A Case Study Of The Noordin Network

Elie Alhajjar, Travis Russell
United States Military Academy
Army Cyber Institute
West Point, NY 10996

May 3, 2019

Abstract

The military is constantly flooded with incomplete and sometimes inaccurate intelligence data concerning malicious organizations. Military leaders want to make the best decisions possible given the current information. Cyber analysts are challenged to filter through data, extract useful information, and provide meaningful recommendations that enhance decision-making. In this paper, network centrality techniques are applied to an incomplete or *dark network* to provide useful analysis for military decision makers. We investigate these techniques through the Noordin network data set and discuss potential future applications.

Network Science Counter-Terrorism Centrality Measures.

1 Introduction

The National Security Archive [7] defines *cyberspace* as a global domain within the information environment consisting of the interdependent network of information systems infrastructures including the internet, telecommunications networks, computer systems, and embedded processors and controllers. Within this framework, a *cyber attack* is an attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure, or destroying the integrity of the data or stealing controlled information. In other words, it is a deliberate exploitation of computer systems, digitally-dependent enterprises and networks to cause harm.

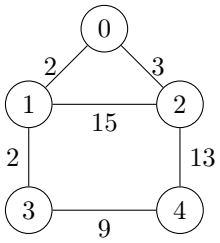
Terrorists' activities via cyberspace include creating website/blog, communication via email, discussion via chat room, e-transaction (e-commerce/e-banking), using search engines to collect data and find information, phishing/hacking, viruses, malicious code, etc... As an example, we discuss the website *www.anshar.net* created by *Noordin Mohammed Top* in Indonesia. Established for propaganda purposes, this website published successful terrorist attacks, recruited fellow prospective "soldiers" and distributed training material for agents.

From an online presence in cyberspace grew a terrorist cell, the *Noordin network*. Over the years, this network claimed responsibility for many terrorist attacks such as the JW Marriott Hotel bombing in Jakarta (2003), the Australian Embassy bombing in Jakarta (2004), the Bali bombing (2005) and the JW Marriott and Ritz Carlton bombings in Jakarta (2009).

The initial data pertaining to the Noordin terrorist network were first published in 2006 - and later updated in 2009 - by students at the Naval Postgraduate School (NPS). The data consist of 139 actors, 22 relationships and 13 attributes between them. For a complete description of the Noordin network data set, we refer the reader to the book [6].

Sean Everton, co-director of the Common Operational Research Environment (CORE) Lab at the Naval Postgraduate School, has published several research papers concerning dark networks [1, 2, 3, 4]. Everton uses subsets of the Noordin network data set to demonstrate multiple military applications including tracking and disrupting dark networks. The findings in the present paper are aimed at supplementing these results.

The paper is organized as follows. In section 2, we review basic concepts from graph theory and network science. In section 3, we discuss the details of our methodology for collapsing the multiple layers of the network in hand. In section 4, we present the results obtained by performing



$$\begin{pmatrix} 0 & 2 & 3 & 0 & 0 \\ 2 & 0 & 15 & 2 & 0 \\ 3 & 15 & 0 & 0 & 13 \\ 0 & 2 & 0 & 0 & 9 \\ 0 & 0 & 13 & 9 & 0 \end{pmatrix}$$

Figure 1: A graph and its adjacency matrix

centrality measure computations on the adjusted data set. Section 5 summarizes the main ideas of the paper and raises some questions for future investigation.

We conclude this section with a quote by General Tito Karnavian, the head of the Indonesian police strike team that tracked down Noordin Mohammed Top [8]: *"Knowledge of the interconnected networks of friendship, kinship and marriage groups was very crucial to uncovering the inner circle of Noordin."*

2 Background

The terms *graphs* and *networks* are used indistinctly in the literature. The only nuance is that the term *graph* usually refers to the abstract mathematical concept of nodes and edges, while the term *network* refers to real-world objects in which nodes represent entities of some system and edges represent the relationships between them. We will give some formal definitions below. In most of this section, we follow the terminology established in [5] and we encourage the reader to refer to this book for further details on the topic.

Let $V = \{v_1, v_2, \ldots, v_n\}$ be a finite set of elements and $V \times V$ the set of all ordered pairs $\{v_i, v_j\}$ of elements of V. A relation on the set V is any subset $E \subseteq V \times V$. A *simple graph* is a pair $G = (V, E)$, where V is a finite set of *nodes* (or *vertices*) and E is a relation on V such that $\{v_i, v_j\} \in E$ implies $\{v_j, v_i\} \in E$ and $v_i \neq v_j$, that is G has no *loops*. The elements of E are called *edges* or *links*, we shall denote them as $E = \{e_1, e_2, \ldots, e_m\}$.

In this paper, we will be interested in *weighted graphs*. A *weighted graph* is a quadruple $G = (V, E, W, \phi)$ where V and E are as above, $W = \{w_1, w_2, \ldots, w_s\}$ is a set of *weights* (i.e. real numbers) and $\phi\colon E \to W$ is a *weight function*, that is, a surjective mapping that assigns a weight to each edge. In our work, we assume the weights are natural numbers. This means that if the weight between two nodes is equal to k, then there are k edges joining the two nodes.

If an edge e joins two nodes v_i and v_j, then we say that v_i and v_j are *adjacent* and they are *incident* to e. The simplest characteristic of a node is its *degree*, which is defined as the number of nodes adjacent to it.

The *adjacency matrix* $A = (a_{ij})_{i,j=1}^{n}$ of a weighted graph G is an $n \times n$ array defined as

$$a_{ij} = \begin{cases} \phi(\{v_i, v_j\}) & \text{if } \{v_i, v_j\} \in E \\ 0 & \text{otherwise} \end{cases}$$

Note that for a simple undirected graph, the adjacency matrix is symmetric and the entries on the main diagonal are all equal to zero. Figure 1 shows an example of a simple graph with 5 vertices along with the corresponding adjacency matrix.

As mentioned in Section 1, the Noordin network contains 139 nodes. Each node represents an actor who had some type of connection to the several attacks conducted by the terrorist organization during the period $2003-2009$. In a series of papers [1, 2, 3, 4], S. Everton et al. examined this network from different sets of lenses, two of which are relevant in our context. On one hand, they looked at the kinetic and non-kinetic approaches to countering terrorism based on the dynamics of the network. On the other hand, they used social network analysis (SNA) to identify key actors through performing centrality statistics on the network.

The main method in these previous works is to consider each attribute separately by projecting it on the set of nodes present in the network. This procedure attaches to each such attribute a single graph to depict it. The final product becomes a so-called *layered network* and the strategy employed boils down to studying the statistics in the set of layers, one layer at a time.

3 Methodology

Inspired by the layered network strategy and motivated by finding a more unifying method, we define herein the concept of *layered network collapse*. Informally, given a network formed by a set of layers, the idea is to 'collapse' the layers into only one such layer without losing the overall network information. This is done via a prescribed 'rule' that dictates the way in which the collapsing phenomenon happens.

Before delving into the formal definition, we need to filter the data set and tailor it to fit our study. In order to capture the contribution of each actor in the terrorist organization, we focus on the following attributes in particular: organizational affiliation, classmate-ship, internal communication, kinship ties, training events, recruiting ties, business affiliation, operations, friendship ties, religious affiliation, logistical places, mentor ties and meeting attendance. Below is a short description of the above attributes. For more details, we refer the reader to [cite].

- Organizational affiliation: an actor being listed as a member of a terrorist organization such as Abu Bakar Batallion, Al-Qaeda, Darul Islam, etc...
- Classmate-ship: actors involved in any type of educational activity at the same institution at the same time.
- Internal communication: actors relaying messages between them inside the network through some sort of medium.
- Kinship ties: actors who share family or matrimonial ties.
- Training events: actors who participate in any sort of activity that teaches knowledge and skills of terrorism in general.
- Recruiting: an actor who successfully recruited another actor to enlist in a terrorist activity.
- Business affiliation: actors who are a part of a profit or non-profit organization that employ people.
- Operations: actors involved in preparing and executing terrorist operations.
- Friendship ties: actors who share some type of close attachments.
- Religious affiliation: actors who attend the same mosque.
- Logistical places: actors providing key places to facilitate the execution of operations.
- Mentor ties: an actor who mentored another actor on the ideological, supervisory or technological levels.
- Meeting attendance: actors who met face-to-face in a specific location.

With the collected data in hand, we proceed to the main definition. Let G be a multi-layered network, where each layer is an unweighted simple graph $G_t = (V, E_t)$. Here V has 139 vertices corresponding to actors in the terrorist network and each E_t has n_t edges, where E_t depicts the relations within an attribute from the above list. We define a function ϕ on $V \times V$ as follows

$$\phi(\{v_i, v_j)\} := \sum_{\{v_i, v_j\} \in E_t} 1 \tag{1}$$

In other words, we combine all the edges present in all layers and assign a unit weight to each one of them. The resulting graph $G' = (V, E)$ is a weighted graph with weight function given by Equation (1) and whose weights are natural numbers. This is equivalent to stacking the layers of the network vertically and projecting the relations onto the bottom, hence the 'collapse' effect.

In terms of adjacency matrices, the layered network collapse translates in a straightforward manner. Let A_t be the adjacency matrix of layer G_t. Then the adjacency matrix of the new graph G' is simply the sum of the adjacency matrices of the layers of the original network

$$A = \sum_t A_t. \tag{2}$$

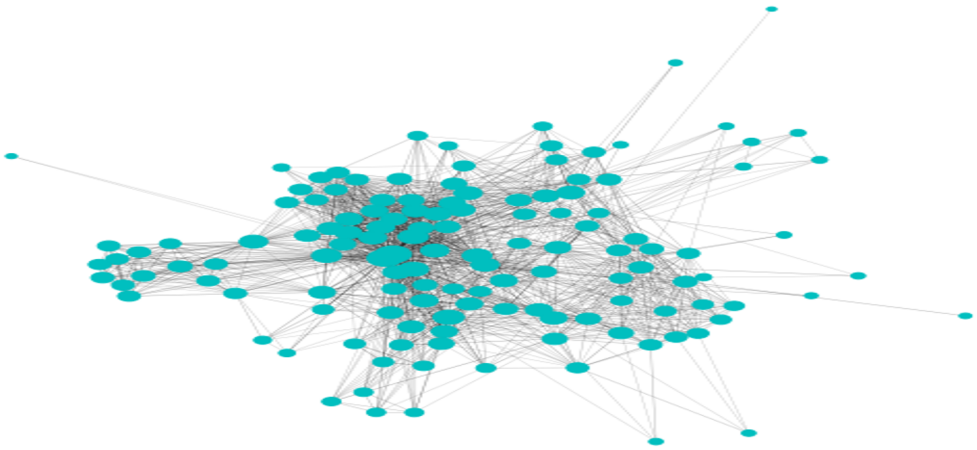


Figure 2: The Noordin Network after Collapse

The study of the original network is now transformed into the study of a more compact graph in which the involved actors are ranked by their overall contribution to the terrorist organization through its multiple facets of operation. Figure 2 shows a snapshot of the resulting network, where blue dots represent agents and gray lines represent relationships between them. We omit the weights of the edges for the sake of clear visualization.

4 Results

As mentioned in the previous section, the idea of the layered network collapse aims at compressing the multiple layers of a given network into a dense layer without losing too much information. Once the final network is achieved, the study boils down to performing centrality measure computations on the underlying graph and hence identifying the main players in the network.

There are plenty of centrality measures in the literature and efficient algorithms to compute them for large networks. Due to space constraints, we focus in this paper on three such metrics: the degree centrality, the eigenvector centrality and the betweenness centrality. Below is a concise definition of each of these measures. For a more detailed study of centrality measures, the book [5] is a great reference.

1. The degree centrality counts how many neighbors a node has. In terms of the adjacency matrix, the degree centrality of a vertex v_i is simply the sum of the entries in row i.

2. The eigenvector centrality measures the influence a node has in the network. In terms of the adjacency matrix, the eigenvector centrality of a vertex v_i is the i-th entry of the eigenvector corresponding to the highest eigenvalue of the matrix.

3. The betweenness centrality measures the extent to which a node lies on paths between other nodes. The betweenness centrality of a vertex v_i is given by

$$Betweenness(v_i) = \sum_{s \neq v \neq t \in V} \frac{\sigma_{st}(v)}{\sigma_{st}},$$

where σ_{st} is the total number of shortest paths from node s to node t and $\sigma_{st}(v)$ is the number of those paths that pass through v. The betweenness centrality is normalized by dividing by the number of pairs of vertices not including v, which is $\frac{(n-1)(n-2)}{2}$.

The table below summarizes the results obtained after applying these three centrality measures to the collapsed network. It is no surprise that Mohammed Noordin Top was the central player

in the terrorist network! However, other main players needed to be unveiled in order to dismantle the operational aspect of the group. We mention the five players with the highest scores, all our computations were done in MATLAB. We note that the main actors revealed in our study coincide with the ones declared by the Indonesian Police Department, once the terrorist cell got unfolded.

	Degree Centrality	Eigenvector Centrality	Betweenness Centrality
Azhari	0.104	0.3502	0.061
Iwan Darwish	0.0591	0.1968	0.0496
Ahmad Rofiq	0.0551	0.2043	0.0521
Ubeid	0.0576	0.2049	0.0496
Abdallah Sangkar	0.0515	0.1988	0.0506

5 Conclusion and Future Work

In summary, we have implemented a new method for identifying central players in a terrorist network. Our results match the previously discovered and adopted findings in this setting, concerning the main agents in the Noordin terrorist network. One advantage of our method is that it provides a compact study space where operations can be performed and reduces the focus from multi-layer to single-layer networks.

We conclude by summarizing future work we hope to pursue. In our initial work, we defined the function ϕ on $V \times V$ as $\phi(\{v_i, v_j)\} := \sum_{\{v_i,v_j\}\in E_t} 1$, i.e. we assumed equal contribution from each attribute. The next step would be to assign an influence factor e_t (a real number) to every graph E_t. The function hence becomes

$$\psi(\{v_i, v_j)\} := \sum_{\{v_i,v_j\}\in E_t} e_t, \tag{3}$$

and the centrality analysis follows.

Another line of research that would be a natural follow up to this project is the application of this proof-of-concept to a variety of other networks, different from the terrorist realm. Networks are one of the most vital tools to translate information into graphs and performing operations on them. Such instances may occur in the spread of diseases, social networks and malware propagation just to name a few.

References

[1] Fox, W. and Everton, S.: Using Mathematical Models in Decision Making Methodologies to Find Key Nodes in the Noordin Dark Network. American Journal of Operations Research **4**, 255–267 (2014)

[2] Roberts, N. and Everton, S.: Strategies for Combating Dark Networks. Journal of Social Structure **12**, 1–32 (2011)

[3] Fox, W. and Everton, S.: Using Data Envelopment Analysis and the Analytical Hierarchy Process to Find Node Influences in a Social Network. Journal of Defense Modeling and Simulation **11**, 1–9 (2014)

[4] Everton, S.: Network Topography, Key Players and Terrorist Networks. Terrorist Networks **1**, 12–19 (2009)

[5] Newman, M.: Networks: An Introduction. Oxford University Press, Oxford. (2010)

[6] Everton, S.: Disrupting Dark Networks. Cambridge University Press, Cambridge, UK and New York, USA (2012)

[7] National Security Archive Homepage, https://nsarchive.gwu.edu/news/cyber-vault/2018-09-19/cyber-glossary. Last accessed 4 May 2019

[8] Private communication between Gen. Tito Karnavian and Scott Atran, 10 December 2009