# Disrupting Transnational Criminal Organizations: *Logical Methods* for *Target Identification*

***by Justin Cole***

## Introduction

In today's dynamic and complex environment, as the nation's focus is drawn to irregular and asymmetric threats, establishing joint and interagency task forces (JIATF) is becoming common. These JIATFs, established in various locations around the globe, often require individuals who have not worked together before to work as a team. The pressure to provide results in a timely manner is great. The intent of this article is to provide the individuals responsible for identifying the organizational network of these threats a different way to think about developing recommended targets.

In July of 2011, President Barack Obama released the "Strategy to Combat Transnational Organized Crime." In the strategy, President Obama highlighted transnational organized crime (TOC) as a threat to national and international security. The President's strategic end state is "to reduce transnational organized crime from a national security threat to a manageable public safety problem."[1] One of the ways listed to achieve this end state is to "defeat transnational criminal networks that pose the greatest threat to national security."[2]

Networks are "comprised of people, processes, places, and material components that are identifiable, targetable, and exploitable."[3] Governments must first understand the nature of the threat before they can develop effective options to defeat TOC networks. Once governments understand the TOC network's economic, political, and social goals and its influence on society, government analysts can determine appropriate approaches to target the TOC network. Using center of gravity (COG) analysis and social network analysis (SNA) techniques, agencies can more efficiently operate to defeat and disrupt these networks.

TOC networks are often described as "dark networks," or networks whose activities are illegal

**Major Justin Cole is an Army Military Intelligence Officer with thirteen years of service. He is a Army Reserve officer assigned to the Joint Staff in Suffolk, VA. In his civilian career, he is a principal analyst for the Counter-Insurgency Targeting Program (CITP) of the National Ground Intelligence Center (NGIC) in Charlottesville, VA. His past experience includes deployments to Afghanistan, Iraq, and Kosovo.**

and attempt to be as invisible as possible.[4] COG analysis can lead investigators to an assessment of the critical requirements of the network that may be vulnerable to targeting. Effective use of SNA techniques can help investigators illuminate previously unknown links between nodes (the term for nouns within the network) as well as the importance of these links within the TOC network. As a better picture emerges about how TOC networks operate and are organized, investigators are able to make well-informed decisions concerning the most appropriate ways to disrupt and dismantle them.

## Transnational Organized Crime

The short explanation of TOC refers to organizations that operate by illegal means across international borders. The national strategy offers a more definitive definition:

> Transnational organized crime refers to those self-perpetuating associations of individuals who operate transnationally for the purpose of obtaining power, influence, monetary and/or commercial gains, wholly or in part by illegal means, while protecting their activities through a pattern of corruption and/or violence, or while protecting their illegal activities through a transnational organizational structure and the exploitation of transnational commerce or communication mechanisms.[5]

**In reality, TCOs are comprised of a complex system of relationships that connect licit (white market) with illicit (black market) economies**

For the purposes of this article, a transnational criminal organization (TCO) is comprised of a network involved in transnational, organized crime. In some ways, TCOs are not much different from multinational corporations (MNC). MNCs and TCOs are constantly looking for growth opportunities, new markets, and ways to realign their structures and strategies to maximize profits. TCOs recruit the right employees, build coalitions and partnerships with other TCOs, conduct hostile takeovers if necessary, and operate within the legitimate economy if it serves their best interests. The aim of TCOs is to "derive as much profit as possible from their activities—within the limits of acceptable risk."[6] In some instances, they will accept higher risk for higher profits; in others, they will avoid risk and accept lower profits.

"There is no single structure under which transnational organized criminals operate; they vary from hierarchies to clans, networks, and cells, and may evolve to other structures."[7] The crimes they commit also vary from drug, weapons, and human organ trafficking, to human smuggling, illegal piracy, and intellectual property-rights crime. In the past, these criminal networks operated using a hierarchical structure. Today, criminal networks are fluid and involved in striking new alliances with other networks around the world and engaging in a wide range of illicit activities. Labeling TCOs as gangs, groups, cartels, terrorist organizations, or even irregular forces is only putting a name to the most visible part of the network and may confuse the understanding of the organization. In reality, TCOs are comprised of a complex system of relationships that connect licit (white market) with illicit (black market) economies, which means TCOs often operate in the gray area between these two markets. Analysts must use a logical method to identify and target these networks effectively.

## Targeting

Targeting is "the process of selecting and prioritizing targets and matching the appropriate

response to them, considering operational requirements and capabilities."[8] This article suggests additional ways analysts and staffs can select targets for future engagement. These targets may be an area, compound, installation, force, equipment, capability, function, individual, group, system, entity, or behavior identified for possible action.[9] Critical in the understanding of the targeting definition is determining the "appropriate response." Often agencies and organizations outside the Department of Defense relate targeting to lethal responses usually associated with the military. Targeting encompasses lethal and non-lethal responses to identified targets. The appropriate response may be to influence a key leader by attending a meeting, or it may be to engage the target with direct or indirect weapons with the purpose of destroying it. When working with interagency and multinational partners, it is important all participants understand this terminology and agree on a common language.

The joint targeting cycle seeks to continuously analyze, identify, develop, validate, assess, nominate, and prioritize targets.[10] This article's intent is to highlight ways to determine appropriate targets.[11] COG analysis and the use of SNA techniques provide a logical approach to determining and selecting appropriate targets. Using these two approaches will, at a minimum, offer a structured procedure that (1) explains why a target was selected, (2) helps the analyst prioritize the target among others, and (3) describes the approach to engage it.

## Center of Gravity Analysis

While there is no single structure under which the TCOs operate, there are similar functions or capabilities required to operate. The same functions required for running a business can be applied to the analysis of a TCO. These functions do not convey a hierarchical structure, but to be successful, a TCO must conduct some common functions. Conducting COG analysis using these required capabilities is a useful way to determine appropriate approaches to effectively target TCO networks.

The COG analysis described in this article is based on the work of retired, U.S. Army Colonel Dale C. Eikmeier and the U.S. Army Asymmetric Warfare Group's (AWG) *Understanding the Threat* series.[12] Eikmeier's 2004 and 2007 *Military Review* articles offer a logical method to help analysts determine the COG of an entity. Eikmeier uses the ends, ways,

| Function | Description |
|---|---|
| **Accounting/ Finance** | **Manage revenue, costs, and profit through legitimate and illegitimate means** |
| **Personnel/ Staffing** | **Recruit for all required positions in network** |
| **Distribution** | **Movement of product from development to retail** |
| **Marketing** | **Introduction of product into new areas** |
| **Business Development** | **Search for growth opportunities; monitor and support growth** |
| **Business Intelligence** | **Analyze market; understand competitors and consumers** |
| **Operations Management** | **Minimize operational costs while maximizing profit** |
| **Communications/ IT** | **Communicate with all segments** |
| **Security** | **Secure employees and associated entities as well as product** |
| **Strategic Leadership** | **Develop and communicate vision for continued growth** |

**Table 1: Business Functions and Description**

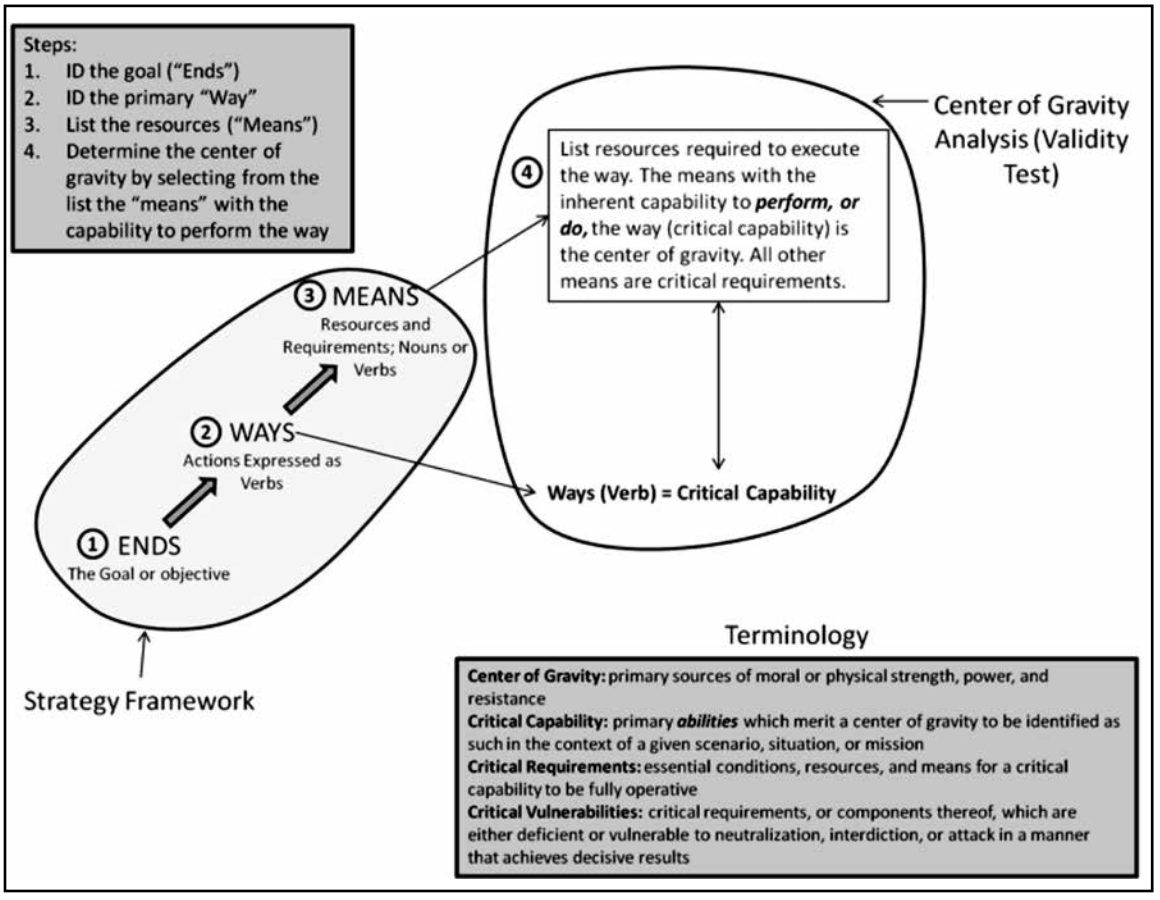


**Figure 1. Eikmeier's Logical Center of Gravity Determination**
**Source: Modified by the author, original version is found in Dale C. Eikmeier, "A Logical Method for Center-Of-Gravity Analysis," *Military Review* (September-October 2007): 63-64.**

and means strategic framework; a validation test; and clear terminology to logically determine the COG.[13] This logical determination is depicted in Figure 1. The AWG's *Understanding the Threat* series is based on the vulnerability assessment method, which involves conducting a complete COG analysis to determine friendly element actions (FEA) to engage threat critical vulnerabilities.

Eikmeier's method provides a logical process to determine a COG, giving an analyst a starting point for the AWG's vulnerability assessment method. Following these two methods will allow an analyst to determine a logical COG, complete with critical vulnerabilities available for targeting. As critical vulnerabilities (CV) are identified, they have the possibility to become decisive points or operational objectives to be achieved to reach a desired state. For the context of this article, that desired state is "to reduce transnational organized crime (TOC) from a national security threat to a manageable public safety problem."[14] By targeting the COG, either through direct means or indirectly through CVs, the strength of the TCO is challenged. Challenging the strength of the TCO and ultimately defeating it positively changes the operational environment toward the desired state. (See Figure 2)

Following Eikmeier's logical method for COG determination and using the business functions previously described, the COG for TCOs can be identified as the "operations management" function of the organization that

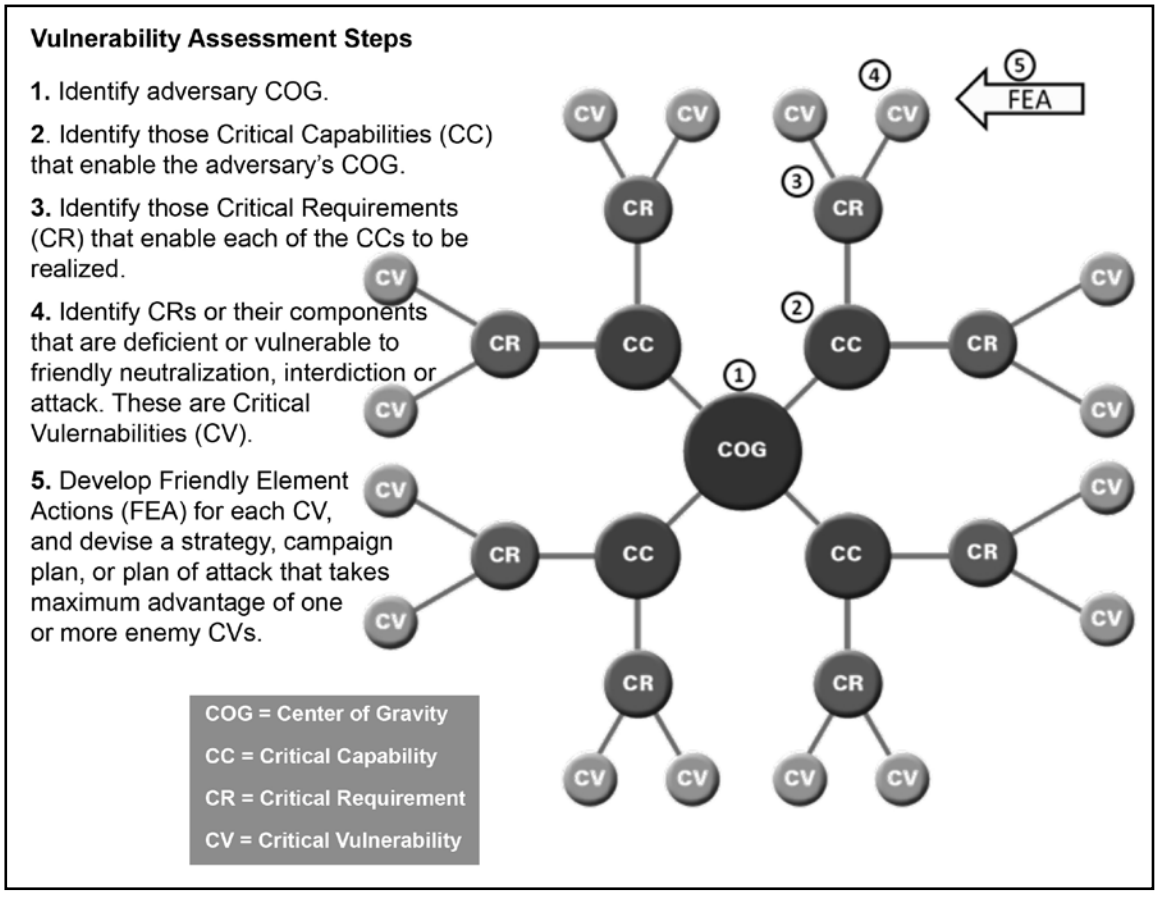


**Figure 2. AWG Vulnerability Assessment Method**
**Source: Modified by author, original version can be found in U.S. Army Asymmetric Warfare Group, "Transnational Criminal Organizations and Criminal Street Gangs in the Northwestern Hemisphere: Vulnerability Assessment Workbook," *Understanding the Threat Series*, Volume 5 (Fort Meade, MD: Government Printing Office, May 16, 2011), 3-5.**

conducts illicit trafficking, while minimizing loss. The operations management function of the organization, which acts as middle management, controls operations at the local and regional levels. (See Figure 3)

Once the COG is identified, the critical capabilities (CC), critical requirements (CR), and CVs can be determined. Using the COG determined through Eikmeier's method, analysts can determine that a CC of maintaining security by using a CR of a decentralized command structure has the CV of the identification of key facilitators. They can now recommend further FEAs to identify these key facilitators, or, if they have already been identified, make recommendations for engagement. The proper application of SNA techniques can help identify key facilitators (CVs) and other relationships within the TCO network. (See Figure 4)

The COG determined in this example was identified using a theoretical model of a TCO in a vacuum. COGs will be different for each TCO based on its operational environment and the way it operates. Not all TCOs may require the functions used in the COG determination method above. To determine an accurate COG, analysts must conduct a thorough analysis and have a basic understanding of the TCO and its critical functions. Following the methods described will enable the analyst to explain the selection of CVs for further investigation or targeting.

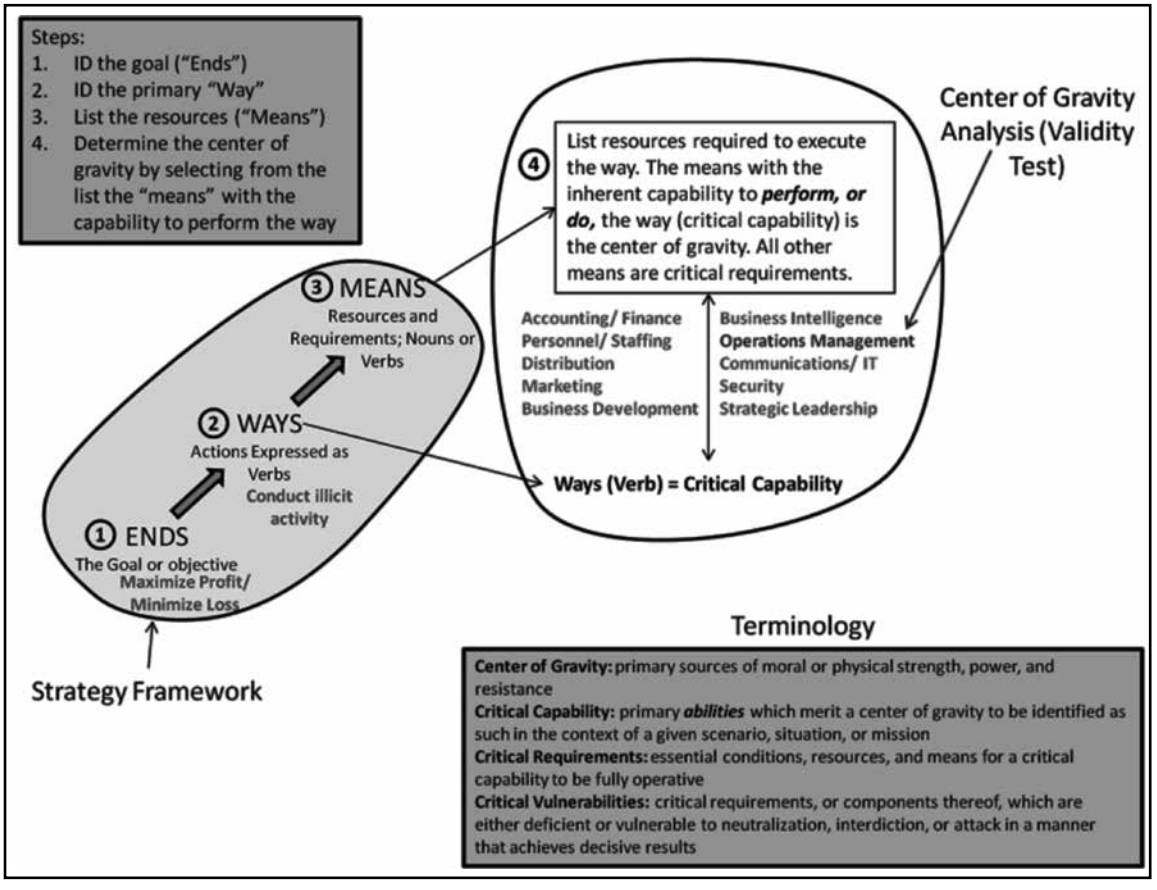


**Figure 3. TCO Center of Gravity Identification**
**Source: Modified by author, original version is found in Dale C. Eikmeier, "A Logical Method for Center-Of-Gravity Analysis," *Military Review* (September-October 2007): 63-64.**

## Social Network Analysis

SNA is the scientific study of social networks. True SNA will go beyond the mathematical properties of the social network and analyze the human dimension of the social relationships. Humans tend to create social links based on influences from their culture and peer groups. The techniques highlighted in this article are based on the mathematical techniques used to measure an entity's centrality in a social network or organization. SNA is more useful than traditional link analysis to determine subgroups, detect patterns of interaction, identify critical entities within the organization, and uncover a more realistic view of the organization and structure. Analysts who employ SNA can detect and highlight the connections between the visible parts of the TOC and legitimate businesses that may be operating as brokers or facilitators for the TCOs, which allows the analyst to continue to further develop an understanding of the organization.

Studies conducted by Shishir Nagaraja and Ross Anderson at Cambridge University concluded that the best organizational structure for criminal organizations to survive are cellular structures that displayed small-world properties.[15] A network displays small-world properties when cliques or groups form. This structure results in an organization with few individuals who may have many connections. Upon further statistical analysis, these individuals may be determined to hold key facilitator positions within the larger

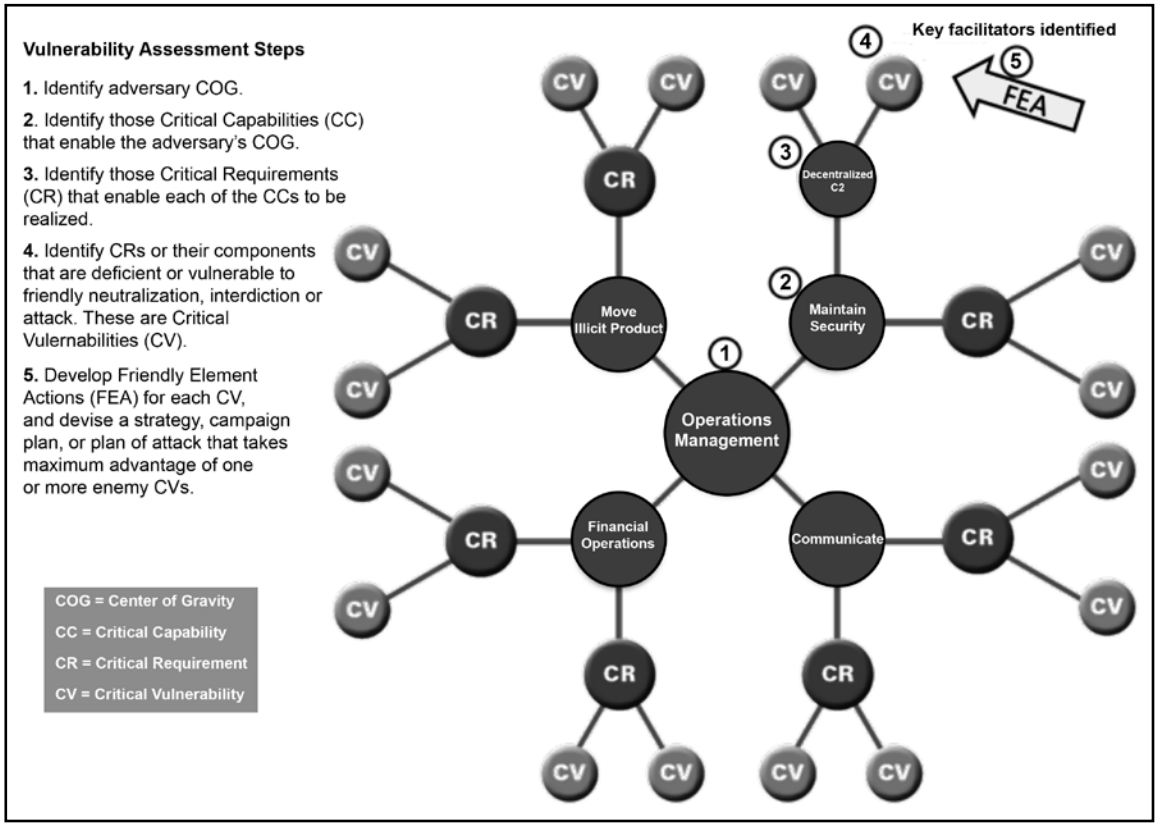


**Figure 4. CV Determination Using Vulnerability Assessment Method**
**Source: Created by author, base model derived from US Army Asymmetric Warfare Group, "Transnational Criminal Organizations and Criminal Street Gangs in the Northwestern Hemisphere: Vulnerability Assessment Workbook," *Understanding the Threat Series*, Volume 5 (Fort Meade, MD: Government Printing Office, May 16, 2011), 3-5.**

organization. Although this article will not delve into the statistics involved in determining these positions, it is important to highlight the utility of using these techniques to help locate critical positions within the network.

A common analytical technique used throughout the intelligence community is link analysis, which allows the analyst to visually depict the organization and present it for situational awareness. Analysts generally conduct link analysis by describing key relationships between organization members as information becomes available. These links generally resemble simple, hub-and-spoke network structures, with a leader at the top or center and key members added as they are determined. As more information is obtained, the resulting graphic can become difficult to read and analyze. Analysts using the link analysis method generally rely on visual analysis to determine nodes with high-degree centrality based on their placement within the network rather than on statistics. This issue is compounded as transnational groups and multiple subgroups are added to the overall network. Conducting a meaningful visual analysis of this type of graphic illustrated in Figure 5 is time consuming and can be a daunting challenge for most analysts.

In mathematical terms, a network is a graph in which the nodes and their links have associated values. Centrality is the primary mathematical measurement used in SNA. Centrality measurement generally highlights the

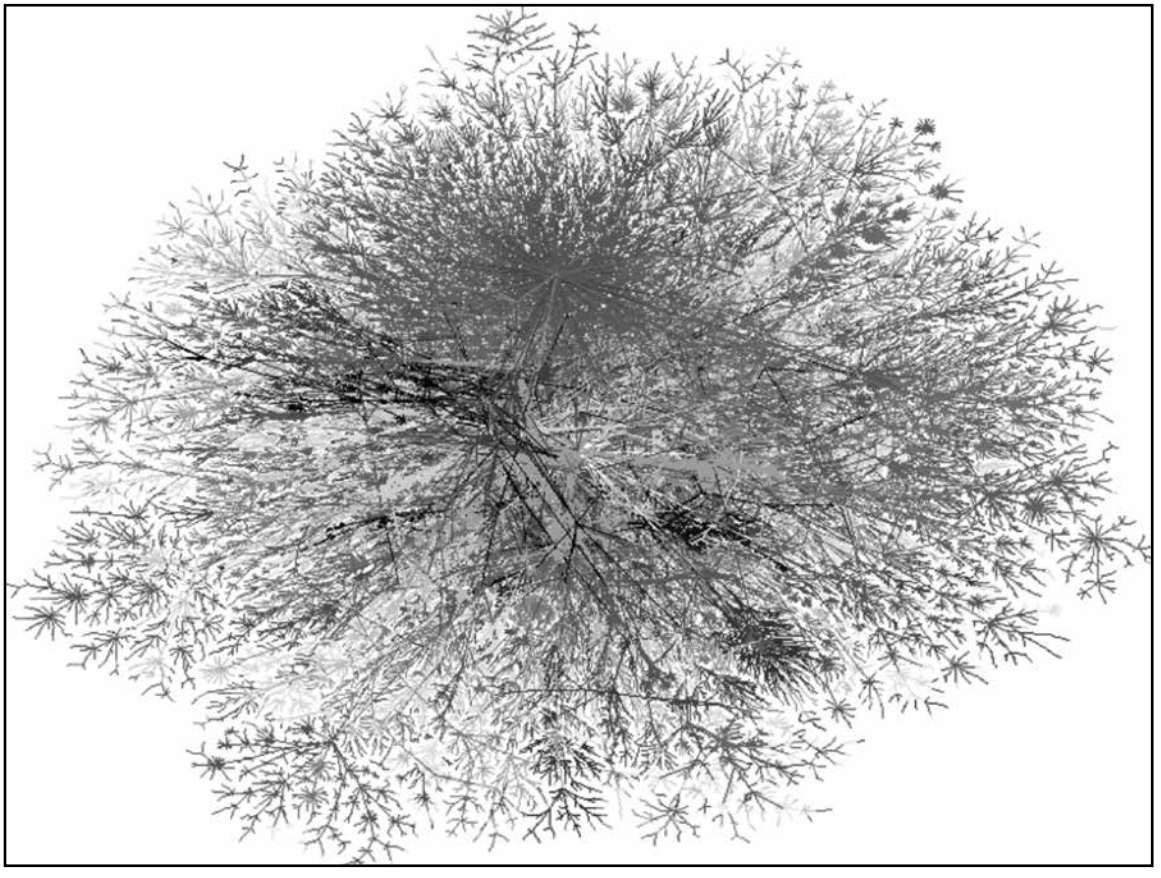

**Figure 5. Map of the Internet**
**Source: Internet Mapping Project, http://www.cheswick.com/ches/map/gallery/index.html (accessed May 29, 2012).**

importance of a node within the network. The simplest way to measure centrality is to simply determine the number of other nodes connected to the node being analyzed. The node connected to the most additional nodes is deemed to be the most influential in terms of degree centrality. Generally targeting the nodes that are high in degree centrality causes significant network disruption.[16] In Figure 6, node seven has the highest degree centrality as it has the most connections to other nodes.

Another measurement useful to the targeting process is that of "between-ness" centrality. "Between-ness" centrality measures the influence of a node on different cliques or subgroups within the larger network. This influence occurs when the node acts as a broker to control the flow of resources or information within the network. In Figure 6, node eight has the highest "between-ness" centrality, as it controls the flow between nodes nine and ten from the remainder of the organization.[17]

Closeness centrality is another measure of influence within the network. This centrality measures the shortest average distance between all other nodes in the network. A higher closeness centrality score could signify that the node is able to receive information at a higher rate than most others in the network. This node might also be able to spread information quickly throughout the network. Analysts should keep this in mind for engagement options; high closeness centrality measures might signify a likely target for engagement with the intent to influence. Nodes four and five in Figure 6 have the highest closeness centrality.

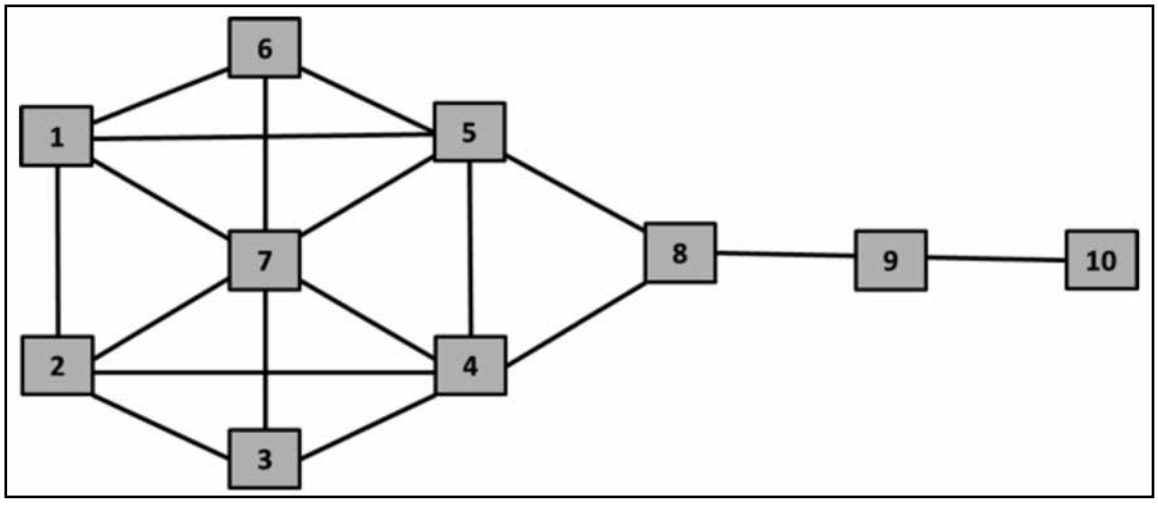


**Figure 5. Krackhardt's Kite Model**
**Source: Image modified by author, original found at Eric W. Weisstein, "Krackhardt Kite," From MathWorld--A Wolfram Web Resource, http://mathworld.wolfram.com/ KrackhardtKite.html (accessed May 30, 2012).**

The fourth and last centrality measure is the eigenvector centrality measure. This measure assigns more weight to links or edges between nodes with high-degree centrality than with those nodes on the periphery with fewer links. These nodes are able to influence the larger group by influencing the nodes with more links throughout the group. It is possible that these nodes will become the future leaders of the network, as they have close ties to the most influential nodes within the network. For targeting purposes, it may be beneficial to include nodes with high eigenvector centrality as follow-on targets to achieve maximum disruption of the network.

Centrality measures are not a panacea for determining an organization's structure. These are tools that assist the JIATF in determining which nodes may warrant further investigation. One of the weaknesses of these measurements is that they give weight to the importance of nodes within a network irrespective of the actual relationships of the connections. Data may show connections between nodes but not any corresponding relationship data. Mathematical models assume all connections as positive, as opposed to reality, where some connections within social networks may be negative. For example, a node may be connected to another through attendance at the same school, but the nodes may have no actual interaction. Another weakness in using SNA techniques is that complete knowledge of the TCO network is not possible. While conducting measurements on the network, analysts must be aware that links may be missing, as not all nodes may have been identified. For example, a node may not be identified in the data because within the timeframe there may not have been a reported connection to other nodes within that organization. The absence of the reported data does not mean the connection does not exist. The analyst must be aware of the limitations of using SNA techniques before they use them to identify possible targets for further investigation and analysis within the TCO network.

There are a number of different, commercially-available, software programs to assist the analyst in conducting these measurements. Organization Risk Analyzer, or ORA, is a tool designed to specifically look for vulnerabilities within an organization's design structure.[18] It is free for download and has been used by organizations on secure networks.

UCINET is a software package designed for the social analysis of networks.[19] This tool is available as a free download for the first 90 days and is available at cost afterwards. The R Project for Statistical Computing, commonly referred to as R, is a free software environment that can also be used to conduct SNA.[20] Pajek is another free software download also commonly used to complete and display SNA centrality measures.[21] Tutorials on conducting SNA measures are readily available for each of these software programs.

## Conclusion

As analysts and staffs seek and recommend targets for engagement with the TCO networks, they need a logical method to determine critical targets for maximum network disruption. Techniques and methods will continue to be refined and developed to assist analysts in their job of analyzing the threat. Currently, determining CVs of the TCO network through COG analysis and further refinement of target identification using SNA techniques offer analysts a logical method of connecting the dots and assisting in the situational understanding of the TCO threat. ***IAJ***

## NOTES

1 Barack Obama, "Strategy to Combat Transnational Organized Crime," National Strategic Document, The Office of the President of the United States of America, Washington, July 25, 2011, p. 1.

2 Ibid., p. 14.

3 *Commander's Handbook for Attack the Network*, U.S. Joint Chiefs of Staff, U.S. Government Printing Office, Washington, May 20, 2011, p. III-1.

4 H. Brinton Milward and Jörg Raab, "Dark Networks as Organizational Problems: Elements of a Theory," *International Public Management Journal*, Vol. 9, No. 3, July 1, 2006, p. 334.

5 Obama, Preface.

6 Phil Williams, "Violent Non-State Actors and National and International Security," International Relations and Security Network, Swiss Federal Institute of Technology, 2008, p. 15.

7 Obama, Preface.

8 Joint Publication (JP) 1-02, *Department of Defense Dictionary of Military and Associated Terms*, U.S. Joint Chiefs of Staff, U.S. Government Printing Office, Washington, November 2010, p. 362.

9 JP 3-60, *Joint Targeting*, U.S. Joint Chiefs of Staff, U.S. Government Printing Office, Washington, April 13, 2007, p. vii.

10 Ibid., p. I-6.

11 The Joint Targeting Cycle consists of six phases and can be found in JP 3-60, Chapter 2.

12 U.S. Army Asymmetric Warfare Group, "Transnational Criminal Organizations and Criminal Street Gangs in the Northwestern Hemisphere: Vulnerability Assessment Workbook," *Understanding the Threat Series*, Volume 5, U.S. Government Printing Office, Fort Meade, May 16, 2011.

13 Dale C. Eikmeier, "A Logical Method for Center-Of-Gravity Analysis," *Military Review*, September-

October 2007, p. 62.

14 Obama, p. 1.

15 Shishir Nagaraja and Ross Anderson, "The Topology of Covert Conflict," University of Cambridge Laboratory, Technical Report, No. 637, July 2005, p. 14.

16 Yong Lu, Michael Polgar, Xin Luo, and Yuanyuan Cao, "Social Network Analysis of a Criminal Hacker Community," *Journal of Computer Information Systems*, Vol. 51, No. 2, Winter 2010, pp. 31–41.

17 Ibid.

18 ORA Software home page, <http://www.casos.cs.cmu.edu/projects/ora/software.php>, accessed on September 28, 2012.

19 UCINET Software home page, <https://sites.google.com/site/ucinetsoftware/home>, accessed on June 1, 2012.

20 The R Project for Statistical Computing home page, <http://www.r-project.org/>, accessed on June 1, 2012.

21 Pajek home page, <http://vlado.fmf.uni-lj.si/pub/networks/pajek/>, accessed on June 1, 2012.