

# Rational Terrorists and Optimal Network Structure

Walter Enders\* and Xuejuan Su<sup>+</sup>

August 2006

Keywords: Terrorist Cells, Network structure, Counterterrorism

---

\* Corresponding author address: Department of Economics, Finance and Legal Studies, the University of Alabama, Tuscaloosa, AL 35487-0224. Phone: 205-348-8972. Email address: wenders@cba.ua.edu.

<sup>+</sup> Author address: Department of Economics, Finance and Legal Studies, the University of Alabama, Tuscaloosa, AL 35487-0224. Email address: xsu@cba.ua.edu.

## Abstract

After the events of 9-11, US counterterrorism became more proactive in that the Patriot Act allowed the authorities far more freedom to directly attack terrorist network structures. We argue that rational terrorists will attempt to thwart such policies and restructure themselves to be less penetrable. We model the trade-off between security and intra-group communication faced by terrorists. The model is used to derive the anticipated changes in network structure and the consequent changes in the type, complexity and success rate of potential terrorist attacks.

## 1. Introduction

After the events of 9/11, US counterterrorism policy switched from being almost purely defensive towards being more proactive. As detailed in Enders and Sandler (2006), the US Patriot Act (HR 3162) allowed the authorities far greater latitude in surveillance and intelligence gathering than had ever been thought possible. For our purposes, it is noteworthy that many features of the Patriot Act were designed to launch a direct assault on terrorist networks by monitoring their communications. Particularly controversial was the fact that the act (i) expanded authority to intercept wire, oral, and electronic communications of suspected terrorists; (ii) allowed for shared criminal investigative findings among foreign and domestic law enforcement agencies; (iii) eased the restrictions on foreign intelligence gathering inside the United States; (iv) allowed voice-mail message seizures; (v) augmented the access of domestic law-enforcement agents to Foreign Intelligence Surveillance Act records; and (vi) reduced congressional oversight on intelligence gathering. The current firestorm surrounding National Security Agency's monitoring the communications of suspected terrorists shows the extent of the Bush Administration's infiltration efforts. In addition, actions against money laundering enhanced the government's ability to track the international flow of funds that might be used to finance terrorist activities.

It would be naive to think that terrorists and their networks would remain invariant to measures designed to track and infiltrate the inner workings of their organizations. For example, most observers believe that the organizational structure of Hamas was altered in response to the Israeli crackdown against the group. After Israel outlawed Hamas and arrested many of its leaders, including Sheikh Ahmad Yassi, its military wing (Izz al-Din al-Qassam Battalions) abandoned its centralized, hierarchical leadership structure. In its place, the leadership developed

a compartmented organizational structure such that the individual cells operate secretly from each other. The cells are connected to the extent that they operate under the directorship of local commanders.<sup>1</sup> Although it is hard to put too much credence in the popular view that the al Qaeda affiliates act like MacDonald's franchises, it is clear that the network has become far less hierarchical and far less structured as a result of the Patriot Act and the ouster of the Taliban from Afghanistan. This is in accord with the type of 'swarming' behavior discussed in Arquilla, Ronfeldt, and Zanini (1999). Although there is no precise definition of the term 'swarming,' the connotation is one of groups of killer bees on the attack. A swarming terrorist network would be one with a nonhierarchical deployment of small terrorist subgroups communicating with each other. No one sting would be critical, but the sum total of all attacks could be fatal. Rodriguez (2004) reports that Spain's March 11<sup>th</sup> terrorist network is based on weak ties in the sense that the structure is not hierarchical and that most of the links are not based on intense (such as familial) relationships.<sup>2</sup> In a 12 July, 2005 interview with Mark Colvin on Australia's ABC radio network [see Wilkinson (2005)], Paul Wilkinson of St. Andrew's University argues that the group responsible for the London metro bombings is loosely organized. Consider:

Colvin: "But does that mean that Osama bin Laden would have given the order [regarding the London bombings], or is it a new al-Qaeda which operates almost like a sort of McDonalds franchise, with people working much more independently of a large organisation?"

Wilkinson: "I think that bin Laden has only rarely been in a position since the removal of the Taliban regime in Afghanistan to actually coordinate the detail of any operations. That is left to the sections of the worldwide network that are

involved in that particular area. ... But they would know that this was in accord with the wishes and strategic objectives of the al-Qaeda movement."

Colvin: "So ... if bin Laden or somebody like him ... has to give the go-ahead, how come ... no chatter was picked up? Are they getting better at getting the messages through to each other?"

Wilkinson: "Well, I think that they've always been very clever at hiding their communications and they've got more sophisticated as they've had to adapt to the severe measures taken against them by the international community. So what we've seen is the morphing of the al-Qaeda movement."

Because terrorists act in secret, most of the evidence concerning these adaptations of their network structures is anecdotal. Yet, this need for secrecy is precisely the reason that terrorist networks are organized differently from other types of networks. In a social, familial or business setting, network design can be focused on the efficiency and robustness of the information flow. Information flows are most likely to be unfettered when all individuals are well-connected. However, the illegal nature of a terrorist group dictates that its network design balance the trade-off between information flow and group security.

The aim of this paper is to model the process by which terrorists select between the competing ends of security versus the unbridled flow of information. Obviously, counterterrorism policy based on the assumption of a static group network is bound to be inferior to one based on the recognition a dynamic group structure. This is not to say that we are the first to consider changing terror network structures. Papers such as Arquilla, Ronfeldt, and Zanini (1999), Carley, et. al. (2003), and Rodriguez (2004), all discuss the possibility that the structures

of terrorist groups evolve over time. However, we attempt to place the choice within a micro-theoretic optimizing framework. Our model is designed to illustrate the relationship between the network structure and the types of counterterrorism measures carried out by governments. Specifically, terrorists rationally allocate their scarce resources so as to promote a general climate of intimidation and fear. Highly connected groups can conduct logistically complex attacks (such as simultaneous embassy bombings) but are subject to infiltration. Transference can occur because counterterrorism policies, such as previously mentioned changes in the Patriot Act, will induce groups to substitute toward a more secure network structure. Similarly, technological innovations enhancing secure links, such as the internet, will allow groups to be more dense without sacrificing security.

The next section of the paper discusses the application of the rational-actor approach to the study of terrorist optimizing decisions. The key insight of the approach is that rational terrorists optimize their behavior so as to bring about their most preferred outcomes. Also discussed is the structural approach to terrorist networks. The structural approach uses graph theory to analyze the linkages, importance, and reachability among the various participants in a terrorist organization. We argue that by combining the two approaches, it is possible to meaningfully discuss adaptations in the optimal structure of groups such as al Qaeda. It is also possible to show how these adaptations will alter the types of incidents orchestrated by the group. In Section III we focus on the costs and benefits of forming communication links within a terrorist network. The complete choice-theoretic model is developed in Section IV. We show how a rational terrorist organization will adapt its network structure in response to increased counterterrorism measures and to innovations in communications technology. A discussion of the results is contained in Section V.

## 2. Models to Combat Terrorism

There are two primary types of models of terrorism that have been used to formulate anti-terrorism policy. The rational-actor model posits that the choices made by a terrorist group are the result of an economic optimization process. Specifically, the model assumes that a terrorist group uses its scarce resources to maximize its expected utility. In contrast, the structural approach attempts to find and connect the links among the participants in the network. A graphical depiction of all such linkages is called a sociogram. Individuals with many links to others can be deemed 'important' potential targets for counterterrorist actions. Both approaches have their strengths and weaknesses. Typically, rational-actor models do not address the issue of how different individual preferences can be aggregated into a group decision, how information flows within the group, or how the individual group members form a consensus. The structuralist approach never addresses the issue of how and why links are formed and maintained. Since sociograms are static, they are unable to indicate how the group's structure is likely to respond to changes in its environment. Combining the two approaches allows us to model the ways that terrorists might use to protect the network from infiltration and ways that they might respond to technological developments such as the internet.

### 2.1 The rational-actor approach

The basic premise of the rational-actor approach is that the utility of a terrorist group is derived from a shared political goal. The shared goal might be the elimination of a grievance stemming from income inequality, ideological differences, historical inequities, or a lack of political, economic or religious freedom. As discussed in Enders and Sandler (1993), this shared goal can be obtained from the consumption of a number of basic commodities such as media attention, political instability, popular support for their cause, and the creation of an atmosphere

of fear and intimidation. The terrorist group has access to a finite set of resources including financial assets, weapons and buildings, personnel, and entrepreneurial abilities. Given its resources a rational terrorist group selects the set of activities that maximizes the expectation of its attaining the shared goal.

The choices made by the group will be influenced by the relative prices of the basic commodities. The full price of any particular attack mode includes the value of the resources used to plan and execute the attack, the loss of group members due to deaths and casualties, and the costs of defending the group from a security breach. Certain attack modes are more likely to expose the group's membership to capture and infiltration than others. For example, the price of a suicide bombing includes the direct costs of the bomb, the costs of grooming the perpetrator to ensure that the attack takes place, and the cost to protecting the group's security against a failed attack. On the other hand, threats and hoaxes typically require few inputs and personnel so that costs are low. Rational terrorists will incorporate all of these costs into their calculations when selecting their optimal tactics.

The key feature of any counterterrorism policy is that it can influence the prices, resource supplies and the payoffs faced by terrorists. Enhanced airport security increases the logistical complexity of a skyjacking and raises its price. If, at the same time, governments do not increase security at ports-of-entry, attacks relying on contraband become relatively cheaper. Similarly, if immigration officials make it more difficult for terrorists to enter the United States, a terrorist group might attack US interests located abroad (for example, tourists and firms). Enders and Sandler (1993, 2004) summarize two of the key propositions of the model as:

*Proposition 1: An increase in the relative price of one type of terrorist activity will cause the terrorist group to substitute out of the relatively expensive activity and into activities that are*

*now relatively less expensive.* The direct implication is that an increase in the costs of maintaining intra-group connections will induce the group to substitute away from a tightly organized network structure towards a more loosely organized form.

Proposition 2: *An increase in the group's opportunity set will induce it to produce and consume more normal goods and fewer inferior goods.* If logistically complex events are normal goods while logistically simple events are inferior goods, improvements in the technology available to the group should increase the occurrence of complex events and reduce the number of events such as threats and letter bombs. As complex events require more coordination than simple events, connectivity will tend to increase as the technology available to terrorists improves.

These propositions have been used to explain many of the substitutions that terrorists seem to make in response to changing circumstances. Notice, however, that the approach never directly addresses the issue of how the group's decisions are made and how they are passed along to various members of the group. Unlike the model of a single consumer or firm, some members of a terrorist group have no direct way of communicating with other members. For security reasons, the lines of communication between various members are necessarily guarded. As such, some group members may not even know the identities of many of the other members.

## 2.2 The structuralist approach: sociograms

The alternative way of viewing terrorists is to map the structure of their organizations using network or graph theory. As summarized by Farley (2003), each individual terrorist or terrorist cell within an organization can be represented by a point called a *node*. Lines, sometimes called *links* or *edges*, connecting two nodes represent a direct communications tie between these subcomponents of the overall network. Even if two nodes are not directly

connected, it is still possible for them to communicate through the use of multiple links. The *density* of a network is defined as the number of links in the network divided by the maximum number of all possible links. Typically, the speed through which information travels through a network is an increasing function of the density of the network. Dense networks have many links so that information can quickly travel from one node to any or all of the others.

Figure 1 contains Krebs' (2001) sociogram of the nineteen 9/11 hijackers. The key insight of the structuralist approach is that the effectiveness of the network can be eroded by breaking the links between the nodes. Notice that Nawaf al Hazmi is directly connected to the network with six links. Eliminating such a well-connected individual is likely to undermine the effectiveness of the entire organization. Since Abdulaziz al Omari is a bridge to three of the network's members (Satam al Suqami and the brothers Waleed and Wail al Shehri), eliminating him would leave these three hijackers disconnected. In contrast, Ahmed al Ghamdi and Majed Moqed are not well-connected; as such, if the network structure is known, the counterterrorism authorities might want to target other network members.

[Figure 1 about here]

Figure 2 shows the basic schematics for the two fundamental network types---the star and the chain. For simplicity, we describe the pure forms of each type using only 5 nodes. Note that the nodes can represent individuals or groups of individuals that we refer to as cells. For expositional purposes, we suppose that there is a cell leader (1) needing to transmit information, funds, or weaponry to the others in the network. Of course, actual networks contain features of both types of linkages. However, we focus on the two pure structures since each has its own distinct advantages and disadvantages for a terrorist network. A rational terrorist group will

select the structure that best suits the types of operations it intends to carry out given its available resources.

The chain structure is clearly sequential in that communications flow from the leader to nodes 2 through 5 in a predetermined order. In contrast, each node has a direct tie to the leadership in the star structure. As such, all communications flow from 1 directly to the individual nodes. Notice that this structure allows the leadership to simultaneously coordinate the behavior of the individual cells but the individual nodes do not communicate directly with each other. Since communication links to the leadership are all direct, this structure is not especially secure since every node has the possibility of providing useful information about the location of the leadership. The strength of the star structure is that it is less vulnerable to logistical failure than the chain structure. If, say, node 3 is compromised, members of the other nodes can continue to carry out their assigned mission. To take a specific example, it is possible to suppose that nodes 2 through 5 represent the four hijacked planes of 9/11. Even though United Airlines flight 93 crashed near Shanksville, PA, the remaining planes were tragically successful.

[Figure 2 about here]

Arquilla, Ronfeldt and Zanini (1999) suggest that the chain structure is secure so that it is especially well-suited for smuggling types of operations. Viewers of the classic film, *The Battle of Algiers*, will recall Colonel Mathieu's famous characterization of the purported chain formation of the FLN:<sup>3</sup>

"The military head of the Executive Bureau finds a competent person and names him: No 1. No. 1 finds others: nos. 2 and 3. ... Now 2 and 3 each select 2 men: nos. 4, 5, 6 and 7. The reason for these geometrics is that each organization

member knows only three other members: the one who chose him and the two he himself chose. . . . in point of fact, they don't know each other."

Although the chain structure is secure, it is vulnerable to logistical failure. Infiltration of the network can occur at any of the communications junctures. Suppose that node 3 is compromised as a result of anti-terrorism efforts. Since 1 and 2 no longer have a direct or indirect communication link with 4 and 5, these two nodes are cut off from the remaining members of the network. Any operations requiring 4 and/or 5 will lead to a logistical failure. On the other hand, the leadership is secure since 3 cannot inform the authorities about the location of the leadership. Moreover, the chain pattern has greater long-run viability in that there is a natural order of accession should the leadership be compromised. For example, after 9/11, the Bush administration targeted the top leadership of the al Qaeda network by placing special emphasis on Osama bin Laden and Ayman al Zawahiri. If al Qaeda were arranged as a star network, the successful execution of the plan would leave it with no natural successor. In contrast, the chain pattern suggests a clear successor in the chain of command.

Panels 3 and 4 indicate the effects of allowing an additional linkage between two of the nodes. Begin with a basic chain structure and allow nodes 2 and 5 to communicate directly with each other. The additional linkage allows the terror mission be more logistically sophisticated in that 2 and 5 are able to directly coordinate their actions. The possibility of logistical failure is diminished in that 5 may not be isolated if the network is infiltrated. If, node 3 is compromised, 2 can relay any important information directly to 5. The disadvantage of the additional link is that the network becomes less secure in that 2 and 5 now have information about each other.

Similar remarks can be made about the star structure. The additional linkage allows the terror mission to be more logistically sophisticated in that 2 and 5 are able to directly coordinate their actions. However, allowing 2 and 5 to directly interact compromises the security of the network. After all, if node 5 is infiltrated it could compromise the security of 1 and/or 2.

Before proceeding, we want to emphasize the limitations of the use of sociograms for formulating a counterterrorism policy. The standard procedure is to collect information about the key individuals in the network and the links connecting them. The aim is to identify and remove those individuals who are important in the social network. Importance is typically identified by the number of links to the other nodes. Thus, importance is measured by how many individuals one knows rather than on the role that the individual plays in the system. Consider the following statement of Brams, Mutlu and Ramirez (2005): "... point  $i$  is more important than point  $j$  if it has more direct links to other points" and that "... more important persons influence less important persons." Nevertheless, as the authors themselves acknowledge, in many circumstances the number of links does not necessarily correspond to importance. For example, in Panel 4 of Figure 2, the leader is the least connected node even though it influences all nodes and no node has a direct influence over the leader. The four pilots of 9/11 (Mohamed Atta, Marwan al Shehhi, Hani Hanjour, and Ziad Jarrah) are neither 'important' nor 'weakly connected' in Krebs' sociogram. The issue is that a sociogram does not distinguish individuals in terms of their function. In addition, papers such as Farley (2003) and Rodriguez (2004) argue that it is the weakly-linked individuals that provide the most opportunity for successful infiltration. After all, eliminating an individual such as Abdulaziz al Omari, who serves as a bridge, may segment the group. Moreover, there is always the issue of how accurately the authorities actually know the network's structure since government intelligence operations can be

faulty. Clearly, incomplete information about the network can result in missing nodes and/or links.

### 2.3 Density and the security-communication trade-off

The trade-off between network density and information flows is illustrated in Figure 3. Notice that each panel of the figure depicts a non-hierarchical network structure containing four nodes. Even though the individual panels could each represent a complete network, it is more likely that they represent a substructure of a more complete terrorist organization. Panel 1 contains six links so that each node is directly connected to each other node. The density of the group ( $\rho$ ) is unity since each node is connected to every other node. Not only are the communications flows maximized, but the group has maximum flexibility in that it is possible to create a number of sub-groups, or teams, that can be used for various types of terrorism missions. Note that it is possible to create one team with four members, a team with three members in four different ways, a team with two members in six different ways, and two teams with two members each in three different ways.<sup>4</sup> Panel 2 shows the effects of removing a link. Since the group is not hierarchical, it does not matter which of the six links is removed; all five-link patterns are necessarily transformations of each other. With only five links ( $\rho=5/6$ ), group flexibility and communication becomes more difficult since there is not a direct path from 1 to 4. Resiliency and flexibility decline since it is impossible to have a team of four members because nodes 1 and 4 are not directly connected. Similarly, there are only two ways to form a three-member team, there are only five ways to form a team with two members, and there are only two ways to form two groups of two-member teams.<sup>5</sup> Panels 3a and 3b show the two distinct ways to connect four nodes using four links ( $\rho=4/6=2/3$ ). If you examine these two panels, it should be clear that communication and flexibility are further diminished by the elimination of the second link. The

point is made even more forcefully in Panels 4a and 4b wherein there are only three links connecting the nodes ( $\rho=3/6=1/2$ ). Note the chain in Panel 4a and the star of Panel 4b are the only two possible structures with three links among four nodes. Even though there is no leader, the lines of communication are necessarily linear in Panel 4a and all communications must go through 2 in Panel 4b.

[Figure 3 about here]

If we move through the figure from Panel 1 through Panel 4, the structures become less flexible and communication becomes more difficult. However, in most circumstances, we would expect the structure in Panel 1 to be the least secure because it has the most links. If the anti-terrorism authorities are able to compromise any node in Panel 1 by means such as infiltration, torture, or bribery, the entire network is placed in jeopardy. In Panel 2, only nodes 2 and 3 place the entire network at risk since 1 and 4 are not directly linked. If we use a modification of the argument made by Farley (2003), suppose that the anti-terrorism authority can infiltrate a single node with a probability of success equal to  $p_I$ . Further suppose that the agency is unsure of the network structure so that it is equally likely to attempt to infiltrate any one particular node (i.e., we assume that the probability that authority attempts to infiltrate any one particular node is 0.25). Thus, in Panel 1, the probability that the entire network is brought down is  $p_I$ , regardless of which node is infiltrated. If eliminating any one node has a payoff of 1, the expected cost to the terrorists of infiltration in Panel 1 is  $p_I*4$ . In Panel 2, there is a 0.5 chance that the authority attempts to infiltrate node 2 or 3 and a 0.5 chance that it attempts to infiltrate node 1 or 4. Thus, the probability that the entire network is brought down is  $p_I*0.5$  and the probability that three of the nodes are eliminated is also  $p_I*0.5$ . In this case the expected cost to the terrorists of infiltration is  $p_I*(0.5*4+0.5*3) = p_I*3.5$ , which is less than that in Panel 1. In Panel 3a, the

successful infiltration of any one node leads to the elimination of three terrorists. Thus, the expected cost of infiltration is  $p_I * 3$ . In Panel 3b, the successful infiltration of node 1 and 3 leads to the elimination of 3 nodes, the successful infiltration of node 2 leads to the elimination of the entire network and the elimination of node 4 leads to the elimination of 2 nodes. As such, the expected cost of infiltration is  $p_I * (0.5 * 3 + 0.25 * 4 + 0.25 * 2) = p_I * 3$ . Finally, the expected costs of infiltration can be shown to be  $p_I * (0.5 * 2 + 0.5 * 3) = p_I * 2.5$  in Panel 4a and  $p_I * (0.75 * 2 + 0.25 * 4) = p_I * 2.5$  in Panel 4b.

A concept related to a network's density is the 'reachability' or 'detectability' of specific individuals within the network. Given an infiltration, a node is likely to be detectable if there are many direct and indirect links to that node. Suppose that, if successfully infiltrated, each node reveals a directly connected node with a probability of 0.5. Hence, returning to Panel 1 of Figure 2, the successful infiltration of node 1 reveals the identity of node 1 with probability 1, and the successful infiltration of nodes 2, 3, 4, or 5 reveals the identity of node 1 with probability 0.5. As such, the reachability of node 1 is given by  $1 + 4(0.5) = 3$ . As such, with five identical individuals in the network, the probability a successful infiltration will 'reach' node 1 is  $p_I * 3/5$ . Node 2 can be reached by direct infiltration and indirectly by infiltrating node 1, 3, 4, or 5. The infiltration of node 1 reveals 2 with probability 0.5 and the infiltration of any of nodes 3, 4, or 5 reveals the identity of node 2 with probability of  $(0.5)(0.5) = 0.25$ . Hence, the reachability of node 2 is given by  $1 + (0.5) + 3(0.25) = 2.25$ . It should be clear that the reachability of nodes 3, 4, and 5 are precisely the same as that as node 2. Hence, in the star pattern, node 1 is the most detectable in the network. Nevertheless, there is not a one-to-one relationship between density and reachability. To illustrate the point, note that the density of the network in Panel 2 is identical to that of Panel 1 but the reachability of the various individuals differs across the

panels. In Panel 2, the reachability of node 1 is  $1 + 0.5 + (0.5)^2 + (0.5)^3 + (0.5)^4 = 1.9375$  in that it can be reached directly and through routes passing along (2, 1), (3, 2, 1), (4, 3, 2, 1) and (5, 4, 3, 2, 1). By using similar calculations, the reachability of nodes 2, 3, 4 and 5 can be shown to be 2.375, 2.5, 2.375, and 1.9375, respectively. Thus, for the same density, individuals in the star pattern have different degrees of reachability than those in the chain. However, for our purposes, the distinction between density and reachability is not especially important because, for a given structure, adding an additional link increases both the network's density and the reachability of the nodes.

Even though reachability can be useful for cases in which the counterterrorism authority has detailed knowledge of the network's structure, in most cases such information is not available. Nevertheless, the point of the exercise is to argue that, all else equal, terrorists would want to minimize the number of links if their sole goal was to minimize the expected damage to the network. If the network is hierarchical, the network would want to protect 'important' individuals by reducing their reachability.

#### 2.4 Combining the two approaches

The rational-actor and structuralist approaches each have their own distinct advantages. A strength of the rational-actor approach is that it recognizes that a terrorist group will optimize over all dimensions of its choice set. However, as discussed above, there is little recognition of the communication flows within the organization itself. In contrast, the structuralist approach highlights the links within an organization, but it usually takes the form of the network as given. However, once the counterterrorist authorities target the lines of communication within the network, terrorists will find that the relative price of links has increased. As links become less secure (or are expected to become less secure), a rational group will want to economize on the

number of communication links within the organization. As such, counterterrorism policy will alter the form of the organization itself. Not only will the group's density decline, but the group will find that the relative price of tactics that are intensive in communications links has increased. In contrast to a coordinated armed attack, a suicide bombing is a very secure attack mode since it involves few individuals and the authorities have little means to trace the successful bomber back to the network. In the same vein, Merrari (1999) argues that terrorist groups adopting loosely connected organizational structures to minimize infiltration risk are also acting to limit their ability to conduct logistically complex activities such as the acquisition and use of chemical, biological, radioactive or nuclear (CBRN) weapons. A high degree of centralization allows a group to acquire and coordinate the resources and personnel necessary to conduct this type of logistically sophisticated attack. Similarly, Enders and Sandler (2006) argue that al Qaeda's decentralized structure protected it during the post-9/11 attacks, but at the price of not being able to develop CBRN weapons. In contrast, Aum Shinrikyo was a highly centralized group. Until the recent spate of anthrax attacks immediately following 9/11, it was the only terrorist group using a CBRN weapon. However, the group stayed centralized and sustained an organization-wide setback once their headquarters were raided in 1995.

### 3. The Terrorists' Optimization Problem

In this section we develop a model designed to capture how the optimal network density (and the logistical complexity of terrorist operations) changes in response to technological change and counterterrorism policies. As such, we abstract from the actual pattern of the links that form the network in that we pay no attention to whether the group chooses a star pattern, a chain, or a complex combination of the two. The precise pattern will depend on the various types

of attacks the group plans to undertake and on other micro factors such as kinship, childhood friendship, who goes to the same training camp as whom, etc.<sup>6</sup>

Before proceeding, some preliminary relationships need to be developed. Suppose there are  $N \geq 2$  members in the group. It is easy to show that the maximum number of links connecting the members is  $N(N-1)/2$ .<sup>7</sup> Also suppose that the actual number of links is  $L$ . Since the density ( $\rho$ ) is the number of links ( $L$ ) divided by the maximum possible number of links, it follows that  $\rho = L / ((N(N-1))/2) \in [0, 1]$ . In a sense, the density parameter  $\rho$  is a summary measurement of the complexity of the network structure in that it shows the degree of connectivity among the cells. Notice that if the network is connected, the minimum number of links is  $N-1$ . Consequently, when  $\rho \in [0, 2/N]$ , the group necessarily falls apart into subgroups that are disconnected from one another; only when  $\rho \in [2/N, 1]$  is it possible that the entire group forms a connected network.

### 3.1 Density and infiltration risk

The essential feature of our model is to capture the relationship between a group's optimal density and the intensity of governmental efforts, such as the Patriot Act, to infiltrate the group and to curtail its activities. To model this process, we assume that the successful infiltration of node  $j$  compromises  $j$  and all nodes directly connected to  $j$ . It should be clear that the greater the number of links, the greater the expected cost of any one infiltration. For example, in Panel 1 of Figure 3, the infiltration of a single group member can cause the downfall of the entire group. However, in Panel 4a, the infiltration of nodes 1 or 4 will cause only one other member to be compromised and the infiltration of 2 or 3 will cause only two others to be compromised. More generally, if node  $j$  is connected to  $k$  other nodes, the number of individuals compromised from a successful infiltration of  $j$  is  $1+k$ . In principle, it is also possible to allow

a successful infiltration of node  $j$  to compromise  $j$ , all  $k$  nodes connected to  $j$ , and with some probability less than unity, the individuals connected to this latter set of individuals. However, nothing of substance would be changed so long as the infiltration of one node does not cause the entire network to be compromised. In the circumstance that a successful infiltration compromises the entire network, there is a corner solution such that all agents are connected or all act individually. As such, we focus on the network's density and abstract from the issue of individual reachability.

Suppose that the counterterrorism authority wants to infiltrate a single node and that the probability of a successful infiltration is given by  $p_I$ . If the group is not hierarchical and the authority does not know the group structure, it seems reasonable to assume that each node has an equal probability of being infiltrated. Hence, if there are  $N$  group members, the probability that any particular node is infiltrated is  $1/N$ . Given the group's size and the number of links,  $L$ , it is straightforward to show that the expected number of compromised nodes ( $I$ ) from an attempted infiltration is<sup>8</sup>

$$(1) \quad I = p_I (1 + 2L/N)$$

Intuitively, if there are  $L$  links among  $N$  people, the average person is connected to  $L/(N/2) = 2L/N$  others. Hence, an infiltration compromises  $1 + 2L/N$  others with probability  $p_I$ .

Since we want to express  $I$  as a function of the density  $\rho$ , it is useful to rewrite the equation as

$$(2) \quad I = p_I [1 + (N-1)\rho]$$

For example, in Panel 1 of Figure 3,  $\rho = 1$  and  $N - 1 = 3$ , so that any attempted infiltration would be expected to compromise 4 people with probability  $p_I$ . Similarly, in Panels 4a and 4b, an attempted infiltration would be expected to compromise 2.5 ( $2.5 = 1 + 3 * 0.5$ ) people with probability  $p_I$ . The point of the exercise is to show that the expected number of

compromised individuals ( $I$ ) is an increasing function of  $p_I$ ,  $N$  and  $\rho$ . Although it is relatively straightforward to extend the analysis to situations where the counterterrorism authority tries to infiltrate two nodes, in order to conserve space, we do not pursue that exercise. For our purposes, the key point is that the expected number of compromised individuals is increasing in the group's density; hence, the group can decrease its infiltration risk by reducing  $\rho$ . We can also use equation (2) to illustrate Krebs' (2001) sociogram of the 9/11 network shown in Figure 1. There are 19 nodes ( $N=19$ ) and 27 links ( $L=27$ ). Since the maximum possible number of links is  $17*16/2 = 136$ , the value of  $\rho = 27/137 = 0.19708$ . Although we do not know the value of  $p_I$ , we can calculate  $I/p_I = 1+(N-1)\rho$  as  $1+18*0.19708 = 4.5474$ . Had there been a 10% chance of a successful infiltration, the expected number of compromised members would have been 0.45474.

### 3.2 The probability of a logistical failure.

Following the existing literature, we divide the government's counterterrorism policies into those that are primarily offensive and those that are primarily defensive. As described in Enders and Sandler (2006), defensive policies,  $G_D$ , represent measures such as enhanced airport security, embassy fortification, and inspection of containers at ports-of-entry. Offensive (or proactive) policies,  $G_O$ , attack the terrorists, their resource base, or those who support them. Since our focus is to model the network structure, we let  $G_O$  represent policies, such as the aforementioned features of the Patriot Act, designed to infiltrate terrorist network structures. The distinction is important since an increase in the governments' infiltration efforts should result in an increase in  $p_I$ . In contrast, defensive policies have no direct impact on the value of  $p_I$ .

Similarly, the technology that the terrorist group uses to plan, organize and conduct an attack can be divided into two categories. The terrorist offensive technology,  $T_O$ , represents innovations in weaponry such as improvised explosive devices (IEDs) or CBRN weapons. The

terrorist defensive technology,  $T_D$ , represents innovations in the communications technology employed by terrorists. Developments such as the internet, wireless telephones, and message encryption devices all improve the ability of terrorists to form secure links. In our framework, such technological advances act to reduce the value of  $p_I$  while changes in the level of  $T_O$  have no direct effect on  $p_I$ .

The point is that the probability of a successful infiltration  $p_I$  depends on the magnitude of the government's offensive policy efforts  $G_O$  and the terrorist defensive technology  $T_D$ . As such, we can model the probability of a successful infiltration as  $p_I = p_I(G_O, T_D)$ , where the partial derivative with respect to the first argument is positive, while that with respect to the second argument is negative. However, to keep the notation simple, we let  $A$  denote any autonomous increase in the value of  $p_I$  so that

$$(3) \quad p_I = p_I(A)$$

where  $d p_I / d A > 0$  and an increase in  $A$  represents an increase in  $G_O$  relative to  $T_D$ .

At this point, we can model the probability of a failed attack  $p$ . Besides the extent of infiltration,  $I$ , a logistical failure might be due to enhanced defensive counterterrorism efforts,  $G_D$ . As such, we let the probability of a failed attack be increasing in  $G_D$  and  $I$ :

$$(4) \quad p = p(G_D, I) = p(G_D, p_I(A)[1+(N-1)\rho])$$

where we have used (2) and (3) so that we can express  $I$  as  $p_I(A)[1+(N-1)\rho]$ . Consider the function<sup>9</sup>

$$(5) \quad p = p(A, G_D, \rho, N)$$

From the discussion above, it follows that:

**Assumption 1.**  $p_1 > 0, p_2 > 0, p_3 > 0; p_{13} > 0, p_{23} = 0, p_{33} = 0$ .

Note that defensive policies combat terrorism by increasing the value of  $G_D$  while the types of offensive policies we consider act to combat terrorism by increasing  $A$ . Both types of policies work by increasing the probability of a failed attack so that  $p_1 > 0$  and  $p_2 > 0$ . An increase in density increases the expected loss of an attempted infiltration so that  $p_3 > 0$ .

Papers by Bueno de Mesquita (2005) and Faria and Arce (2005) provide formal models of the recruitment process (i.e., the selection of the optimal value of  $N$ ). In contrast, we treat  $N$  as a fixed factor of production so that we can focus on other determinants of the group's optimal density. This is not to say the density and size are independent of each other; instead, we want to refrain from making specific assumptions concerning the partial effects of  $N$  on  $\rho$ . Of course, a straightforward extension of the model is to allow for the simultaneous choice of  $N$  and  $\rho$ . Moreover, we could also generalize the model to allow for proactive policies that directly aim to reduce the terrorists' resources or personnel.

Now that we have discussed the signs of the first-order derivatives, we turn to the second-order derivatives. The assumption that the cross derivative between  $A$  and  $\rho$  is positive (i.e.,  $p_{13} > 0$ ) implies that better proactive policies makes the problem of a security breach on existing links more severe. In the same way, a technological change that enhances secure communications within the terrorist group makes the problem of a security breach on existing links less severe. The cross derivative between  $G_D$  and  $\rho$  is 0 because the government's defensive efforts do nothing to directly facilitate or impede the information flow within the terrorist network structure. And last, the second-order derivative of  $\rho$  is 0 (i.e.,  $p_{33} = 0$ ) because, from equation (2), the infiltration probability is linear in  $\rho$ .

### 3.3 The terrorists' production technology

Terrorists produce basic commodities using a number of factors of production. However, in order to keep the problem tractable and to focus on connectivity, we assume that the output of the basic commodity  $F$ --say 'fear and intimidation'--can be represented by:

$$(6) \quad F = F(T_O, N, \rho)$$

**Assumption 2.**  $F_1 > 0$ ,  $F_3 > 0$ ,  $F_{13} > 0$ ,  $F_{33} < 0$ .

Note that  $F_1 > 0$  since the expression  $T_O$  represents technological change in the production of the basic commodity. For example, the development of plastic explosives might mean that terrorists can create more 'intimidation and fear' holding constant the other factors of production. With fixed technology, more links within the network imply better information flow and better coordination among the members, so that marginal product of density on the output of 'fear' is positive (i.e.,  $F_3 > 0$ ). The positive cross derivative between  $T_O$  and  $\rho$  (i.e.,  $F_{13} > 0$ ) implies that better technology to plan and organize attacks enhances the marginal value of forming additional links. And it is a conventional assumption that the marginal benefit of an additional link diminishes as there are more and more existing links, hence  $F_{33} < 0$ .

### 3.4 The cost function

The cost function faced by the terrorist organization depends only on the number of people in the organization and the density of the organization. Hence, we posit a cost function of the form:

$$(7) \quad C = C(N, \rho)$$

**Assumption 3.**  $C_2 \geq 0$ ,  $C_{22} \geq 0$ .

Given that it takes additional effort to establish and maintain an additional link, we make the assumption that the marginal cost of increasing density is positive ( $C_2 \geq 0$ ). Also as the

number of existing links increases, it is more and more costly to build an additional link, so that  $C_{22} \geq 0$ .<sup>10</sup>

#### 4. Determinants of the Density

The aim of the group is to maximize the expected output of the basic commodity,  $(1-p)F$ , minus costs  $C$ . With fixed group size  $N$ , a terrorist group chooses the optimal group density  $\rho$  to solve the following maximization problem:

$$(8) \quad \max_{\rho} [1 - p(A, G_D, \rho, \bar{N})] F(T_O, \bar{N}, \rho) - C(\bar{N}, \rho)$$

where the expression  $\bar{N}$  reflects the assumption that the number of group members is fixed or predetermined.<sup>11</sup> Hence, for a given value of  $\bar{N}$ , the group selects its optimal density  $\rho$ . Since the only choice variable is  $\rho$ , the arguments of a function are omitted when there is no risk of confusion. The first-order condition on  $\rho$  (assuming an interior solution) is

$$(9) \quad (1 - p)F_3 - p_3F - C_2 = 0$$

The first term,  $(1-p)F_3$ , is positive and represents the expected marginal product of an additional link. The second and third terms are negative and represent the marginal cost of an additional link;  $p_3F$  represents the marginal cost of a link due to a security breach and  $C_2$  represents the marginal cost of setting up and maintaining the link. The marginal benefit equals the marginal cost at the optimum, so that the terrorist group has no incentive either to increase or to decrease the number of links. In this problem the second-order condition for maximization is also satisfied:

$$(10) \quad (1 - p)F_{33} - 2p_3F_3 - C_{22} < 0$$

Given Assumptions 1, 2 and 3, the optimal density ( $\rho^*$ ) is the solution to (9) and is unique. Since this optimal value is implicitly a function of  $A$ ,  $G_D$  and  $T_O$ , it is straightforward to

derive the determinants of  $\rho^*$  and the consequent changes on  $p$  and  $F$  using the Implicit Function Theorem (IFT).

#### 4.1 Counterterrorism: infiltration effort

One important result of the model is that rational terrorists will substitute out of high-density activities as infiltration risk increases. Similarly, if internet connections become more secure (so that  $T_D$  increases), the group should seek to add links in order to take advantage of the lower risk. In fact, it is straightforward to derive these predictions. If we apply the Implicit Function Theorem to (9) and take the total derivative with respect to  $A$ , we have

$$(11) \quad ((1 - p)F_{33} - 2p_3F_3 - C_{22})(d\rho^*/dA) = p_1F_3 + p_{13}F$$

Since the left-hand-side (LHS) coefficient is negative while the right-hand-side (RHS) is positive, it immediately follows that  $d\rho^*/dA < 0$ . Since  $A$  is increasing in  $G_O$  and decreasing in  $T_D$ , the group's density will fall as a result of increased infiltration efforts and rise as a result of improved communications technology. In the extreme, counterterrorism efforts could split the network. If the optimal density falls such that  $\rho^* < 2/N$ , the network would find it more efficient to work in completely separate subgroups than in a single large group. Like the Jenin Martyrs' Brigade, formed as a break-away group from Hamas after an Israeli raid on a Palestinian refugee camp in 2003, the break-away group could act autonomously from the larger group.<sup>12</sup> Alternatively, the original network could simply be an umbrella group for the resultant subgroups.

In point of fact, increased infiltration efforts and improvements in the internet and wireless communication technologies, have occurred simultaneously (i.e., both  $G_O$  and  $T_D$  have been increasing over time). Nevertheless, if the MacDonald's-franchise or swarming views of

terrorism have any validity, it would be the case that the efforts of the counterterrorism authorities have kept ahead of the terrorists' adoption of internet technologies.

The substitution towards a lower density implies a substitution from logistically complex attacks to logistically simple ones. All else equal, logistically complex incidents should further the terrorist's cause more than simple incidents. Yet, because many factors are in play, some relatively simple incidents can have dramatic consequences. For example, there is little doubt that the March 11, 2004 Madrid commuter train bombings had a larger total impact than the more coordinated simultaneous attacks on the US embassies in Nairobi, Kenya and Dar es Salaam, Tanzania on August 7, 1998. Nevertheless, to the extent that the density of al Qaeda has decreased, the model predicts a substitution towards events like the Madrid bombings and away from highly sophisticated and coordinated attacks.

One interesting result is that enhanced infiltration activities may actually result in the terrorists adopting attack modes with a higher success rates. In a sense, the terrorist substitute out of complex attacks with a lower probability of success and into simpler attacks that are more likely to succeed. To obtain this result, take the differential of  $p = p(A, G_D, \rho)$ :

$$(12) \quad dp/dA = p_1 + p_3(d\rho^*/dA).$$

Since the first term  $p_1$  is positive and the second term  $p_3(d\rho^*/dA)$  is negative, it follows that at the optimal network structure  $\rho^*$ ,  $dp/dA$  may be positive, zero or negative. Simply put, more intense proactive policies to fight terrorism need not necessarily make it harder to carry out an attack successfully. On one hand, the government becomes more efficient at infiltrating each link. On the other hand, the terrorism group becomes more discreet, establishes fewer links and switches to logistically simple attacks that are harder to infiltrate. The net effect depends on the

comparison of the two effects. Of course, it also follows that an increase in  $T_D$  will have an ambiguous effect on  $p$ .

Although the effect of  $A$  on the probability of a logistical failure  $p$  is ambiguous, the overall impact of an increase in  $A$  is to decrease the expected output of the basic commodity. To obtain this result, take the total derivative of expected output  $(1-p)F$  with respect to  $A$

$$(13) \quad d(1-p)F/dA = -p_1F + (-p_3F + (1-p)F_3)(d\rho^*/dA)$$

From the first-order condition  $(1-p)F_3 - p_3F - C_2 = 0$ , it follows that

$$(14) \quad d(1-p)F/dA = -p_1F + C_2(d\rho^*/dA) < 0$$

Thus, even though  $d\rho^*/dA$  is ambiguous, enhanced infiltration makes does effectively reduce the expected output of the group.

#### 4.2 Counterterrorism: defensive policies

The signs of the comparative statics of an increase in defensive policies are identical to those of enhanced infiltration policies. In particular  $d\rho^*/dG_D < 0$ , and at the optimal  $\rho^*$ ,  $d\rho^*/dG_D$  is ambiguous while  $d(1-p)F/dG_D < 0$ .

If we apply the IFT to (9) and take the total derivative with respect to  $G_D$ , we obtain

$$(15) \quad ((1-p)F_{33} - 2p_3F_3 - C_{22})(d\rho^*/dG_D) = p_2F_3$$

Since the LHS coefficient is negative and the RHS is positive, it follows that  $d\rho^*/dG_D < 0$ .

Even though the government's defensive technology has no direct impact on the terrorist network structure, it has an indirect effect. Since  $p_1 > 0$ , the direct effect of a defensive policy is to increase the probability of a logistical failure. The group will find it advantageous to offset this by reducing its density; the reduced density acts to make the group more secure and to reduce the likelihood of a failed attack.

It is easy to check that  $dp/dG_D = p_2 + p_3(dp^*/dG_D)$  may be positive, zero or negative. As in the case of increased infiltration efforts (i.e., increased  $A$ ), observing more successful attacks following a stepped-up counterterrorism policy does not necessarily suggest policy failure. Also, it should be clear that  $d(1-p)F/dG_D = -p_2F + (-p_3F + (1-p)F_3)(dp^*/dG_D) = -p_2F + C_2(dp^*/dG_D) < 0$ .

Government proactive and defensive counterterrorism policies target different features in the chain of operation, yet both have similar effects in that they decrease density and expected output of the basic commodity. Moreover, both have ambiguous effects on the probability of a failed attack.

#### 4.3 Terrorist offensive technology

It is straightforward to show that the sign of  $d\rho^*/dT_O$  is ambiguous. Applying the IFT to (9) and taking the total derivative with respect to  $T_O$ , we obtain

$$(16) \quad ((1-p)F_{33} - 2p_3F_3 - C_{22})(d\rho^*/dT_O) = p_3F_1 - (1-p)F_{13}$$

Although the coefficient on the LHS is negative, the two terms on the RHS are of opposite signs. Hence, unless we impose further structure on the model,  $d\rho^*/dT_O$  has an ambiguous sign. This may seem counterintuitive at the first glance, yet the ambiguity is perfectly consistent with the rational-actor model (see Proposition 2 of Enders and Sandler above). The increase in  $T_O$  acts as a pure increase in the terrorists' income since they can have more of the basic commodity without expending any of their resources. Unless it can be determined whether density is normal, the sign  $d\rho^*/dT_O$  is ambiguous. Intuitively, the complementarity between the terrorists' offensive technology and the density ( $F_{13} > 0$ ) suggests that an increase in  $T_O$  will be accompanied by an increase in  $\rho$ . However,  $T_O$  has a positive income effect in that output of the basic commodity can be increased without an increase in  $\rho$ . As such, in the face of a positive technological change, it might be worthwhile for the terrorists to give up some of the basic

commodity by reducing  $\rho$  in exchange for a higher probability of a successful attack. The net effect depends on the comparison of the two.

However, the ambiguity disappears if we make the rather innocuous assumption that the technological change has the Hicks-neutral form. Specifically, we assume that the output of the basic commodity is proportional to the magnitude of the technological change:

$$(17) \quad F(T_D, N, \rho) = T_D f(N, \rho)$$

where  $F_1 = f(N, \rho) > 0$ ,  $F_3 = T_D f_2 > 0$ ,  $F_{13} = f_2 > 0$ .

Now the term  $p_3 F_1 - (1-p) F_{13}$  can be written as  $p_3 f(N, \rho) - (1-p) f_2 = (1/T_D)[p_3 F - (1-p) F_3]$ .

From the first-order condition, we know that  $p_3 F - (1-p) F_3 = -C_2 < 0$ . Hence, the ambiguity disappears as we can write

$$(18) \quad ((1-p)F_{33} - 2p_3F_3 - C_{22})(d\rho^*/dT_O) = -C_2/T_D$$

so that  $d\rho^*/dT_O > 0$ .

Thus, technological improvements in weaponry can be expected to increase network density and the logistical complexity of terrorists' attack modes.

## 5. Discussion

The fact that network structures can change in response to counterterrorism has important policy implications. Sparrow (1991), Farley (2003), and Carley, et al (2003) discuss methods to destabilize a terrorist network that rely on the structuralist approach. The problem is that the sociogram for period  $t$  may not be the same as that for period  $t+1$ ; this is especially true in the presence of increased counterterrorism efforts. As the structure of the group changes, the types of actions it can successfully hope to undertake also changes. By combining the structuralist approach with an optimizing model of terrorism, it is possible to anticipate how the network will

change in response to counterterrorism policies and to technological innovations such as the internet. We argue that rational terrorists will attempt to counter increased efforts at infiltration and restructure themselves to be less penetrable. We model the trade-off between security and intra-group communication faced by terrorists. The model is used to derive changes in the optimal network structure and the consequent changes in the type, complexity and success rate of potential terrorist attacks.

Although the model is highly stylized, it does lead to a number of potentially important policy implications. First, we do not expect to see the type of extensive swarming behavior envisioned by Arquilla, Ronfeldt, and Zanini (1999). As long as terrorists need to maintain secrecy, they will act to limit their density so as to reduce infiltration risk. While it is true that developments in communications technology have enabled terrorist groups to maintain contact with members across great distances, the need for clandestine behavior remains. Although internet websites can provide some useful information to group members, they cannot provide explicit details about forthcoming attacks. Moreover, it is not possible to be sure who has entered an internet chat room and e-mail messages are not fully secure.

Second, in response to counterterrorism activities directed towards group communications, groups are predicted to reduce their density. As such, the types of activities they are able to conduct will necessarily be altered. Logistically complicated events, such as the 9/11 attacks and the coordinated attacks on the US embassies in Kenya and Tanzania, are predicted to decline in number. Given that infiltration technologies do not reduce the terrorists' grievances or resources, there is a predicted substitution into less coordinated incident types. Clearly, the March 11 attacks on the Madrid commuter trains and more recent London subway

bombings were relatively simple to plan and execute as compared to the embassy attacks or the simultaneous attacks of 9/11.

Third, both defensive and infiltration counterterrorism policies may have the effect of actually increasing the probability of a successful attack (i.e., decreasing the value of  $1-p$ ). The direct effect of either type of counterterrorism policy is to reduce the probability of a successful attack. However, rational terrorists can seek to circumvent counterterrorism efforts by reducing their density and substituting into less complex types of attacks with higher success rates.

There are a number of interesting avenues for further exploration. The first is to extend the model such that there are two explicit attack modes. The logistically complex mode (e.g., hostage taking) could be intensive in 'connectivity' while the other attack mode could be relatively simple (e.g., letter bombs) in that it requires few links to be successful. In this way, it would be possible to trace out the direct substitution of one attack mode for another. Second, since our aim was to focus on connectivity and logistical complexity, we assumed that all factors of production in the terrorist group were fixed. The terrorists simply chose the value of  $p$  that provided the greatest level of 'fear and intimidation' in excess of costs. However, connectivity should be complementary with some factors and substitutes for others. Allowing for variable labor inputs as in Bueno de Mesquita (2005) and Faria and Arce (2005), would make it possible to trace out the effects of changing resource levels on connectivity. Third, in the model, the values of  $G_0$  and  $T_D$  are exogenously given and have opposite effect on the parameter  $A$ . However, as in Arce and Sandler (2005), the terrorists and the authorities could be allowed to play a game against each other such that each selects its optimal strategy. In a static setup, the game theoretical framework would allow us to analyze the government's optimal counterterrorism policies. In particular, facing a total resource constraint, the government can

select the optimal counterterrorism policy by changing the relative emphasis on proactive versus defensive policies. In a dynamic setup, the game theoretical framework would allow us to study the cat-and-mouse innovation game of the type discussed in Enders and Sandler (2006) and Faria (2003). The nature of that game is such that a successful terrorist innovation (such as the use of the internet) puts pressure on the authorities to combat the terrorists (possibly by intercepting e-mail messages). After a successful innovation by the government, the terrorists adopt a new strategy to offset the government's counterterrorism strategy (such as using secure messaging).

Figure 1: Krebs' Sociogram of the 9/11

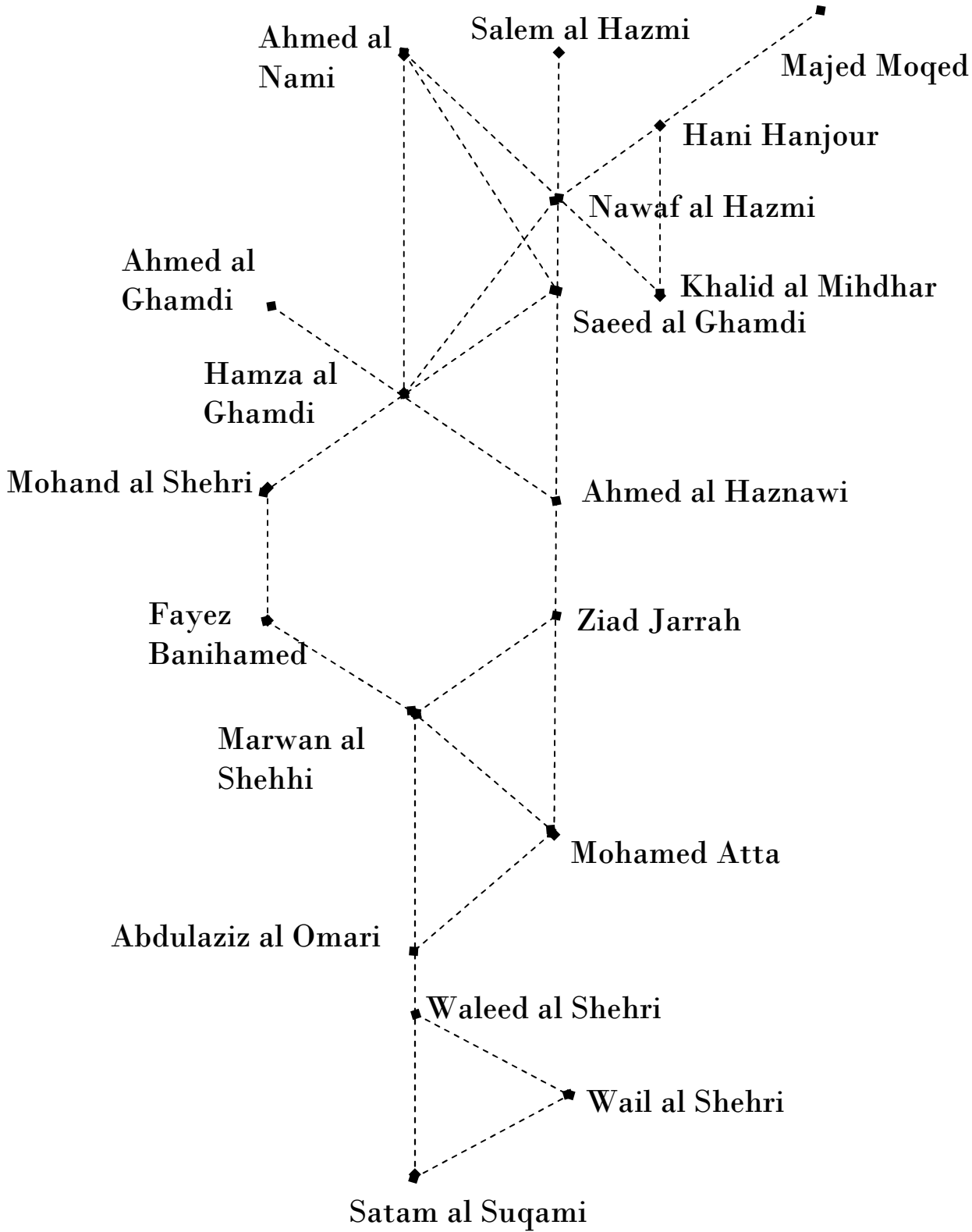
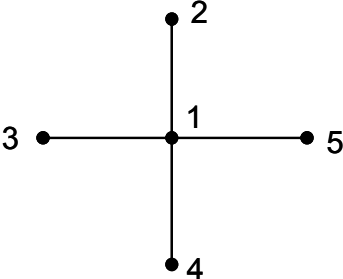
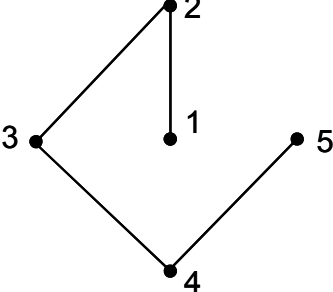


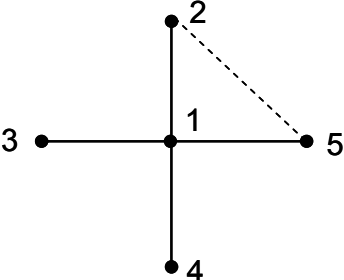
Figure 2: Basic Star and Chain Network Structures



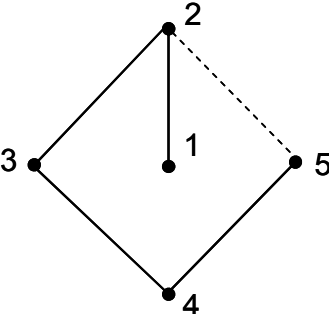
Panel 1: Star Pattern



Panel 2: Chain Pattern



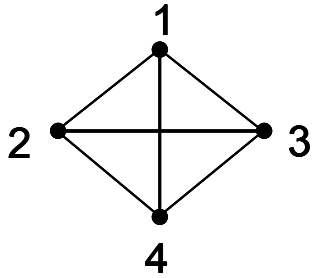
Panel 3: Modified Star



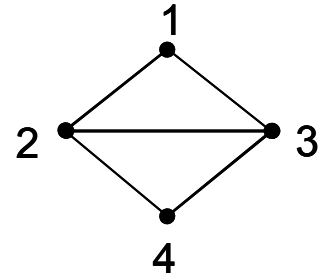
Panel 4: Modified Chain

Figure 3: Density versus Security

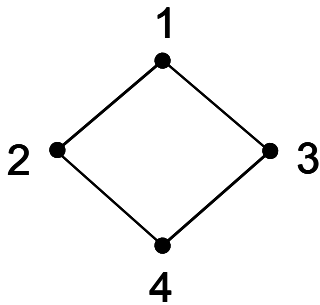
Panel 1:  $\rho = 1$



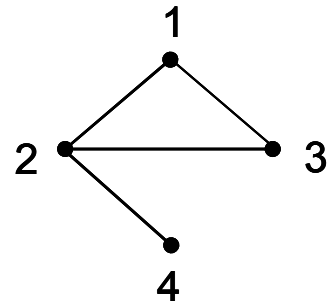
Panel 2:  $\rho = 5/6$



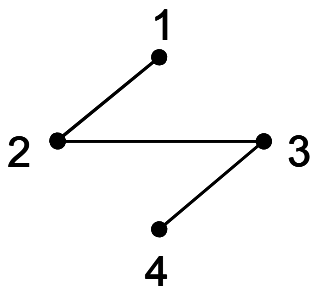
Panel 3a:  $\rho = 2/3$



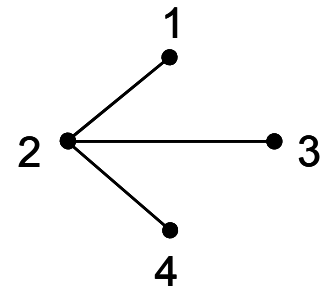
Panel 3b:  $\rho = 2/3$



Panel 4a:  $\rho = 1/2$



Panel 4b:  $\rho = 1/2$



## 6. References

Arce, Daniel G. and Todd Sandler. 2005. Counterterrorism: A game-theoretic approach, *Journal of Conflict Resolution* 49 (2): 183-200.

Arquilla, John, David Ronfeldt, and Michele Zanini. 1999. Networks, netwar, and information-age terrorism. In *Countering the New Terrorism* edited by Ian Lesser, Bruce Hoffman, John Arquilla, David Ronfeldt, and Michele Zanini. Santa Monica, CA: RAND.

Brams, Steven, Hande Mutlu and Shawn Ramirez. 2005. Influence in terrorist networks: from undirected to directed graphs. *Studies in Conflict and Terrorism*. forthcoming.

Bueno de Mesquita, Ethan. 2005. The quality of terror. *American Journal of Political Science* 49 (3): 515-30.

Carley, Kathleen, Matthew Dombroski, Max Tsvetovat, Jeffrey Reminga, and Natasha Kamneva. 2003. Destabilizing dynamic covert networks. In *Proceedings of the 8th International Command and Control Research and Technology Symposium*. Conference held at the National Defense War College. Washington DC. [www.sandia.gov/ACG/focusareas/previousfocusareas/seldon/papers/a2c2\\_carley\\_2003\\_destabilizing.pdf](http://www.sandia.gov/ACG/focusareas/previousfocusareas/seldon/papers/a2c2_carley_2003_destabilizing.pdf) (accessed May 2, 2006).

Enders, Walter and Todd Sandler. 1993. The effectiveness of anti-terrorism policies: A vector-autoregression-intervention analysis. *American Political Science Review* 87 (4): 829-44.

\_\_\_\_\_. 2004. What do we know about the substitution effect in transnational terrorism? In *Research on Terrorism: Trends, Achievements and Failures*, edited by Andrew Silke, 119-37. London: Frank Cass.

\_\_\_\_\_. 2006. *The Political Economy of Terrorism*. Cambridge, England: Cambridge University Press.

- Faria, João R. 2003. Terror cycles. *Studies in Nonlinear Dynamics and Econometrics* 7 (1): 1-11.
- Faria, João R. and Daniel G. Arce. 2005. Terror support and recruitment. *Defence and Peace Economics* 16 (4): 263-73.
- Farley, Jonathan David. 2003. Breaking al Qaeda cells: A mathematical analysis of counterterrorism operations (A guide for risk assessment and decision making). *Studies in Conflict and Terrorism* 26: 399-411.
- Gambill, Gary. 2002. Sponsoring terrorism: Syria and Hamas. *Middle East Intelligence Bulletin* 4 (10). [http://www.meib.org/articles/0210\\_s1.htm](http://www.meib.org/articles/0210_s1.htm) (accessed May 2, 2006).
- Krebs, V. E. 2001. Mapping networks of terrorist cells. *Connections* 24 (3): 43-52.
- National Commission on Terrorist Attacks Upon the United States (2004). *The 9/11 Commission Report*. New York: W.W. Norton & Company.
- Merrari, Ariel. 1999. Terrorism as a strategy of struggle: past and future. *Terrorism and Political Violence* 11 (4): 52-65.
- Rodriguez, Jose. 2004. The March 11th terrorist network: In its weakness lies its strength. Department of Sociology y Analysis of Organizations: University of Barcelona. [www.ub.es/epp/redes.htm](http://www.ub.es/epp/redes.htm) (accessed May 2006).
- Sparrow, Malcolm. 1991. The application of network analysis to criminal intelligence: An assessment of the prospects. *Social Networks* 13: 251-274
- Wilkinson, Paul. 2005. Concerted effort needed to beat al-Qaeda. Transcript of radio interview available at: [www.abc.net.au/pm/content/2005/s1412793.htm](http://www.abc.net.au/pm/content/2005/s1412793.htm) (accessed April 2006).

## Endnotes

---

<sup>1</sup> Gambill (2002) provides a detailed discussion of the ways that the organizational structure of Hamas changed in response to the Israeli counterterror initiative.

<sup>2</sup> This so-called 3/11 network is the al Qaeda affiliate responsible for the four commuter train bombings in Madrid.

<sup>3</sup> Translation from the Criterion Collection (minute 58) of *The Battle of Algiers*. The producer, Saadi Yacef, was the head of the FLN in the Casbah and was arrested in 1957. Granted amnesty, he collaborated with director Gillo Pontecorvo and played himself in the film.

<sup>4</sup> The four possible teams with three members each are (1,2,3), (1,2,4), (1,3,4), and (2,3,4). The six possible teams of two members each are (1,2), (1,3), (1,4), (2,3), (2,4), and (3,4).

<sup>5</sup> The two possible teams with three members each are (1,2,3) and (2,3,4). The five possible teams of two members each are (1,2), (1,3), (2,3), (2,4), and (3,4).

<sup>6</sup> Since we are concerned about density, but not the group's actual structure, it is possible to conceptualize a situation in which the group has a two-step optimization process. In the first stage, the group selects its density and in the second stage it selects the precise pattern of links among the individuals.

<sup>7</sup> The hypergeometric distribution indicates that  $N$  items taken 2 at a time (without regard to order) can be done in  $N!/[(N-2)!2!] = N(N-1)/2$  ways.

<sup>8</sup> Suppose there are  $N$  group members and  $L$  links joining them. Let  $n_i$  denote the number of group members linked to exactly  $i$  other members. Hence,  $n_1$  denotes the number of members linked to only one other member and  $n_2$  denotes the number of members linked to only two

others. As such, it must be the case that  $N = \sum_{i=1}^{N-1} n_i$ . The total number of links in the group must be

---

equal to:  $L = \frac{1}{2}[n_1 + 2n_2 + \dots + (N-1)n_{N-1}]$ ; or more compactly:  $L = \frac{1}{2} \sum_{i=1}^{N-1} i n_i$ . Since  $n_i$  denotes the

number of nodes connected to exactly  $i$  others and each node has a probability of  $1/N$  of being infiltrated, the expected number of nodes whose activities become known to the authorities is

$$I = \frac{p_I}{N} (2n_1 + 3n_2 + \dots + Nn_{N-1}), \text{ or } I = \frac{p_I}{N} \sum_{i=1}^{N-1} (i+1)n_i = \frac{p_I}{N} \left( \sum_{i=1}^{N-1} i n_i + \sum_{i=1}^{N-1} n_i \right) = p_I (1 + 2L/N).$$

<sup>9</sup> Throughout the paper, the notation  $x_i$  denotes the partial derivative of the function  $x$  with respect to its  $i^{\text{th}}$  argument.

<sup>10</sup> If there are economies of scale in creating links such that  $C_{22}$  is sufficiently negative, some of the signs of the comparative statics results are reversed.

<sup>11</sup> The joint maximization of both  $N$  and  $\rho$  depends critically on the cross derivatives of  $N$  and  $\rho$  in the production and cost functions. Since we want to focus on density, and there is little empirical evidence to justify any assumption concerning the sign of the cross derivative, we abstract from the joint optimization.

<sup>12</sup> The MIPT website <http://www.tkb.org./Group.jsp?groupID=3499> contains an extended discussion of the Jenin Martyrs' Brigade.