Studies in Conflict & Terrorism, 29:703–718, 2006

ISSN: 1057-610X print / 1521-0731 online
DOI: 10.1080/10576100600701982

Influence in Terrorist Networks: From Undirected to Directed Graphs

STEVEN J. BRAMS
HANDE MUTLU

Department of Politics
New York University
New York, New York, USA

SHAWN LING RAMIREZ

Department of Political Science
University of Rochester
Rochester, New York, USA

A methodology for converting terrorist networks from undirected graphs to simplified directed graphs (or digraphs), and mapping the flow of influence in them, is described. It is based on an "influence assumption"—that important persons with more links influence less important persons with fewer links. This methodology, which was previously used to analyze the structure of influence relationships in Communist-bloc countries and the international system, is illustrated by its application to two terrorist networks constructed after 9/11. In the second more complex network, the hierarchy sheds light on the leadership and likely terrorist cells embedded in the network. Refined data and alternative assumptions about influence could provide additional insights into the structure of terrorist networks.

Networks may mean many things. For example, networks may be graphs, with points or nodes connected by edges or links, that highlight connections among a set of individuals. Networks sometimes mean flows, or the amounts that pass through links, as in a pipeline network. Recently, there have been a number of popular treatments of the "science of connections," including Barabási (2003) and Watts (2003), which illustrate what insights can be gleaned from the analysis of networks: at a more technical level, see Newman, Barabási, and Watts (2006).

Terrorist networks have been much in the news, of course, since 9/11. Indeed, this article shall have more to say about the network that connected the 19 hijackers in the 9/11 attack. But the aim is not just to describe networks but to present tools for simplifying and

Received 17 September 2005; accepted 5 December 2005.

This is a revised version of a paper presented to the DIMACS Working Group on Applications of Order Theory to Homeland Defense and Computer Security, Rutgers University, 30 September 2004. The authors are grateful to the Working Group participants, the anonymous reviewers of *Studies in Conflict and Terrorism*, and Jonathan David Farley and Bruce Hoffman for valuable comments.

Address correspondence to Steven J. Brams, Department of Politics, New York University, 726 Broadway, 7th Floor, New York, New York 10003, USA. E-mail: steven.brams@nyu.edu

analyzing them in order better to be able to disrupt or neutralize them, which follows in the tradition of Farley (2003).

Graphs with many nodes, and a profusion of links connecting them, rapidly become unwieldy and hard to apprehend. Techniques for simplifying them, and probing their underlying structure, abound. This article focuses on understanding the flow of influence in networks.

For this purpose, the article defines a concept of "importance," which is based on the relationship between pairs of individuals who are connected. If individual i is more important than individual j, then it is said that influence flows from i to j. Thereby direction is imputed to influence relationships between individuals, which might go in one direction, the other, or both.

Converting a graph from one having links without direction, which is called "undirected," to one in which influence is one-way or two-way, which is called "directed," is a first step in understanding the flow of influence in networks. If anything, however, turning an undirected graph into a directed graph complicates the network by introducing additional information about the links. A plausible next step, therefore, is to simplify the resulting directed graph by grouping individuals into what the authors call "mutual influence sets," wherein each individual can influence, directly or indirectly, all other individuals in the set.

The final step described is organizing these mutual influence sets hierarchically, from a top level to a bottom level, so that influence always flows downward. Both the grouping of individuals into sets, and their hierarchical ordering, help to make perspicuous the influence structure of a network, singling out, in particular, its leaders.

This influence analysis is applied to two terrorist networks, one involving the 19 hijackers and the other a much larger network of 62 individuals, whose many connections make it difficult to render intelligible. It turns out that the latter network has a well-defined hierarchical structure, which jibes well with observations that have been made about its leaders and the different kinds of operatives that the network subsumes.

To be sure, the quality of conclusions one can draw about a network is highly dependent on the quality of data used to construct it. The most sophisticated analysis cannot turn incomplete or poor information into compelling insights about the nature of terrorist threats, much less predict how the threats will unfold. It is hoped that the insights of the graph-theoretic analysis presented will stimulate the search for better information that, ultimately, sheds new light on terrorist threats and the most effective means to deal with them.

Basic Notions and Assumptions

This article next outlines and illustrates a methodology for converting terrorist networks from undirected graphs to simplified directed graphs (or digraphs) and mapping the flow of influence in them. "Methodology" is perhaps the wrong word, because the conversion requires an assumption about *substance*. Given this assumption, a graph-theoretic methodology can be applied to simplify, and hierarchically organize, networks into more intelligible influence maps.

By *network* is meant an *undirected graph*. Such a graph comprises points and edges. It is *connected* if every point is linked to every other point, directly or indirectly, through one or more edges.

A *digraph* imputes a direction to each edge, usually indicated by an arrowhead, as in $i \rightarrow j$, which is called a *unidirectional link*. The direction may be two-sided, or a *bidirectional link*, as in $i \leftrightarrow j$. To go from an undirected graph to a directed graph, the authors first define "importance" in an undirected graph:

> **Importance**. Assume point *i* is directly linked to point *j* in a network. Point *i* is more important than point *j* if it has more direct links to other points—by some margin (to be defined)—than does point *j*. Points *i* and *j* are equally important if they have (approximately) the same number of direct links to other points.

If a point is a person, as assumed in terrorist networks, then for every pair of directly linked persons, *i* and *j*, either *i* is more important than *j*, *j* is more important than *i*, or they are equally important. This leads to the main assumption, which relates influence to importance:

> *Influence Assumption*. For every pair of directly linked persons (points), more important persons influence less important persons. If two linked persons are equally important, they influence each other.

Thereby every network can be converted into a digraph, called an *influence digraph*, in which every link between a pair of persons is either unidirectional or bidirectional.

Figure 1 shows a terrorist network, constructed by Krebs (2002) soon after the terrorist attacks on 11 September 2001, as an undirected graph. The criteria used to determine the links of terrorists to each other are based principally on similarities in their (i) backgrounds (e.g., kinship, nationality, schooling, training) and (ii) associations (e.g., apartments they shared, meetings they attended together, messages they sent to each other).

Many terrorist networks have been constructed since 9/11, based on a variety of criteria.[1] Although different methods have been proposed for drawing networks and graphs (Di Battista et al. 1999; Jünger and Mutzel 2003), this article focuses on converting networks into influence digraphs and hierarchically organizing them.

Figure 2 shows the influence digraph derived from Figure 1, based on the Influence Assumption in which a 1-link difference renders an influence relationship unidirectional. For example, person #14 (4 links) directly influences four persons with fewer links—#12 (2 links), #13 (3 links), #15 (3 links), and #16 (3 links)—as indicated by the unidirectional arrows pointing from person #14 to each of these people.

Influence may also be indirect. For example, person #5 (6 links) influences person #3 (3 links), who in turn influences person #4 (2 links) and person #2 (1 link).

Finally, influence may be two-way. For example, there are bidirectional influence relationships between person #13 and person #10 (3 links each), and between person #5 and person #9 (6 links each), indicating a relationship of equal importance or mutual influence.

The unidirectional and bidirectional influence relationships make explicit the information that is only implicit in the Figure 1 network. The authors next simplify the Figure 2 influence digraph by defining a *mutual influence set* (MIS) to be a set of persons who can, directly or indirectly, influence and be influenced by every other person in the set. Thereby they constitute *influence cycles*, which are enclosed in loops in Figure 3.

These loops define the MISs. (If an MIS encloses a single person, it is assumed that person is in a cycle with himself.[2]) To illustrate, consider the largest MIS in Figure 3, which includes persons #10, #13, #15, #16, and #17, all of whose members have single bidirectional influence relationships with one other member: Person #10 influences and is influenced by person #13, person #13 influences and is influenced by person #15, and so on. Therefore, influence flows from every member to every other member, and then back again, in a cycle. This MIS is written as MIS $\{10, 13, 15, 16, 17\}$.

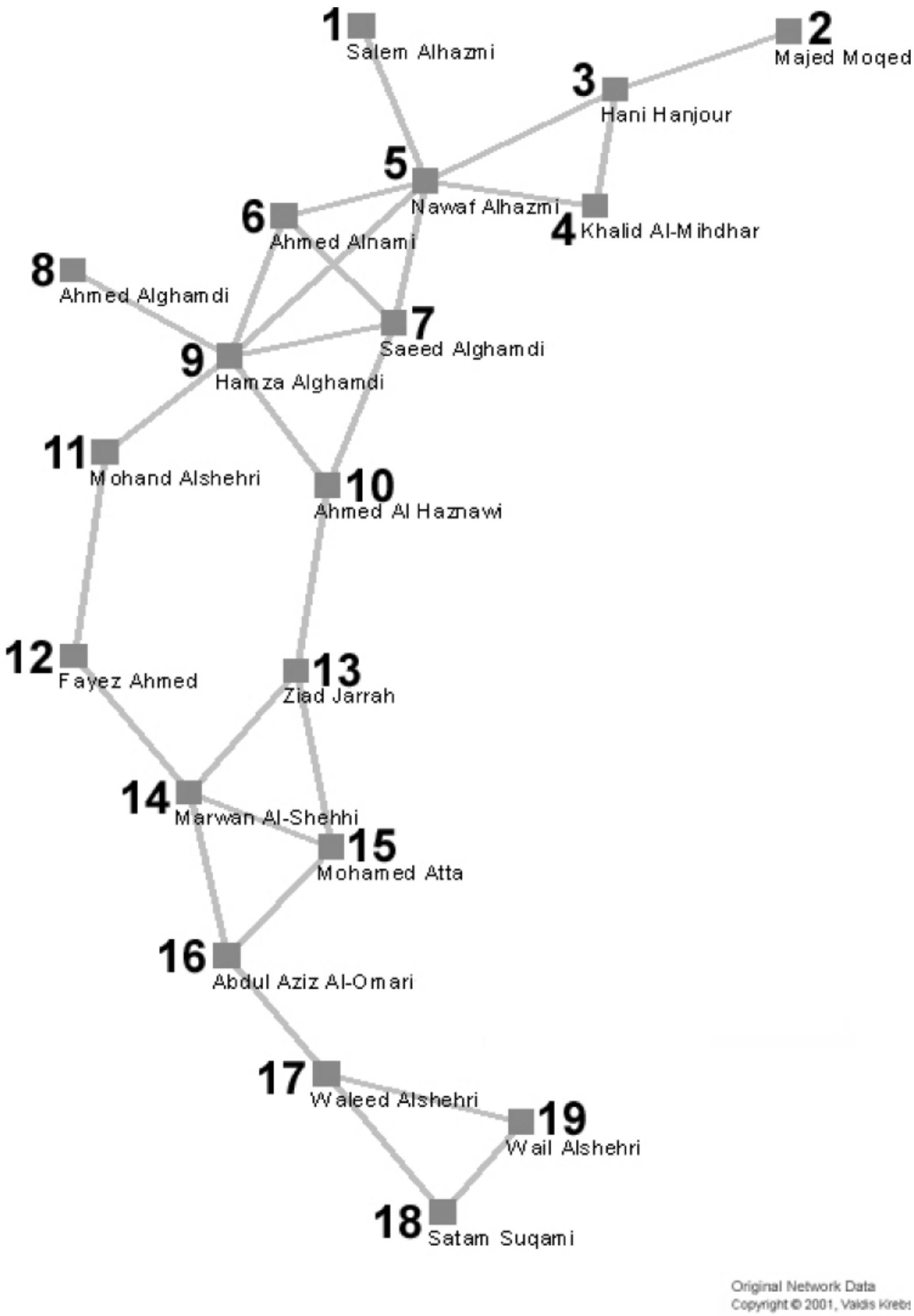

Figure 1. Network of 9/11 hijackers.

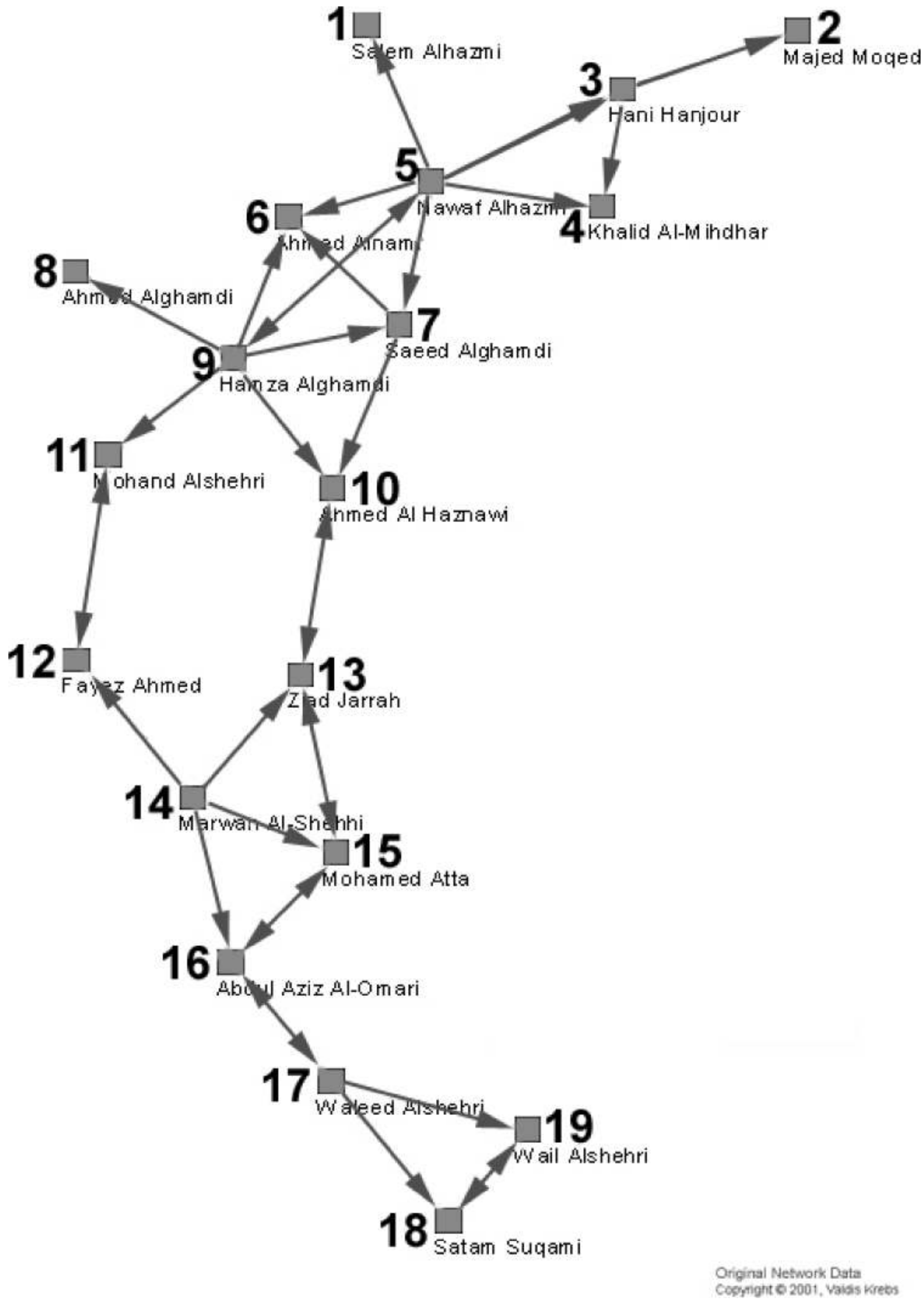

Figure 2. Influence digraph of 9/11 hijacker network.

Notice that members of an MIS need not be directly connected to other members of the set. Thus, person #10 is only indirectly connected to person #17, with influence flowing through persons #13, #15, and #16—and then back again to person #10. By contrast, person #17 (3 links) influences persons #18 and #19 (2 links each), who are in a bidirectional influence relationship, but he is not influenced by them.

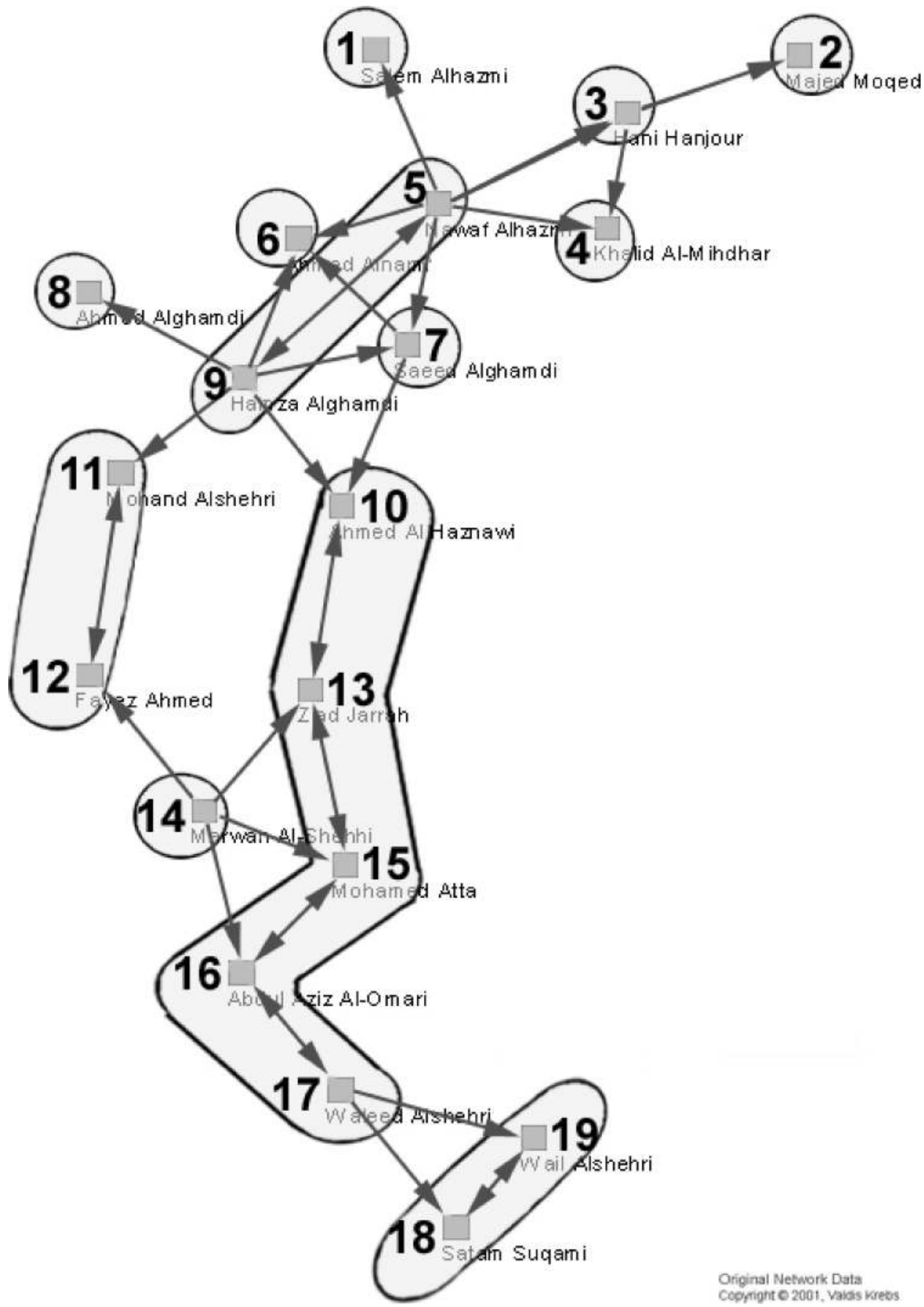

Figure 3. Mutual influence sets in 9/11 hijacker network.

Observe that the MISs are disjoint. If a person were a member of two MISs, that person would link all persons in the two MISs, making it a single MIS. The next section makes MISs the basic unit of analysis in order to simplify the 9/11 digraph and a more complex one presented later.

Hierarchical Organization of a Network

MISs, which are called "strong components" of a digraph, can be hierarchically decomposed into a unique, acyclic structure (Harary, Norman, and Cartwright 1965). In the present context, this means that all MISs can be ordered at different levels in a hierarchy so that influence always flows downward.

At the top level, the members of the MISs influence, but are not influenced by, other MISs. As a case in point, persons #5 and #9 are in a bidirectional influence relationship (6 links each) and, therefore, an MIS. Because they are not influenced by any other persons with more links, they are shown in Figure 4 as an MIS at the top level (level 1). So is MIS {14}, because no members of any other MIS influence him, including persons #5 and #9, to whom he is not connected.

How does one know where to place an MIS when at least one of its members is directly influenced by another person? The rule of placement is that an MIS occupies the highest level just below that of the lowest-level MIS by which it is influenced.

As an example, observe in Figure 3 that MIS {6} is influenced by MIS {5, 9}, so one might think that MIS {6} could be placed at level 2, one level below MIS {5, 9}. However, because MIS {5, 9} also influences MIS {7}, which in turn influences MIS {6}, MIS {6} must be placed below MIS {7}, which must be placed below MIS {5, 9}. Consequently, MIS {5, 9} is at level l, MIS {7} is at level 2, and MIS {6} is at level 3.

Figure 4 does not indicate influence relationships (either unidirectional or bidirectional) *within* MISs. Between any two MISs, there is an influence relationship if and only if there exists at least one between some members of each of the MISs. These are always unidirectional, because all bidirectional influence relationships are subsumed within the MISs.

Figure 4 shows the flow of influence downward from higher to lower levels. The average number of links of persons at different levels (based on Figure 1) is as follows:

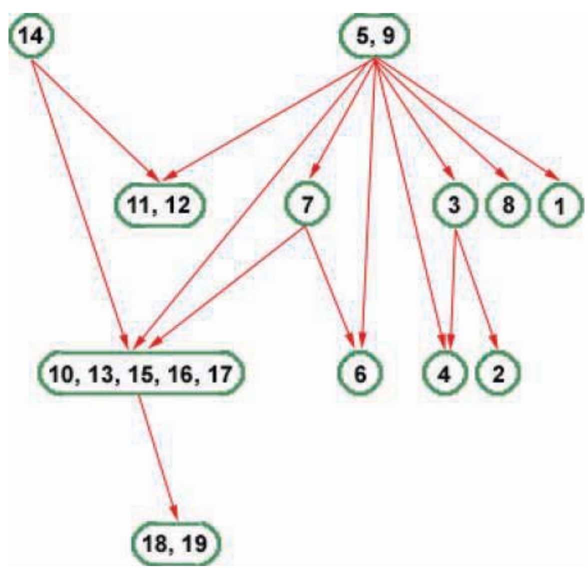

Figure 4. Hierarchical directed graph of 9/11 hijacker network.

Level 1	Level 2	Level 3	Level 4
$16/3 \approx 5.3$	$13/6 \approx 2.2$	$21/8 \approx 2.6$	$4/2 = 2$

As expected, those at the top level, who might be considered the leaders because they are uninfluenced (except within their own MISs), are the most connected. However, the members of lower-level MISs (e.g., those at level 3) may have more links, on average, than members of higher-level MISs (e.g., those at level 2).

This occurs when members of a lower-level MIS (e.g., MIS $\{10, 13, 15, 16, 17\}$), which is farther down in the hierarchy, have a relatively large number of internal links compared to MISs at higher levels. When the internal links within MISs are eliminated, higher-level MISs always have more external (unidirectional) links than lower-level ones:

Level 1	Level 2	Level 3	Level 4
$14/3 \approx 4.7$	$11/6 \approx 1.8$	$13/8 \approx 1.6$	$2/2 = 1$

Although each member of MISs at higher levels may be directly connected with a member of an MIS at the next-lower level, in some cases members of lower-level MISs are connected to MISs at higher levels only indirectly through other members of their own MISs. For example, in the large 5-member MIS $\{10, 13, 15, 16, 17\}$ at level 3, which constitutes more than 1/4 of the network, one person (#17) in this MIS is not influenced from above at all. Instead, he is connected to a level 1 MIS (i.e., MIS $\{14\}$) only through person #16 in his own MIS, and to MIS $\{7\}$ at level 2 and MIS $\{5, 9\}$ at level 1 by the chain of bidirectional influence relationships within his own MIS.

So far this article has shown that influence relationships can be hierarchically organized into MISs, wherein influence cycles. Influence always flows downward from higher-level to lower-level MISs. The number of levels of a hierarchy is endogenous, dependent on the configuration of unidirectional and bidirectional links.

The next section analyzes a more complex terrorist network that dramatically illustrates the advantages of grouping persons into MISs and hierarchically organizing them. The leaders and possible terrorist cells that it suggests seem plausible based on evidence to be presented in the next section.

A More Complex Terrorist Network

Figure 5 presents a network of 62 persons (Krebs 2002) that is so dense with links that it is hard to apprehend as a whole. To render it more intelligible, this section will make different simplifying assumptions.

Recall that in Figures 1 through 4, only persons with an equal number of links were considered to be in a bidirectional influence relationship. To allow for some degree of error in working with incomplete, and possibly inaccurate, data on a covert network—in which a 1-link difference may be idiosyncratic—the authors adopt more stringent standards to analyze influence in the larger terrorist network. It is assumed that a bidirectional influence relationship exists if the difference between the more-linked and the less-linked connected persons is (i) in absolute terms, 2 or fewer links; (ii) in relative terms, 25% or fewer links.

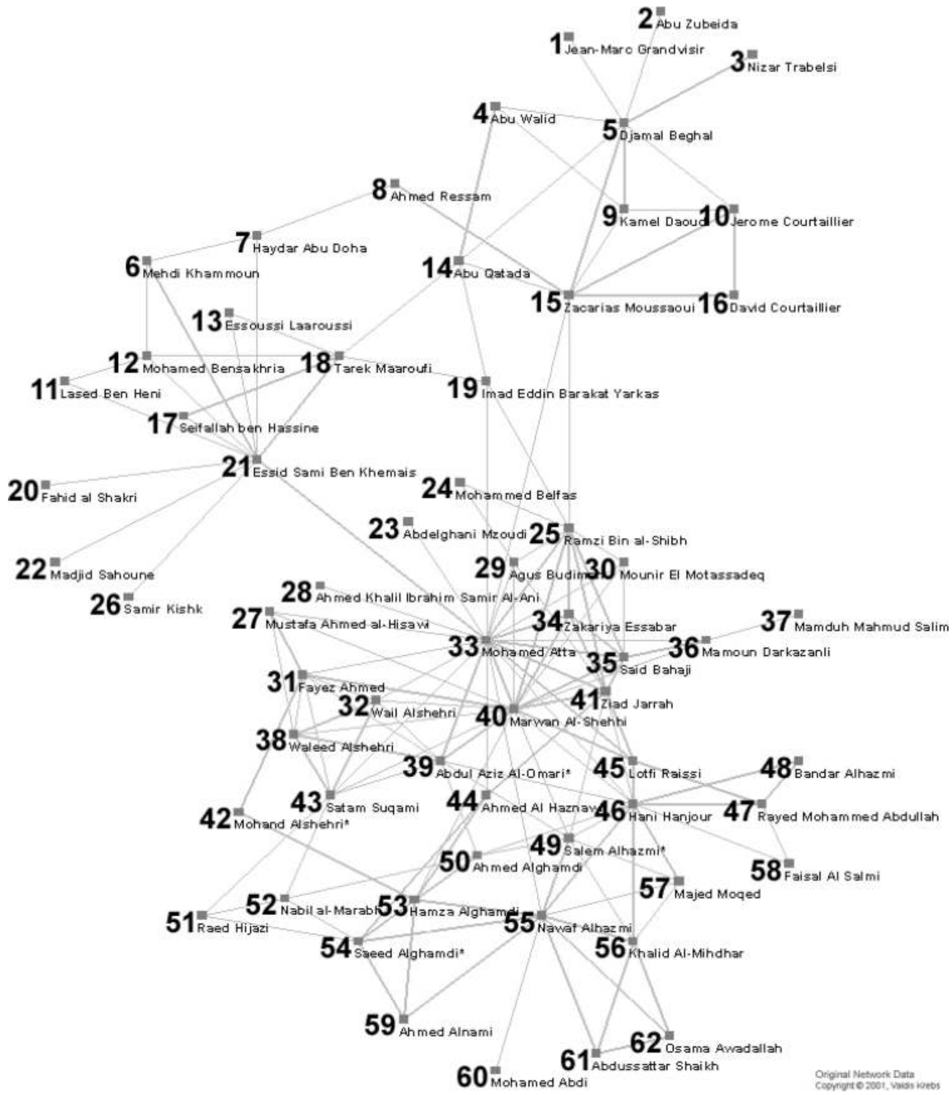

Figure 5. Large terrorist network.

If two connected persons are not in a bidirectional influence relationship, they are in a unidirectional relationship.

To illustrate, if one person has 4 links and the other person has 2 links, they are in a bidirectional influence relationship by standard (i) but not by standard (ii), because one person has 50% more links than the other person. By contrast, if 1 person has 13 links and the other person has 10 links, they are in a bidirectional influence relationship by standard (ii), because one person has 3/13 $\approx$ 23% fewer links than the other person, but they are not in such a relationship by standard (i).

Figure 6 shows the MISs based on the absolute standard, and Figure 7 by the relative standard.[3] Note the MISs containing two or more members tend to be somewhat larger in

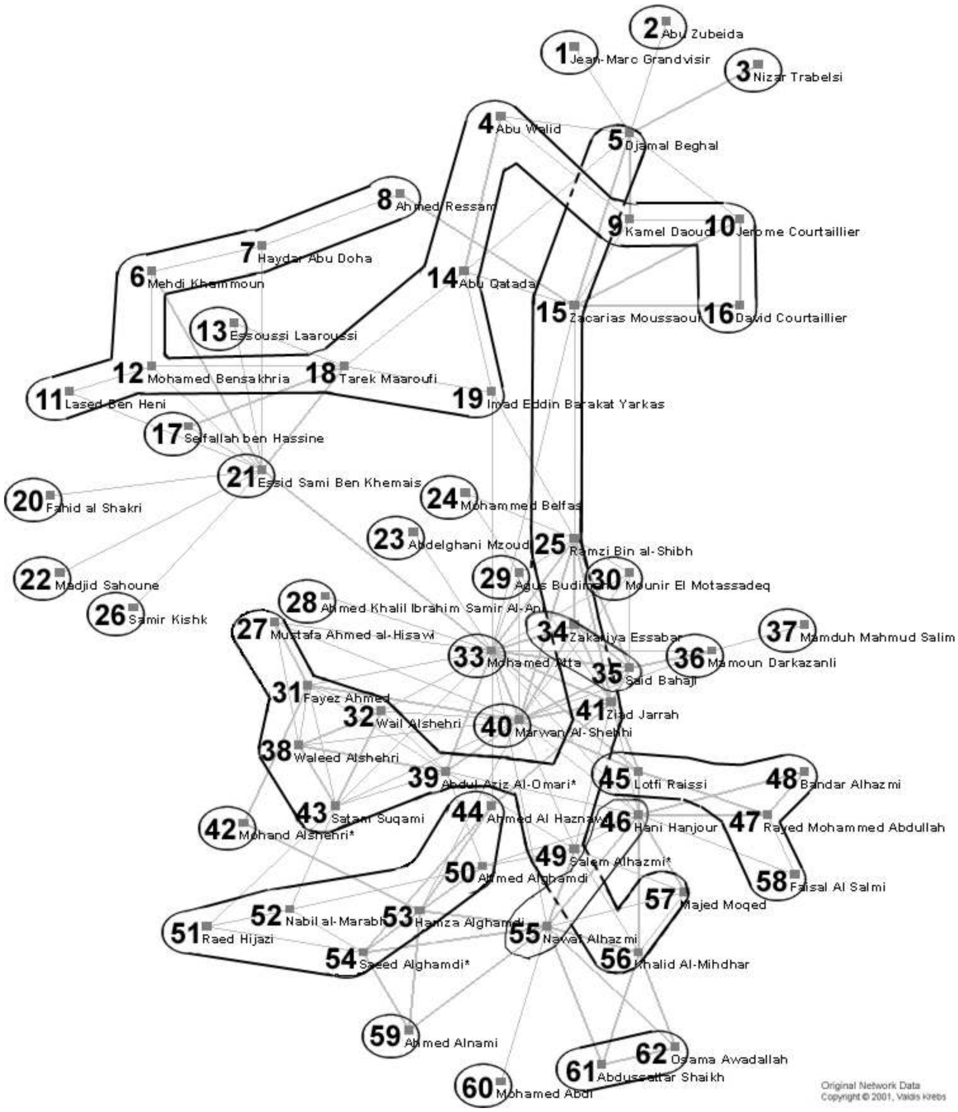

Figure 6. Mutual influence sets in large terrorist network (absolute standard of 2 or fewer links for bidirectional influence relationship).

Figure 6 than in Figure 7. Correspondingly, there are fewer singleton MISs in Figure 6 (21) than in Figure 7 (29).

Still, there are striking similarities between the pictures given in Figures 6 and 7. Some of the multiple-member MISs in these figures are identical or nearly identical. Although the smaller MISs in Figure 7 often are subsets of larger MISs in Figure 6, sometimes the reverse is the case.

Despite the simplification that the groupings in Figures 6 and 7 lend to Figure 5, the former figures are still hard to read and make sense of. But the digraphs of MISs shown in Figures 8 and 9 make the hierarchical structures of the networks transparent.

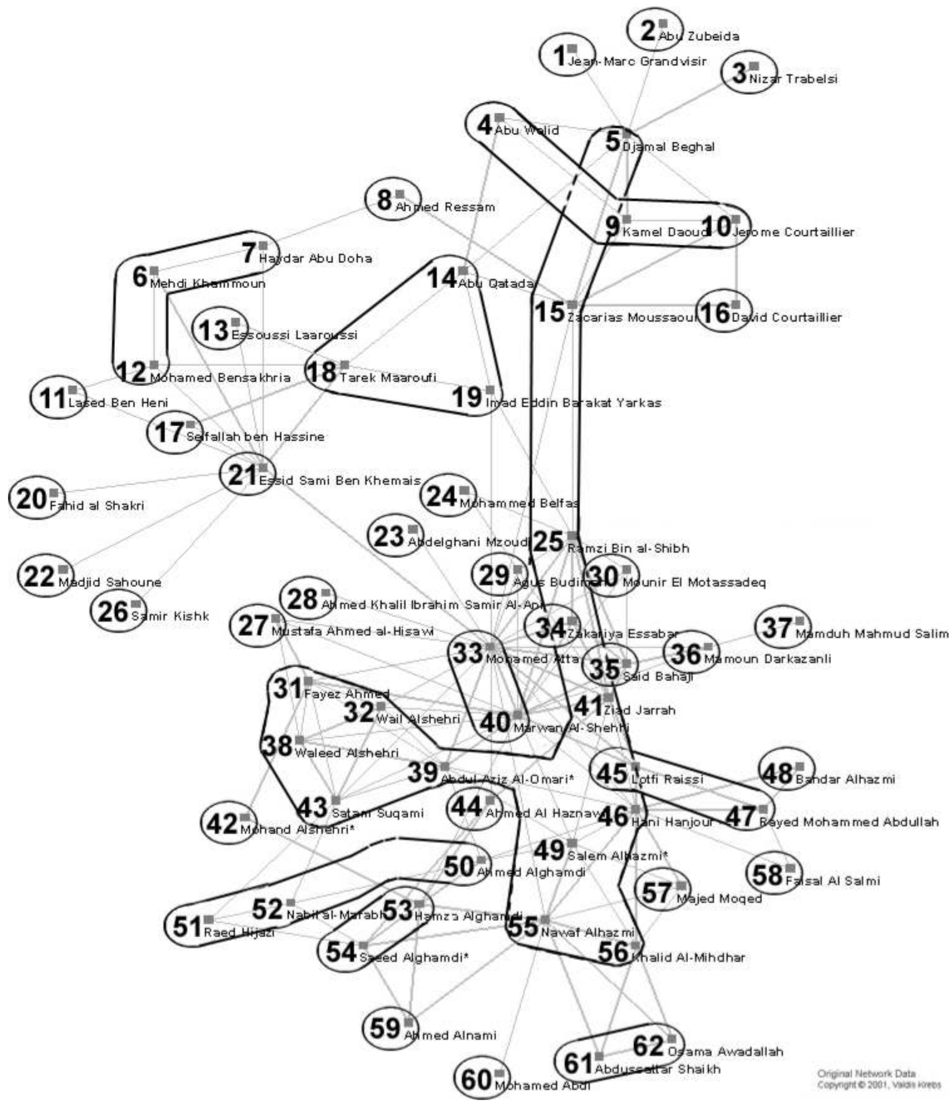

Figure 7. Mutual influence sets in large terrorist network (relative standard of 25% or fewer links for bidirectional influence relationship).

In these hierarchies (sometimes called partially ordered sets, or posets), only unidirectional influence relationships that span one level are included—namely, from level n to level $n + 1$, one level below. Omitted from Figures 8 and 9 are the numerous unidirectional influence relationships that are two or more levels apart. These omissions eliminate unnecessary clutter and thereby highlight the overall structure of the hierarchy and its levels.

The seven levels of Figure 8 make perspicuous the downward flow of influence from the key leader, MIS $\{33\}$, at the top. Person #33 also appears in an MIS with person #40 at the top level in Figure 9, which has fewer levels (five) and more singleton MISs at the

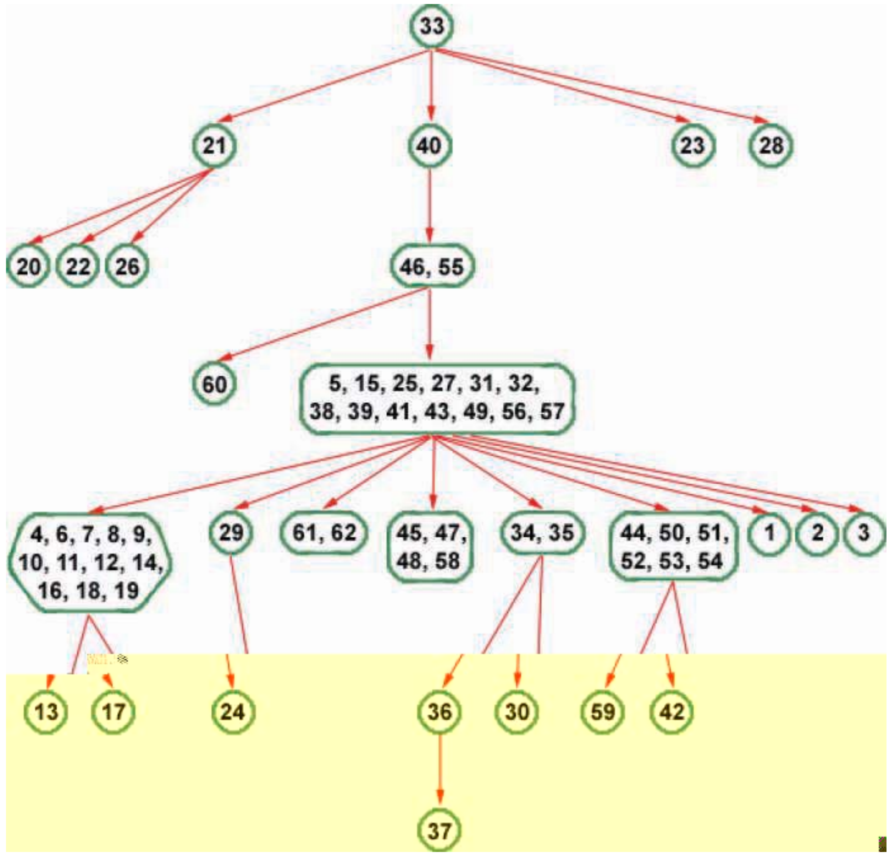

Figure 8. Hierarchical directed graph of large terrorist network (absolute standard of 2 or fewer links for bidirectional influence relationship).

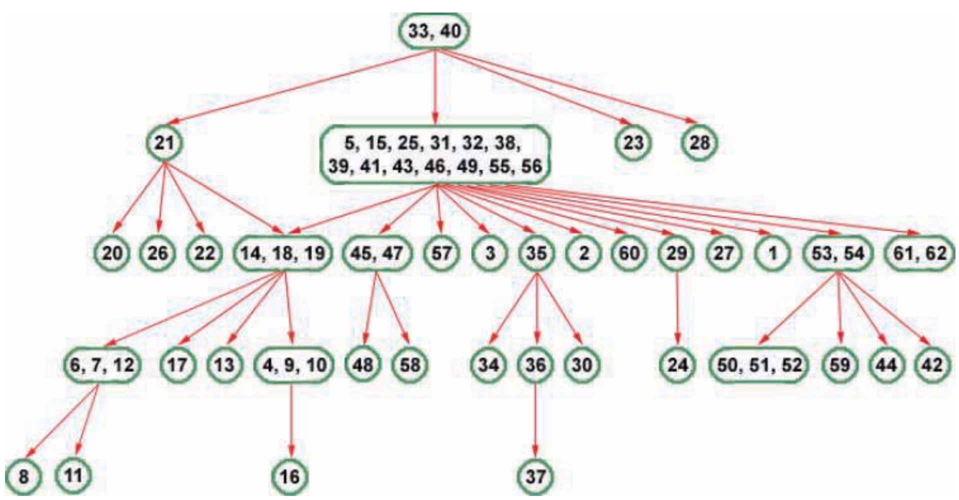

Figure 9. Hierarchical directed graph of large terrorist network (Relative standard of 25% or fewer links for bidirectional influence relationship).

bottom levels. Because persons have fewer links at these levels, they are less likely to be in a bidirectional influence relationship based on the 25% standard.

Interpretation of the Hierarchies

In both the Figure 8 and 9 hierarchies, the persons at or near the top appear to be the most important figures in the networks. For example, person #33 is Mohamed Atta, who was the operational leader of the 9/11 attacks (*9/11 Commission Report*, 88). He was also a member of the Hamburg cell, a group whose fluency in English and whose familiarity with Western ways led to their involvement as prime conspirators (*9/11 Commission Report*, 160). Other members of the Hamburg cell included Marwan Al-Shehhi (#40) at level 2 in Figure 8 and at level 1 in Figure 9; Ziad Jarrah (#41) at level 4 in the largest group in Figure 8, and at level 2 in the largest group in Figure 9; and Ramzi Bin al-Shibh (#25), who is in the same groups as Jarrah in Figures 8 and 9.

That the members of the Hamburg cell are found at different levels also makes empirical sense. Atta (#33) and Al-Shehhi (#40) were the only 9/11 terrorists mentioned as team leaders in the *9/11 Commission Report* (7). They led their respective teams of hijackers on American Airlines flight 11 and United Airlines flight 175 (*9/11 Commission Report*, 1–14). In fact, Atta's last phone call was a three-minute conversation with Al-Shehhi at Logan Airport just before the hijackings (*9/11 Commission Report*, 1).

Ziad Jarrah (#41), as the only trained pilot on his team, was critical to its success (*9/11 Commission Report*, 12). Bin al-Shibh's (#25) participation was plagued by his inability to secure a visa (his requests were rejected four times), but he still played a crucial role in assisting with the conspiracy (*9/11 Commission Report*, 168). As noted earlier, both Jarrah and al-Shibh are in the largest groups in Figures 8 and 9.

The authors also find the placement of less important figures to be consistent with the findings of *The 9/11 Commission Report*. For example, Said Bahaji (#35) was connected to the Hamburg cell, had lived with Atta and Bin al-Shibh, and was "an insecure follower with no personality and with limited knowledge of Islam . . . Atta and Bin al-Shibh used Bahaji's computer for Internet research" (*9/11 Commission Report*, 164). Bahaji is at level 5 in Figure 8 and at level 3 in Figure 9, just below members of the Hamburg cell.

The identities and importance of the outliers toward the tops of the two hierarchies, who are unconnected to lower-level terrorists, deserve comment. It is believed they may fall into two categories. First, they are possibly reliable resources called on at some point for specific purposes by the connected members of the hierarchy. For example, Abdelghani Mzoudi (#23) was acquitted in a German trial in connection with the 9/11 attacks, due to lack of evidence, and the extent of his involvement is currently unknown (Boston 2004). In both hierarchies, he is at level 2, just below Atta (#33).

Although little is also known about the details of Ahmed Khalil Ibrahim Samir Al-Ani's (#28) involvement with Atta and the 9/11 attacks, it is known that he was the former Iraqi intelligence chief. He is suspected of having provided funding to the terrorist groups ("Decision Brief: Terror-tied" 2003).

Some outliers are probably persons involved in terroist networks of their own but operating under the aegis of Al Qaeda. Samir Kishk (#26), who is located in both hierarchies at level 3, is a member of the Salafist Group for Call and Combat (GSPC), which is an Algerian-based terrorist organization operating in North Africa, Spain, and Italy. It is known for supporting and financing terrorism around the world ("United States and Italy Designate Twenty-Five New Financiers of Terror" 2002).

That such outliers could be leaders or members of other terrorist organizations raises the intriguing question of how these different organizations are connected. With more complete and refined linkage data, this methodology could provide new insights.

Previous Applications and Underlying Assumptions

Because the main purpose of this article has been to illustrate a data-reduction methodology for a network, not systematically analyze its application to terrorist networks, it now returns to the Influence Assumption made earlier. This assumption is similar in spirit to that which one of the authors made in determining influence relationships, and measuring the concentration of power, among different sets of countries (Brams 1968b, 1969).

The data in these studies were visits of high-level government officials to other countries. If an official of country A visited country B more often than an official of country B visited country A, their influence relationship was assumed to be unidirectional, with B having influence over A.[4] If they visited each other equally or almost equally often, then the influence relationship was considered bidirectional—each country had influence over the other. These assumptions produced a hierarchy of 8 Communist countries in the 1950s (Brams 1968b), and virtually the entire world of 121 countries in the 1960s (Brams 1969), that seemed to mirror the flow of influence in these systems at these times.[5]

The application of this methodology to terrorist links may not be as persuasive as to visit links. First, a leader in a terrorist network may be so primarily because of his or her leadership qualities or personality, not because of the number of his or her ties or associations with others.

For example, a top leader may have only a few lieutenants who report to him or her, whereas the lieutenants may have more numerous relationships with subordinates. In this case, the lieutenants would appear to influence the top leader rather than vice versa. Because the top leader would not usually be linked to subordinates of the lieutenants, however, he or she would not be influenced by them and, therefore, buried still lower in the network.

Although data on visits, communication traffic, and other contacts—and who initiates them—are not perfect measures of influence, they provide some basis for charting influence relationships, and their direction, in terrorist networks. Thus, MISs might well indicate terrorist cells because of the ties that all their members have with each other. Furthermore, the hierarchy of MISs can provide clues about the identity of leaders at different levels—and, ultimately, how to disrupt or manipulate the leadership of a network (Arquilla and Ronfeldt 2001).

It is cautioned, however, that terrorists may be able to do their own manipulation of a network (e.g., by increasing "chatter" to create a false impression of activity). Thus, a network should not be considered a *tabula rasa*, to be read uncritically, but rather as an object that might be manipulated to deceive or otherwise influence an opponent.

Conclusions

Although this article has focused on terrorist networks, the methodology described can be applied to more benign networks, as it was originally intended (Brams 1968b, 1969). This article, by contrast, focused on terrorist networks in order to illustrate the methodology's potential to identify those who are threats to world order. By providing an organizational blueprint of a network, especially its leadership, one is better able to understand and possibly disrupt it.

The tie-ins made to influence, and its direction, will not always be accurate. Refinements in the data, and a careful consideration of what they measure, should make interpretations more defensible. Alternative assumptions about importance, based on whom one is linked to and how—as well as to how many others—should provide additional insights. As a first approximation, the methodology presented offers a compelling way to simplify complex networks and pinpoint key players and cells within them.

The authors believe that an enhanced understanding of the structure of terrorist networks may help policymakers deal with the very serious threats they pose. Although the destruction of the top leadership, or decapitation, may abet the disruption of a large-scale attack that requires a high degree of coordination, it may not damage individual cells. For that purpose, identifying these cells, and where they are in the hierarchy, is also necessary. The construction and simplification of directed graphs will, it is hoped, contribute to this task.

Notes

1. The most comprehensive assessment of terrorism relating to 9/11 is given in *9/11 Commission Report* (2004), but this report presents no methodology for analyzing terrorist networks.
2. Because all terrorists in these networks are males, only the masculine pronoun is used.
3. The authors have experimented with other absolute and relative standards. The two chosen are a compromise between those that lead to a few very large MISs on the one hand, and many small ones on the other. They seem to give a reasonable representation of the leadership structure, as argued in section 4.
4. This assumption has a basis in social psychology and experimental evidence (Brams 1968a, 1969), but it also seems to mirror everyday relationships that people have with each other. Thus, the subordinate in a company usually goes to his or her superior's office, just as students adjust their schedules to a professor's office hours, and visit him or her at that time, rather than vice versa. In the present study, influence depends not on who initiates a contact—although this would be interesting information to try, if possible, to gather—but, rather, on the sheer number of linkages a person has with others, with more connected people assumed to be more influential.
5. To analyze this large network, a FORTRAN computer program that is no longer operational was used (Brams 1968a).

References

Arquilla, John, and David Ronfeldt, eds. 2001. *Networks and Netwars: The Future of Terror, Crime, and Militancy*. Santa Monica, CA: RAND.

Barabási, Albert-László 2003. *Linked: How Everything Is Connected to Everything Else and What It Mean for Business, Science, and Everyday Life*. New York: Penguin/Plume.

Boston, William 2004. "Terror Case Sets Washington and Berlin at Odds," *Christian Science Monitor*. (9 February). See also (http://www.csmonitor.com/2004/0209/p06s02-woeu.html)

Brams, Steven J. 1968a. "DECOMP: A Computer Program for the Condensation of a Directed Graph and the Hierarchical Ordering of Its Strong Components." *Behavioral Science* 13(July), pp. 344–345.

Brams, Steven J. 1968b. "Measuring the Concentration of Power in Political Systems." *American Political Science Review* 62(2) (June), pp. 461–475.

Brams, Steven J. 1969. "The Structure of Influence Relationships in the International System," In *International Politics and Foreign Policy: A Reader in Research and Theory,* 2nd edn. edited by James N. Rosenau. New York: Free Press, pp. 583–599.

"Decision Brief: Terror-tied." 2003. *Center for Security Policy*. (17 November). See also (http://www.centerforsecuritypolicy.org/index.jsp?section=papers&code=03-D_44)

Di Battista, Giuseppe, Peter Eades, Roberto Tamassia, Ioannnis G. Tollis. 1999. *Graph Drawing: Algorithms for the Visualization of Graphs*. Upper Saddle River, NJ: Prentice-Hall.

Farley, Jonathan David. 2003. "Breaking Al Qaeda Cells: A Mathematical Analysis of Conterterrorism Operations (A Guide for Risk Assessment and Decision Making)." *Studies in Conflict & Terrorism* 26, pp. 399–411.

Harary, Frank, Robert Z. Norman, and Dorwin Cartwright. 1965. *Structural Models: An Introduction to the Theory of Directed Graphs*. New York: Wiley.

Jünger, Michael, and Petra Mutzel. eds. 2003 *Graph Drawing Software*. Germany: Springer-Verlag.

Krebs, Valdis E. 2002. "Mapping Networks of Terrorist Cells." *Connections* 24(3), pp. 43–52.

Newman, Mark. Alert-Lázió Barabási, and Duncan J. Watts, eds. 2006. *The Structure and Dynamics of Networks*. Princeton, NJ: Princeton University Press.

The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks upon the United States. 2004. New York: W.W. Norton.

"The United States and Italy Designate Twenty-Five New Financiers of Terror." 2002. *United States Department of Treasury: Office of Public Affairs* (29 August). See also (http://www.ustreas.gov/press/releases/po3380.htm)

Watts, Duncan J. 2003. *Six Degrees: The Science of a Connected Age*. New York: W.W. Norton.