Studies in Conflict & Terrorism, 26:399–411, 2003

ISSN: 1057-610X print / 1521-0731 online
DOI: 10.1080/10576100390242857

Taylor & Francis
Taylor & Francis Group

Breaking Al Qaeda Cells: A Mathematical Analysis of Counterterrorism Operations (A Guide for Risk Assessment and Decision Making)

JONATHAN DAVID FARLEY

Department of Mathematics
Massachusetts Institute of Technology
Cambridge, MA, USA

How can we tell if an Al Qaeda cell has been broken? That enough members have been captured or killed so that there is a high likelihood they will be unable to carry out a new attack, and military resources can be redirected away from them and toward more immediate threats? This article uses order theory to quantify the degree to which a terrorist network is still able to function. This tool will help law enforcement know when a battle against Al Qaeda has been won, thus saving the public's money without unduly risking the public's safety.

Winning the Shadow War

In the war on terror, how can we tell if we have won a battle? Recently, Woo[1] (public lecture) has suggested modeling Al Qaeda cells as *graphs* or *networks*—that is, as collections of points or nodes connected by lines. The nodes represent individual terrorists, and a line is drawn between two nodes if the two individuals have a direct communications link. Figure 1 illustrates an organization with four members, Mel, Jean-Claude, Arnold, and Sylvester. Mel, Jean-Claude, and Arnold share a flat in Hamburg and communicate directly with each other, but Sylvester communicates only with Jean-Claude.

The task of law enforcement is to remove nodes from a graph representing a terrorist cell by capturing or killing members of that cell so that its organizational structure is disrupted. Woo suggests modeling this idea mathematically by asking the following question: How many nodes must you remove from the graph before it becomes disconnected (that is, before it separates into two or more pieces)? We might call this the *Connectedness Criterion.*

Received 30 May 2003; accepted 9 June 2003.
The author thanks Ryan Klippenstine, Jane Ryan, Stefan Schmidt, and Enaame Farrell for proofreading this article. The author also thanks Juliette Kayyem for suggesting publication venues and Gordon Woo for referring him to the work of Kathleen Carley. The author is founder of Phoenix Mathematical Systems Modeling, Inc., which is not connected with the Massachusetts Institute of Technology. United States Patent and Trademark Office Provisional Patent Application Number 60/471,545.
Address correspondence to Jonathan David Farley, Department of Mathematics, Massachusetts Institute of Technology, Cambridge, MA 02139.

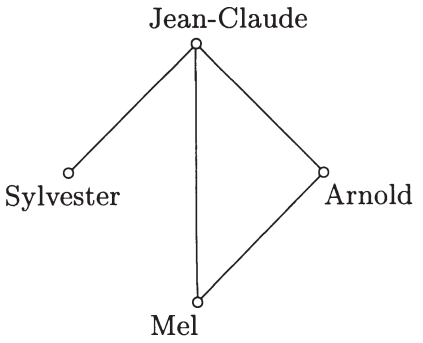

Figure 1. A graph illustrating an organization.

Figure 2a illustrates a terrorist network with seven members. If terrorist *A* is captured, the six remaining nodes are still connected and remain a cohesive whole (Figure 2b). If, on the other hand, terrorists *E* and *G* are captured, then the graph breaks up into two parts that can no longer communicate directly with one another (Figure 2c). Figure 3 illustrates a typical graph from the literature (Krebs, 2001) illustrating the connections between the alleged September 11 hijackers.

There is a growing literature on modeling terrorist networks as graphs, an outgrowth of the existing literature concerning other types of criminal networks.[2] There is also literature on destabilizing networks, modeled as graphs, by seeing how connections do or do not dissipate when nodes are removed (Carley, Lee, and Krackhardt, 2001).

Our view is that modeling terrorist cells as graphs does not give us enough information to deal with the threat. Modeling terrorist cells as graphs ignores an important aspect of their structure, namely, their hierarchy, and the fact that they are composed of leaders and of followers. It is not enough simply to seek to disconnect terrorist networks. For although doing so may succeed in creating two clusters of terrorists incapable of communicating directly with each other, one of the clusters may yet contain a leader and enough followers to carry out a devastating attack.[3]

For example, consider the terrorist cell depicted in Figure 4. If terrorists *B* and *E* were captured, the remaining cell would certainly be disconnected. Indeed, the cell would be broken into three components (Figure 5). Nonetheless, there would still be a chain of

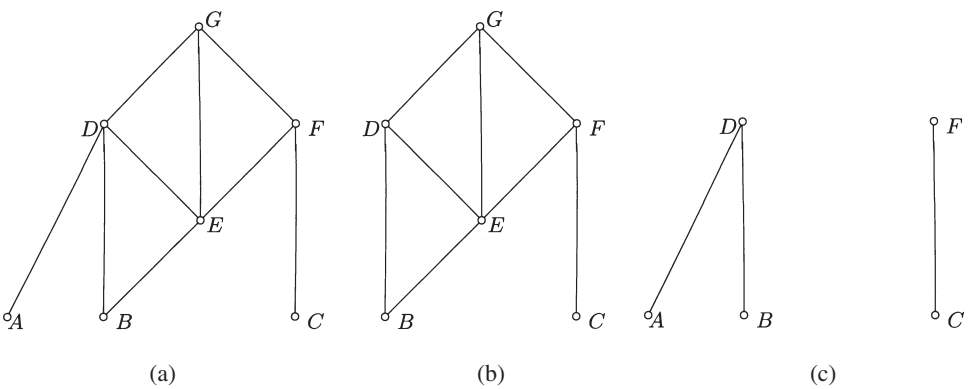

Figure 2. (a) A graph illustrating a terrorist network Γ. (b) The graph Γ after agent *A* is captured. (c) The graph Γ of (a) is disconnected after the capture of agents *E* and *G*.

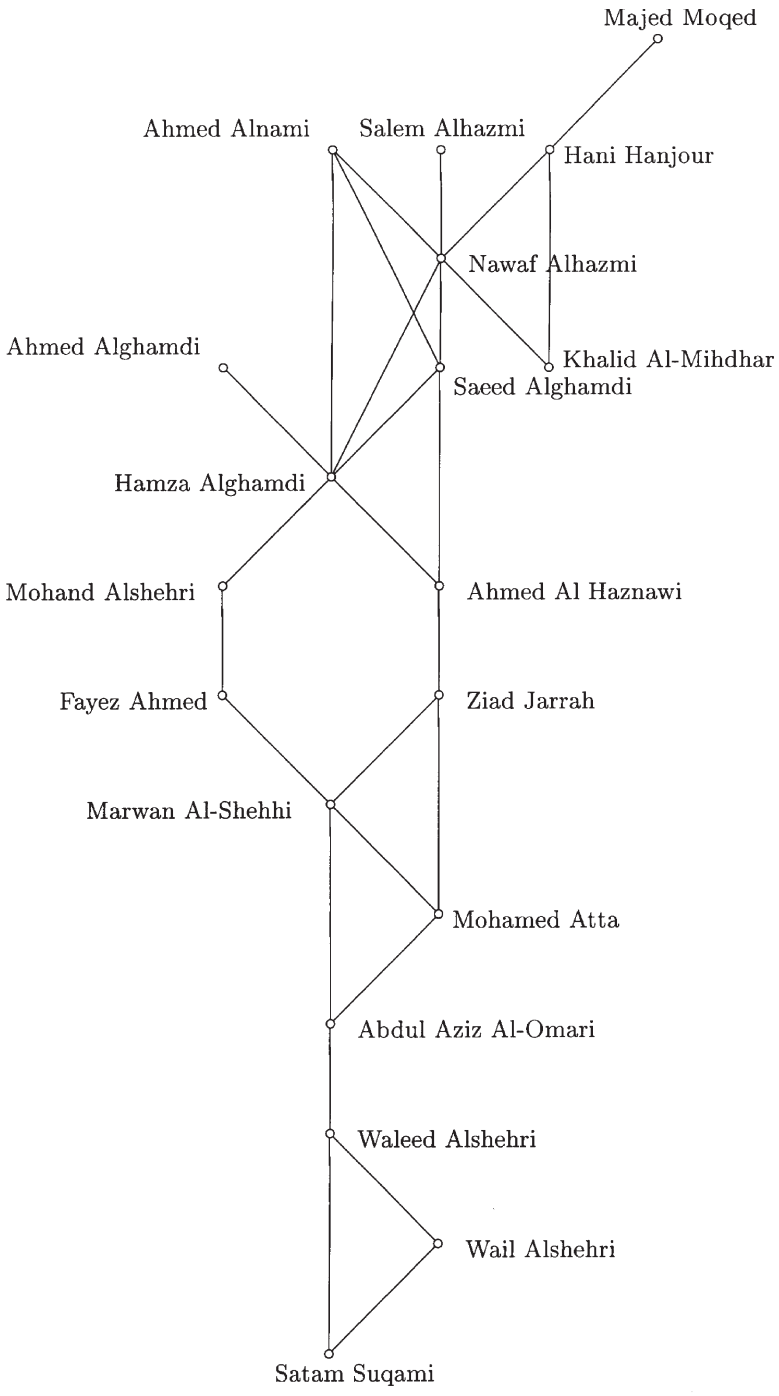

Figure 3. A graph illustrating some of the relationships between the alleged September 11 hijackers (Krebs, 2001).

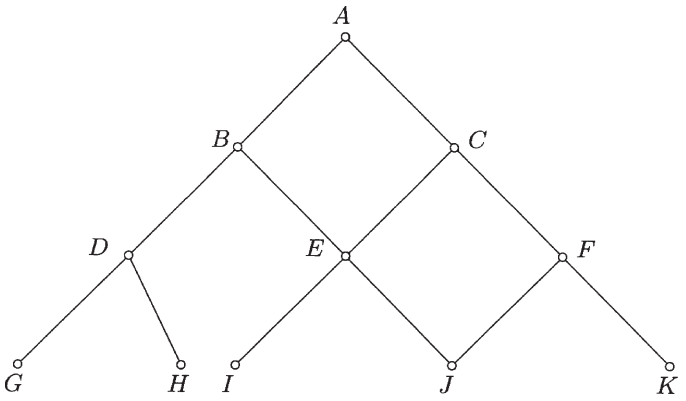

Figure 4. A graph Γ of a terrorist cell.

command from the leader A down to two foot soldiers (J and K) capable of carrying out attacks.

The proper framework for our investigations is therefore that of *order theory*. We do not merely want to break up terrorist networks into disconnected (noncommunicating) parts. We want also to cut the leaders off from the followers. If we do that, then we can reasonably claim to have neutralized the network.

Why does this matter? It may not always be feasible to capture *every* member of a terrorist cell. It may not even be cost effective to capture a majority of the members. The analysis we present later will enable intelligence agencies to estimate better the number of terrorist agents they must eliminate in order to cripple a cell. That way they may decide—based on *quantitative* information—how many millions of dollars they wish to devote toward targeting a particular cell, or whether they wish to spend their scarce resources in another theater of operations in the war on terror.

Refinements of our ideas should enable intelligence agencies to state, for example, that they are 85% certain that they have broken the terrorist cell they are investigating. Of course, our definition of what it means to have "broken" a terrorist cell is something one could debate, for even lone actors, from the Unabomber to the Shoe Bomber, can inflict serious damage. And we recognize the fact that even if we are 85% sure that we

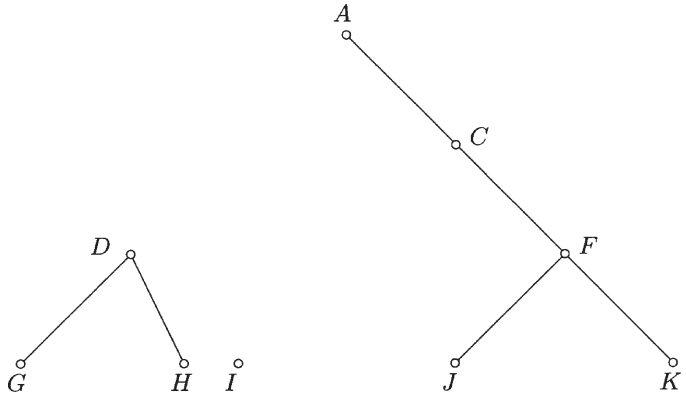

Figure 5. The terrorist cell Γ after the capture of two agents.

have broken a terrorist cell, there is still a 15% chance that we have not—and thus a chance that they might commit another September 11. Nevertheless, law enforcement and intelligence agencies must allocate money and personnel, and our analysis would enable them to do so more rationally than at present.

This article is organized as follows: The next section shows how one mathematically analyzes the extent to which a terrorist cell has been broken. *The key formula is equation* (*). The shortcomings of this analysis and a presentation of ways in which it could be improved by intelligence agencies are discussed in the third section.

Mathematical Interlude: Breaking the Chains of Command

In this section we explain how one can estimate the degree to which a terrorist cell has been crippled. Our tools come from order theory.

First we explain what we mean by an "ordered set" and argue that it is sensible to use ordered sets as models for terrorist cells. Then we define, in mathematical terms, precisely what it means to break a terrorist cell. Finally we illustrate, with examples, how one calculates the probability a terrorist cell has been broken, provided that one knows that a certain number of its members have been captured or killed. The mathematics is elementary, but our use of it is novel.

Modeling A1 Qaeda Cells as Ordered Sets

A common way to represent visually a group of people and the relationships between them is by means of a *graph* or *network.* We have seen several examples already. The individuals are represented by dots or nodes, and, if two individuals are related in some fashion (for instance, if they are friends), then a line is drawn between the corresponding nodes. In the case of a terrorist cell, one might draw a line if the two individuals can communicate directly with one another.

A graph inadequately represents a terrorist cell, however, because it fails to capture the fact that, in any cell, there will most likely be a hierarchy—leaders and followers—with orders passed down from leaders to followers. Figure 6 makes this point clear. All three graphs represent three people: Mary, George, and Robin. Mary can communicate to both George and Robin; Robin and George can each communicate only to Mary. What the graphs fail to capture is the fact that Mary might be the boss with two employees reporting to her, as in the middle picture, or Mary might be a secretary shared by two professors, as in the right-hand picture. The last two pictures represent the same relationship-graph but different *ordered sets.* (Technically, an "ordered set" is a set with a binary relation that is reflexive, transitive, and antisymmetric; but this is not relevant here.)[4]

The simplest examples of ordered sets come from ordinary numbers. The number 1 is less than 2, which is less than 3, and so on, and Figure 7 illustrates this. If the nodes

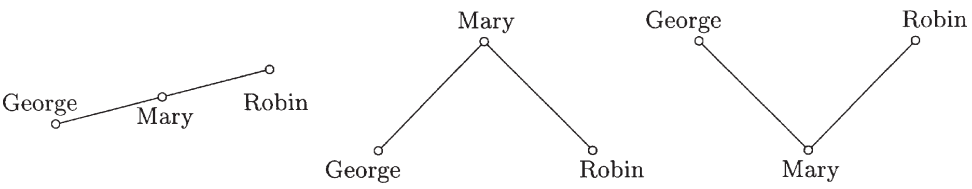

Figure 6. The difference between a graph and an ordered set.

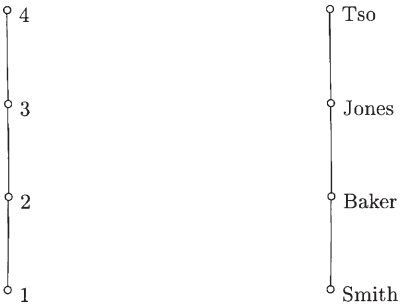

Figure 7. Two simple ordered sets.

represent people, 1 might be a lieutenant, 2 a captain, 3 a colonel, and 4 a general. Just as we would write $1 < 2 < 3 < 4$, we use the symbol "<" and write

Lieutenant Smith < Colonel Jones.

Note that lines only connect individuals who are *directly* related to one another. It is unlikely that a general would communicate directly with a lieutenant. Of course a given general would normally have more than one colonel reporting to him, with neither colonel subordinate to the other, so in general we would not have a *total* order as before but a *partial* order.

Is it valid to use ordered sets to model terrorist cells? In his study of criminal networks, Klerks (2001) argues that we should not assume they are organized hierarchically simply because law enforcement agencies are so organized. If we were to follow Klerks, we would not be so quick to model criminal networks as ordered sets. But although Klerks's conclusions may be valid for ordinary criminal networks, it seems as if terrorist networks are in fact organized hierarchically, sometimes even along military lines.

Now suppose operations are being conducted against a specific terrorist cell. Short of capturing all of its members, how can we ascertain whether or not we have successfully disabled the cell? One criterion might be to say that a terrorist cell has been broken if it is no longer able to pass orders down from the leaders to the foot so1diers—the men and women who, presumably, will carry out the attacks. This is by no means the only possible criterion, but it enables us to make precise estimates of the possibility that our operations have successfully disabled a terrorist cell.

The leaders are represented by the topmost nodes in the diagram of the ordered set and the foot soldiers are represented by the bottommost nodes. (In order theory, these are called *maximal* and *minimal* nodes, respectively.) A chain of command linking a leader with a foot soldier is called a *maximal chain* in the ordered set.

In Figure 8, the four agents *C, E, F,* and *J* form a maximal chain with the ordering from highest rank to lowest rank being $C > E > F > J$. We could also more simply write *CEFJ*.

Next are listed all of the maximal chains:

ADFI	*ADFJ*	*ADGI*	*ADGK*
AEFI	*AEFJ*	*AEHJ*	
BEFI	*BEFJ*	*BEHJ*	
CEFI	*CEFJ*	*CEHJ*	
CK			

Each of these chains represents a chain of command through which terrorist leaders *A, B,* and *C* could pass instructions down to terrorist foot soldiers *I, J,* and *K.* In order to prevent such orders from being passed down and carried out, each of these 14 chains must be broken by means of the removal (death or capture) of at least one agent from each chain. A collection of nodes that intersects every maximal chain is called a *cutset* (El-Zahar and Zaguia, 1986).

In Figure 8, the collection *DEK* forms a cutset because every one of the maximal chains above contains one of *D, E,* and *K.* Another cutset would be *ABC.* The collection *DGHK* would *not* be a cutset because it misses the maximal chain *CEFJ.*

Quantifying the Effectiveness of an Operation against an Al Qaeda Cell

How can law enforcement *quantify* how effective it has been in disrupting a particular terrorist cell? As we have stated, one way to make this precise is to say that a terrorist cell has been disrupted *not* when all of its members have been captured or killed (which might be too costly in terms of money, agents, and agents' time), but when all chains of command have been broken. That is, the collection of nodes in the network corresponding to the terrorists who have been killed or captured should be a cutset.

This enables us to *calculate*—not merely guess—the probability that a terrorist cell has been disrupted. Let Γ be a terrorist cell with n members ($n = 19$ in the case of the alleged September 11 hijackers). Denote by $\Pr(\Gamma, k)$ the probability that Γ has been disrupted once k members have been captured or killed, where k is some number. Let $\mathrm{Cut}(\Gamma, k)$ be the number of cutsets in the ordered set Γ with k members. Then

$$(*) \qquad \begin{array}{r} \text{the probability terrorist cell } \Gamma \text{ has been} \\ \text{broken after } k \text{ members have been captured} \end{array} = \Pr(\Gamma, k) = \frac{\mathrm{Cut}(\Gamma,k)}{\binom{n}{k}}$$

where $\binom{n}{k} = n!/k!(n-k)!$ and $r! = r(r-1)(r-2)\cdots 3 \cdot 2 \cdot 1$ for a positive whole number r.

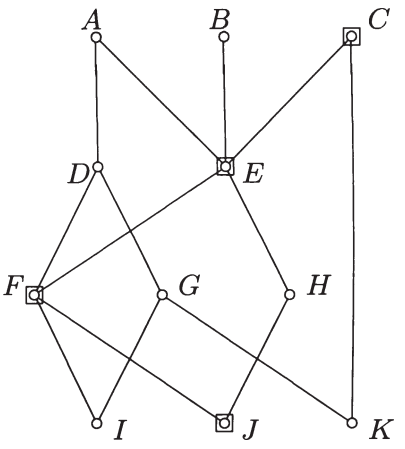

Figure 8. A maximal chain in an ordered set.

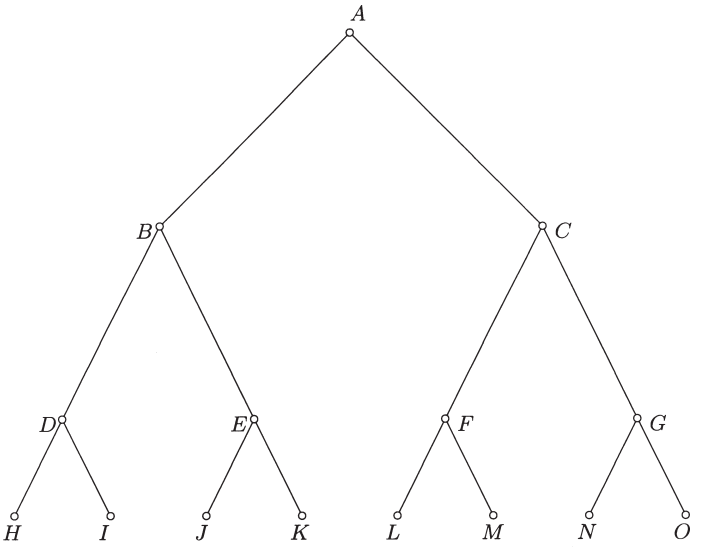

Figure 9. A "binary tree" *T*.

For example, consider the terrorist cell T with $n = 15$ members (Figure 9). What is the probability $\Pr(T, 4)$ that T will be broken if $k = 4$ members are captured or killed? We must first find the number of cutsets $\mathrm{Cut}(T, 4)$ with 4 members. To do this, let us count the number of *minimal* cutsets with 4 or *fewer* members. These are the cutsets that cease to be cutsets if we ignore any one of the members.

minimal cutsets with 1 member	*A*	
minimal cutsets with 2 members	*BC*	
minimal cutsets with 3 members	*BFG*	*CDE*
minimal cutsets with 4 members	*BFNO*	*BGLM*
	CDJK	*CEHI*
	DEFG	

Although we will not explain why, a simple calculation shows that the number of 4-member cutsets $\mathrm{Cut}(T, 4)$ is

$$\binom{14}{3} + \binom{12}{2} + 10 + 10 + 5 = 455 = \binom{15}{3}$$

so

$$\Pr(T, 4) = \frac{455}{\binom{15}{4}} = \frac{455}{1365} = \frac{1}{3}\,.$$

This means that our chances are 1 out of 3 that we will have broken this terrorist cell once we have captured 4 of its members. (We are assuming that we are as likely to capture the leader *A* as a foot soldier such as *J*.) Perhaps we will get lucky and the first 4 people we capture will be *A, B, C,* and *D,* in which case the cell T will have been broken. But we might also be unlucky and only capture *D, H, I,* and *J,* leaving several chains of command—like $A > C > G > O$—intact and capable of committing terrorist

attacks. The fact that $\Pr(T, 4) = \frac{1}{3}$ means that we are twice as likely to be unlucky as lucky.

Note that if we were to use the Connectedness Criterion, which involves asking for the probability that T will become disconnected if we remove 4 members, then we would get a probability of

$$1 - \frac{\left[\binom{8}{4} + 4 \cdot 6\right]}{\binom{15}{4}} = \frac{1271}{1365} > 0.93$$

In other words, we would feel 93% "safe" when in fact we would only be 33% "safe."

Conclusions: Shortcomings of, and Possible Improvements to, the "Break the Chains" Model

Terrorism is not an academic subject. When academies suggest new tools for combating terrorism, we should be skeptical. This is especially true when it comes to an abstruse field such as mathematics and, in particular, order theory.

Yet it remains true that, in the war on terror, decisions have to be made—quantitative decisions, concerning the allocation of resources, money, and manpower. Our methods should help law enforcement and intelligence agencies make these decisions—or at least give them credible arguments with which to defend their decisions before the public and Congressional oversight committees.

Our tools help answer the question, "Have we disabled a terrorist cell, or is it still capable of carrying out attacks?" Although we cannot answer such a question with certainty, our methods help us determine the probability that we have disrupted a particular terrorist cell.

We treat the cell Γ as an *ordered set,* a network with a built-in hierarchy (leaders, foot soldiers, and so on). We say that a terrorist cell has been rendered incapable of carrying out attacks if we have *broken the chains of command,* that is, disrupted every possible line of communication between leaders and foot soldiers. We do this by capturing or killing terrorists who collectively form a *cutset* of the ordered set. By counting all of the cutsets with k members in Γ, we can compute the probability $\Pr(\Gamma, k)$ of disrupting Γ by capturing or killing k of its members.

There are three ways our model could be improved. First, we do not consider the situation where there are several terrorists in a particular cell who have the same rank. (For instance, suppose two or more terrorists share the same apartment in Hamburg. All of them are in direct communication with one another, but none of them outranks the others.) This can be handled by considering *preordered* or *quasiordered* sets.[5]

Second, we could consider the fact that terrorist operations take time. For instance, suppose agent B of Figure 10 is captured on Wednesday, thus breaking that terrorist cell. Perhaps agent A passed down plans to B on Monday, and on Tuesday B passed these attack plans down to C. Then there might still be an attack even though the cell was broken.

Counterterrorist operations also take time. For instance, after B's capture, the cell will be broken. But if too much time passes, the cell may reorganize (Figure 11). For a general ordered set, the collection of cutsets will change after a reorganization. But, assuming the changes are local (that is, if they only involve a node and its neighboring nodes), this situation, too, can be handled with only a slightly more detailed analysis.

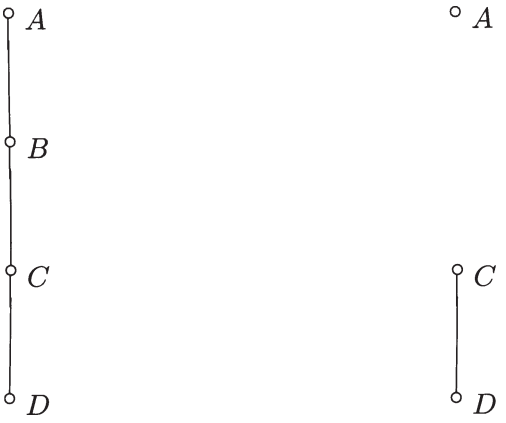

Figure 10. A terrorist cell Γ before and after agent *B* is captured.

Third, we assumed in our model that all the terrorists had an equal chance of getting captured. In reality, it may be the case that foot soldiers have the highest chance of being captured because they are less well protected. Or it may be the case that leaders and foot soldiers are more likely to be captured than mid-level captains because law enforcement might place a greater emphasis on capturing prominent leaders than mid-level ones. Our overall analysis, however, remains the same even if we vary the probability distribution.

Our model has shortcomings. For instance, we do not necessarily know the structure of the particular terrorist cell under investigation. A priori, it could be any ordered set. A naive way around this might be to try to calculate $\Pr(\Gamma, k)$ for every possible ordered set Γ. This option is not feasible, however, as there are 4,483, 130, 665, 195, 087 possible ordered sets to which a 16-member cell, for instance, might correspond (Brinkmann and McKay, 2002).

In fact, the situation is not as bleak as that. The order structure of a terrorist cell Γ is an empirical question. Presumably intelligence sources can tell us who the leaders are, who the captains are, and who the foot soldiers are. There are also tools available for piecing together the structure of a terrorist network (Dombroski and Carley, 2002).

We could perhaps say a bit more. It is likely that terrorist cells are organized as *trees* (Figures 9 and 12a, b, c). Trees have exactly one maximal element—corresponding to the fact that a terrorist cell, like a military unit, probably has just one leader—and

Figure 11. Terrorist cell Γ after it has reorganized.

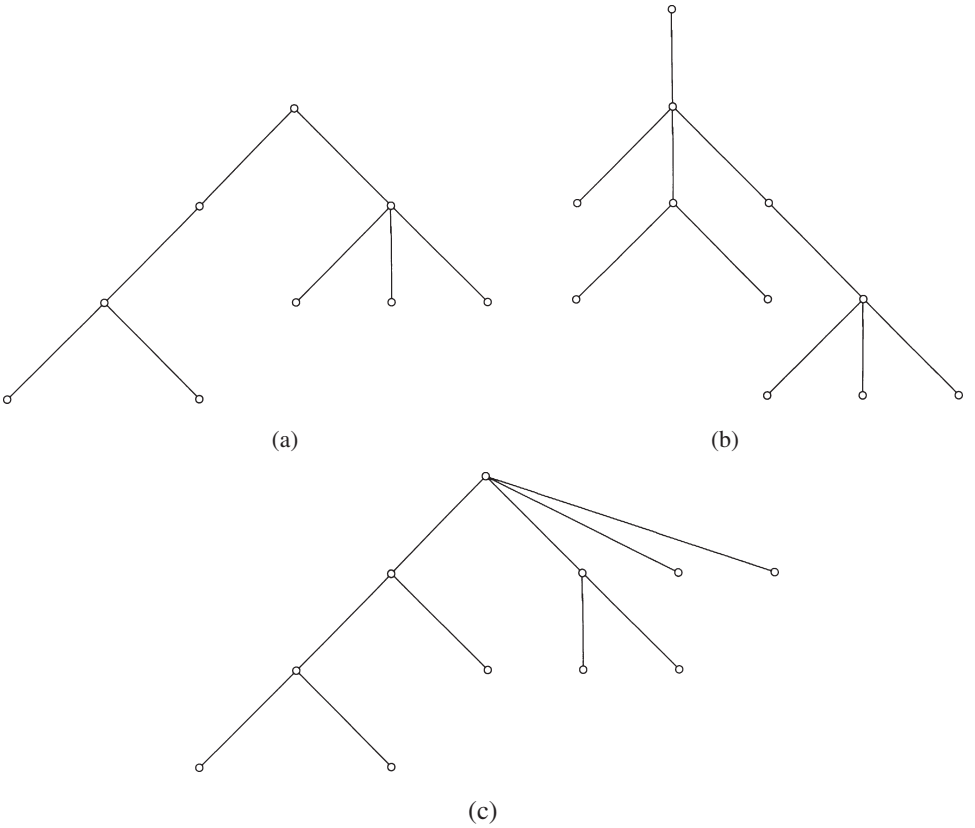

Figure 12. (a) An example of a tree. (b) An example of a tree. (c) An example of a tree.

no portion of a tree resembles the "V" structure of Figure 13. This corresponds to the fact (recall Figure 6) that it is unlikely that a terrorist would have direct contact with more than one superior: if he were captured, he could give away information about several other conspirators more valuable than himself.

Of course, there are still 235, 381 possible "tree" structures to which a 16-member cell might correspond (Sloane, *Encylopedia of Integer Sequences*). We can eliminate most trees, however, as it is unlikely that a terrorist cell would have more than 20 or 30 members, and the hierarchy would probably have no more than 5 levels. This, along with empirical data concerning the cell under investigation, greatly reduces the number of possible order structures the cell might have.

Our model has more serious problems, however; namely its two assumptions. First, we assume that terrorist attacks occur when orders are passed down from leaders to foot

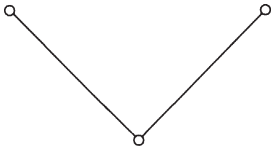

Figure 13. A forbidden structure for a tree.

soldiers. It may be instead that some terrorists act on their own (for instance, the so-called Shoe Bomber). This does not invalidate our model, though, as in these cases the terrorists are not properly part of a larger cell at all, but instead effectively form their own one-person cell.

Second, critics might charge that being 90% sure that a cell has been broken may be dangerously misleading. Even a 10% chance that another September 11 might occur gives the public little comfort. Nonetheless, decisions do have to be made about how to allocate scarce resources in the war against terror, and, even when terrorist attacks do succeed, intelligence agencies will want quantitative data at their disposal to defend themselves from the ensuing public criticism concerning why they did not devote the resources necessary to foil the attack. This model enables law enforcement to plan its operations in less of an ad hoc fashion than they might be able to do otherwise.[6]

Notes

1. Dr. Gordon Woo is a Catastrophe Consultant for Risk Management Solutions.

2. See, for example, Klerks (2001) and Krebs (2001). In this article, the terms "network" and "cell" are used interchangeably.

3. Indeed, according to the U.S. Defense Department's (2001) transcript of the video allegedly made by Osama bin Laden, bin Laden says, "Those who were trained to fly didn't know the others. One group of people did not know the other group." It might be inferred, therefore, that at that low level in the network, the clusters of nodes corresponding to the hijackers were already disconnected. But they posed a danger because it was still possible for orders to filter down from above: According to the tape, "[T]hey were trained and we did not reveal the operation to them until . . . just before they boarded the planes." The author makes no claims about the authenticity of the video or the accuracy of the transcript.

4. For the basics of order theory, see Davey and Priestley (2002).

5. These are sets with a binary relation that is reflexive and transitive but not necessarily antisymmetric.

6. The author is not liable for any actions that may result from the use of the information contained herein. The author does not endorse the use of extralegal measures in intelligence gathering or military operations. The use of this material is not authorized against any but criminal terrorist organizations that illegally target noncombatant civilian populations in violation of international law and custom. No political views or affiliations on the part of the author are implied or should be inferred.

References

Brinkmann, G., and B. D. McKay. 2002. "Posets on up to 16 Points." *Order 19,* pp. 147–179.

Carley, K. M., J.-S. Lee, and D. Krackhardt. 2001. "Destabilizing networks." *Connections* 24(3), pp. 79–92.

Davey, B. A., and H. A. Priestley. 2002. *Introduction to Lattices and Order* (2nd edition). Cambridge: Cambridge University Press.

Dombroski, M. J., and K. M. Carley. 2002. "NETEST: Estimating a terrorist network's structure—Graduate student best paper award, CASOS 2002 Conference," *Computational and Mathematical Organization Theory* 8, pp. 235–241.

El-Zahar, M. H., and N. Zaguia. 1986. "Antichains and cutsets." *Contemporary Mathematics* 57, pp. 227–261.

Klerks, P. 2001. "The network paradigm applied to criminal organisations: Theoretical nitpicking or a relevant doctrine for investigators? Recent developments in the Netherlands." *Connections* 24(3), pp. 53–65.

Krebs, V. E. 2001. "Mapping networks of terrorist cells." *Connections* 24(3), pp. 43–52.

Sloane, N. J. A. *The On-Line Encyclopedia of Integer Sequences.* Available at (http://www.research.att.com/cgi-bin/access.cgi/as/njas/sequences/eisA.cgi?Anum=A000081).

U.S. Department of Defense. *Transcript of Usama bin Laden Video Tape,* December 13, 2001. Available at (http://www.defenselink.mil/news/Dec2001/d20011213ubl.pdf).

Gordon Woo, "Modeling the Al-Qaeda Threat," public lecture, January 30, 2003, Cambridge, Massachusetts.