

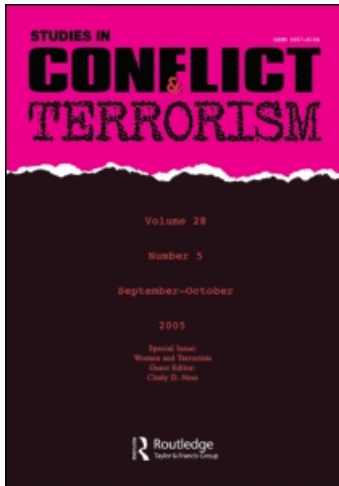
This article was downloaded by: [Stanford University]

On: 1 July 2010

Access details: Access Details: [subscription number 917268594]

Publisher Routledge

Informa Ltd Registered in England and Wales Registered Number: 1072954 Registered office: Mortimer House, 37-41 Mortimer Street, London W1T 3JH, UK



Studies in Conflict & Terrorism

Publication details, including instructions for authors and subscription information:

<http://www.informaworld.com/smpp/title~content=t713742821>

An Overlapping Networks Approach to Resource Allocation for Domestic Counterterrorism

Michael P. Atkinson^a; Lawrence M. Wein^b

^a Operations Research Department, Naval Postgraduate School, Monterey, CA, USA ^b Graduate School of Business, Stanford University, Stanford, CA, USA

Online publication date: 21 June 2010

To cite this Article Atkinson, Michael P. and Wein, Lawrence M.(2010) 'An Overlapping Networks Approach to Resource Allocation for Domestic Counterterrorism', *Studies in Conflict & Terrorism*, 33: 7, 618 — 651

To link to this Article: DOI: 10.1080/1057610X.2010.484028

URL: <http://dx.doi.org/10.1080/1057610X.2010.484028>

PLEASE SCROLL DOWN FOR ARTICLE

Full terms and conditions of use: <http://www.informaworld.com/terms-and-conditions-of-access.pdf>

This article may be used for research, teaching and private study purposes. Any substantial or systematic reproduction, re-distribution, re-selling, loan or sub-licensing, systematic supply or distribution in any form to anyone is expressly forbidden.

The publisher does not give any warranty express or implied or make any representation that the contents will be complete or accurate or up to date. The accuracy of any instructions, formulae and drug doses should be independently verified with primary sources. The publisher shall not be liable for any loss, actions, claims, proceedings, demand or costs or damages whatsoever or howsoever caused arising directly or indirectly in connection with or arising out of the use of this material.

An Overlapping Networks Approach to Resource Allocation for Domestic Counterterrorism

MICHAEL P. ATKINSON

Operations Research Department
Naval Postgraduate School
Monterey, CA, USA

LAWRENCE M. WEIN

Graduate School of Business
Stanford University
Stanford, CA, USA

Motivated by the links between terror and crime and the difficulty in directly detecting terror activity, this article formulates and solves 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 the 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.

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

Received 4 September 2009; accepted 18 November 2009.

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.).

Supporting material can be found in the Online Appendix located at http://faculty-gsb.stanford.edu/wein/personal/documents/terror_network-appendix-sct.pdf

Address correspondence to Lawrence M. Wein, Graduate School of Business, 518 Memorial Way, Stanford University, Stanford, CA 94305, USA. E-mail: lwein@stanford.edu

Giguère 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, Giguère, and Petit 2007). Criminal networks are primarily profit driven and must sacrifice secrecy for efficiency (Morselli, Giguère, and Petit 2007), while terrorists put a higher premium on maintaining secrecy at the expense of efficiency (Morselli, Giguère, and Petit 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. This article analyzes the overlap among terror and criminal networks to determine if the government can exploit these connections to more effectively identify terrorists. The authors 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. The model is illustrated with data collected from Smith, Damphousse, and Roberts (2006). This dataset consists of 452 terrorists from 54 domestic cases during 1971–2003. In the next section the model is described; the third section estimates the model parameters; the fourth section presents the results; and the fifth section is the conclusion.

Model

The model has three components: the overlapping networks, the investigation process, and the optimization problem.

The Overlapping Networks

The model contains one terror network indexed by $k = 1$ and $K - 1$ criminal networks indexed by $k = 2, \dots, K$. 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. (m_1, \dots, m_K) is defined 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 multinomial 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 it is assumed 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; how the model changes if this assumption is relaxed is discussed at the end of the article. However, if two nodes are in the same network, their degrees may be correlated (as in the data analysis in a later section). Activities on each edge in network k occur according to a Poisson process with parameter λ_k , and it is assumed that 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 λ_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 one 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 the model is independent of the networks' structures other than the degree distributions (as explained below Equation (1)), there is no need to define an algorithm to generate specific types of networks that are appropriate for the model. Furthermore, it is possible to analyze a broad range of network topologies in the model depending on the application of interest. For example, the terror network could be scale-free with exponential truncation as in Qin et al. (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 earlier. The government identifies only the node it is investigating and not the people the node is interacting with; this issue is discussed at the end of the article. The government investigates each node independently; that is, 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, two budget allotments are considered, 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 $b_1 = 0$. From the viewpoint of the 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_k^I 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 the optimization problem for identifying additional criminals with B_k^I). It is assumed that the government spends $\frac{b_k + B_k^I}{N_k}$ to investigate each of the N_k nodes in network k . Let θ_k^I be a parameter that determines how efficient the government is at detecting activities in network k during the initial investigation. The parameter θ_k^I 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 θ_k^I is the fraction of resources spent following up on false leads and investigating individuals who are not terrorists or criminals. Although θ_k^I implicitly accounts for false-positive investigations, the 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_k^I be the random number of nodes in network k identified during the initial investigation. In Equation (1), the mean of Y_k^I is the product of three factors: the average

activity rate in network k ($\mathbf{E}[n_k]\lambda_k$), the resources spent on the initial investigation of network k ($b_k + B_k^I$), and the government's efficiency during the initial investigation of network k (θ_k^I). Under the assumption that the number of nodes in network k (N_k) approaches infinity, it is shown in section 1 of the Online Appendix that each node is identified in at most one network during the initial investigation, and

$$\mathbf{E}[Y_k^I] = \theta_k^I (b_k + B_k^I) \mathbf{E}[n_k] \lambda_k. \quad (1)$$

To derive Equations (1), it is assumed 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 Equation (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_k^S to the secondary investigation of network k for $k = 2, \dots, K$. 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 article; that is, the focus is on maximizing the number of terrorist cells identified, and the analysis ignores how to optimally investigate a terrorist cell after a terrorist in this cell has been identified. Because the initial and secondary investigations are viewed as ongoing, the budget decisions are made in advance and the government allocates $\frac{B_k^S}{\mathbf{E}[Y_k^I]}$ 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 λ_1 . The government detects the terror interactions during the secondary investigation with efficiency parameter θ_1^S .

T_k^S is defined to be the number of terrorists identified during the secondary investigation of network k . In Equation (2), the mean of T_k^S is equal to the expected number of criminals identified in network k during the initial investigation ($\mathbf{E}[Y_k^I]$ from Equation (1)) times the probability that a criminal in network k is a terrorist ($\mathbf{P}[m_1 = 1 | m_k = 1]$) times the probability that the government will detect terror interactions during the secondary investigation ($\mathbf{E}[1 - e^{-\theta_1^S \frac{B_k^S}{\mathbf{E}[Y_k^I]} n_1 \lambda_1}]$). These factors in turn depend on the allocation between the initial and secondary investigative resources ($b_k + B_k^I$ and B_k^S), the total activity rates ($\mathbf{E}[n_k]\lambda_k$), and the investigative efficiencies (θ_k^I and θ_1^S). In section 2 of the Online Appendix, it is shown that as the number of nodes (N_k) tends to infinity,

$$\mathbf{E}[T_k^S] = \mathbf{E}[Y_k^I] \mathbf{P}[m_1 = 1 | m_k = 1] \mathbf{E}\left[1 - e^{-\theta_1^S \frac{B_k^S}{\mathbf{E}[Y_k^I]} n_1 \lambda_1}\right]. \quad (2)$$

Because the assumptions to calculate the values in Equations (1)–(2) may break down for large budget allocations, the mean number of nodes detected during the investigation is capped by the actual number of nodes (N_k). Therefore, $\mathbf{E}[Y_k^I]$ is hereafter replaced with $\min\{\mathbf{E}[Y_k^I], N_k\}$.

The Optimization Problem

Formulation of the Optimization Problem. The government chooses the investigative budgets B_k^I and B_k^S to maximize the expected number of terrorist nodes identified during the investigation, which includes $\min\{\mathbf{E}[Y_1^I], N_1\}$ from the initial investigation plus $\sum_{k=2}^K \mathbf{E}[T_k^S]$ from the secondary investigation, subject to a total budget constraint of B dollars. This optimization problem is

$$\max_{B_k^I, B_k^S} \min\{\mathbf{E}[Y_1^I], N_1\} + \sum_{k=2}^K \mathbf{E}[T_k^S], \quad (3)$$

$$\text{s.t. } B_1^I + \sum_{k=2}^K (B_k^I + B_k^S) = B, \quad (4)$$

$$B_k^I \geq 0 \text{ for } k = 1, \dots, K, \quad (5)$$

$$B_k^S \geq 0 \text{ for } k = 2, \dots, K, \quad (6)$$

where $\mathbf{E}[Y_1^I]$ and $\mathbf{E}[T_k^S]$ are given in Equations (1)–(2). By Equations (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 ($\mathbf{E}[n_k]$ for $k = 2, \dots, K$), the number of nodes in each network (N_k), and the probability that a criminal is a terrorist ($\mathbf{P}[m_1 = 1 \mid m_k = 1]$).

Two variants of problem Equations (3)–(6) are considered that differ by the value of b_k in Equation (1). In the *coordinated* case, the authors 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 *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 Drug Enforcement Administration [DEA]) and the counterterrorism resources funded by $B_k^I + B_k^S$ (e.g., Federal Bureau of Investigation [FBI]). Hence, $b_k = 0$ in the uncoordinated case.

Solution to the Optimization Problem. The optimization problem is easier to analyze if the decision variables (B_k^I, B_k^S) are transformed 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 one can first solve for the optimal γ_k^* in terms of B_k . The optimal fraction of resources is written as $\gamma_k^*(B_k)$ (defined in Equation (42) of the Online Appendix) to explicitly denote its dependence on the budget allocation. After solving for $\gamma_k^*(B_k)$ for each network, the analysis next solves for the optimal resource allocation across all networks, which is denoted by B_k^* . For more details on the solution to the optimization problem, see section 3 of the Online Appendix.

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 . $P_k^S(\gamma_k, B_k)$, e_k^I , and e_k are defined in Equations (41), (43), and (50)–(51) of the Online Appendix, respectively.

The optimization problem simplifies considerably in the uncoordinated case where $b_k = 0$. Both the probability $P_k^S(\gamma_k, B_k)$ and the optimal resource allocation $\gamma_k^*(B_k)$ are independent of B_k , and therefore, these quantities are written as $P_k^S(\gamma_k)$ and γ_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 Online Appendix and is the product of four factors: the government's cost-effectiveness during the initial investigation (e_k^I), the probability that a criminal is a terrorist ($\mathbf{P}[m_1 = 1 \mid m_k = 1]$), the fraction of the budget allocated to the initial investigation (γ_k^*), and the likelihood of detecting a criminal as a terrorist in the secondary investigation ($P_k^S(\gamma_k^*)$).

Parameter Estimation

This section estimates the model parameters. By Equations (1)–(3), the parameters in the optimization problem that need to be estimated are the probability that a criminal in network k is a terrorist ($\mathbf{P}[m_1 = 1 \mid m_k = 1]$), the number of nodes in network k (N_k), the mean degree of network k ($\mathbf{E}[n_k]$), the activity rate over each edge in network k (λ_k), the efficiency parameter of network k for the initial investigation (θ_k^I), 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 (θ_1^S), and the degree distribution of the terror network (n_1).

The authors do not directly estimate the probabilities $\mathbf{P}[m_1 = 1 \mid m_k = 1]$, but instead use Bayes's theorem:

$$\mathbf{P}[m_1 = 1 \mid m_k = 1] = \mathbf{P}[m_k = 1 \mid m_1 = 1] \frac{\mathbf{P}[m_1 = 1]}{\mathbf{P}[m_k = 1]}. \quad (7)$$

Hence, $\mathbf{P}[m_1 = 1 \mid m_k = 1]$ is indirectly estimated by estimating the probability $\mathbf{P}[m_k = 1 \mid m_1 = 1]$ that a terrorist is a criminal. In addition, $\frac{\mathbf{P}[m_1 = 1]}{\mathbf{P}[m_k = 1]}$ is estimated by comparing the relative sizes of the networks (i.e., $\mathbf{P}[m_1 = 1]$ is estimated by the number of terrorists in the terrorist network, N_1 , and $\mathbf{P}[m_k = 1]$ is estimated by the number of criminals in network k , N_k). However, the estimate for the number of terrorists (N_1) is particularly crude. Furthermore, the parameters θ_k^I , $\mathbf{E}[n_k]$, and λ_k appear in the optimal solution only as the aggregate quantity $\theta_k^I \mathbf{E}[n_k] \lambda_k$, which can be interpreted as the number of criminals or terrorists detected per initial investigative dollar spent in network k . Therefore, the product $\theta_k^I \mathbf{E}[n_k] \lambda_k$ is estimated rather than the individual factors.

The estimated parameter values all appear in Table 1 except for n_1 , which is given by the empirical distribution appearing in Figure 1.

The main data source is a report entitled *Pre-Incident Indicators of Terrorist Incidents* (Smith, Damphousse, and Roberts 2006) and is described in the next section. The terror parameters and the criminal parameters are then estimated in subsequent sections.

Table 1
Parameter estimates

Network	$\mathbf{P}[m_k = 1 m_1 = 1]$	N_k	$E[n_1]$	λ_1	θ_1^I	θ_1^S	$\theta_k^I \mathbf{E}[n_k] \lambda_k$
Terror	1	2000	5.09	5.5×10^{-2}	1.79×10^{-6}	1.79×10^{-4}	5.00×10^{-7}
Explosives	0.451	6000	—	—	—	—	2.42×10^{-6}
Illegal Firearms User	0.350	2×10^6	—	—	—	—	2.88×10^{-5}
Illegal Firearms Distributor	0.064	6000	—	—	—	—	7.03×10^{-6}
Bank Robbery	0.217	5000	—	—	—	—	1.88×10^{-5}
False Documents User	0.155	10^7	—	—	—	—	1.60×10^{-4}
False Documents Distributor	0.022	5000	—	—	—	—	1.31×10^{-5}

Note: These parameters are the probability that a terrorist is in a given criminal network ($\mathbf{P}[m_k = 1 | m_1 = 1]$), the network size (N_k), the mean of the degree distribution of the terror network ($E[n_1]$), the annual interaction rate of the terror network (λ_1), the efficiency parameters for the terror network (θ_1^I and θ_1^S), and the megaparameter $\theta_k^I \mathbf{E}[n_k] \lambda_k$, which is the cost-effectiveness of the initial investigation (defined as E_k^I in equation (43) in the Online Appendix).

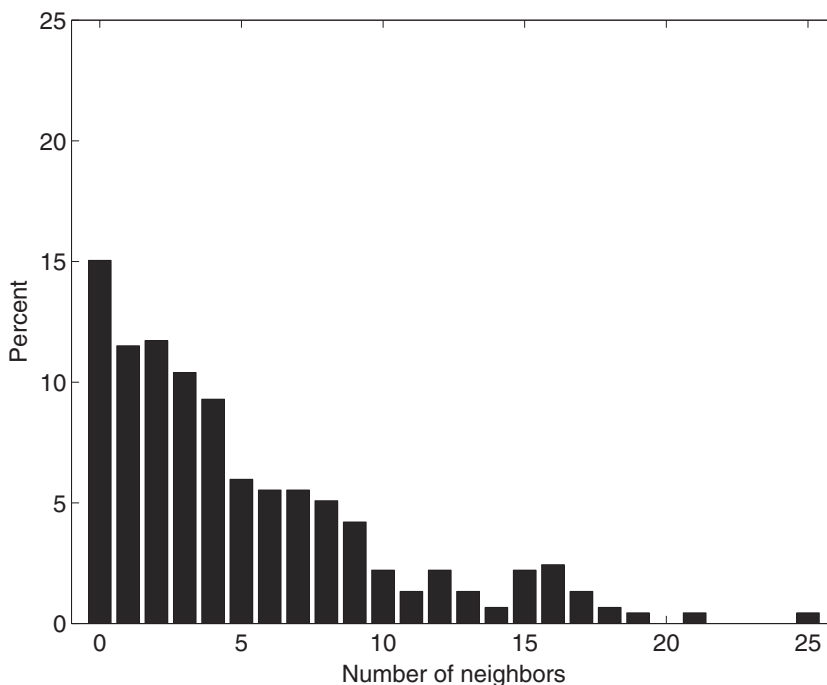


Figure 1. Empirical degree distribution for the terror population in Tables 2 and 3.

Pre-Incident Indicators of Terrorist Incidents

The *Pre-Incident Indicators of Terrorist Incidents* report is partially derived from the American Terrorism Study (ATS) (Smith and Damphousse 2002), which is the primary database for existing empirical studies on the connections between crime and terror (Smith, Damphousse, and Roberts 2006; Smith et al. 2008; Hamm 2005). The ATS collects information on individuals indicted as a result of “domestic security/terrorism investigations” (Smith and Damphousse 2002). Indictments and other court documents also provide the detailed information necessary for the empirical study: which terrorists interact with each other, how frequently they interact, and what criminal activities each terrorist is involved with.

The analysis uses the population of terrorists in the 60 cases analyzed in Smith, Damphousse, and Roberts (2006), which focuses on the activities (both legal and illegal) terrorists are involved with prior to an attack. Court documents associated with the 60 terror cases in Smith, Damphousse, and Roberts (2006) were available through the Terrorism Knowledge Base (TKB) (Memorial Institute for the Prevention of Terrorism 2008), but unfortunately as of March 2008 the TKB is no longer available. The TKB was created and sponsored by the Memorial Institute for the Prevention of Terrorism and has transferred to the University of Maryland’s Study of Terrorism and Responses to Terrorism (START). However, it is uncertain if and when the court documents from the TKB will be available through START (University of Maryland 2008; Straw 2008). The authors did not gain access to court documents for every case in Smith, Damphousse, and Roberts (2006) because either the TKB did not have court documents associated with a given case (seventeen cases) or the authors were unable to download the court documents before the TKB became unavailable (four cases). For those cases for which court documents were not available, the authors had

to appeal to other sources (including the descriptions in Smith, Damphousse, and Roberts 2006).

Each case focuses primarily on one individual or group and a particular incident or string of incidents associated with that group. The 60 cases were aggregated into 54 cases by merging several cases from Smith, Damphousse, and Roberts (2006) when the same terrorists were associated with multiple cases. These 54 cases occur in the United States between 1971–2003 and—according to the classification scheme used by Smith, Damphousse, and Roberts (2006) and the FBI (Federal Bureau of Investigation 2002b)—contain 26 right-wing cases, 6 left-wing cases, 14 single-issue cases, and 8 international cases.

Table 2 (for the 26 right-wing cases) and Table 3 (for the 28 cases from the remaining three categories) provide a list of the terror cases from Smith, Damphousse, and Roberts (2006) included in the analysis, information about each case—including the number of terrorist interactions that occur prior to an attack and the number of edges (connecting terrorist nodes) upon which these interactions occur—and sources for this information. The authors identified 452 terrorists in these 54 cases, and present data on the number of terrorists in each of the four categories in Table 4.

Results presented later are derived from all 54 terror cases. However, in section 4.1 of the Online Appendix each of the four terror categories are analyzed separately (these results are discussed in a later section). The right-wing cases involve individuals associated with Aryan groups, the Ku Klux Klan, or anti-government groups (Smith, Damphousse, and Roberts 2006). The Oklahoma City Bombing is the most well-known and devastating example. The left-wing cases include leftist student groups, all-Black groups, and Puerto Rican independence movement groups (Smith, Damphousse, and Roberts 2006). There has been limited activity from these groups since the mid-1980s. The single-issue cases focus either on anti-abortion acts or environmental groups associated with the Earth Liberation Front or the Animal Liberation front. The international cases involve foreign individuals plotting an attack in the United States or collecting money or other goods to send to terrorist groups abroad (such as Hezbollah or the Irish Republican Army [IRA]). The first World Trade Center attack in 1993 is one of the eight international cases, but the 11 September 2001 attacks are not included.

Terror Network

The authors construct a terror network of the 452 individuals involved in the cases in Tables 2 and 3. In the next section what fraction of these 452 individuals are involved in various crimes is determined to estimate $\mathbf{P}[m_k = 1 \mid m_1 = 1]$, which also guides the choice for the criminal types to include in the analysis. In subsequent sections the constructed terror network is used to estimate the interaction rate λ_1 and the distribution of the degree n_1 , respectively. Other data sources are used (i.e., not based on the terror population in Tables 2 and 3) to estimate the size of the terror network N_1 (which is proportional to $\mathbf{P}[m_1 = 1]$) and the efficiency parameters θ_1^I and θ_1^S .

Overlap Distribution. Table 5 presents the relevant part of the overlap distribution, which is $\mathbf{P}[m_k = 1 \mid m_1 = 1]$. The values in Table 5 are the fraction of terrorists in the data set that are involved with each criminal activity; 98 percent of the criminal connections are included in this table, which represent all but the rarest of overlap criminal activities. It is determined which criminal networks each terrorist is a member of by going through the sources listed in Tables 2 and 3. Four of the criminal networks in Table 5 are divided into different levels that correspond to being a consumer or a distributor of some illicit good. In

Table 2

List of right-wing terror cases from Smith et al. (2006), along with the number of terrorists, the number of terror interactions, and the number of edges in the terror network

Name of terror case	Category	Terrorists	Interactions	Edges	Case number in Smith et al. (2006)	Sources
Arizona Patriots	Right-wing	18	35.50	41	1.1	Smith et al. (2006) USA vs. Oliphant, Schlect, Arthur, and Ross (1986) USA vs. Hagan (1986); USA vs. Christensen (1986) USA vs. Gumaer and Christensen (1986) Smith et al. (2006); USA vs. Winslow, Nelson, and Baker (1990)
Aryan Nations I	Right-wing	5	18	7	1.2	Smith et al. (2006)
Aryan Nations II	Right-wing	3	0	0	1.2	Keenan vs. Aryan Nations, Saphine Inc, Butler, et al. (1999)
Buiford Furrows Incident	Right-wing	1	0	0	1.3	Smith et al. (2006)
Aryan People's Republic	Right-wing	6	31.5	14	1.4	Smith et al. (2006) USA vs. Thomas, Langan, Stedeford, McCarthy, et al. (1997)
The Kehoe Cell	Right-wing	5	1	0	1.5	Smith et al. (2006); USA vs. Kehoe (2002) Southern Poverty Law Center (1998)
Bixby SC	Right-wing	3	2.5	3	1.6	Smith et al. (2006)
The Order	Right-wing	49	189.5	231	1.7, 1.15, 1.17	Smith et al. (2006); USA vs. Ellison and Thomas (1985) USA vs. Ellison and Noble (1985); USA vs. Ellison and Yates (1985) USA vs. Ellison, Stone, Russell, Noble, Loewen, and Giles (1985)

(Continued on next page)

Table 2

List of right-wing terror cases from Smith et al. (2006), along with the number of terrorists, the number of terror interactions, and the number of edges in the terror network

Name of terror case	Category	Terrorists	Interactions	Edges	Case number in Smith et al. (2006)	Sources
Jewish Defense League	Right-wing	3	13	3	1.8	USA vs. Miles, Beam, Butler, Scutari, Pierce, Bamhill, et al. (1988)
Ku Klux Klan Barefoot	Right-wing	6	14	10	1.9	USA vs. Smalley and Brugle (1985); USA vs. Scott (1985)
Ku Klux Klan Fusilier	Right-wing	6	0	0	1.10	USA vs. Lane and Pierce (1985)
Ku Klux Klan Hull	Right-wing	5	10	10	1.11	Smith et al. (2006); Holthouse and Sanchez (2007)
Krar IDC	Right-wing	3	7	1	1.12	Smith et al. (2006)
Minnesota Patriots Council	Right-wing	5	14	6	1.13	Smith et al. (2006); USA vs. Krar, Bruey, and Feltus (2003)
Oklahoma City Bombing	Right-wing	3	9	2	1.14	Smith et al. (2006); USA vs. Henderson and Oelrich (1995)
Phineas Priests	Right-wing	4	10	3	1.18	USA vs. Wheeler and Baker (1995)
Seace Conspiracy	Right-wing	3	5	2	1.19	Smith et al. (2006); USA vs. McVeigh and Nichols (1995)
Third Continental Congress	Right-wing	10	39.5	45	1.20	Smith et al. (2006); USA vs. Merrell, Barbee, and Berry (1996)
						USA vs. McVeigh and Nichols (1996)
						Smith et al. (2006); USA vs. Dorsett and Glover (1997)
						USA vs. Hobeck and Hobeck (1997); USA vs. Newman and Newman (1997) USA vs. Glover (1997); USA vs. Lingenfelter (1997)

Up the IRS, Inc.	Right-wing	1	6	0	1.21	Smith et al. (2006); USA vs. Hicks (1991a) USA vs. Hicks (1991b)
Washington State Militia	Right-wing	18	90.5	97	1.22	Smith et al. (2006) USA vs. Pitzer, Mack, Kuehnoel, Fisher, Kirk, et al. (1996)
Woodring Homrich Standoff	Right-wing	1	0	0	1.23	Smith et al. (2006)
West Virginia Mountaineer Militia	Right-wing	9	33.5	14	1.24	Smith et al. (2006); USA vs. Looker, Johnson, and Lewis (1996) USA vs. Looker, Phillips, and Moore (1996); USA vs. Rogers (1996) USA vs. Coon and Phillips, (1996); USA vs. Looker, and Coon (1996)
Vance Assassination	Right-wing	2	3	1	1.25	Smith et al. (2006); USA vs. Moody (1992)
White Patriot Party	Right-wing	11	36	26	1.26	Smith et al. (2006); USA vs. Miller, Jackson, Wydra, et al. (1987) USA vs. Jackson, Sheets, and Miller (1987); USA vs. Miller (1987)
Oklahoma Constitutional Party	Right-wing	5	16	7	1.27	Smith et al. (2006); USA vs. Lampley, Lampley, Crow, and Baird (1995)
Felton-Chase	Right-wing	5	30.5	8	1.28	Smith et al. (2006); USA vs. Felton and Chase (2001)

Note: Full bibliographical information for the sources appears in the Online Appendix.

Table 3

List of left-wing, single-issue, and international terror cases from Smith et al. (2006), along with the number of terrorists, the number of terror interactions, and the number of edges in the terror network

Name of terror case	Category	Terrorists	Interactions	Edges	Case number in Smith et al. (2006)	Sources
EI Runks	Left-wing	13	131	38	2.1	Smith et al. (2006) USA vs. Fort, Mayes, Knox, Davis, et al. (1986) USA vs. McAnderson, Hawkins, Fort, et al. (1990)
FALN	Left-wing	6	34.5	12	2.2	Smith et al. (2006); USA vs. Jordan (2000)
EPB Macheteros	Left-wing	24	108.5	143	2.3	Smith et al. (2006) USA vs. Gerena, Rios, Palmer, Claudio, et al. (1985) USA vs. Carrion, Diamante, Osorio, Rios, et al. (1987)
May 19th Communist Organization	Left-wing	25	6	30	2.4, 2.5, 2.6	Smith et al. (2006); USA vs. Shakur and Buck (1989) USA vs. Whitehorn (1987); Gado, M. (2008) USA vs. Chumurenga (1985)
United Freedom Front	Left-wing	22	508	81	2.7	Smith et al. (2006); USA vs. Gros (1985) USA vs. Levasseur, Gros, Manning, Manning, et al. (1986)
Yahweh	Left-wing	18	5	12	2.8	Smith et al. (2006); Scheeres (2008)
Griffin Florida Assassination	Single-issue	3	21	2	3.1A, 3.2A	Smith et al. (2006); Booth (1993)
Kopp Amherst Assassination	Single-issue	3	9	3	3.4A	Smith et al. (2006); Arena (2001)
Ellerman Utah Bombing	Single-issue	6	3	6	3.5B	Smith et al. (2006)
EcoRaiders	Single-issue	6	18	11	3.6B	Smith et al. (2006)
Sherman Oregon Firebombing	Single-issue	4	16	6	3.7B	Smith et al. (2006); USA vs. Cesario (2002)
ELF Long Island Arsons	Single-issue	4	0	0	3.8B	USA vs. Sherman, Cesario, Rosenbloom, and Scarpetti (2002)
Fairfield Snow Bowl	Single-issue	13	87.5	32	3.9B	USA vs. Sherman and Scarpetti (2002) Smith et al. (2006)
Vandalism (EMETIC)						Smith et al. (2006) USA vs. Davis, Millett, Foreman, et al. (1989)

Free Critter Eugene Arson	Single-issue	2	4	1	3.10B	Smith et al. (2006)
Nebraska Golf Vandals	Single-issue	3	0	0	3.11B	Smith et al. (2006)
Coronado MSU Arson	Single-issue	8	45.5	11	3.12B	Smith et al. (2006); USA vs. Coronado (1993)
Santa Cruz 2	Single-issue	2	4	0	3.13B	Smith et al. (2006)
Unabomber	Single-issue	1	12	0	3.14B	Smith et al. (2006)
Wisconsin Mink Release	Single-issue	2	1	1	3.15B	Smith et al. (2006)
Dr. Robert Goldstein	Single-issue	3	9	3	3.16C	Smith et al. (2006); McGraw (2008a)
Hezbollah: Cigarette Smuggling	International	9	39	19	4.1	Smith et al. (2006); Crowley (2004)
Japanese Red Army	International	2	11	1	4.2	Smith et al. (2006); USA vs. Kikumura (1988)
Millenium Conspiracy	International	20	88	48	4.3	Smith et al. (2006); USA vs. Haoari and Meskini (2000)
New York City Subway Bombing	International	4	19	5	4.4	Smith et al. (2006); USA vs. Mezer and Khalil (1997) USA vs. Mezer and Khalil (2000); Office of the Inspector General (1998)
Omega—7	International	12	59	25	4.5	Smith et al. (2006); USA vs. Remon, Garcia, and Fernandez (1985)
Provisional IRA: Valhalla Incident	International	7	16	21	4.6	USA vs. Arocena and Badia (1983); USA vs. Arocena (1983) Smith et al. (2006); USA vs. Murray and Andersen (1987)
Provisional IRA: Tuscon Incident	International	14	39.5	22	4.6	USA vs. Murray, Andersen, Nee, Crawley, et al. (1986) Smith et al. (2006)
NYC Conspiracy	International	26	135.5	86	4.7, 4.8	Smith et al. (2006); McGraw (2008b) USA vs. Rahman, Nosair, El-Gabrowny, Ali, et al. (1993) USA vs. Salameh, Ayyad, Abouhalima, Ajaj, et al. (1997) USA vs. Rahman, El-Gabrowny, Nosair, et al. (1999)

Note: Full bibliographical information for the sources appears in the Online Appendix.

Table 4
Number of terrorists in each case, in total and by terror category

	Number of cases	Number of terrorists	Mean number of terrorists per case	Median number of terrorists per case	Standard deviation of terrorists per case
Total	54	452	8.37	5	8.76
Right-wing	26	190	7.31	5	9.59
Left-wing	6	108	18	20	7.35
Single-issue	14	60	4.29	3	3.15
International	8	94	11.75	10.5	8.12

Table 5
Fraction of terrorists involved with other criminal activities, $\mathbf{P}[m_k = 1 | m_l = 1]$

	Total	Right-wing	Left-wing	Single-issue	International
Explosives, total	0.451	0.558	0.398	0.150	0.489
Explosives, users	0.425	0.542	0.398	0.150	0.394
Explosives, retail distributors	0.022	0.011	0.000	0.000	0.085
Explosives, wholesale distributors	0.004	0.005	0.000	0.000	0.011
Firearms, total	0.414	0.563	0.398	0.083	0.340
Firearms, users	0.350	0.489	0.389	0.083	0.191
Firearms, retail distributors	0.046	0.074	0.009	0.000	0.064
Firearms, wholesale distributors	0.018	0.000	0.000	0.000	0.085
Bank Robbery	0.217	0.242	0.482	0.000	0.000
False Documents, total	0.177	0.121	0.259	0.100	0.245
False Documents, users	0.155	0.095	0.250	0.100	0.202
False Documents, distributors	0.022	0.026	0.009	0.000	0.043
Violent Acts	0.091	0.089	0.176	0.017	0.043
Drugs, total	0.053	0.011	0.074	0.050	0.117
Drugs, users	0.013	0.011	0.019	0.017	0.011
Drugs, retail distributors	0.029	0.000	0.056	0.033	0.053
Drugs, wholesale distributors	0.011	0.000	0.000	0.000	0.053
Fraud	0.051	0.042	0.009	0.017	0.138
Counterfeit Money	0.035	0.084	0.000	0.000	0.000
Immigration Violations	0.033	0.000	0.000	0.000	0.160
Illegal Smuggling	0.027	0.000	0.000	0.000	0.128
Money Laundering	0.027	0.000	0.028	0.000	0.096
Arson	0.020	0.016	0.056	0.000	0.000
Extortion	0.011	0.000	0.000	0.000	0.053
Kidnapping	0.007	0.016	0.000	0.000	0.000
Tax Evasion	0.004	0.000	0.000	0.017	0.011

three of the networks the authors distinguish between “retail distributors” and “wholesale distributors,” where retail distributors deal in smaller quantities, primarily to users, and wholesale distributors deal in larger quantities, primarily to other distributors. While it is possible to refine the model to account for these levels explicitly (see Atkinson 2009), for the purposes of this article, the separate levels of a criminal network are equivalent to different criminal networks.

Because of the effort involved in estimating the parameters for each criminal network, coupled with the fact that the overlap probabilities are small (e.g., < 10 percent) for most of the criminal networks in Table 5, the analysis is restricted to six criminal networks: explosives, illegal firearms distributor, illegal firearms user, bank robbery, false documents distributor, and false documents user.

Interaction Rate. For the terror cases in Tables 2 and 3, the authors tabulate how many terror interactions or activities the nodes associated with each case participate in. These interactions might be meetings to plan the logistics of an attack or discuss a group’s radical ideology, or some other preparatory event. If there is a meeting of several individuals then it is assumed that each individual takes part in only one interaction (the meeting); however, that one interaction is assumed to occur between that individual and every other participant at the meeting, and therefore there can be fractional interactions between neighbors. The primary sources used to tabulate these interactions are affidavits, transcripts, indictments, and other court documents.

To compute the interaction rate λ_1 one needs the total number of interactions within the terror network, the number of edges in the network (upon which these interactions occur), and the time period when the interactions take place. With these three pieces of information, the interaction rate is $\lambda_1 = \frac{\text{interactions}}{\text{edges} \times \text{time}}$. If interactions_j is defined to be the number of interactions associated with terror case j and edges_j to be the number of edges associated with terror case j , and $t = 32.5$ years is set to be the length of the time period these terror cases pertain to (1971–2003), then the interaction rate is

$$\lambda_1 = \frac{\sum_{j=1}^{54} \text{interactions}_j}{t \times \sum_{j=1}^{54} \text{edges}_j}. \quad (8)$$

The values of interactions_j and edges_j for each of the 54 cases appear in Tables 2 and 3, where each interaction between neighbors is counted only once when tabulating interactions_j . The interaction rate is $\lambda_1 = 5.5 \times 10^{-2}/\text{year}$ (Table 6).

This estimate assumes that the terror network is static over the period between 1971–2003, while in reality these terrorists are only active for a short period of time.

Table 6
Average annual interactions per edge in the terror network, λ_1

	Interaction rate
Total	5.47×10^{-2}
Right-wing	3.56×10^{-2}
Left-wing	7.73×10^{-2}
Single-issue	9.32×10^{-2}
International	5.52×10^{-2}

Therefore, the interaction rate for active terrorists will be greater than the estimate given by Equation (8). However, λ_1 appears in the optimization problem only in the product $\lambda_1\theta_1^I$ or $\lambda_1\theta_1^S$ (see Equations (1), (2), and (3)). A later section estimates θ_1^I as a function of λ_1 (see Equation (9)), and thus the product $\lambda_1\theta_1^I$ is determined by Equation (9). One could absorb λ_1 into θ_1^I and still compute θ_1^S as is done in a later section, and therefore the estimate of λ_1 is not crucial for this analysis.

Degree Distribution. Two nodes are defined as neighbors in the terror network if it is determined that they interact in a terror activity (i.e., their interactions when tabulating interactions_j are counted in the preceding section). For meetings involving several individuals, it is assumed that every participant of the meeting is a neighbor with every other participant. The empirical degree distribution is illustrated in Figure 1 and the mean degree is $\mathbf{E}[n_1] = 5.1$ (Table 7). This empirical distribution is used to compute the moment generating term, $\mathbf{E}[e^{tn_1}]$, appearing in Equation (2).

It is not expected that the authors' network will have the same properties (e.g., small-world or scale-free) as the criminal and terror networks in Xu and Chen (2008) because the authors' network consists of 54 disconnected and relatively small cells. Using the methods described in Clauset, Shalizi, and Newman (2009), it is found that a power law distribution is a poor fit to the degree distribution of the network, as are Poisson and discretized log-normal distributions. The geometric distribution does not fit the data well, but it cannot be rejected at the 0.05 level. The terror network has a high degree correlation among neighboring nodes, which is consistent with the Global Salafi Jihad terror network analyzed in Xu and Chen (2008) and many other social networks (Newman 2002). The assortativity coefficient (defined in Equation (4) of Newman (2002) and equivalent to the Pearson correlation coefficient) for the authors' network is 0.473.

Size of Terror Network. Several sources report that there have been on the order of 100 terror incidents in the United States over the last decade (see Lawson Terrorism Information Center 2008; Federal Bureau of Investigation 2008c; Jarboe 2002; Blejwas, Griggs, and Potok 2005). These incidents primarily involve environmental or right-wing terrorists. As an order-of-magnitude estimate, it is assumed that there are 1,000 domestic terrorists. It is further assumed that there is an equal number of international terrorists in the United States, which is not inconsistent with a report that states a "very small fraction" of the over 200,000 individuals on an international terrorist list are in the United States (*Washington Post* 2006). Therefore it is assumed that there are $N_1 = 2000$ nodes in the terror network.

Table 7
Characteristics of the degree distribution of the terror network, n_1

	Mean degree	Median degree	Standard deviation of degree
Total	5.09	4	4.91
Right-wing	5.59	4	5.36
Left-wing	5.85	4	5.62
Single-issue	2.53	2	2.28
International	4.83	5	3.66

Efficiency Parameters. The efficiency parameters, θ_1^I and θ_1^S , are aggregate parameters that account for several different factors, and therefore are difficult to directly estimate. The authors' approach is to indirectly estimate θ_1^I using Equation (1) and then estimate the ratio $\frac{\theta_1^I}{\theta_1^S}$. There is an estimate of $\mathbf{E}[n_1]$ and an estimate of λ_1 from previous sections. If one also estimates the resources spent on an initial investigation of the terror network, \hat{B}_1^I , and the number of terrorists identified during that initial investigation, \hat{Y}_1^I , then one can estimate θ_1^I via Equation (1),

$$\theta_1^I = \frac{\hat{Y}_1^I}{\hat{B}_1^I \mathbf{E}[n_1] \lambda_1}, \quad (9)$$

where it is assumed that the estimate \hat{Y}_1^I is a reasonable approximation to $\mathbf{E}[Y_1^I]$ in Equation (1). \hat{B}_1^I and \hat{Y}_1^I are now estimated. $\hat{B}_1^I = \$1.4\text{B}$, which is the FBI domestic counterterrorism budget for 2005 (Harlow 2006). The FBI investigated 248 suspects in 2005 for offenses related to terrorist activity (Bureau of Justice Statistics 2005) (using the category "Suspects in Investigations Initiated" from Bureau of Justice Statistics 2005, which is also used in the next section). In addition, out of 1,067 individuals referred to federal prosecutors and classified as "international terrorists" during 2001–2006, only 372 had a lead charge directly related to terrorism (Transactional Records Access Clearinghouse 2007). The authors therefore multiply 248 by $\frac{1067}{372}$ to estimate the number of terrorists identified by the FBI in 2005. Rounding down this product, $\hat{Y}_1^I = 700$ is set. Substituting these estimates into the right side of Equation (9) yields $\theta_1^I = 1.79 \times 10^{-6}$.

Because much of the initial investigation budget involves investigating false leads, the ratio $\frac{\theta_1^I}{\theta_1^S}$ is estimated by the fraction of preliminary investigations that lead to legitimate terror investigations. One report states that of nearly 10,000 terrorism investigations in 2000, only about 500 individuals were charged, which leads to an estimate of 0.05 (Transactional Records Access Clearinghouse 2003). A Department of Justice report states that between 2004 and 2007 there were 108,000 terrorism-related threats, but only 600 terrorism-related investigations, which leads to an estimate of 0.006 (Office of the Inspector General 2008). This same report later states that in 2006 there were 219,000 terrorism tips by the public to the FBI, and this resulted in 2,800 terror threats entered into its system, yielding an estimate of 0.01 (Office of the Inspector General 2008). The analysis uses the median of these three estimates and sets $\theta_1^S = 100\theta_1^I = 1.79 \times 10^{-4}$, although it varies θ_1^S in section 4.2 in the Online Appendix because there is uncertainty about its relationship to θ_1^I (these results are discussed in a later section).

Criminal Networks

The four subsections in this subsection are devoted to estimating the parameters for the four types of criminal networks with the greatest overlap with the terror network: explosives, illegal firearms (distributor and user), bank robbery, and false documents (distributor and user) (although there are six criminal networks, it is easier to present the parameter estimates for the two illegal firearms networks together and for the two false documents networks together). By Equations (1) and (2), one needs to estimate the size of network k , N_k , which is proportional to $\mathbf{P}[m_k = 1]$, and the aggregate quantity $\theta_k^I \mathbf{E}[n_k] \lambda_k$. Using the same method used to estimate θ_1^I in Equation (9), if one estimates the resources spent on an

initial investigation of network k , \hat{B}_k^I , and the number of nodes identified during that initial investigation, \hat{Y}_k^I , then the aggregate quantity can be estimated via Equation (1):

$$\theta_k^I \mathbf{E}[n_k] \lambda_k = \frac{\hat{Y}_k^I}{\hat{B}_k^I}. \quad (10)$$

For each criminal network the analysis focuses on one agency that investigates that crime and estimate the resources the agency spent to investigate that criminal network, \hat{B}_k^I , and the number of nodes the agency identified during its investigations, \hat{Y}_k^I ; for consistency, the year 2005 is used for these calculations whenever possible. In addition, for the criminal networks the estimates for \hat{B}_k^I are also used for b_k in the coordinated version of the optimization problem.

Explosives Network. Out of 452 terrorists in the study, 192 use explosives, 10 are retail distributors, and 2 are wholesale distributors (Table 5). However, because of a lack of data for N_k , \hat{B}_k^I , and \hat{Y}_k^I for these three levels, the analysis does not distinguish between different levels of the explosives network and only considers the aggregate explosives network.

Network size. There were 3,693 explosives investigations by the Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF) in 2005 (Bureau of Alcohol, Tobacco, and Firearms 2005), which is a similar value to the number of reported explosives incidents per year between 2004 and 2006 (Bureau of Alcohol, Tobacco, and Firearms 2006). These values are approximately 50 percent more than the reported number of bombing incidents per year in the 1990s (Pastore and Maguire 2003; Bureau of Alcohol, Tobacco, and Firearms 1996b).

There were 369 defendants in 218 explosives-related cases in 1997 (Bureau of Alcohol, Tobacco, and Firearms 1997). These values are 315 and 196, respectively, for 1996 (Bureau of Alcohol, Tobacco, and Firearms 1997) and 409 and 244, respectively, for 1995 (Bureau of Alcohol, Tobacco, and Firearms 1996a), implying that there were ≈ 1.66 defendants per case during these years. If it is assumed that there were 1.66 people per bombing incident in 2005, then the total population in the explosives network would be approximately 6,000 individuals. Although many criminals are repeat offenders that commit several crimes per year (Blumstein et al. 1986), the authors could not find any information to estimate how many explosives incidents each criminal is involved with, and therefore it is assumed that there are $N_k = 6,000$ nodes in the explosives network.

Budget. The authors set $\hat{B}_k^I = b_k = \$119\text{M}$, which is the amount allocated by the ATF to explosives enforcement in 2005 (Bureau of Alcohol, Tobacco, and Firearms 2005).

Number of nodes identified during the investigation. $\hat{Y}_k^I = 228$ for the explosives network, which is the number of suspects investigated by the ATF in 2005 for offenses related to explosives (Bureau of Justice Statistics 2005).

Illegal Firearms Network. Out of 452 terrorists, 158 use illegal firearms, 21 are retail distributors, and 8 are wholesale distributors (Table 5). In this analysis, users and distributors of illegal firearms are considered as being in separate networks.

Network size. There are $\approx 2\text{M}$ criminal firearm acquisitions per year (Pierce et al. 2004), and offenders purchase about one handgun per year (Koper and Reuter 1996). Therefore, it is assumed that there are $N_k = 2\text{M}$ users in the illegal firearms user network. Approximately 30 percent of criminals obtain their firearm through a drug dealer, off the street, a fence, or the black market (Harlow 2001). It is assumed that these suppliers are

the population of illegal firearm distributors, and therefore 600,000 criminals obtain their firearm from an illegal firearms distributor each year. The average gun distributor sells on the order of 100 firearms per year (Koper and Reuter 1996), and thus it is assumed that are $N_k = 6,000$ distributors in the illegal firearms distributor network.

Budget. The 2005 ATF Report states \$591 M went to firearms enforcement (Bureau of Alcohol, Tobacco, and Firearms, 2005). In the ATF's budget for 2008, \$337.5 M were allocated to firearms trafficking out of \$730.1 M allocated to firearms enforcement (46.2%) (Bureau of Alcohol, Tobacco, and Firearms 2007). Assuming the same percentage allocation in 2005, $\hat{B}_k^I = b_k = \$318\text{M}$ is set as the investigative budget for users of illegal firearms, and $\hat{B}_k^I = b_k = \$273\text{M}$ as the investigative budget for distributors of illegal firearms.

Number of nodes identified during the investigation. The ATF investigated 11,068 suspects in 2005 for offenses related to firearms (Bureau of Justice Statistics 2005). Out of 8,353 convictions for firearm offenses in 2005, 1,448 were for trafficking offenses (Bureau of Alcohol, Tobacco, and Firearms 2005). This fraction ($\frac{1448}{8353}$) is assumed from the Bureau of Alcohol, Tobacco, and Firearms (2005) to also hold for the values from the Bureau of Justice Statistics (2005), and set the number of individuals identified during the investigation of the illegal firearms network in 2005 is set to be $\hat{Y}_k^I = 9149$ for users of illegal firearms and $\hat{Y}_k^I = 1919$ for distributors of illegal firearms.

Bank Robbery Network: Network size. There are on the order of 10,000 bank robberies per year (Federal Bureau of Investigation 2006a; Weisel 2007; Federal Bureau of Investigation 2002a, 2005). A Department of Justice report on bank robberies states that in London each apprehended bank robber is associated with an average of 2.8 bank robberies (Weisel 2007). The Bank Crime Statistics report published by the FBI in 2005 states that there were an average of 1.2 known people associated with each bank robbery (Federal Bureau of Investigation 2005), and the 2002 Uniform Crime Report states that 80 percent of bank robberies are carried out by one offender and 15 percent involve two offenders (Federal Bureau of Investigation 2002a) (and therefore the average number of offenders per robbery is at least 1.25 according to Federal Bureau of Investigation 2002a). If it is assumed that there are 1.3 offenders per bank robbery, 10,000 bank robberies per year, and 2.8 bank robberies per individual, then the population of bank robbers would be 4,643. Rounding up, it is assumed that there are $N_k = 5,000$ nodes in the bank robbery network.

Budget. The FBI allocated \$2.1 B in 2008 for federal criminal law enforcement, and \$1.1 B of this amount was allocated to reduce violent crime (Federal Bureau of Investigation 2008a) (robbery is considered a violent crime; Federal Bureau of Investigation 2006a). The FBI spent \$2.0 B on federal criminal law enforcement in 2005 (Federal Bureau of Investigation 2006b). If it is assumed that the FBI allocated the same fraction of the criminal enforcement budget to reduce violent crime in 2005 as it did in 2008 ($\frac{1.1}{2.1}$), then the FBI spent \$1.0 B to reduce violent crime in 2005. Unfortunately, more specific information could not be found on the amount of resources the FBI spends investigating bank robberies. The FBI investigates several types of activities related to violent crime including bank robberies, murder for hire, and crimes against children (Federal Bureau of Investigation 2008a,b). The authors make the rough estimate that the FBI spends 10 percent of its budget to reduce violent crime on bank robbery investigations. $\hat{B}_k^I = b_k = \$100\text{M}$ is therefore set as the investigative budget for the bank robbery network.

Number of nodes identified during the investigation. $\hat{Y}_k^I = 1877$ for the bank robbery network, which is the number of suspects the FBI investigated in 2005 for offenses related to bank robberies (Bureau of Justice Statistics 2005).

False Documents Network. Out of 452 terrorists, 70 use false documents and 10 are distributors (Table 5). The analysis considers both a user network and a distributor network for false documents.

The focus here is on the use of false documents to obscure or alter one's identity. However, there are many related criminal activities involving identity theft, fraud, forgery, counterfeiting, and immigrations violations that are not included in this analysis. Unfortunately, the definitions in reports and databases do not always clearly distinguish these various criminal categories (Federal Bureau of Investigation 2006a; Koops and Leenes 2006). There are also many populations who use false documents (Associated Press 2006), there are several types of false documents (Dinerstein 2002), and there are various agencies that investigate false documents (General Accounting Office 1998). Therefore, it can be difficult to obtain information about false documents that is relevant for the present purposes (Gordon and Willox 2003). This analysis uses data from Immigration and Customs Enforcement (ICE) and Customs and Border Protection (CBP) because those agencies provide data that are most pertinent to the analysis.

Network size. The largest group of false document users is illegal immigrants (Associated Press 2006). It is assumed that there are $N_k = 10\text{M}$ users in the false documents user network, which is roughly the illegal immigrant population in the United States in 2005 (Passel 2006).

Approximately 500,000 new illegal immigrants enter the United States every year (Passel 2006). If it is assumed that all of these individuals need false documents and another 500,000 people already in the United States also need false documents, then there are on the order of 1 M consumers of false documents per year. A sophisticated false documents operation called the Castorena Family Organization sells 50–100 document sets per day (Fitzgerald 2007) and their cells consist of 10–20 individuals (Immigrations and Customs Enforcement 2005). Thus, a distributor would sell to ≈ 5 consumers a day or $\approx 1,000$ consumers per year, implying that there are $\approx 1,000$ false document distributors. However, this value assumes the characteristics of one of the largest and most complex operations is the norm. Because many distributors are involved with much smaller operations and only serve a few clients, it is assumed that there are $N_k = 5,000$ distributors in the false documents distributor network.

Budget. The budget for the CBP in 2005 was 6.2B dollars (Department of Homeland Security 2005a). The investigative category that is most relevant to this analysis is "Border Security Inspections and Trade Facilitation at Points of Entry," which has a budget of \$2.72 B (Department of Homeland Security 2005a). Unfortunately, there is no more information regarding how much of these resources are spent investigating users of false documents. However, a reasonable amount of the effort at ports of entry is analyzing documents to ensure that the people who enter the United States are who they claim to be and are entering for legitimate purposes. Therefore, the authors roughly estimate that $\hat{B}_k^I = b_k = \$500\text{M}$ for users of false documents.

The 2007 ICE budget was \$4.7 B, and \$1.3 B of that went to domestic investigations (Immigrations and Customs Enforcement 2006). These investigations include visa security, illegal arms exports, financial and smuggling violations, immigration and customs fraud, human trafficking, identity and benefit fraud, child pornography, and sex tourism (Immigrations and Customs Enforcement 2006). The category "Identity and Benefit Fraud" is most relevant to this analysis. There are eight categories that ICE investigates, and it is assumed that roughly 10 percent of the budget is allocated to each category. It is further assumed that ICE targets primarily distributors of false documents with these resources, and therefore $\hat{B}_k^I = b_k = \$100\text{M}$ is used for distributors of false documents.

Number of nodes identified during the investigation. CBP confiscated 75,000 false documents in 2005 and apprehended 84,000 individuals trying to enter the United States with false documents (Department of Homeland Security 2005b). Therefore, $\hat{Y}_k^I = 80k$ for users of false documents. In 2007, ICE initiated 1,309 fraud investigations that targeted document and immigration benefit fraud that supported illegal immigrants (Immigrations and Customs Enforcement 2007), and thus $\hat{Y}_k^I = 1309$ is assumed for distributors of false documents.

Numerical Results

Main Results

This section begins with the solution to the uncoordinated case (i.e., $b_k = 0$). These results are presented in Table 8. Although the overall cost-effectiveness parameters e_k are the most important numerical output in Table 8, the initial focus is on the various components of e_k from Equations (50)–(51) in the Online Appendix. 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 e_k^I in Table 8), with its effectiveness ranging from a factor of 5 to a factor of 320 lower than 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^I in Table 8 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)): for example, even though 35 percent 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 Equation (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 $\mathbf{P}[m_1 = 1|m_k = 1]$ varies by a factor of 4,800, which is much greater than the variation in the initial effectiveness e_k^I .

Relative to e_k^I and $\mathbf{P}[m_1 = 1|m_k = 1]$, there is little variation in $P_k^S(\gamma_k^*)$ in Table 8, which is consistent with the fact that secondary investigations avoid the needle-in-the-haystack effect. The values of γ_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 8) 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 ($\mathbf{P}[m_1 = 1|m_k = 1]$) 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 8. The range of e_k in Table 8 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 8, although the values of e_k for the terror

Table 8
Numerical results for the uncoordinated case

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

Note: 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 ($\mathbf{P}[m_1 = 1 | m_k = 1]$), and the probability that a terrorist is detected during the secondary investigation (P_k^S). The optimal solution is given by the fraction of the budget used for the initial investigation (γ_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 9
Numerical results for the coordinated case

Network	b_k	$\gamma_k^*(B_k^*)$	$P_k^S(\gamma_k^*, B_k^*)$	$\frac{B_k^*}{B}$	Terrorists detected
Terror	—	—	—	0.73	511
Explosives	1.19×10^8	0	0.69	0.01	30
Illegal Firearms User	3.18×10^8	—	—	0	0
Illegal Firearms Distributor	2.73×10^8	0	0.31	0.01	13
Bank Robbery	10^8	0.48	0.62	0.25	270
False Documents User	5×10^8	—	—	0	0
False Documents Distributor	10^8	—	—	0	0

Note: 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.

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 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 5). 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 8).

The optimal solution in the uncoordinated case uses 32 percent of the counterterrorism budget to investigate the bank robbery network, with a 60–40-percent split between the initial and secondary investigations. This within-network allocation for the bank robbery network is slightly different than the γ_k^* quantity listed in Table 8 because the value in Table 8 is only valid if the min operators in Equations (41)–(42) of the Online Appendix return the first term. At this level of resources, every bank robber is identified in the initial investigation, and the remaining 68 percent 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 9), the authors find that it is optimal to spend 25 percent 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 counterterrorism budget is used to investigate the terror network, and a small fraction (1 percent each) of the budget is also used to perform secondary investigations of illegal firearms distributors and the explosives network.

The current \$1.4 B 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, Damphousse, and Roberts (2006) were also caught via the criminal networks). If $B = \$1.4B$ in the uncoordinated version of the problem, the solution leads to

the detection of 748 terrorists (Table 8) (i.e., coordination leads to a 10 percent increase in the number of detected terrorists). If the \$1.4 B was restricted to being used solely in the terror network, then 700 terrorists would be detected.

The two versions of the problem were also solved for other budget values (Figure 2). In the uncoordinated case, the government uses its first \$0.4 B 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, $\mathbf{P}[m_1 = 1|m_k = 1]$ (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 solutions to the two cases become more similar as the budget increases.

Sensitivity Analyses

Three variations of the analysis are performed in section 4 of the Online Appendix. The terrorist population in this study is partitioned into four categories by Smith, Damphousse, and Roberts (2006): right-wing, left-wing, single issue, and international (section 4.1 of the Online Appendix and Tables 2 and 3). The authors estimate the terror parameters and compute the optimal uncoordinated solution for each category, and the results (section 4.1 and Table 1 of the Online Appendix) are similar to the results in Table 8. The main difference between Table 8 and Table 1 of the Online Appendix is that the terror network has the largest value of e_k for all four categories in Table 1 of the Online Appendix. 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 the present results are quite insensitive to the degree distribution n_1 of the terror network (section 4.1 of the Online Appendix).

The authors also vary the secondary efficiency parameter θ_1^S , 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 θ_1^S by two orders of magnitude in each direction, the networks with the four smallest values of e_k in Table 8 maintain their relative rankings (Table 2 of the Online Appendix). However, for the networks with the three largest values of e_k in Table 8, there is some variation in their relative rankings.

The authors do not have enough information to estimate confidence intervals for the e_k values in Table 8. However, to illustrate how the uncertainty in the parameter values affects e_k , the authors 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 (section 4.3 of the Online Appendix). The simulation results show that the e_k rankings in Table 8 are fairly robust for this level of parameter value uncertainty.

Although the 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

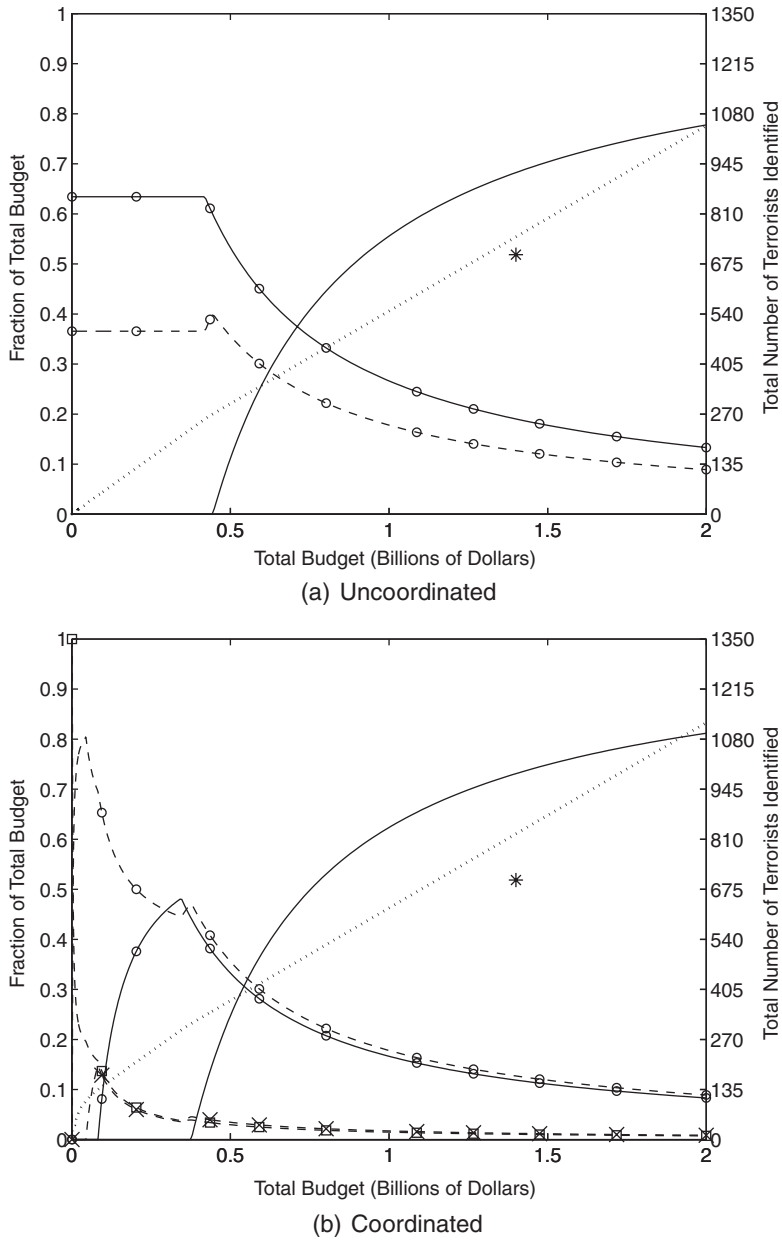


Figure 2. The solution to the (a) uncoordinated and (b) coordinated versions of problem (3)–(6) for varying budget levels. The right vertical axis measures the optimal number of terrorists identified (...) and the number of terrorists identified if the entire \$1.4B budget is allocated to investigating 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 (no symbol), the bank robbery network (○), the explosives network (□), and the illegal firearms distribution network (×).

Downloaded By: [Stanford University] At: 19:50 1 July 2010

relative rankings of the networks change only if the true values of the parameters e_k^I and $\mathbf{P}[m_1 = 1 \mid m_k = 1]$ are much different than the estimates in Table 8.

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, Damphousse, and Roberts 2006; Hamm 2005; Smith et al. 2008; Smith and Damphousse 2002), the authors are not aware of any mathematical network studies of the crime–terror nexus. Their overlapping networks model has some similarities to several existing models, but the orientation is much different; for example, while the authors' focus is on explicitly optimizing centralized network interdiction, the goals in Palla et al. (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, the problem considered in the article is loosely related to two other problems that are concerned with hidden populations: capture-recapture models and contact-tracing models. While the authors 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 the 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 the present 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 the analysis from making specific recommendations for how the government should allocate its domestic counterterrorism resources. However, the authors have developed a new mathematical framework for thinking about these issues and the 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, it is left to government counterterrorism analysts to assess this study's usefulness.

Turning to the 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 Online Appendix reveals that the cost-effectiveness of identifying terrorists in each criminal network depends on 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, the 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 8 the variation in $\mathbf{P}[m_1 = 1 | m_k = 1]$ is 1–2 orders of magnitude greater than the variation in e_k^I , 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 the 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 the empirical study, these networks 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 percent 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 percent vs. 60 percent) 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 this empirical study cannot directly inform current counterterrorism policy is that the terror population from Smith, Damphousse, and Roberts (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 the 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, Damphousse, and Roberts (2006) was not fruitful due to the low frequency rate of terror attacks. Furthermore, the cases in Smith, Damphousse, and Roberts (2006) may not be representative of the terrorists active between 1971–2003 for two reasons. First, there could be selection bias; for example, perhaps larger terror cells, or terrorists of certain types (e.g., right-wing terrorists appear to be less professional than left-wing terrorists in the present study) were easier to detect during this time period. Second, this study selects cases for analysis based on the availability of sources, and thus the “ability to infer to all terrorists groups is negatively affected” (Smith, Damphousse, and Roberts 2006).

Court documents provide a valuable source to determine which nodes interact with each other and how frequently, but the authors were unable to gain access to court documents for every case in the data set (see earlier section). However, even if the authors did have court documents for each case, they are not perfect sources for the 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 the estimates of the degree distribution n_1 and the frequency λ_1 in the terror network as lower bounds on the true values, this data censoring could be offset by the selection bias mentioned earlier.

Another shortcoming of the data is that the specific information needed to estimate the parameters in Table 1 does not always exist (or the authors could not find them). It is assumed 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 versus secondary investigation would be helpful. Furthermore, it is assumed that 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 and the parameters for users and distributors of false documents are rough estimates (see earlier sections).

Model Extensions

One limitation of the model is that it fails to allow the terrorists to modify their participation in criminal activities based on the government's budget allocation. However, this failure to model the problem in a game-theoretic framework is not as big a concern in the 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 the present 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, for example, money-making activities (e.g., drug dealing) for which safer options exist (note that in the data set used from Smith, Damphousse, and Roberts 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.

It is assumed 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 $\mathbf{P}[n_1 = r]$. If there are correlations between a node's degree in the terror network and its degree in network k , then the last term in Equation (2) would be computed with respect to the degree distribution defined by $\mathbf{P}[n_1 = r] \frac{\mathbf{E}[n_k | n_1=r]}{\mathbf{E}[n_k]}$ (the steps to show this are similar to the analysis in section 2 of the Online Appendix). 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 this 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 section 1 of the Online Appendix). 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 the present model, the government could determine not only other networks that nodes belong to, but also neighbors of nodes. The 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 section 4.2 of Kaplan, Craft, and Wein 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 the present 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, one 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 the present 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 the optimization problem, it would not affect the model's basic qualitative behavior.

References

- Associated Press. 2006. Fake immigration ID sellers unfazed by threats. 2 June, MSNBC.com. <http://www.msnbc.msn.com/id/13105209/> (last accessed 2 January 2009).

- Atkinson, M. 2009. Mathematical models of terror interdiction. Ph.D. Dissertation, Stanford University.
- Blejwas, A., A. Griggs, and M. Potok. 2005. Terror from the right. *Intelligence Report* (Summer) (118).
- Blumstein, A., J. Cohen, J. Roth, and C. A. Visher. 1986. *Criminal careers and "career criminals."* Washington, DC: National Academies Press.
- Buckley, C. and W. K. Rashbaum. 2007. The J.F.K. airport case. *New York Times*. 3 June.
- Bureau of Alcohol, Tobacco, and Firearms. 1996a. 1996 highlights of the Bureau of Alcohol, Tobacco and Firearms. US Department of the Treasury (Washington, DC). http://www.atf.gov/pub/gen_pub/annualrpt/1996/index.htm (last accessed 31 December 2008).
- Bureau of Alcohol, Tobacco, and Firearms. 1996b. 1996 selected explosives incidents. US Department of the Treasury (Washington, DC). http://www.atf.gov/pub/fire-explo_pub/eir/type.htm (last accessed 31 December 2008).
- Bureau of Alcohol, Tobacco, and Firearms. 1997. ATF annual report. US Department of the Treasury (Washington, DC). http://www.atf.gov/pub/gen_pub/report97/1997ann.pdf (last accessed 31 December 2008).
- Bureau of Alcohol, Tobacco, and Firearms. 2005. ATF 2005 annual report. US Department of Justice (Washington, DC). http://www.atf.gov/pub/gen_pub/2005annual_report.pdf (last accessed 31 December 2008).
- Bureau of Alcohol, Tobacco, and Firearms. 2006. United States Bomb Data Center. US Department of Justice (Washington, DC). <http://www.atf.gov/aaxis2/bombingrpts/bombings2004-2006-rev.pdf> (last accessed 31 December 2008).
- Bureau of Alcohol, Tobacco, and Firearms. 2007. Congressional budget submission: Fiscal year 2008. US Department of Justice (Washington, DC). http://www.usdoj.gov/jmd/2008justification/pdf/36_atf.pdf (last accessed 31 December 2008).
- Bureau of Justice Statistics. 2005. Federal Justice Statistics Resource Center. Grant number 2005-BJXC-K0004, Urban Institute (Washington, DC). <http://fjsrc.urban.org/index.cfm> (last accessed 31 December 2008).
- Clauset, A., C. R. Shalizi, and M. E. J. Newman. 2009. Power-law distributions in empirical data. *SIAM Review* 51: 661–708.
- Department of Homeland Security. 2005a. Budget in brief: Fiscal year 2005. http://www.dhs.gov/xlibrary/assets/FY_2005_BIB_4.pdf (last accessed 1 January 2009).
- Department of Homeland Security. 2005b. Fact sheet: Combating fraudulent documents. http://www.dhs.gov/xnews/releases/pr_1158347347660.shtm (last accessed 1 January 2009).
- Dinerstein, M. 2002. Americas identity crisis: Document fraud is pervasive and pernicious. Center for Immigration Studies, (Washington, DC). <http://www.cis.org/articles/2002/back302.pdf> (last accessed 2 January 2009).
- Dishman, C. 2005. The leaderless nexus: When crime and terror converge. *Studies in Conflict & Terrorism* 28(3): 237–252.
- Farley, J. D. 2003. Breaking Al Qaeda cells: A mathematical analysis of counterterrorism operations (A guide for risk assessment and decision making). *Studies in Conflict & Terrorism* 26(6): 399–411.
- Federal Bureau of Investigation. 2002a. Crime in the United States 2002. US Department of Justice (Washington, DC). http://www.fbi.gov/ucr/cius_02/pdf/02crime5.pdf (last accessed 31 December 2008).
- Federal Bureau of Investigation. 2002b. Terrorism 2000/2001. US Department of Justice (Washington, DC). http://www.fbi.gov/publications/terror/terror2000_2001.htm (last accessed 5 January 2009).
- Federal Bureau of Investigation. 2005. Bank crime statistics. US Department of Justice (Washington, DC). <http://www.fbi.gov/publications/bcs/bcs2005/bcsreport2005.pdf> (last accessed 1 January 2009).
- Federal Bureau of Investigation. 2006a. Crime in the United States 2005. US Department of Justice (Washington, DC). <http://www.fbi.gov/ucr/05cius/> (last accessed 31 December 2008).

- Federal Bureau of Investigation. 2006b. FBI budget 2006. US Department of Justice (Washington, DC). http://www.usdoj.gov/jmd/2006summary/pdf/36_FBI.pdf (last accessed 1 January 2009).
- Federal Bureau of Investigation. 2008a. FY 2008 authorization and budget request to Congress. US Department of Justice (Washington, DC). http://www.usdoj.gov/jmd/2008justification/pdf/33_fbi_se.pdf (last accessed 1 January 2009).
- Federal Bureau of Investigation. 2008b. Major Thefts & Violent Crimes. US Department of Justice (Washington, DC). <http://www.fbi.gov/hq/majorthefts/majorthefts.htm> (last accessed 1 January 2009).
- Federal Bureau of Investigation. 2008c. Terrorism 2002–2005. US Department of Justice (Washington, DC). <http://www.terrorisminfo.mipt.org/pdf/Terrorism2002–2005.pdf> (last accessed 5 January 2009).
- Fitzgerald, P. J. 2007. U.S. charges 22 defendants in alleged fraudulent identification document ring based in Chicago's Little Village Community. 25 April 2008, Federal Bureau of Investigation (Washington, DC). http://chicago.fbi.gov/dojpressrel/pressrel07/apr25_07a.htm (last accessed 31 December 2008).
- General Accounting Office. 1998. Identity fraud: Information on prevalence, cost, and Internet impact is limited. Report GAO/GGD-98-100BR (Washington, DC). <http://www.gao.gov/archive/1998/gg98100b.pdf> (last accessed 2 January 2009).
- Gibbons, R. 1992. *Game theory for applied economists*. Princeton, NJ: Princeton University Press.
- Gordon, G. R. and N. A. Willox. 2003. Identity fraud a critical national and global threat. Economic Crime Institute and LexisNexis. <http://veracity.lexis-nexis.com/presscenter/hottopics/ECIReportFINAL.pdf> (last accessed 2 January 2009).
- Gutfraind, A. 2008. Understanding terrorist organizations with a dynamic model. *Studies in Conflict & Terrorism* 32(1): 45–59.
- Hamm, M. 2005. Crimes committed by terrorist groups: Theory, research, and prevention. Report 211203, US Department of Justice (Washington, DC).
- Harlow, C. W. 2001. Weapon use and violent crime. NCJ Report 189369, Bureau of Justice Statistics (Washington, DC). <http://www.ojp.gov/bjs/pub/pdf/fuo.pdf> (last accessed 31 December 2008).
- Harlow, C. W. 2006. Combating terrorism: Determining and reporting federal funding data. Report GAO-06161, US Government Accountability Office (Washington, DC). <http://www.gao.gov/new.items/d06161.pdf> (last accessed 5 January 2009).
- Hutchinson, S., and P. O'Malley. 2007. A crime–terror nexus? Thinking on some of the links between terrorism and criminality. *Studies in Conflict & Terrorism* 30(12): 1095–1107.
- Immigrations and Customs Enforcement. 2005. Fact sheet: The Castorena family criminal organization. US Department of Homeland Security (Washington, DC). http://www.ice.gov/pi/news/factsheets/050720castorena_family.htm (last accessed 23 October 2008).
- Immigrations and Customs Enforcement. 2006. FactSheet. US Department of Homeland Security (Washington, DC). <http://www.ice.gov/doclib/pi/news/factsheets/2007budgetfactsheet.pdf> (last accessed 1 January 2009).
- Immigrations and Customs Enforcement. 2007. ICE fiscal year 2007 annual report. US Department of Homeland Security (Washington, DC). http://www.ice.gov/doclib/about/ice07ar_final.pdf (last accessed 1 January 2009).
- Jarboe, J. F. 2002. Testimony before the House Resources Committee, Subcommittee on Forests and Forest Health. US Department of Justice (Washington, DC). <http://www.fbi.gov/congress/congress02/jarboe021202.htm> (last accessed 5 January 2009).
- Jordan, J. and N. Horsburgh. 2005. Mapping Jihadist terrorism in Spain. *Studies in Conflict & Terrorism* 28(3): 169–191.
- Kaplan, E. H., D. L. Craft, and L. M. Wein. 2003. Analyzing bioterror response logistics: The case of Smallpox. *Mathematical Biosciences* 185: 33–72.
- Koops, B. J. and R. E. Leenes. 2006. ID theft, ID fraud and/or ID-related crime—definitions matter. *Datenschutz und Datensicherheit* 30(9): 553–556.
- Koper, C. S. and P. Reuter. 1996. Suppressing illegal gun markets: Lessons from drug enforcement. *Law and Contemporary Problems* 59: 119.

- Krebs, V. E. 2002. Mapping networks of terrorist cells. *Connections* 24(3): 43–52.
- Lawson Terrorism Information Center. 2008. Terrorism incidents and significant dates. Memorial Institute for the Prevention of Terrorism (Oklahoma City, OK). <http://www.terrorisminfo.mipt.org/incidentcalendar.asp> (last accessed 4 January 2009).
- Memorial Institute for the Prevention of Terrorism. 2008. Terrorism knowledge base. <http://www.tkb.org> (last accessed 15 March 2008).
- Morselli, C. and C. Giguère. 2006. Legitimate strengths in criminal networks. *Crime, Law and Social Change* 45(3): 185–200.
- Morselli, C., C. Giguère, and K. Petit. 2007. The efficiency/security trade-off in criminal networks. *Social Networks* 29(1): 143–153.
- Müller, J., M. Kretzschmar, and K. Dietz. 2000. Contact tracing in stochastic and deterministic epidemic models. *Mathematical Biosciences* 164: 39–64.
- Newman, M. 2002. Assortative mixing in networks. *Physical Review Letters* 89: 208701.
- Nichols, J. D. 1992. Capture–recapture models. *BioScience* 42: 94–102.
- O’Neil, S. 2007. Terrorist precursor crimes: Issues and options for Congress. Report RL34014, Congressional Research Service (Washington, DC).
- Office of the Inspector General. 2008. The Federal Bureau of Investigation’s terrorist threat and suspicious incident tracking system. Audit Report 09-02, US Department of Justice (Washington, DC). <http://www.usdoj.gov/oig/reports/FBI/a0902/final.pdf> (last accessed 6 January 2009).
- Palla, G., I. Derenyi, I. Farkas, and T. Vicsek. 2005. Uncovering the overlapping community structure of complex networks in nature and society. *Nature* 435: 814–818.
- Passel, J. S. 2006. The size and characteristics of the unauthorized migrant population in the U.S. Pew Hispanic Center (Washington, DC). <http://pewhispanic.org/files/reports/61.pdf> (last accessed 1 January 2009).
- Pastore, A. L. and K. Maguire. 2003. Sourcebook of criminal justice statistics. University at Albany (Albany, NY). <http://www.albany.edu/sourcebook/pdf/t3170.pdf> (last accessed 31 December 2008).
- Pierce, G. L., A. A. Braga, C. Koper, J. McDevitt, D. Carlson, J. Roth, A. Saiz, R. Hyatt, and R. Griffith. 2004. Characteristics and dynamics of crime gun markets: Implications for supply-side focused enforcement strategies. Report 208079, US Department of Justice (Washington, DC). <http://www.ncjrs.gov/pdffiles1/nij/grants/208079.pdf> (last accessed 31 December 2008).
- Qin, J., J. Xu, D. Hu, M. Sageman, and H. Chen. 2005. Analyzing terrorist networks: A case study of the Global Salafi Jihad network. In *Intelligence and security informatics*, ed. P. Kantor, G. Muresan, F. Roberts, D. Zeng, F. Wang, H. Chen, and R. Merkle, vol. 3495 of Lecture Notes in Computer Science, 287–304. Berlin: Springer.
- Raab, J. and H. B. Milward. 2003. Dark networks as problems. *Journal of Public Administration Research and Theory* 13(4): 413–439.
- Ressler, S. 2006. Social network analysis as an approach to combat terrorism: Past, present, and future research. *Homeland Security Affairs* 2(2): 1–10.
- Rodriguez, J. A. 2005. The March 11th terrorist network: In its weakness lies its strength. Working Paper EPP-LEA. <http://www.ub.edu/epp/wp/11m.PDF> (last accessed 31 December 2008).
- Smith, B. L. and K. R. Damphousse. 2002. American terrorism study: Patterns of behavior, investigation and prosecution of American terrorists, Final Report. Report 193420, US Department of Justice (Washington, DC).
- Smith, B. L., K. R. Damphousse, and P. Roberts. 2006. Pre-incident indicators of terrorist incidents: The identification of behavioral, geographic, and temporal patterns of preparatory conduct. Report 214217, US Department of Justice (Washington, DC).
- Smith, B. L., J. Cothren, P. Roberts, and K. R. Damphousse. 2008. Geospatial analysis of terrorist activities: The identification of spatial and temporal patterns of preparatory behavior of international and environmental terrorists. Report 222909, US Department of Justice (Washington, DC), p. 77.
- Stockton, P. N. 2009. Reform, don’t merge, the Homeland Security Council. *The Washington Quarterly* 32(1): 107–114.

- Straw, J. 2008. New life for terror databases. *Security Management* (December).
- Transactional Records Access Clearinghouse. 2003. A special TRAC report: Criminal enforcement against terrorists. Syracuse University. <http://trac.syr.edu/tracreports/terrorism/report011203.html> (last accessed 6 January 2009).
- Transactional Records Access Clearinghouse. 2007. Criminal terrorism enforcement in the United States during the five years since the 9/11/01 Attacks. Syracuse University. <http://trac.syr.edu/tracreports/terrorism/169/> (last accessed 5 January 2009).
- University of Maryland. 2008. Terrorist organization profiles. Study of Terrorism and Responses to Terrorism. <http://www.start.umd.edu/data/tops/> (last accessed 5 January 2009).
- Washington Post*. 2006. 325,000 names on terrorism list. 15 February. <http://www.washingtonpost.com/wp-dyn/content/article/2006/02/14/AR2006021402125.html> (last accessed 5 January 2009).
- Watts, D. J., P. S. Dodds, and M. Newman. 2002. Identity and search in social networks. *Science* 296(5571): 1302–1305.
- Weisel, D. L. 2007. Bank robbery. Problem-oriented guides for Police 48, US Department of Justice (Washington, DC). <http://www.cops.usdoj.gov/files/ric/Publications/e03071267.pdf> (last accessed 31 December 2008).
- Xu, J. and H. Chen. 2008. The topology of dark networks. *Communications of the ACM* 51(10): 58–65.