and analyzing high ranking criminals. Therefore, this paper proposed the used of eigenvector centrality for extraction of high rank members that social network analysis considered passive. Furthermore, this approach could offer a robust platform to detect clandestine nodes that attempt to escape detection.

Keywords: *counterterrorism, hierarchy, network destabilization, and network builder,*

1. INTRODUCTION

Generally, Metadata from communication and social media networks are new trends of procuring comprehensive information about relationships of mobile phone users. Phone calls, Short Messages Services (SMS), social media data can be collected and rendered into graph of relationships or connections for particular set of mobile phone users, or other social activities (Butt, Qamar, & Khan, 2014; Karthika & Bose, 2011). The graph of relationships is called social network structure (SNS) or network graph. From a SNS, all members are given equal representation or status; this gives description of SNS and that of criminal network structure (CNS) as a flat organizational structure, because members cannot be distinguished from one another. Criminal groups akin to flat structure in order to protect high profile members from cheap detection (Eiseit & Bhadury, 2015; Husslage, Lindelauf, & Hamers, 2012; Minor, 2012).

Minor (2012) classified members of a criminal group into expendable and non-expendable. Expendable are overt members who execute agenda of the non-expendable ones. It is learnt that high profile members always keep away from activities of the organization which can cheaply roll them up with overt members, and they can also play their roles through intermediaries (Butt et al., 2014). Collection of data from telecommunication servers and social media networks can only provide information on relationships within the reach of surveillance. Such information can accord law enforcement agent opportunity to know if there is a valid relationship between ordinary floor members who are actual perpetrators and high-profile members who are non-expendable members. Unfortunately, there are no means to distinguish expendable members from non-expendable ones within a criminal/covert social network (CSN).

Criminal networks flourish on the flat organizational structure, because roles and real life status of members cannot be represented in the network graph or SNS. Roles and responsibilities are not confined on any member; criminal members are responsible to any task at his/her disposal. Therefore, they are bound to act like leader and take any decision based on their discretion/wisdom (Manning, 2010; Roberts & Everton, 2011). This describes the leaderless principle in CSN and lack of pragmatic orders and hierarchies within the CSN (Minor, 2012).

The sort of relationships among members of criminal organization and lack of hierarchies offer opportunities to criminal organizations to wax stronger and sustain securities attacks despite the fact that some members can be eliminated. Detective techniques are designed to identify main leader(s) or key player(s), whose roles are pertinent to the existence of the criminal organizations within the social network. This compels researchers, network analysts and security agencies to search for leader(s) of a criminal group in order to destabilize criminal organizational structure (Carley, Reminga, Kamneva, & Carley, 1998; Catanese, Ferrara, & Fiumara, 2013; Ferrara, De Meo, Catanese, & Fiumara, 2014; Fortunato, 2010; Galar, Fern, Barrenechea, & Bustince, 2012; Karthika & Bose, 2011; Martonosi et al., 2011; Molinero, Riquelme, & Serna, 2014).

Obviously, all detective techniques require features upon which covert nodes can be extracted from SNS or CNS. Such features for detecting covert members should be graph-based features because external features may be inaccessible or difficult to build with SNS. Graph-based features are adopted in the absence of personal node attribute or feature PNA or PNF(Costa, Rodrigues, & Travieso, 2008; Gregory, 2007; Mahyar, 2015; Zhang, Levina, & Zhu, 2015). Structural or graph-based features are substituted for PNA or PNF for identification of determinant node i.e. the intended node that might be of interest to analysts. Structural features are accomplished through Social network analysis (SNA) (Ahajjam, Badir, & Haddad, 2015; Ahsan, Singh, & Kumari, 2015; Butt et al.,

2014; Carter, Idika, Streilein, & Member, 2014; Catanese et al., 2013; Clauset & Woodard, 2013; Ferrara et al., 2014; Karthika & Bose, 2011).

Literatures acknowledged various techniques for detecting covert members in a SNS or CSN. However, they are ineffective in counterterrorism, because elimination of few detected members do not destabilize criminal organizations network (Eiseit & Bhadury, 2015). Failure on counterterrorism is as a result of flat organizational structure and leaderless principle of criminal. A node identified as leader could be an errant or ordinary floor member while non-expendable member(s) in the organization remain undetected i.e. continue cloaking and remain clandestine in the network by manipulating relationship to evade detection.

Rhode opined that members of criminal network do swap their roles i.e. through relationships or communications networks, a leader may have floor/ordinary member attributed value, while an ordinary member may be found as a leading member (Eiseit & Bhadury, 2015; Rhodes & Keefe, 2007). Another factor gathered is that there is discrepancy between the two concepts: actual/real life leader and accrued/ascribed leader through connections. Destabilization of criminal networks cannot be actualized when wrong node(s) is mistakenly taking for real leader. And no method has been found to establish connection between the duo, that is, the real leader and ascribed leader through accrue connections(Butt et al., 2014; Eiseit & Bhadury, 2015). Though this is a false alarm, but its implication is that wrong information will be used in decision making (Butt et al., 2014; Carley et al., 1998; Minor, 2012).

The remainder of this paper is presented as follows. Section 2 presents related works on counterterrorism and network destabilization. Section 3 discuses, hierarchical structural towards network destabilization and counterterrorism and Section 4 presents three cadres/categories of members in the covert network with flat organizational structure and Section 5 concludes this paper.

2. REVIEW OF RELATED LITERATURE

This section presents some of the works that identified the problem under discussion.

Sageman (2008 & 2005) describes terrorist groups like Al-Qaeda as leaderless organizations (Husslage et al., 2012; Sageman, 2005). Husslage et al., (2012) corroborated Sageman's assertion on leaderless principle and flat organizational structure using mathematical correlation analysis. Husslage et al., (2012), presented structures that denote flat organizational structure, in which leading nodes within the structure cannot be identified visually or through graph-based tools: SNA.

Husslage et al., (2012) proved that secrecy and efficiency on criminal relationships and transactions are relatively to trade off performance μ and variance $\sigma^2$of members'

centrality values. Correlation analysis results show that low variance indicates that no significant individual(s) or key player(s) can be identified /detected within the structure; since low variance indicates low differences between individual members' centrality values; thus all members could have equal status. Ranking them again may also give insignificant traits values (Husslage et al., 2012). This does not nullify presence of key players, but it attests that high profile members cannot be distinguished and will remain undetected.

It was inferred from Husslage's correlation analysis that mathematical correlations of member's links contain clue if high-profile member(s) or key player can be detected within the network structure. Husslage opined that optimal covert networks do have very low variance σ^2on members' centrality values, an indicator that high-profile member(s) may not be detected because of very low variance. Network graphs of any social media can also exhibit low variance provided that network participators have equal number of connections; when they are well embedded. Finally, flat organizational structure is not limited to CSN, it cut across all social networking and communication networks where key player and high profile individual cannot be identified based on links/ relationships in the network.

Butt et al.,(2014) proposed technique for identifying key player(s) in a multiple-layer of transactions. The authors affirm that key players in CSN always evade detection by hiding behind intermediary node(s) or hidden mediator(s). The method showed that exploration of more than one network platforms can make covert members to become more vulnerable to detection. Butt et al., (2014) deployed degree centrality on each transaction/ social record to identify tendency of culpable nodes found of hiding i.e. key players. The SNS of suspicious individuals used was not presented for observation and assessment, to ascertain location of detected nodes if it agrees on centrality-driven concept: if detected nodes are close to or located at centre of the network graph. The authors' approached identified different leaders according to degree centrality from financial transactions record, SMS, email and phone calls log data, and no hierarchical structure was presented or implemented.

Karthika and Bose (2011) presented SNA tools for detecting covert members in a CSN. The work compared results of SNA tools for covert or hidden node extraction. The study did not limit covert nodes to only actors in the network but all elements which involved in relationships or interactions are included. To show that covert node(s) are not distinguishable provided that such node is located at the centre of the network. Comparison was made on the detected nodes using degree centrality, betweenness centrality and closeness. The graph of relationships between hijackers, conspirators and various locations in 9/11attack was presented as sources where the various statistical measure were obtained. Khalid Al-Midhar (KAM) was detected and presented as covert node in the 9/11 graph using betweenness and degree centrality. Rayed and Bandar are

two locations acknowledged with the highest closeness centrality values, i.e. detected as the most closed locations or interacted with but not centrally located from network graph.

Ahajjam, Badir and Haddad (2015), Ahsan, Singh and Kumari(2015), Molinero, RiquelmeandSerna, (2014) reformed the SNA tools towards network extraction and community detection. The SNA was viewed as a factor which could have aided community evolution better than non-established paradigm. Community's evolution was conceived around set of nodes that have influence i.e. influential nodes; nodes that have better relationships with other nodes. It is quite understood that new groups can form or break away from main graph if there is a node that can pull them (other nodes). Community's detection based on influential nodes set new rule towards network partitioning (NP) by identifying influential nodes within the network along which the main graph can be divided.

Influential approach for community evolution has contrary phenomenon to existing paradigm for NP; where a network graph is divided haphazardly or arbitrarily using sort of algorithms which can divide network graph base on specified number of researchers' order or on ground truth basis. This was also used in Maeno's work (Maeno & Ohsawa, 2007). Thereafter, modularity (Q) is always employed to validate the communities structures authenticity i.e. if evolving communities/ portioned graphs are well connected internally than outside (Chen, Zaïane, & Goebel, 2010; Choudhury & Paul, 2013; Duch & Arenas, 2005; Pujol, Bejar, & Delgado, 2006; Salehi, Rabiee, & Rajabi, 2012; Smith, Senne, Philips, Kao, & Bernstein, 2013; Zhang et al., 2015).

According to Eiseit and Bhadury(2015), hidden node is easier to find through centrality than nodes that occupy peripheral position in the network. It draws clue that hidden nodes are well embedded because all relationships, communications, interaction revolve around well embedded or central node(s). However, lesser attention is given to nodes that occupy peripheral positions. Therefore mining for covert nodes stop immediately after the general covert nodes; network leader emerges.

Further probing of member(s) next in rank/hierarchy to the leading node has been overlooked or underestimated as irrelevant. Exploring nodes which are next in centrality values to the overall leading nodes could be potential future leaders to criminal groups. They could be nodes that occupy peripheral locations in the network. Next in rank nodes may be special tasks managers in which clandestine of their actual roles prevent analysts from acknowledge that they are worthy to be eliminated along with network leader. Finally, next in raking nodes could be strategic operators which are nearly classified among passive nodes but potential network builders immediate after elimination of incumbent network leader (Eiseit & Bhadury, 2015).

Catanese et al., (2013) and Ferrara et al., (2014)developed SNA-based techniques for extracting hierarchies using visualization concept from phone communications of

criminal members. Each study presents different route to accomplish their paradigms. Baseline to duo: forensic analysis of phone call networks and detecting criminal organizations in mobile phone networks employed SNA tools. The results of visualization reveal elements/members contributing to the main leader, though other technicalities were incorporated making it not to be purely SNA-based concept.

3. METHODOLOGY

There are three different members of criminal organization whose roles are pertinent to continuity of criminal groups: network leader, network builder and sleeper partner. Bhadury and Eiseit (2105) referred to covert members who are very important but occupy peripheral positions in the criminal network. The peripheral positions include special task like coupling of improvised explosive devises (IED), recruiting new members, and training of infantry (Eiseit & Bhadury, 2015). These set of members may not be discovered because they are not occupying central positions and only very few information may passes through them. Nevertheless, they are worthy of being removed because of the positions they hold in the network (Maeno, 2009; Maeno & Ohsawa, 2007; Rhodes & Keefe, 2007). Detective techniques fail to identify them because they occupy peripheral positions of the network. SNA techniques detect central figure; not peripheral nodes that are involved in special tasks.

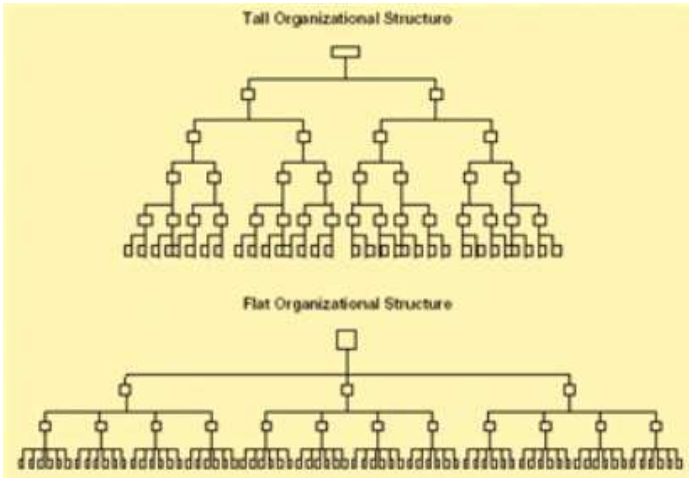

Figure 1: Tall and Flat Organizational Structures

Figure 1 presents tall/hierarchical organizational structure T/HOS and flat organizational structure FOS. The tall hierarchical structure has its top structure being narrow while flat has wider top. This implies that TOS has distinct compartment or departmental or functional sections than flat organization. The base line which is operational sections for the FOS cannot be distinguished because floor members could not be subjected under any distinct supervisor: to any superior nodes irrespective of

departments, while base line of T/HOS are distinct, because lower nodes are only beckon or answerable to their departmental or sectional superior nodes. One good analysis from the FOS is that more nodes including less expected node can succeed the current leader while T/HOS has limited number of nodes possible of succeeding current leader node; two nodes in TOS and three nodes in the FOS.

Hierarchy extractions based on SNA tools are proposed for mopping of high rank nodes and potential leaders. Mopping as being used is to identify and clear those nodes having next scoring centrality values close to a network leader as nodes occupying peripheral positions of the criminal network. The peripheral positions may be equivalent to special tasks an organization. Hierarchy is chosen to cater for some abnormal behaviour often exhibit by covert members like:

(1) Actual leader in a criminal network cannot be ascertained: detectable or not (Eiseit & Bhadury, 2015; Husslage et al., 2012).

(2) Criminal members always evade detection by swapping of their roles.

(3) SNA technique prioritizes or take cognizance of the highest scoring node(s) only, in all these cases, the leading node is the only relevant node while others are less important nodes.

Constraints to Hierarchy extraction in FOS

The chief executive officer (CEO) of T/HOS emerges from one of functional units of the organizations equivalent to special tasks in CSN (Carley et al., 1998; Eiseit& Bhadury, 2015; Kettley, 1995). The SNA tools are used to identify the general leader only. Nevertheless, the first constraint is that, FOS obtained through members' communications, relationships or social media networks cannot be further partitioned into distinct sections of work/ tasks/ department because communication network cannot include member's task features like PNA. Thus, mining hierarchies in CSN can be limited to few top members as movement towards the bottom of structures, the more it becomes difficult to separate members into sections or units due to lack features to cluster them into sections. Second constraint is that by convention, there is cord connecting upper hierarchy members to their subordinates. This might be vehemently missing because subordinates in FOS have no particular upper member(s) they are permanently and strictly taking orders from: FOS blocks identification of members from a particular unit or section. Further research can delve into how operational members can be split into sections or units.

PDF-XChange Viewer Click to buy NOW! www.docu-track.com

Reliability of SNA tools for Mining Hierarchy

The SNA tools are known for data mining, specifically hidden node. The most common tools of the task are: betweenness centrality, closeness centrality, degree centrality and eigenvector centrality. Each tool attests to the fact that a hidden node could be the one closely located at centre of the network graph. Setting that aside, a central figure that emerges from eigenvector centrality is the one who takes advantage of being connected with neighbour nodes with high eigenvector values. A node will have the highest eigenvector centrality score as a result of its neighbouring nodes having high score eigenvector centrality as well. Besides, occupants of peripheral locations or special tasks in the FOS are probably the nodes with next high eigenvector values.

In addition, occupants of special tasks must be experienced, qualified personnel before it can participate in the decision making. There is no metric to quantify experience and skills of members, therefore, the next lower scores could be assumed for this qualification in the absence of none. Discretion of taking the next lower scoring nodes for nodes to occupy second cadre or hierarchy is more appealing than any others as participators in decision making. Though, individual metric values should claim the position rather than arbitrary allocated to nodes. As earlier emphasized, any of nodes in second cadre / hierarchy could be emerged as a leader after the incumbent criminal leader might have been eliminated. Finally, another opportunity in this set of nodes is that, they may require less effort to reunite falling-away nodes (operational/floor members) after elimination of the top leader. That is more reason why, they should be addressed as network builder.

Eigenvector-Mechanism

Eigenvector centrality identifies a leading node based on quantity and quality of links. The first condition which can earn a node to be a leading node or central node is that if it has the highest number of link in the network, this represents ‘quantity of link’ which degree centrality offers to identify leading node. It is important to admit that criminal group can structure their relationships in which ordinary errant members can have highest number of links. The Matrix in Figure 2 can be used for illustrations. Each element is a neighbour to other elements. These elements denote nodes or actors in a criminal network.

A node can emerge as highest scoring eigenvector value if majority or all other nodes have links with it. That is, node id: a_{11} will be considered as central nodes provided all other nodes communicate with a_{11}. This would earn such node to automatically appear at the central. But, this is too extreme to occur in CSN because of secrecy, security, efficiency and large area expected to. A criminal leader communicates with subordinates (members) who can get his work done and not all.

$$M = \begin{bmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ a_{31} & a_{32} & a_{33} & a_{34} \end{bmatrix}$$

Figure 2: Elements Constituting Flat Organizational Structure

The 'quality of links' can also determine which node will make it up to the central. It shows that for a node to have the highest eigenvector value. its neighbouring nodes too should have significant values of influence or they are locally central in their locations. For instance, a node a_{21} has other nodes as neighbours: not onlya_{11}, a_{12}, a_{31} and a_{32} . If a node has high number of neighbour that pull crowd or nodes, such a neighbour will emerge at central irrespective of location.

Extraction of hierarchies from CSN only demands setting of threshold for eigenvectors values of nodes to be clustered in each hierarchy. First of all, hierarchical structure presented in this work adopts the highest scoring eigenvector node as the top most hierarchy which is equivalent to leading node. Second hierarchy contains nodes with equal eigenvector centrality values in which three nodes appeared. And the next lower hierarchy which is third has set of nodes that are close in eigenvector values.

4. RESULT AND DISCUSSION

The hierarchical structure presented below is from covert social network of Greece Nov 17 attacks. Names of actors in the network have been replaced with actor identity number (actor-id), for easy representation of members TOS.

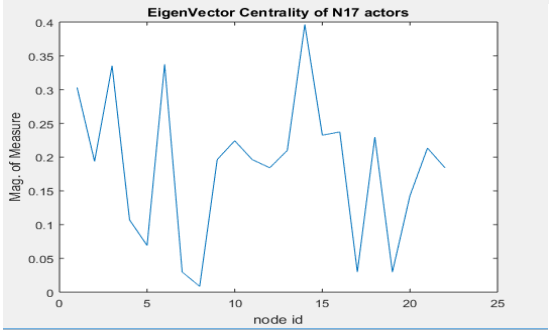

Figure 3: Eigenvector Centrality Graph

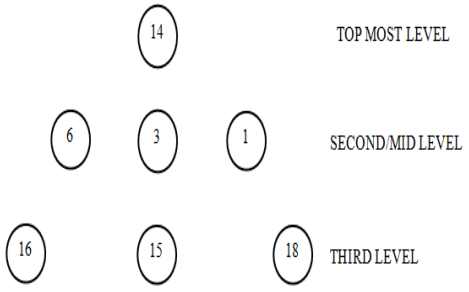

Figure 4: Eigenvector-Based Hierarchies

Figure 3 prsents eigenvector centrality graphs for actors in the N17 Greece attacks, while Figure 4 shows two more hierarchies below the leading node: node id 14. The second cadre in Figure 4 is the second hierarchy. This level is assumed to be occupied by the nodes with special tasks. The third hierarchy/cadre present set of people next in hierarch or rank to second cadre. Considering the constraints, it cannot be categoricaly

stated which node in the second cadre the node id 16 is a sub-ordinate to. Similarly, the same is appplicable to other nodes in the third cadre.

Discussion

This section presents relationship between eigenvector-based hierarchical structure and sections/factions in the N17 network. Figure 5 is the covert social network-CSN of N17 and three special tasks in the network encompasses:Generation leadership, Sardanopoulos faction and Koufontnas faction(Rhodes & Keefe, 2007). Members to each faction have relationship with members in other factions. Figure 6 is the 'gold standard' selection of members in each faction. Though, it was reported that the selection was arbitratry.

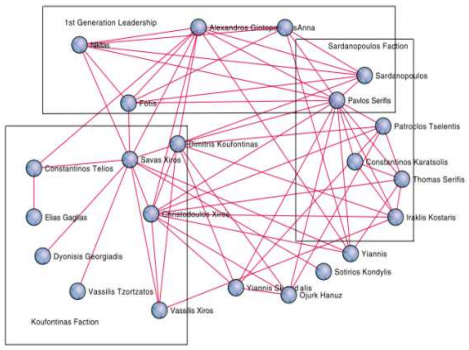

Figure 5: Covert social Network of N17

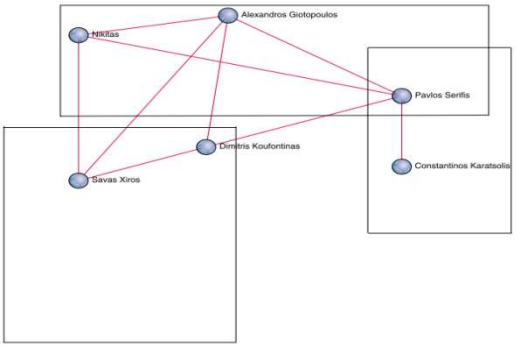

Figure 6: 'gold standard' selection (Rhodes & Keefe, 2007)

The order of nodes in Eigenvector-hierarchy are:14, 6, 3, 1, 16 , 15, and 18 are actors: Pavlos Serifis, Dimitris Koufontinas, Christodoulos Xiros, Alexandrous Giotopoulos, Savas Xiros, Sardanopoulos, and Thomas Serifis respectively. This shows that nodes id 6, 3, and 1 are prominent heads of the three factional sections in the group, but covered by FOS: so they appear in different locations i.e. not close to the actual section they control. Using the eigenvector-hierarchy, sectional heads of the CSN are nodes id 6, 3, and 1. In addition, Pavlos Serifis is the central leader according to the eigenvctor-hierarchy mechanism which is located in the faction Sardanopoulos. Then Sardanopoulos is located in the third lower hierarchy of the eigenvector based TOS. It is obvious that SNS is an illustration of flat organizational structures where section, departement individual members in an organizations belong cannot be easily categorized or classified.

5. CONCLUSION

Flat organizational structure considers all nodes to be of equal position and status in the network graph. This structure allows any node to assume any designated position in the network just to fill the gap out of exigensies. Nonetheless, current behaviours of high profile criminals in CSN necessitate the need for security agencies to utilize formidable

pragmatic concept to identify high placed covert members. Thus extraction of hierarchies using Eigenvector-based concept presents another opportunity to mop of high profile members in a CSN. Specifically, the Eigenvector-based TOS could be more robust in fixing hidden members who control the peripheral sectors of the criminal organization.

REFERENCES

Ahajjam, S., Badir, H., & Haddad, M. E. L. (2015). Towards a new approach for community detection algorithm in social networks. *International Conference on Big Data, Cloud and Applications Tetuan, Morocco, May 25 - 26, 2015 Towards*, 23–28. http://doi.org/10.1109/AICCSA.2015.7507215

Ahsan, M., Singh, T., & Kumari, M. (2015). Influential Node Detection in Social Network During Community Detection. *IEEE Cognitive Computing and Information Processing (CCIP), 2015 International Conference*.

Butt, W. H., Qamar, U., & Khan, S. A. (2014). Hidden Members and Key Players Detection in Covert Networks Using Multiple Heterogeneous Layers. *Journal of Industrial and Intelligent Information*, *2*(2), 142–146. http://doi.org/10.12720/jiii.2.2.142-146

Carley, K. M., Reminga, J., Kamneva, N., & Carley, K. M. (1998). Destabilizing Terrorist Networks. *Institute for Software Research , Carnegie Mellon University*.

Carter, K. M., Idika, N., Streilein, W. W., & Member, S. (2014). Probabilistic Threat Propagation for Network Security. *IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY*, *9*(9), 1394–1405.

Catanese, S., Ferrara, E., & Fiumara, G. (2013). Forensic analysis of phone call networks. *Social Network Analysis and Mining*, *3*(1), 15–33. http://doi.org/10.1007/s13278-012-0060-1

Chen, J., Zaïane, O. R., & Goebel, R. (2010). Detecting Communities in Social Networks using Local Information. *From Sociology to Computing in Social Networks*, 197–214. http://doi.org/10.1007/978-3-7091-0294-7_11

Choudhury, D., & Paul, A. (2013). COMMUNITY DETECTION IN SOCIAL NETWORKS : AN OVERVIEW. *International Journal of Research in Engineering and Technology*, *2*(2), 83–88.

Clauset, A., & Woodard, R. (2013). Estimating the historical and future probabilities of large terrorist events. *Annals of Applied Statistics*, *7*(4). http://doi.org/10.1214/12-AOAS614

Costa, L. F., Rodrigues, F. A., & Travieso, G. (2008). Characterization of Complex Networks : A Survey of measurements.

Duch, J., & Arenas, A. (2005). Community detection in complex networks using extremal optimization. *Physical Review E - Statistical, Nonlinear, and Soft Matter Physics*, *72*(2), 1–4. http://doi.org/10.1103/PhysRevE.72.027104

Eiseit, H. A., & Bhadury, J. (2015). The Use of Structures in Communication Networks

PDF-XChange Viewer Click to buy NOW! www.docu-track.com

to Track Membership in Terrorist Groups. *Journal of Terrorism Research*, *6*(1), 1–18.

Ferrara, E., De Meo, P., Catanese, S., & Fiumara, G. (2014). Detecting criminal organizations in mobile phone networks. *Expert Systems with Applications*, *41*(13), 5733–5750. http://doi.org/10.1016/j.eswa.2014.03.024

Fortunato, S. (2010). *Community detection in graphs*. Complex Networks and Systems Lagrange Laboratory, ISI Foundation, Viale S. Severo 65, 10133, Torino, I-ITALY. The.

Galar, M., Fern, A., Barrenechea, E., & Bustince, H. (2012). Hybrid-Based Approaches, *42*(4), 463–484. http://doi.org/10.1109/TSMCC.2011.2161285

Gregory, S. (2007). An algorithm to find overlapping community structure in networks, *4702 LNAI*, 91–102. Retrieved from http://www.scopus.com/inward/record.url?eid=2-s2.0-38049120277&partnerID=40&md5=086384ad72be41a9db115c1f2f428fa5

Husslage, B. G. M., Lindelauf, R., & Hamers, H. J. M. (2012). Leadeless Covert Networks: A Quantitativive Approach. *CentER Discussion Paper;2012 Tilburg: Econometrics. General*, *2012–57*, 1–15.

Karthika, S., & Bose, S. (2011). A COMPARATIVE STUDY OF SOCIAL NETWORKING. *International Journal on Web Service Computing (IJWSC)*, *2*(3), 65–78.

Kettley, P. (1995). *IS FLATTER BETTER ?: DELAYERING THE MANAGEMENT HIERARCHY*. The Institute for Employment Studies, Mental Building University of Sussex Brighton BM 1 9rF UK.

Maeno, Y. (2009). Node discovery in a networked organization. *IEEE International Conference on Systems, Man, and Cybernetics*, (October), 3522–3527.

Maeno, Y., & Ohsawa, Y. (2007). Analyzing covert social network foundation behind terrorism disaster. *International Journal of Services Sciences*, *2*(x), pp.125-141. http://doi.org/10.1504/IJSSci.2009.024936

Mahyar, H. (2015). Detection of Top-K Central Nodes in Social Networks : A Compressive Sensing Approach. *IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining*, 902–909.

Manning, J. D. (2010). Dark Networks. *U.S. Army College, Carlisle Barrack*.

Martonosi, S. E., Altner, D., Ernst, M., Ferme, E., Langsjoen, K., Lindsay, D., … Ronan, A. S. (2011). A New Framework for Network Disruption. Retrieved from http://arxiv.org/abs/1109.2954

Massa, M., & Zhang, L. (n.d.). The Role of Organizational Structure : Between Hierarchy and Specialization The Role of Organizational Structure : Between Hierarchy and Specialization, 1–39.

Minor, T. (2012). Attacking the Nodes of Terrorist Networks. *Global Security Studies*, *3*(2), 1–13.

Molinero, X., Riquelme, F., & Serna, M. (2014). Power indices of influence games and

PDF-XChange Viewer Click to buy NOW! www.docu-track.com

new centrality measures for agent societies and social networks. In *Advances in Intelligent Systems and Computing*. http://doi.org/10.1007/978-3-319-07596-9_3

Pujol, J. M., Bejar, J., & Delgado, J. (2006). Clustering algorithm for determining community structure in large networks. *The American Physical Society*, (March), 1–9. http://doi.org/10.1103/PhysRevE.74.016107

Rhodes, C. J., & Keefe, E. M. J. (2007). Social network topology: a Bayesian approach. *Journal of the Operational Research Society*, *58*(12), 1605–1611. http://doi.org/10.1057/palgrave.jors.2602352

Roberts, N., & Everton, S. F. (2011). Strategies for Combating Dark Networks. *Journal of Social Structure*, *12*, 2. http://doi.org/10.1007/s10796-010-9271-z

Sageman, M. (2008). The Origins of the Jihad, (January), 1–20.

Sageman, M., & D, P. (2005). Understanding Jihadi Networks Strategic Insights , Volume IV , Issue 4 (April 2005) The Evolution of the Global Salafi Jihad Ideology The History of the Global Salafi Jihad. *Europe*, *IV*(4).

Salehi, M., Rabiee, H. R., & Rajabi, A. (2012). Sampling from complex networks with high community structures. *Chaos (Woodbury, N.Y.)*, *22*(2), 23126. http://doi.org/10.1063/1.4712602

Smith, S. T., Senne, K. D., Philips, S., Kao, E. K., & Bernstein, G. (2013). Network detection theory and performance. *arXiv:1303.5613v1 [cs.SI] 22 Mar 2013*, 1–13. Retrieved from http://arxiv.org/abs/1303.5613

Zhang, Y., Levina, E., & Zhu, J. (2015). Community Detection in Networks with Node Features. *arXiv Preprint arXiv:1509.01173*, 1–16. http://doi.org/10.1109/ICDM.2013.167