An Overlapping Networks Approach to Resource Allocation for Domestic Counterterrorism

Michael P. Atkinson, Lawrence M. Wein

September 3, 2009

**Corresponding author:** Lawrence M. Wein, Graduate School of Business, 250 Littlefield, 518 Memorial Way, Stanford University, Stanford, CA 94305, lwein@stanford.edu. Tel: 650-724-1676, fax: 650-725-0468

**Acknowledgments:** This research was supported by an Abbott Laboratories Stanford Graduate Fellowship and by grants from the John D. and Catherine T. MacArthur Foundation (Award #02-69383-000-GSS) and the Defense Threat Reduction Agency (DTRA) University Strategic Partnership (Award # DTRA01-03-D0009/0014 to University of New Mexico) in support of a fellowship at the Center for International Security and Cooperation, Stanford University (M.P.A.), and by the Center for Social Innovation, Graduate School of Business, Stanford University (L.M.W.).

---

*Operations Research Department, Naval Postgraduate School, Monterey, CA 93943, mpatkins@nps.edu
†Graduate School of Business, Stanford University, Stanford, CA 94305, lwein@stanford.edu
Abstract

Motivated by the links between terror and crime and the difficulty in directly detecting terror activity, we formulate and solve a resource allocation problem on overlapping networks to determine if interdiction efforts may be able to take advantage of these connections. The government, knowing only the general structure and overlap of the networks, allocates its scarce resources to investigate each terror and criminal network. There are two stages to the investigation: an initial investigation of all nodes (i.e., terrorists or criminals) and a secondary investigation of criminals identified during the initial investigation to determine if they are terrorists. Applying our model to data derived from a population of terrorists in the United States between 1971–2003 suggests that the government may be able to exploit the terror connections of crimes that are relatively uncommon, somewhat easy to detect, and are attractive to terrorists.

Keywords: networks, optimization, counterterrorism
Terrorists carry out many activities leading up to an attack – including meetings to plan the logistics of an operation and surveillance of potential targets – that by their nature are difficult to detect. While some terrorists may avoid criminal activities for reasons of security or ideology (O’Neil, 2007), there are many reasons why they become involved with crime. To carry out an attack, terrorists might need to obtain weapons or explosives (Jordan and Horsburgh, 2005). Terrorists obtain false documents and launder money to obscure their identities (O’Neil, 2007). Funds may be raised through legitimate means (Morselli and Giguere, 2006) or via drug dealing, petty theft, bank robbery, credit card fraud, or selling contraband merchandise (O’Neil, 2007; Jordan and Horsburgh, 2005; Morselli, Giguère, and Petit, 2007; Smith, Damphousse, and Roberts, 2006). The perceived recent increase in the overlap between terror and crime may be due to the decline in the state sponsorship of terror and the decentralization of terror networks (O’Neil, 2007). Terror and criminal networks are covert or dark networks (Raab and Milward, 2003), and therefore face a tradeoff between secrecy and efficiency (Morselli et al., 2007). Criminal networks are primarily profit driven and must sacrifice secrecy for efficiency (Morselli et al., 2007), while terrorists put a higher premium on maintaining secrecy at the expense of efficiency (Morselli et al., 2007; Krebs, 2002).

These observations suggest that there are significant connections between terror and crime, and that the government should find it more difficult to detect terror activities than criminal activities. In this paper, we analyze the overlap among terror and criminal networks to determine if the government can exploit these connections to more effectively identify terrorists. We formulate and solve a mathematical optimization problem in which the government allocates its scarce resources to investigate each criminal and terror network to maximize the number of terrorists it detects. We illustrate the model with data collected from Smith et al. (2006). This dataset consists of 452 terrorists from 54 domestic cases.

RESULTS

The model has three components: the overlapping networks, the investigation process, and the optimization problem. After solving the optimization problem, we illustrate the analysis using domestic terror data.

THE OVERLAPPING NETWORKS. Our model contains one terror network indexed by $k = 1$ and $K - 1$ criminal networks indexed by $k = 2, \ldots, K$. There are $N_k$ nodes in network $k$ that correspond to individuals who take part in terrorist or criminal activities, and the networks overlap because each individual (i.e., node) belongs to a subset of the $K$ networks. We define $(m_1, \ldots, m_K)$ to be the membership vector of an arbitrary node, where $m_k = 0$ if the node is not a member of network $k$ and $m_k = 1$ if the node is in network $k$. The probability a node has a certain membership vector is determined by a multinominal distribution that defines the overlap among the networks.

Each node in network $k$ has a random number $n_k$ of edges in network $k$, and we assume that the degree distribution has finite mean and variance. If a node is in multiple networks, then its degree in one network is independent of its degree in every other network the node belongs to; we discuss how the model changes if we relax this assumption at the end of the paper. However, if two nodes are in the same network, their degrees may be correlated (as in the data analysis in §4.2.3 of the Supporting Information). Activities on each edge in network $k$ occur according to a Poisson process with parameter $\lambda_k$, and we assume a node’s activities occur independently along each of its edges. For example, for a drug dealer network, $N_k$ is the number of drug dealers, $n_k$ is the random number of different people that the dealer sells to, and $\lambda_k$ is the number of drug deals per unit time between the dealer and each person he sells to. In this model, the drug buyers are not included as nodes in the drug dealer network; these drug user (i.e., buyer) nodes are modeled in the drug user network.
That is, in the drug dealer network we need not explicitly model the nodes (i.e., drug users) at the other end of the edges that emanate from a drug dealer node. In contrast, each edge in the terror network connects two of the $N_1$ terrorists, and activities in the terror network are viewed as interactions between terrorists (e.g., meetings to plan an attack).

Because our model is independent of the networks’ structures other than the degree distributions (as explained below equation (1)), we do not need to define an algorithm to generate specific types of networks that are appropriate for our model. Furthermore, it is possible to analyze a broad range of network topologies in our model depending upon the application of interest. For example, the terror network could be scale-free with exponential truncation as in Qin, Xu, Hu, Sageman, and Chen (2005), or it could consist of many disconnected clusters that represent terror cells.

**NETWORK INVESTIGATION.** The government identifies a node in a criminal or terror network by detecting the node taking part in one of the activities described above. The government identifies only the node it is investigating and not the people the node is interacting with; we discuss this issue at the end of the paper. The government investigates each node independently; i.e., if the government investigates a node this week, it is not more likely the government will also investigate that node’s neighbors this week. The government performs two stages of investigation: an initial investigation of the entire set of nodes, and a secondary investigation of the criminal nodes identified during the initial investigation that attempts to determine if these nodes also belong to the terror network (e.g., instead of immediately apprehending these criminals, the government tracks their future behavior).

For the initial investigation of the criminal networks, we consider two budget allotments denoted by $b_k$ and $B_k^I$. Let $b_k$ be the amount of money that is already being allocated to criminal network $k$ for the purpose of investigating criminals, where we set $b_1 = 0$. From the viewpoint of our counterterrorism resource allocation problem, $b_k$ is a sunk cost and is not a
decision variable. However, $b_k$ generates criminals that can undergo a secondary investigation if there is sufficient coordination between crime-fighting and counterterrorism resources, as discussed further below. Let the decision variable $B^I_k$ be the additional budget (i.e., beyond $b_k$) that is allocated to the initial investigation of network $k$ for the sole purpose of detecting terrorists (i.e., the government is not directly rewarded in our optimization problem for identifying additional criminals with $B^I_k$). We assume that the government spends $\frac{b_k + B^I_k}{N_k}$ to investigate each of the $N_k$ nodes in network $k$. Let $\theta^I_k$ be a parameter that determines how efficient the government is at detecting activities in network $k$ during the initial investigation. The parameter $\theta^I_k$ is in units of time/$\$ and incorporates a conversion factor between dollars and investigative man-hours that determines how many man-hours are spent investigating network $k$, as well as the fact that the government will detect only a fraction of the activities during its hours of active investigation (which generates a random thinning of the Poisson process). Also included in the efficiency parameter $\theta^I_k$ is the fraction of resources spent following up on false leads and investigating individuals who are not terrorists or criminals. Although $\theta^I_k$ implicitly accounts for false-positive investigations, our model makes no attempt (partly due to lack of data) to understand the tradeoff between investigative efficiency and false positives, and hence cannot control the false-positive detection rate, as is typical in some detection problems.

Let $Y^I_k$ be the random number of nodes in network $k$ identified during the initial investigation. In (1), the mean of $Y^I_k$ is the product of three factors: the average activity rate in network $k$ ($E[n_k] \lambda_k$), the resources spent on the initial investigation of network $k$ ($b_k + B^I_k$), and the government’s efficiency during the initial investigation of network $k$ ($\theta^I_k$). Under the assumption that the number of nodes in network $k$ ($N_k$) approaches infinity, we show in §1 of the Supporting Information that each node is identified in at most one network
during the initial investigation, and

\[ E[Y^I_k] = \theta^I_k(b_k + B^I_k)E[n_k]\lambda_k. \] (1)

To derive (1), we assume that detection across nodes is independent and the probability of detecting a node depends only on detecting that node interacting with one of its neighbors, which itself is a function of the node’s degree. Because the number of detected nodes is the sum of random variables, the expectation of which is independent of the correlation structure of these random variables, the quantity in (1) is not impacted by degree-degree correlations; hence, there is no need to further specify the network structure beyond the degree distributions.

The government allocates the budget \( B^S_k \) to the secondary investigation of network \( k \) for \( k = 2, \ldots, K \). While in practice extensive secondary investigations are likely to be performed in order to learn the maximum amount about each terrorist cell identified during the initial investigation (Buckley and Rashbaum, 2007), these secondary investigations of the terror network are beyond the scope of this paper; i.e., we are focused on maximizing the number of terrorist cells identified, and ignore how to optimally investigate a terrorist cell after a terrorist in this cell has been identified. Because we view the initial and secondary investigations as ongoing, the budget decisions are made in advance and the government allocates \( \frac{B^S_k}{E[Y^S_k]} \) to each secondary investigation of network \( k \). The government determines that a criminal is a terrorist during the secondary investigation if the government detects this node participating in a terror interaction. A node in the terror network interacts with each of its neighbors according to a Poisson process with parameter \( \lambda_1 \). The government detects the terror interactions during the secondary investigation with efficiency parameter \( \theta^S_1 \).

We define \( T^S_k \) to be the number of terrorists identified during the secondary investigation of network \( k \). In (2), the mean of \( T^S_k \) is equal to the expected number of criminals identified
in network $k$ during the initial investigation ($\mathbb{E}[Y^I_k]$ from (1)) times the probability that a criminal in network $k$ is a terrorist ($P[m_1 = 1 \mid m_k = 1]$) times the probability that the government will detect terror interactions during the secondary investigation ($\mathbb{E}[1 - e^{-\theta^S_{k} \frac{n^S_{k}}{\mathbb{E}[Y^I_{k}]} n_1 \lambda_1}$]). These factors in turn depend upon the allocation between the initial and secondary investigative resources ($b_k + B^I_k$ and $B^S_k$), the total activity rates ($\mathbb{E}[n_k] \lambda_k$), and the investigative efficiencies ($\theta^I_k$ and $\theta^S_1$). In §2 of the Supporting Information, we show that as the number of nodes ($N_k$) tends to infinity,

$$\mathbb{E}[T^S_k] = \mathbb{E}[Y^I_k] P[m_1 = 1 \mid m_k = 1] \mathbb{E}[1 - e^{-\theta^S_{k} \frac{n^S_{k}}{\mathbb{E}[Y^I_{k}]} n_1 \lambda_1}].$$

(2)

Because the assumptions to calculate the values in equations (1)–(2) may break down for large budget allocations, we cap the mean number of nodes detected during the investigation by the actual number of nodes ($N_k$). Therefore, we hereafter replace $\mathbb{E}[Y^I_k]$ with $\min\{\mathbb{E}[Y^I_k], N_k\}$.

**THE OPTIMIZATION PROBLEM.** The government chooses the investigative budgets $B^I_k$ and $B^S_k$ to maximize the expected number of terrorist nodes identified during the investigation, which includes $\min\{\mathbb{E}[Y^I_1], N_1\}$ from the initial investigation plus $\sum_{k=2}^{K} \mathbb{E}[T^S_k]$ from the secondary investigation, subject to a total budget constraint of $B$ dollars. This optimization problem is

$$\max_{B^I_k, B^S_k} \min\{\mathbb{E}[Y^I_1], N_1\} + \sum_{k=2}^{K} \mathbb{E}[T^S_k],$$

(3)

s.t. $B^I_1 + \sum_{k=2}^{K} (B^I_k + B^S_k) = B,$

(4)

$B^I_k \geq 0$ for $k = 1, \ldots, K,$

(5)

$B^S_k \geq 0$ for $k = 2, \ldots, K,$

(6)

where $\mathbb{E}[Y^I_1]$ and $\mathbb{E}[T^S_k]$ are given in (1)–(2). By (1)–(3), the only knowledge of the network structure required by the government to solve this optimization problem is the degree
distribution of the terror network \( (n_1) \), the mean degree of each criminal network \( (\mathbb{E}[n_k]) \) for \( k = 2, \ldots, K \), the number of nodes in each network \( (N_k) \), and the probability that a criminal is a terrorist \( (\mathbb{P}[m_1 = 1 | m_k = 1]) \).

We consider two variants of problem (3)–(6) that differ by the value of \( b_k \) in (1). In the \textit{coordinated} case, we set \( b_k \) equal to the existing resources used to initially investigate criminal network \( k \). In this case, the counterterrorism resources \( B_k^S \) have the ability to perform secondary investigations of all criminals identified via \( b_k \). In the \textit{uncoordinated} case, the secondary investigations do not have access to the criminals identified via \( b_k \) because of the lack of coordination between the law enforcement resources funded by \( b_k \) (e.g., local police or the DEA) and the counterterrorism resources funded by \( B_k^I + B_k^S \) (e.g., FBI). Hence, we set \( b_k = 0 \) in the uncoordinated case.

**SOLUTION TO THE OPTIMIZATION PROBLEM.** The optimization problem is easier to analyze if we transform the decision variables \((B_k^I, B_k^S)\) into the combined budget to investigate each network, \( B_k = B_k^I + B_k^S \), and the fraction of this combined budget the government allocates to the initial investigation, \( \gamma_k = \frac{B_k^I}{B_k} \). After making this transformation, the problem decouples and we can first solve for the optimal \( \gamma_k^* \) in terms of \( B_k \). We write the optimal fraction of resources as \( \gamma_k^*(B_k) \) (defined in equation (42) of the Supporting Information) to explicitly denote its dependence on the budget allocation. After solving for \( \gamma_k^*(B_k) \) for each network, we next solve for the optimal resource allocation across all networks, which we denote by \( B_k^* \). For more details on the solution to the optimization problem, see §3 of the Supporting Information.

The optimal solution is expressed in terms of three intermediate quantities. The first is \( P_k^S(\gamma_k, B_k) \), which is the probability that the government will determine during the secondary investigation that a criminal in network \( k \) is also a terrorist, given that the criminal is a terrorist. The government’s cost-effectiveness during the initial investigation, \( e_k^I \), is the average
number of nodes that the government identifies per dollar spent in the initial investigation of network $k$. The final intermediate quantity is the government’s overall cost-effectiveness, $e_k$, which is the average number of terrorists identified per dollar spent investigating network $k$. $P^S_k(\gamma_k, B_k)$, $e^I_k$, and $e_k$ are defined in equations (41), (43), and (50)–(51) of the Supporting Information, respectively.

The optimization problem simplifies considerably in the uncoordinated case where $b_k = 0$. Both the probability $P^S_k(\gamma_k, B_k)$ and the optimal resource allocation $\gamma^*_k(B_k)$ are independent of $B_k$, and therefore, we write these quantities as $P^S_k(\gamma_k)$ and $\gamma^*_k$ for the uncoordinated case. In this case the main output of the optimization problem is the government’s overall cost-effectiveness $e_k$. The optimal solution for the uncoordinated case is to allocate the entire budget $B$ to the network where the government is most effective at identifying terrorists (i.e., the network with the largest $e_k$). The value of $e_k$ for criminal networks is defined in equation (51) of the Supporting Information and is the product of four factors: the government’s cost-effectiveness during the initial investigation ($e^I_k$), the probability that a criminal is a terrorist ($P[m_1 = 1 | m_k = 1]$), the fraction of the budget allocated to the initial investigation ($\gamma^*_k$), and the likelihood of detecting a criminal as a terrorist in the secondary investigation ($P^S_k(\gamma^*_k)$).

**PARAMETER ESTIMATION.** We describe the parameter estimation procedure in detail in §4 of the Supporting Information. By equations (1)–(3), the parameters in the optimization problem that we need to estimate are the probability that a criminal in network $k$ is a terrorist ($P[m_1 = 1 | m_k = 1]$), the number of nodes in network $k$ ($N_k$), the mean degree of network $k$ ($E[n_k]$), the activity rate over each edge in network $k$ ($\lambda_k$), the efficiency parameter of network $k$ for the initial investigation ($\theta^I_k$), the fixed law enforcement resources allocated to the initial investigation of network $k$ in the coordinated case ($b_k$), the efficiency parameter of the terror network for the secondary investigation ($\theta^S_k$), and the degree distribution of the
terror network ($n_1$).

We use the population of terrorists in the 60 domestic terrorism cases (we aggregate these 60 cases into 54 cases because the same group of people were involved with several different cases) analyzed in Smith et al. (2006), which focuses on the activities (both legal and illegal) terrorists are involved with prior to an attack. Using data from Smith et al. (2006) and supporting court documents, we construct a terror network of 452 terrorists and also determine which of these individuals are involved in various criminal networks. More specifically, although we cannot directly estimate the probabilities $P[m_1 = 1 \mid m_k = 1]$ that a criminal is a terrorist, we know by Bayes’ theorem that

$$
P[m_1 = 1 \mid m_k = 1] = P[k = 1 \mid m_1 = 1] P[m_1 = 1]
$$

(7)

Hence, we indirectly estimate $P[m_1 = 1 \mid m_k = 1]$ by estimating the probability $P[m_k = 1 \mid m_1 = 1]$ that a terrorist is a criminal from the data in Smith et al. (2006). In addition, we estimate $P[m_1 = 1]$ by the number of terrorists in the terrorist network, $N_1$, and estimate $P[m_k = 1]$ by the number of criminals in network $k$, $N_k$). However, our estimate for the number of terrorists ($N_1$) is particularly crude.

We calculate the conditional probabilities $P[m_k = 1 \mid m_1 = 1]$ for 15 different criminal networks (table 4 in the Supporting Information). Because the criminal-terror overlap is small for many of these networks, we restrict our analysis to the six criminal networks with the largest overlap: the explosives network, the illegal firearms distributor network, the illegal firearms user network, the bank robbery network, the false documents distributor network, and the false documents user network. The data from Smith et al. (2006) also allows us to determine which terrorists interact with each other and how frequently they interact, and we estimate $\lambda_1$ and $n_1$ directly from these data.

The remaining parameters are estimated from other data sources. The parameters $\theta^I_k$,
\( E[n_k] \), and \( \lambda_k \) appear in the optimal solution only as the aggregate quantity \( \theta_k \epsilon E[n_k] \lambda_k \), which can be interpreted as the number of criminals or terrorists detected per initial investigative dollar spent in network \( k \). By equation (1), we estimate this aggregate quantity by the ratio \( \hat{Y}_k \epsilon B_k \), where \( \hat{B}_k \) is the annual budget a particular agency (e.g., FBI) allocates to investigate network \( k \) (\( \hat{B}_k \) coincides with \( b_k \) for \( k = 2, \ldots, K \) in the coordinated version of the optimization problem), and \( \hat{Y}_k \) is the number of nodes (i.e., criminals) identified annually (for consistency, we use 2005 data whenever possible). Similarly, by equation (1), the efficiency parameter \( \theta_1 \) is determined via \( \theta_1 \epsilon \frac{\hat{Y}_1}{\hat{B}_1} \epsilon E[n_1] \lambda_1 \). Finally, the parameter \( \theta_S \) is estimated by equating the ratio \( \frac{\theta_1}{\theta_S} \) with the fraction of preliminary terror investigations that lead to legitimate terror investigations.

The estimated parameter values all appear in table 1 except for \( n_1 \), which is given by the empirical distribution appearing in fig. 1 of the Supporting Information.

**Table 1 about here**

**NUMERICAL RESULTS.** We begin with the solution to the uncoordinated case (i.e., \( b_k = 0 \)). Although the overall cost-effectiveness parameters \( e_k \) are the most important numerical output in table 2, we first discuss the various components of \( e_k \) from equations (50)-(51) in the Supporting Information. During the initial investigation, the government is least effective at directly identifying nodes in the terror network (i.e., the terror network has the smallest value of \( \epsilon e_1 \) in table 2), with its effectiveness ranging from a factor of 5 to a factor of 320 lower that those of the criminal networks. This confirms one of the motivating factors of this work: it should be easier to detect criminals than terrorists. Of the six criminal networks, two are very large (false documents user and illegal firearms user), and the other four are much smaller and of nearly identical size. Perhaps not surprisingly, the values of \( e_k \) in table 2 correlate reasonably well with the size of the network; i.e., nodes in larger networks are easier to detect.
The fraction of criminals who are terrorists is small for the two largest networks due to the needle-in-a-haystack effect (equation (7)): e.g., even though 35% of terrorists are illegal firearms users (table 1), this network is very large and so the fraction of illegal firearms users who are terrorists is very small. By (7), for the four smaller networks that are of nearly equal size, their relative value of the probability a criminal is a terrorist is almost completely dictated by the probability a terrorist is a criminal. Overall, the range of $P[m_1 = 1|m_k = 1]$ varies by a factor of 4800, which is much greater than the variation in the initial effectiveness $e_k^I$.

Relative to $e_k^I$ and $P[m_1 = 1|m_k = 1]$, there is little variation in $P^S(\gamma_k^*)$ in table 2 which is consistent with the fact that secondary investigations avoid the needle-in-the-haystack effect. The values of $\gamma_k^*$ are inversely related to $e_k^I$: if the government is not effective at identifying nodes during the initial investigation, then it has to allocate more resources to the initial investigation to compensate for this ineffectiveness.

The government’s overall cost-effectiveness at identifying terrorists ($e_k$ in table 2) is an order of magnitude greater for the four smaller criminal networks (explosives, illegal firearms distributor, bank robbery, and false documents distributor) and the terror network than it is for the two larger criminal networks (illegal firearms user and false documents user). Even though the government is more effective at directly identifying nodes in the larger criminal networks ($e_k^I$), the variation in the overlap probability ($P[m_1 = 1|m_k = 1]$) is nearly two orders of magnitude greater than the variation in $e_k^I$. Therefore, the government’s overall cost-effectiveness is dominated by the overlap probability in table 2. The range of $e_k$ in table 2 is 960, but the range for the five smaller networks is only 12.

The government is most effective at identifying terrorists through the bank robbery network, which has the greatest value of $e_k$ in table 2, although the values of $e_k$ for the terror
and explosives networks are similar to the bank robbery’s $e_k$. The four smaller criminal networks are almost identical in size, but the probability a terrorist in our population is a distributor of illegal firearms or false documents is much smaller than the probability a terrorist is a member of one of the other criminal networks (table 4 in the Supporting Information). Illegal firearms and false documents are tools that a terrorist uses to carry out his plans, and therefore terrorists are much more likely to be users than distributors of these goods. While there is greater overlap between explosives and terror than bank robbery and terror, the government is almost an order of magnitude more effective at identifying bank robbers than it is individuals involved with explosives ($e_k^I$ in table 2).

The optimal solution in the uncoordinated case uses 32% of the counterterrorism budget to investigate the bank robbery network, with a 60-40% split between the initial and secondary investigations. This within-network allocation for the bank robbery network is slightly different than the $\gamma_k^*$ quantity listed in table 2 because the value in table 2 is only valid if the min operators in equations (42)-(43) of the Supporting Information return the first term. At this level of resources, every bank robber is identified in the initial investigation, and the remaining 68% of the budget is devoted to the network that has the second-highest value of $e_k$, which is the terror network.

Turning to the coordinated solution (table 3), we find that it is optimal to spend 25% of the counterterrorism budget investigating the bank robbery network; at this level of resources, all bank robbers are detected in the initial investigation. Within the bank robbery network, resources are almost evenly divided between the secondary investigations and the additional (i.e., beyond $b_k$) initial investigations. Nearly all of the remaining total counterrorism budget is used to investigate the terror network, and a small fraction (1% each) of the budget is also used to perform secondary investigations of illegal firearms distributors and the explosives network.
The current $1.4B counterterrorism budget detects 824 terrorists in the coordinated version of the problem, with one-third of them caught via the criminal networks (one-third of the 54 cases in Smith et al. (2006) were also caught via the criminal networks). If we set $B = 1.4B$ in the uncoordinated version of the problem, the solution leads to the detection of 748 terrorists (table 2); i.e., coordination leads to a 10% increase in the number of detected terrorists. If the $1.4B was restricted to being used solely in the terror network, then 700 terrorists would be detected.

We also solved the two versions of the problem for other budget values (fig. 1). In the uncoordinated case, the government uses its first $0.4B to investigate the bank robbery network and then allocates the remaining money to the terror network. The number of detected terrorists is piecewise linear and concave in the budget, with the slope equaling the $e_k$ value of the network receiving the marginal budget. For very small budgets in the coordinated case, the government relies on the existing initial investigations of criminal networks and all counterterrorism resources are allocated to the secondary investigation of the network according to their overlap probability, $P[m_1 = 1|m_k = 1]$ (in this case, explosives, then bank robbery, then illegal firearm distributors). Eventually, the government has enough resources to perform additional initial investigations, which are allocated in the order of overall cost-effectiveness (bank robbery, then terror network). The solution to the two cases become more similar as the budget increases.

**SENSITIVITY ANALYSES.** We perform three variations of our analysis in §5 of the Supporting Information. The terrorist population in our study is partitioned into four categories by Smith et al. (2006): right-wing, left-wing, single issue, and international (§5.1 and tables 1 and 2 of the Supporting Information). We estimate the terror parameters and compute the optimal uncoordinated solution for each category, and the results (§5.1 and table 7
of the Supporting Information) are similar to the results in table 2. The main difference between table 2 and table 7 of the Supporting Information is that the terror network has the largest value of \( e_k \) for all four categories in table 7 of the Supporting Information. This is because the probability a criminal is a specific type of terrorist is smaller than the probability of being a terrorist in general. These calculations also suggest that our results are quite insensitive to the degree distribution \( n_1 \) of the terror network (§5.1 of the Supporting Information).

We also vary the secondary efficiency parameter \( \theta^S_1 \), which is difficult to estimate from data and which plays a pivotal role in whether terrorists can effectively be identified via their criminal activities. Even after varying \( \theta^S_1 \) by two orders of magnitude in each direction, the networks with the four smallest values of \( e_k \) in table 2 maintain their relative rankings (table 8 of the Supporting Information). However, for the networks with the three largest values of \( e_k \) in table 2, there is some variation with their relative rankings.

We do not have enough information to estimate confidence intervals for the \( e_k \) values in table 2. However, to illustrate how the uncertainty in the parameter values affects \( e_k \), we use the standard errors for the conditional probabilities in the second column of table 1 and assume the other parameter values are normally distributed with coefficients of variation equal to 0.3, and then generate one million simulated values of \( e_k \) (§5.3 of the Supporting Information). The simulation results show that the \( e_k \) rankings in table 2 are fairly robust for this level of parameter value uncertainty.

Although our most imprecise parameter estimate is the number of terrorists \( (N_1) \), the criminal \( e_k \)'s are linear in \( N_1 \), and hence \( N_1 \) has no impact in the relative rankings of the criminal networks. However, \( e_1 \) is independent of \( N_1 \), and so the value of \( N_1 \) does influence the relative effectiveness of investigating criminal networks compared to directly investigating the terror network. In summary, the sensitivity analyses suggest that the relative rankings
DISCUSSION

RELATED WORK. While there have been studies on mathematical networks of terrorist cells (see Jordan and Horsburgh, 2005; Krebs, 2002; Qin et al., 2005; Rodríguez, 2005; Ressler, 2006; Gutfraind, 2008; Farley, 2003) and work on the connections between crime and terror in the political science, sociology, and criminology fields (e.g., Hamm, 2005; Dishman, 2005; Hutchinson and O’Malley, 2007), including several empirical studies (Smith et al., 2006; Hamm, 2005; Smith, Cothren, Roberts, and Damphousse, 2008; Smith and Damphousse, 2002), we are not aware of any mathematical network studies of the crime-terror nexus. Our overlapping networks model has some similarities to several existing models, but the orientation is much different; e.g., while our focus is on explicitly optimizing centralized network interdiction, the goals in Palla, Derenyi, Farkas, and Vicsek (2005) and Watts, Dodds, and Newman (2002), respectively, are to uncover the overlapping network structure and to perform efficient decentralized search in an overlapping network model.

In addition, our problem is loosely related to two other problems that are concerned with hidden populations: capture-recapture models and contact-tracing models. While we are concerned with maximizing the number of individuals identified in a hidden population, capture-recapture models are used to estimate the size of a hidden population by repeatedly sampling the population (e.g., wildlife populations) with replacement and comparing the number of new captures with repeat captures at each sample (Nichols, 1992); this approach may not be useful in estimating the size of the networks in our model because captured terrorists and criminals are not likely to be released. Contact tracing is used to reduce disease transmission by determining who an infected person has had contact with. Contact tracing models (see Müller, Kretzschmar, and Dietz, 2000; Kaplan, Craft, and Wein, 2003)
have the added complication of being embedded in a dynamic disease transmission model (although these do not employ overlapping networks), whereas in our model the tracing (i.e., interdiction) is the ultimate objective.

**RESULTS.** The main goal of this investigation is to determine the characteristics of a criminal network that would allow the government to effectively exploit its terror connections. In particular, the data caveats discussed below (including the fact that much of the data in the counterterrorism field is classified) precludes us from making specific recommendations for how the government should allocate its domestic counterterrorism resources. However, we have developed a new mathematical framework for thinking about these issues and our empirical results suggest that the possibility of more effectively catching terrorists via their precursor criminal activities is worthy of serious consideration. Nonetheless, due to the secretive nature of this problem domain, we must leave it to government counterterrorism analysts to assess this study’s usefulness.

Turning to our generic results, the key output of the model in the uncoordinated case is $e_k$, which is the number of terrorists detected per investigative dollar. Examination of this quantity in equation (51) of the Supporting Information reveals that the cost-effectiveness of identifying terrorists in each criminal network depends upon three factors: the cost-effectiveness of identifying criminals during the initial investigation, the probability that a criminal is a terrorist, and the effectiveness of the secondary investigation. However, our empirical analysis suggests that the cost-effectiveness is dominated by the probability that a criminal is a terrorist, and to a lesser extent by the effectiveness of the initial investigation (because in Table 2 the variation in $P[m_k = l|m_1 = 1]$ is 1-2 orders of magnitude greater than the variation in $e^I_k$, which in turn is much greater than the variation in $\gamma_k^* P_k^S(\gamma_k^*)$), and that both of these factors are partly determined by the size of the criminal network, with smaller criminal networks generating greater effectiveness. This suggests that the government should
focus on identifying crimes that are relatively obscure, somewhat easy to detect, and have appeal to terrorists. In our empirical study, the bank robbery network ranks highest because it possesses all three characteristics, while explosives ranks next highest among criminal network because it possesses two of the three characteristics (it is not as easy to detect as bank robberies). In contrast, while terrorists are reasonably likely to use illegal firearms and false documents in our empirical study, these network are too large to exploit in a cost-effective manner.

When the counterterrorism resources are allowed to piggyback on the existing crime-fighting resources, the government increases the number of terrorists detected by 10% relative to the uncoordinated case. For realistic budget values, the overall effectiveness $e_k$ again dictates which networks to investigate, although in this coordinated case a lower fraction (48% vs 60%) of the bank robbery budget is allocated to the initial investigation. In practice, the degree of coordination has improved in the last decade (O’Neil, 2007), but there is still often more conflict than cooperation among different parts of the government (Stockton, 2009), and neither of the extreme cases (full coordination and no coordination) is realistic. Several issues would need to be addressed before the government could implement a fully coordinated criminal and counterterrorism program. A high degree of cooperation and communication among state, local and federal authorities (O’Neil, 2007), as well as among the various federal agencies, would be required. An assessment would be needed as to how the core focus and duties of police and other governmental agencies may suffer if their role is expanded to be part of a larger counterterrorism effort (Stockton, 2009).

**DATA CAVEATS.** The primary reason why our empirical study cannot directly inform current counterterrorism policy is that the terror population from Smith et al. (2006) is vastly different than the current relevant terror population. The terror population in this study is from 1971–2003 and includes several categories of terrorism (e.g., left-wing and
environmental) that may not be as much of a concern now or in the future as other types of terrorism (e.g., Islamic Jihad). Indeed, the time span of our empirical data is longer than the time scale over which these operations evolve; however, a temporal analysis (data not shown) of the data from Smith et al. (2006) was not fruitful due to the low frequency rate of terror attacks. Furthermore, the cases in Smith et al. (2006) may not be representative of the terrorists active between 1971–2003 for two reasons. First, there could be selection bias; e.g., perhaps larger terror cells, or terrorists of certain types (e.g., right-wing terrorists appear to be less professional than left-wing terrorists in our study) were easier to detect during this time period. Second, this study selects cases for analysis based upon the availability of sources, and thus the “ability to infer to all terrorists groups is negatively affected” (Smith et al., 2006).

Court documents provide a valuable source to determine which nodes interact with each other and how frequently, but we were unable to gain access to court documents for every case in our data set (§4.1 in the Supporting Information). However, even if we did have court documents for each case, they are not perfect sources for our analysis. The purpose of the court documents is not to provide a detailed account of a terrorist group, and the interactions captured in the court documents represent only a fraction of the activity that actually occurred. While it is tempting to view our estimates of the degree distribution $n_1$ and the frequency $\lambda_1$ in the terror network as lower bounds on the true values, this data censoring could be offset by the selection bias mentioned above.

Another shortcoming of the data is that the specific information needed to estimate the parameters in table 1 does not always exist (or we could not find them). We assume that the data used to estimate $\hat{Y}_k^I$ and $\hat{B}_k^I$ correspond to values from an initial investigation, but this may not be an accurate assumption; data separated by initial vs. secondary investigation would be helpful. Furthermore, we assume all authorities (state, local, and federal) have the
same parameters values. In reality, each agency has its own abilities and efficiencies that determine the agency’s investigative effectiveness for each network. Finally, several of the parameters values in table 1 are derived from assumptions and approximations and are not precise estimates. In particular, the size of the terror network $N_1$ (§4.2.4 in the Supporting Information) and the parameters for users and distributors of false documents (§4.3.4 in the Supporting Information) are rough estimates.

MODEL EXTENSIONS. One limitation of our model is that it fails to allow the terrorists to modify their participation in criminal activities based upon the government’s budget allocation. However, this failure to model the problem in a game-theoretic framework is not as big a concern in our model as it is in other homeland security applications where the budget allocations are more public (e.g., homeland security budget allocations to state governments for protecting critical infrastructure are publicly available - here there is no reason to expect the budget allocation to be made public), and furthermore because the intelligence tracking of individual terrorists and criminals is covert, the effort expended by government agents will be difficult to observe. Nonetheless, one could embed our model into a Stackelberg game (Gibbons, 1992) in which the government makes budget allocation decisions and then the terrorists observe information about this allocation and decide which precursor criminal activities to participate in. A challenge with this model extension is to determine the terrorists’ objective function, which would require data that might be difficult to obtain even in the classified arena.

In such a formulation, the terrorists may require certain types of assets (a weapon, some money, identification documents), and the terrorists may have several legal and illegal ways of obtaining each type of asset. An optimal budget allocation would equalize the net benefit (e.g., the likelihood of success, perhaps minus the cost, if this varies widely across options) of each option to the terrorist. Consequently, a game-theoretic formulation would cause the
government to focus more on criminal activities for which few viable options exist (e.g., false
documents, money laundering, explosives) and less in, e.g., money-making activities (e.g.,
drug dealing) for which safer options exist (note that in the data set we use from Smith et al.
(2006), the bank robberies come from a handful of cases during the early 1980s and are not
representative of the criminal activities of today’s terror population).

A more realistic game would include multiple time periods and would allow terrorists
to update their estimates of the government’s resource allocations indirectly only via the
apprehension of associated terrorists (this local information may not be a reliable signal
about the global resource allocation). Perhaps the most beneficial aspect of a dynamic model
would be to examine how the government could influence the terrorists’ beliefs about the
government’s resource allocation (e.g., by spreading false information about counterterrorism
operations) so that the terrorists update their parameters in a manner that is beneficial to
the government.

We assume that if a node belongs to multiple networks, its degree in one network is
independent of its degrees in all other networks. Consequently, the last term in equation (2)
is an expectation with respect to the terror network degree distribution $P[n_1 = r]$. If there
are correlations between a node’s degree in the terror network and its degree in network $k$,
then the the last term in (2) would be computed with respect to the degree distribution
defined by $P[n_1 = r]E[n_k | n_1 = r]$ (the steps to show this are similar to the analysis in §2 of
the Supporting Information). If this conditional degree distribution is known, then the last
term in equation (2) can be appropriately modified, but the ensuing analysis will remain the
same.

In our model, the government identifies only the node it is directly investigating during
the initial investigation and not the neighbors that the node is interacting with. In practice,
the government may sometimes also identify the neighbor when it detects an interaction.
Asymptotically, the government will detect a node taking part in at most one interaction during the initial investigation (the steps to show this are similar to the analysis in §1 of the Supporting Information). Therefore, the number of criminals and terrorists identified during the initial investigation would be multiplied by two if the neighbor is also identified during an interaction.

On a related note, during the secondary investigations in our model, the government could determine not only other networks that nodes belong to, but also neighbors of nodes. Our model could, in theory, allow the government to walk through the network in this way identifying neighbors-of-neighbors-of-neighbors . . . of a node originally detected in the initial investigation (akin to tracing contacts-of-contacts in §4.2 of Kaplan et al. (2003)). However, this would greatly complicate the analysis (e.g., accounting for clustering and degree correlations within the networks) and require much more data about the overlap distribution and would lead to strategies that consume an unrealistically high level of detection resources.

In our model, the government cannot identify isolated nodes in a network; hence, an isolated terrorist node could never be apprehended as a terrorist, even if he was detected participating in criminal networks. To partially address this shortcoming, we could add nonhuman nodes to the terror network that represent the target (e.g., so that the interaction is surveillance of the target).

Another shortcoming of our model is the assumption that the number of identified nodes is linear in the budget. This relationship would be concave for large budgets due to decreasing marginal returns, and could be convex for very small budgets due to economies of scale. While a smoother nonlinear relationship than the capping by $N_k$ used in equation (3) would change the quantitative solution to our optimization problem, it would not affect the model’s basic qualitative behavior.
References


Table 1: Parameter Estimates. These parameters are the probability that a terrorist is in a given criminal network \( P[m_k = 1 \mid m_1 = 1] \), the network size \( N_k \), the mean of the degree distribution of the terror network \( \mathbb{E}[n_1] \), the annual interaction rate of the terror network \( \lambda_1 \), the efficiency parameters for the terror network \( \theta^I_1 \) and \( \theta^S_1 \), and the mega-parameter \( \theta^I_k \mathbb{E}[n_k] \lambda_k \), which is the cost-effectiveness of the initial investigation (defined as \( e^I_k \) in equation (43) in the Supporting Information).
\[
N_k \quad e_k^I \quad P[m_1 = 1 | m_k = 1] \quad \gamma_k^* \quad P_S(\gamma_k^*) \quad e_k \quad \frac{B_k}{\bar{B}} \quad \text{Terrorists Detected}
\]

| Network                | \(N_k\) | \(e_k^I\) | \(P[m_1 = 1 | m_k = 1]\) | \(\gamma_k^*\) | \(P_S(\gamma_k^*)\) | \(e_k\) | \(\frac{B_k}{\bar{B}}\) | \(\text{Terrorists Detected}\) |
|------------------------|---------|-----------|-------------------------|--------------|---------------------|-------|----------------|-------------------------------|
| Terror                 | \(2 \times 10^3\) | \(5.00 \times 10^{-7}\) | – | – | – | 5.00 \(\times 10^{-7}\) | 0.68 | 478 |
| Explosives             | \(6 \times 10^1\) | \(2.42 \times 10^{-6}\) | 1.5 \(\times 10^{-1}\) | 0.84 | 0.76 | 2.31 \(\times 10^{-7}\) | 0 | 0 |
| Illegal Firearms User  | \(2 \times 10^6\) | \(2.88 \times 10^{-5}\) | 3.5 \(\times 10^{-4}\) | 0.58 | 0.55 | 3.19 \(\times 10^{-9}\) | 0 | 0 |
| Illegal Firearms Distributor | \(6 \times 10^1\) | \(7.03 \times 10^{-6}\) | 2.1 \(\times 10^{-2}\) | 0.74 | 0.68 | 7.62 \(\times 10^{-8}\) | 0 | 0 |
| Bank Robbery           | \(5 \times 10^1\) | \(1.88 \times 10^{-5}\) | 8.7 \(\times 10^{-2}\) | 0.63 | 0.59 | 6.11 \(\times 10^{-7}\) | 0.32 | 270 |
| False Documents User   | \(10^7\) | \(1.60 \times 10^{-4}\) | 3.1 \(\times 10^{-5}\) | 0.36 | 0.35 | 6.36 \(\times 10^{-10}\) | 0 | 0 |
| False Documents Distributor | \(5 \times 10^3\) | \(1.31 \times 10^{-5}\) | 8.8 \(\times 10^{-3}\) | 0.68 | 0.63 | 4.89 \(\times 10^{-8}\) | 0 | 0 |

Table 2: Numerical results for the uncoordinated case. The primary output is the overall cost-effectiveness \(e_k\). Also included are the network size \((N_k)\), the cost-effectiveness of the initial investigation \((e_k^I)\), the probability that a criminal is a terrorist \((P[m_1 = 1 | m_k = 1])\), and the probability that a terrorist is detected during the secondary investigation \((P_S(\gamma_k^*))\). The optimal solution is given by the fraction of the budget used for the initial investigation \((\gamma_k^*)\) and the fraction of the total budget allocated to each network \((\frac{B_k}{\bar{B}})\). The last column gives the number of terrorists identified in each network for a budget of $1.4B.
Table 3: Numerical results for the coordinated case. The original budget for the initial investigations in the criminal networks is $b_k$. The optimal solution is given by the fraction of the budget used for the initial investigation ($\gamma_k^*(B_k^*)$) and the fraction of the total budget allocated to each network ($\frac{B_k^*}{B}$). The last column gives the number of terrorists identified in each network for a budget of $1.4B$.

<table>
<thead>
<tr>
<th>Network</th>
<th>$b_k$</th>
<th>$\gamma_k^<em>(B_k^</em>)$</th>
<th>$P^S_k(\gamma_k^<em>, B_k^</em>)$</th>
<th>$\frac{B_k^*}{B}$</th>
<th>Terrorists Detected</th>
</tr>
</thead>
<tbody>
<tr>
<td>Terror</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>0.73</td>
<td>511</td>
</tr>
<tr>
<td>Explosives</td>
<td>$1.19 \times 10^8$</td>
<td>0</td>
<td>0.69</td>
<td>0.01</td>
<td>30</td>
</tr>
<tr>
<td>Illegal Firearms User</td>
<td>$3.18 \times 10^8$</td>
<td>–</td>
<td>–</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Illegal Firearms Distributor</td>
<td>$2.73 \times 10^8$</td>
<td>0</td>
<td>0.31</td>
<td>0.01</td>
<td>13</td>
</tr>
<tr>
<td>Bank Robbery</td>
<td>$10^8$</td>
<td>0.48</td>
<td>0.62</td>
<td>0.25</td>
<td>270</td>
</tr>
<tr>
<td>False Documents User</td>
<td>$5 \times 10^8$</td>
<td>–</td>
<td>–</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>False Documents Distributor</td>
<td>$10^8$</td>
<td>–</td>
<td>–</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
Figure Legends

**Fig. 1.** The solution to the (a) uncoordinated and (b) coordinated versions of problem (3)–(6) for varying budget levels. The right vertical axis measures the optimal number of terrorists identified (⋯) and the number of terrorists identified if the entire $1.4B budget is allocated to investigating the terror network (*). The left vertical axis measures the fraction of the total budget $B$ allocated to the initial (—) and secondary (−−−) investigations for the terror network (black), the bank robbery network (red), the explosives network (green) and the illegal firearms distribution network (blue).
Figure 1: