

Targeting by Transnational Terrorist Groups

Alexander Gutfraind

Abstract Many successful terrorist groups operate across international borders where different countries host different stages of terrorist operations. Often the recruits for the group come from one country or countries, while the targets of the operations are in another. Stopping such attacks is difficult because intervention in any region or route might merely shift the terrorists elsewhere. Here, we propose a model of transnational terrorism based on the theory of activity networks. The model represents attacks on different countries as paths in a network. The group is assumed to prefer paths of lowest cost (or risk) and maximal yield from attacks. The parameters of the model are computed for the Islamist–Salafi terrorist movement based on open source data and then used for estimation of risks of future attacks. The central finding is that the United States (US) has an enduring appeal as a target, due to lack of other nations of matching geopolitical weight or openness. It is also shown that countries in Africa and Asia that have been overlooked as terrorist bases may become highly significant threats in the future. The model quantifies the dilemmas facing countries in the effort to cut terror networks, and points to a limitation of deterrence against transnational terrorists.

1 Introduction

Despite vast investments in counter-terrorism, victory in the global war on terror remains elusive. In part, this is because terrorist groups are highly adaptive in their tactics and strategy. When airport scanners were installed to detect weapons and explosives, terrorists switched to explosives that cannot be detected using the

A. Gutfraind (✉)

Center for Nonlinear Studies and T-5, Theoretical Division, Los Alamos National Laboratory,
Los Alamos, NM, USA

e-mail: agutfraind.research@gmail.com

The rest of the paper will introduce another method for risk assessment: a quantitative network-based model. The model takes demographic and economic information pertaining to violent Islamist–Salafi groups – the most probable source of future attacks – and estimates the risk of various transnational terror plots. The model suggests that the future of transnational terrorism may be substantially different from the past:

1. Several regions will become large new sources of transnational terrorism (Sect. 4)
2. The US will rise as the terrorists’ preferred attack destination (Sect. 4)
3. Successes in stopping foreign-based plots against the US will increase the threat to other countries (Sect. 4.1)
4. Deterrence will be hard to achieve (Sect. 4.2)

The model is based on an activity network for stages of terrorist attacks. The network represents decisions required for terrorist operations on the global scale, such as which country to attack. No distinction is made between “transnational” and “international” terrorism, both referring to terrorist groups that operate using foreign bases, support or inspiration. This coarsened scale of analysis exposes the strategic picture and can guide counter-terrorism decision making at the national and international levels. It also quantifies a kind of unintended effect from counter-terrorism measures known as “transboundary externality” [36, 37]: the redirection of terrorists from one country to another, because the latter is less protected.

To the author’s knowledge, this is the first model in the open literature that models transnational networks and estimates which countries might be selected for future attacks. Previous work considered target selection by terrorists but where targets are implicitly within a single country so the costs of bringing the attackers and their weapons to their target are negligible (see e.g. [6]). In contrast, for transnational terrorism security measures and international logistics play a central role in attack planning [22, Chap. 3]. Other work considered the structure of the terrorist networks at the level of individual operatives or functions, rather than as the global network presented here (cf. [9, 14, 19, 29, 44].)

The model’s findings imply that policymakers across the world should increase their coordination of counter-terrorism measures and be watchful for several emerging threats. The model also advances methodology in the analysis of terrorism. Based on this network model, future work could examine the risk from specific groups and to additional types of targets.

2 A Model of Transnational Terrorism

Transnational terrorist groups are characterized by their global aims, as opposed to regional conflicts; they recruit and attack in several countries. Transnational Islamic fundamentalist groups will serve as the central application of this model. These include al-Qaida, Hezbollah but also possibly extremist groups not currently thought to be violent, such as Hizb-ut-Tahrir. Those groups are at the focus because

they are probably the most potent present-day transnational terrorist threat. Instead of looking at any particular fundamentalist group, we will estimate the risk from a potential world-wide violent Islamist movement. Other violent transnational ideologies or even a specific existing group can be quantified through this model by re-estimating the model's parameters.

It is sometimes argued that estimation of terrorism risk is near impossible because terrorism is irrational behavior. Indeed, how can one explain the fanaticism of suicide bombers? However, the preponderance of evidence supports the alternative view – the rational choice theory (RCT) [40]. RCT claims that terrorist groups and leaders are rational agents capable of strategic decision-making. Their decisions are expressions of “instrumental rationality”, that is, in line with their values and objectives [26]. The sophistication and technological adaptability of terrorists, such as in developing triggers for explosives, is strong evidence for their intelligence [21, 24]. More evidence for RCT comes from studies of target selection [37]. Those consistently find evidence for a substitution effect – as governments improve protection to certain targets, terrorists substitute them with less protected targets [2, 10, 21]. Indeed, the defining feature of terrorism – the use of violence against civilians rather than against military targets – is a strategic substitution effect because the latter are harder targets. Another line of evidence for rationality comes from analyzing the internal dynamics of terrorist groups. Rather like non-violent organizations, they perform cost-benefit analyses and produce volumes of documents [38, 39]. Even the behavior of suicide bombers is sometimes viewed as expression of selfish utility maximization, where the benefits of such acts are either to the agent in paradise or to family members on earth (for a nuanced “rationally irrational” model see [7], for a critique of the terrorist strategy see [1]). The strength of the rational choice model is its predictive power. One can not only correctly anticipate which strategies terrorists would adopt (see e.g. [5]) but also how counter-terrorist policies would affect those strategies.

2.1 Operations Submodel

Suppose a transnational group controls a cell in a country, and must decide where to dispatch this cell (the cell might also be self-mobilizing, in which case it must solve its own targeting problem.) The three options are (1) do a domestic attack, (2) send the cell to attack another country (a transnational attack), and (3) do nothing. Option (1) entails certain risks and costs for collecting intelligence and preparing weapons. Dispatching the cell into another country, (2), incurs the additional cost and risk of interception due to security barriers, such as visas, intelligence collection in a foreign environment, and cultural difficulties. However, the other country might have more favorable security environment or offer better targets – more significant or less protected. Option (3) – abandon the attack and hide – has little or no risk or accounting cost and preserves the cell for future operations.

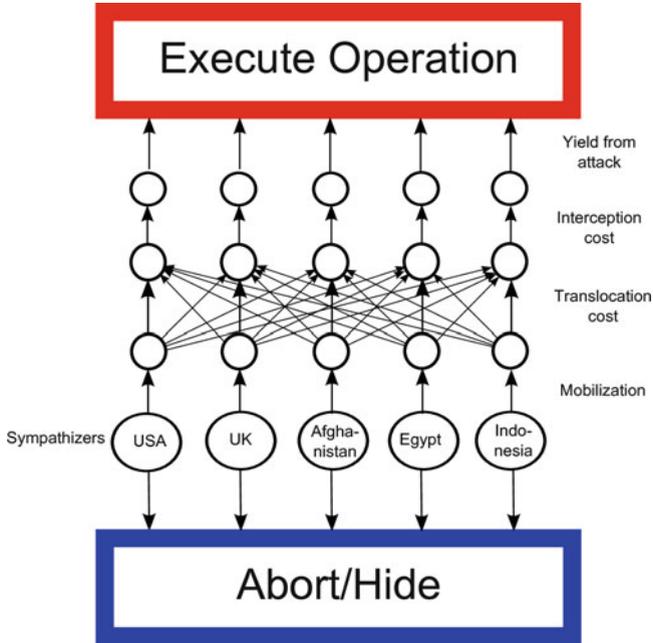


Fig. 2 Illustration of the model for five countries. The vertical direction represents countries while the horizontal represents different stages in execution of plots. Domestic attack plans correspond to motion upwards, while transnational attacks also make a diagonal transition. The full model includes many more countries

Any rational decision maker must weight the costs and benefits, and take the action offering the greatest net benefit. Surely then terrorists would also do such analysis, weighing at least the most obvious target choices and travel routes. A simple way of representing this is with an activity network, where nodes represent different stages of terrorist operations at different countries, and edges show the cost and risk involved in each stage (Fig. 2). In this figure, the vertical direction corresponds to the countries, including the country of origin, while the horizontal direction corresponds to the postures of the cells: the stages of the plots.

The network represents the options of the rational decision maker as directed paths – chains of nodes and directed edges that start in the source country node and lead to either the “attack” node or the “abandon/hide” node. If complete information is available about the costs and benefits of each option, then the rational decision is to select the path with the highest utility, that is the path with highest net benefit (benefit minus cost). For any path p , the cost $c(p)$ is found by adding the weights on the edges (tasks) constituting the path.

The edge weights of this network could represent resources like money or materiel that are consumed and produced by terrorist operations. The network could also be used to perform a probabilistic risk assessment (PRA): to evaluate

the gains from possible operations and the probabilities of successfully completing intermediate stages in the operations. Such a PRA is what we will do. In other words we will take the perspective of the terrorists: determine what they want and what they fear in order to anticipate how they will act.¹

It is an open question whether terrorist groups can or will use such an algebraic method to analyze their operations. However, given their sophistication they may well come to the same decisions using other means or through operational experience. Of course, they might also intentionally avoid the most probable attacks to achieve surprise, but only at a cost (and models could also be constructed to anticipate that too).

Consider now the following specific model for transnational terrorist attacks, Fig. 2. A cell that was mobilized at country i experiences (1) the translocation cost/risk, T_{ij} , representing the barriers for moving from country i to country j ; (2) the risk of interception at country j , I_j ; and (3) the yield Y_j from attacks at country j . Yield reflects the gain to the terrorists from a successful attack, and so has the opposite sign from cost. A domestic attack at country i has cost $c(p) = T_{ii} + I_i + Y_i$ while a transnational attack has cost $c(p) = T_{ij} + I_j + Y_j$ ($i \neq j$). Because costs represent risks, the words “cost” and “risk” will be used interchangeably. Sometimes attackers reach country j through one or several intermediate countries (exploiting e.g. the Schengen treaty), a possibility we ignore for simplicity. From the counter-terrorism point of view, the likelihood of a particular plot depends also on the supply of operatives originating at each country. Therefore, we will estimate for each country i the number of cells that originate there, S_i . If the group decides to abandon, its path has cost $c(p) = A$. The parameter A may be a negative, representing the preservation of the cell, or positive, if the cell cannot be reactivated. It is possible to include in the model additional costs like cost of recruitment or training but this will be left for future studies because the data is hard to estimate.

The model’s parameters can be estimated from open source information with a modest degree of confidence (see Sect. 3). Briefly, transit costs were estimated from data on global migration, the risk of interception from national expenditure on internal security and attack yields based on the political power of the targeted country, represented by its Gross Domestic Product (GDP). The supply of plots is estimated from public opinion surveys measuring support for terrorist attacks and from demographic data.

¹Here is how PRA is represented by networks. Suppose in a multi-stage terrorist operation r_s is the probability of success at stage s (out of k stages in total) conditional on success at every previous stage. Suppose the gain from a successful operation is G (≥ 1). Then the *expected* gain from the operation is $E = r_1 r_2 \dots r_k G$. Let us now relate r_s values to costs ($c_s \geq 0$) using exponentiation: $r_s = e^{-c_s}$, and let the gain be a function of yield Y : $G = e^{-Y}$. Thus, an attack has expected gain $E = \exp[-(c_1 + c_2 + \dots + c_k + Y)]$. In the network representation of terrorist operations, we can compute the sums in the exponent by adding edge weights along network paths that trace through all the stages. Paths of lower weights translate to attacks of greater expected gain. By comparing such paths we could anticipate which attacks would have the highest expected gain.

2.2 Stochastic Decisions Submodel

If transnational terrorist groups could determine the values of the parameters precisely (the next section discusses this problem), then they should be able to plot the optimal attack from each country i by considering all possible options and finding the path that minimizes cost:

$$\min_j \left[\underbrace{T_{ij} + I_j + Y_j}_{c(p_{ij})} \right].$$

However, one of the general difficulties in decision making is uncertainties about costs and risks. Terrorists, like other decision makers should therefore occasionally identify the optimal attack incorrectly. Reliable risk assessment must therefore take into account the possibility that adversaries make mistakes (and ideally even the use of unpredictability to achieve surprise.) Fortunately, suitable stochastic prediction methods have already been developed for activity network models like in Fig. 2. With those methods probabilities can be assigned to different terrorist plans based on the costs of the corresponding paths on the network.

The methods to used here were introduced in [18, 20] and are based on Markov chains. In those chains, the path of least cost is typically assigned the highest probability but other paths have non-zero probabilities, and these probabilities can be quite high (for details see Appendix 2).² From this Markov chain model it is possible to compute the number of times any particular country would be targeted as well as to compute the changes in targeting due to various defensive actions, which are represented as increases in edge weights. It is also possible to determine whether defensive actions would materially increase the costs for the adversaries or merely lead them to change targets. Finally, the Markov chain model will incorporate our uncertainty about the parameters in the transnational network. Therefore, it automatically provides predictions that are robust under this uncertainty.

²One of the advantages of the stochastic model is that it can interpolate between the two extremes of complete ignorance and perfect information using a single parameter λ (≥ 0) that describes the amount of information available to the adversaries. For a given level of information, the probability that a path p would be selected is proportional to $\exp(-\lambda c(p))$. When λ is very large the path of least cost has a much higher probability than any of the alternatives, while λ close to 0 assigns all paths approximately the same probability. We set $\lambda = 0.1$ in the following but its value has a smooth effect on the predicted plots (i.e. the sensitivity is low). A value of 0.1 means that if the terrorist group learns of a increase in path cost by 10 units, its probability of taking the path will decrease by a multiplicative factor of ≈ 2.72 . The exact amount of change depends on the original path probability: it is not as great a decrease when the original probability is high.

3 Estimation of Parameters

The model contains several sets of inputs: (1) the supply of plots at country i , S_i ; (2) barriers for moving from country i to country j , T_{ij} ; (3) risk of interception at country j , I_j ; and (4) the yield from attacks at country j , Y_j . The yield of abandoning, A will be set to ∞ (no abandoned plots) and its effect will be analyzed separately. Because (1)–(4) contain security-related information that is also difficult to measure, the information is not public. Luckily, one can derive estimates from publicly-available demographic and economic data. Readers wishing to see the final results of estimates should open Tables 1–3 and skip the rest of this section.

Table 1 Information about countries: the interception cost (*left*) and the yields from attacks (*right*)

Country	Intercept. Cost I_j	Country	Yield Y_j
New Zealand	2.3	United States	−54.0
United Kingdom	2.1	Japan	−24.1
Czech Republic	1.6	Germany	−9.5
Hungary	1.6	United Kingdom	−7.8
United States	1.5	France	−6.8
Slovakia	1.5	Italy	−5.3
Estonia	1.5	Canada	−3.8
Portugal	1.4	Spain	−3.2
Italy	1.3	South Korea	−3.1
Spain	1.3	Australia	−2.2
Poland	1.2	Netherlands	−1.8
Netherlands	1.2	Sweden	−1.2
Israel	1.1	Belgium	−1.1
Belgium	1.1	Austria	−0.9
Slovenia	1.0	Poland	−0.9
Germany	1.0	Norway	−0.8
Canada	0.9	Denmark	−0.7
Austria	0.9	Greece	−0.6
Iceland	0.8	Finland	−0.6
Ireland	0.8	Ireland	−0.5
Japan	0.8	Portugal	−0.4
Sweden	0.7	Czech Republic	−0.2
Finland	0.6	New Zealand	−0.2
France	0.6	Hungary	−0.2
South Korea	0.6	Slovakia	−0.0
Greece	0.5	Luxembourg	−0.0
Denmark	0.3		
Luxembourg	0.2		
Norway	0.2		
Australia	0.0		

Table 2 Translocation costs T_{ij} (country i to country j) for select country pairs

Destination ->	Australia	Canada	France	Germany	Italy	Japan	South Korea	Spain	UK	US
Afghanistan	0.0	0.0	1.9	0.1	29.5	44.2	44.2	18.1	0.3	0.1
Algeria	0.2	0.1	0.1	9.9	15.1	32.4	32.4	9.2	6.2	1.9
Azerbaijan	0.6	0.3	10.3	4.3	50.2	71.6	71.6	9.3	5.1	0.2
Bangladesh	0.4	0.1	8.1	3.2	1.2	12.9	8.9	5.4	0.1	0.3
Burkina Faso	6.3	2.0	1.1	5.4	2.5	192.0	192.0	27.8	44.1	11.2
Chad	2.8	0.6	0.7	12.2	43.9	407.2	407.2	62.4	15.3	9.3
Cote d'Ivoire	2.1	0.5	0.1	2.8	0.8	17.7	17.7	8.1	1.5	1.2
Egypt	0.0	0.1	1.9	1.1	2.7	12.8	12.8	13.9	1.4	0.2
France	0.0	0.1	0.0	34.6	1.9	1.8	2.7	1.3	28.2	0.2
Guinea	2.2	0.4	0.3	0.4	3.4	4.8	4.8	0.6	8.3	1.2
India	0.2	0.1	4.9	3.5	5.9	64.4	153.1	9.4	0.3	0.2
Indonesia	0.3	0.2	2.5	0.9	7.6	5.0	3.2	7.0	1.3	0.3
Iran	0.0	0.0	1.2	0.5	4.4	3.1	3.1	4.0	0.5	0.1
Iraq	0.0	0.0	3.0	0.5	13.6	98.3	98.3	5.3	0.3	0.1
Jordan	0.0	0.0	3.5	1.4	2.9	9.2	9.2	1.2	0.8	0.0
Kazakhstan	0.5	0.1	7.4	23.1	5.9	81.6	81.6	8.8	2.9	0.4
Libya	0.0	0.1	6.3	4.3	0.8	55.4	55.4	15.1	0.7	0.4
Malaysia	0.0	0.0	0.8	0.1	4.1	1.8	14.8	3.7	0.0	0.1
Morocco	0.2	0.1	0.1	1.0	0.3	13.1	13.1	0.7	3.3	0.6
Mozambique	0.7	0.4	1.8	0.8	3.8	472.8	472.8	2.0	0.4	1.7
Nigeria	0.7	0.5	14.3	1.8	3.1	8.3	8.3	4.4	0.4	0.4
Pakistan	0.2	0.1	2.3	1.6	2.2	11.6	9.7	1.4	0.1	0.2
Palestine	0.0	0.0	2.7	1.5	15.5	1e+200	1e+200	3.9	0.7	0.0
Russia	0.1	0.1	6.8	38.3	6.8	10.3	10.3	3.1	7.5	0.2
Saudi Arabia	0.2	0.1	4.4	3.7	20.7	32.4	32.4	15.6	0.6	0.2
Senegal	0.4	0.4	0.0	1.3	0.1	6.3	6.3	0.4	4.7	0.8
Somalia	0.0	0.0	0.8	0.0	0.2	463.3	463.3	6.0	0.0	0.0
Sudan	0.1	0.1	7.9	2.8	23.6	34.5	34.5	34.5	0.8	0.5
Tajikistan	2.3	1.5	56.7	27.3	29.8	1967.0	1967.0	80.3	12.3	0.6
Tanzania	0.3	0.0	7.9	1.0	6.2	19.5	19.5	24.5	0.1	0.6
Tunisia	0.2	0.1	0.1	1.5	2.4	7.8	7.8	19.2	5.2	0.8
Turkey	0.0	0.2	0.4	0.1	24.4	10.8	10.8	38.2	1.1	0.3
UK	0.0	0.0	32.2	23.7	2.9	0.7	2.7	1.3	0.0	0.1
US	0.0	10.6	1.2	0.9	0.7	0.7	0.9	1.7	0.3	0.0

Rows are countries of departure, columns are the destinations. Notice that Japan has relatively large barriers, as estimated by its abnormally low population of immigrants. OECD data was key to those estimates, and when it was not available, it was sometimes possible to use neighboring countries to impute the missing information.

In building the estimates, it will be assumed for simplicity that each stage of terrorist operations carries about the same amount of risk. Namely, that the medians of T_{ij} ($i \neq j$) and of I_j both equal 1. Both T_{ij} and I_j show considerable variability around the median because some plots are much less risky than others. The yield from attacks is also normalized by its median.

Table 3 The supply of plots for the default weight, and change under two alternative weightings (high commitment and low commitment)

Country	Supply S_i	High commitment (%)	Low commitment(%)
Indonesia	52745.4	-46.2	24.6
Nigeria	52687.8	-33.3	17.8
India	49624.7	-43.1	23.0
Bangladesh	39960.8	-33.8	18.0
Iran	26723.7	-30.6	16.3
Egypt	24731.6	-41.0	21.8
Pakistan	16537.8	-22.1	11.8
Algeria	12387.6	-30.6	16.3
Iraq	11021.7	-30.6	16.3
Sudan	10910.5	-30.6	16.3
Afghanistan	10168.3	-30.6	16.3
Saudi Arabia	9037.1	-30.6	16.3
Yemen	8462.6	-30.6	16.3
Ethiopia	8278.6	-39.7	21.2
Mali	8247.4	-23.2	12.4
Uzbekistan	8161.3	-43.1	23.0
Syria	7315.4	-30.6	16.3
Morocco	6878.5	-26.5	14.1
China	6680.7	-43.1	23.0
Niger	6497.3	-32.2	17.2
Malaysia	6466.6	-47.7	25.4
Turkey	5521.4	-44.0	23.5
Russian Federation	5081.9	-43.1	23.0
Palestine	4632.0	-21.1	11.2
Burkina Faso	4004.9	-32.2	17.2
Tunisia	3700.5	-30.6	16.3
Senegal	3668.5	-40.3	21.5
Guinea	3664.4	-32.2	17.2
Cote d'Ivoire	3338.1	-32.2	17.2
Somalia	3258.2	-30.6	16.3

Certain countries are unusually dependent on the level of support the most radical segment provides, while others see relatively broad support for violence. Only the 30 largest sources are shown. For some countries in a particular region the sensitivity is identical because national survey data was not always available. In those countries, the radicalization values (σ^r , σ^s , σ^o) were imputed from regional averages.

Transformations of this kind on costs and yields are unavoidable if we wish to remove the effect of units, but they do reduce the reliability of the model. However, the core findings of the model regarding certain countries agree well with intuition, as will be seen. As well, the stochastic Markovian decision model is not sensitive to the exact values of the parameters. In computational simulations, we found the sensitivity to be low, with variation of $\pm 50\%$ in parameter values leading to only $\pm 10\%$ change in attack predictions (see Appendix 1).

3.1 Estimating the Supply of Plots, S_i

The task here is to determine the potential supply of recruits that a violent worldwide Islamic movement can command. Surprisingly, this task is easier than to determine the support for a particular group like al-Qaida: with a particular group, its past actions and current platform can significantly affect its support base. Focusing on a particular group, even a well-known group like al-Qaida could also lead to underestimation of the risk involved from its ideological pool. Another concern is self-mobilization of violent cells without any connection to an existing group [35].

A comprehensive picture on possible plots can be obtained from surveys. Over the last decade, most recently in 2009, the Pew charitable trusts run several global attitude surveys. Among other questions the survey asked Muslims about their support for suicide bombings [42]. In each of the surveyed countries, respondents were asked to state whether suicide bombings is “never justified” (σ^n), “rarely justified” (σ^r), “sometimes justified” (σ^s), and “often justified” (σ^o). These are given as fractions of the respondents. For some countries no data was available, so the quantities were extrapolated from countries in the same geographic region (e.g. Middle East, Americas, etc.) Pew also collected data on the Muslim population in 235 different countries and territories (J_i) [30] (of course, the overwhelming majority of Muslims everywhere are opposed to terrorism in the name of their religion.) The supply of violent plots can be estimated by taking the population and multiplying by the weighted fraction of respondents professing support for violence (the weights are s_r, s_s, s_o). One must also take into account that only a small fraction of those who profess radical ideology would actually be involved in a plot and that several people are involved in each plot (a factor Q):

$$S_i := Q \cdot J_i \cdot (s_r \sigma^r + s_s \sigma^s + s_o \sigma^o).$$

The support weights were set by default based on the assumption that every increase in professed support leads to an increase by a factor of 2 in the resources available to terrorist groups: $(s_r, s_s, s_o) = (0.25, 0.50, 1.00)$. We can explore the sensitivity of supply S_i to this assumption through two alternatives: most of the tangible support come from the narrow but committed minority, $(s_r, s_s, s_o) = (0.1, 0.2, 1.0)$, and a situation where even the least-committed supporters materially boost the terrorists, $(s_r, s_s, s_o) = (0.33, 0.66, 1.00)$. Note that the weights effect only the relative importance of countries as sources of terrorism, not the targets of plots originating in a given region.

In certain countries, such as Malaysia, Indonesia, and Turkey support for violence is relatively broad. This can be seen from the large decrease in supply under the high-commitment scenario, $(s_r, s_s, s_o) = (0.1, 0.2, 1.0)$, compared to the default weights $(s_r, s_s, s_o) = (0.25, 0.50, 1.00)$. In regions such as the Palestinian Territories, Pakistan, and Morocco the support is more dependent on the radical minority, as seen from the relatively small increase under the scenario $(s_r, s_s, s_o) = (0.33, 0.66, 1.00)$. Overall, the 10 largest sources of plots are not more sensitive to those parameters than other sources.

The factor Q enters as a multiplicative term at all source countries, and so its value has no bearing on the relative risk estimates. Nevertheless, it could be crudely estimated as follows. In 2006, the head of the British Security Service (MI5) reported that: “. . . my officers and the police are working to contend with some 200 groupings or networks, totaling over 1,600 identified individuals (and there will be many we don’t know) who are actively engaged in plotting, or facilitating, terrorist acts here and overseas” [31]. Furthermore, “over 100,000 of our citizens consider that the July 2005 attacks in London were justified.” This implies active participation at a rate of at least 1.6% and 8 people per plot ($Q = 0.002$).

3.2 *Estimating the Barriers for Moving from Country i to Country j , T_{ij}*

Barriers to transnational attacks include both deliberate barriers such as screening and intelligence and unofficial barriers such as differences in language and culture. Official barriers depend on factors such as the intelligence available on targets in the destination country, the cooperation the targeted country received from both the country of departure and the transport agent (e.g. airline). None of those figures are publicly available but a proxy measure can be found, as follows. Transnational terrorists often use tourism, education or immigration as cover to obtain travel documents and permits [17]. Indeed, travel in all of those categories became more difficult across the developed world as a result of the security measures introduced after the 9/11 attacks. Migration patterns thus provide an estimate of official barriers. Unofficial barriers to terrorism are likewise similar to the unofficial barriers to migration, including differences in language, culture, ethnicity, and others. Therefore, the foreign-born migrant population, suitably normalized, could be used as a proxy of transnational freedom of travel. Migration into most OECD countries is documented by the OECD [34].

It is to be expected that the number of migrants would be positively correlated with the population of the countries and negatively correlated with distance. This is known as a “gravity law” model. Many national and international relationships such as trade flows are well-approximated by gravity laws [13, 25], named for their similarity to Newton’s law for the force of gravity. Therefore, an estimate for the number of migrants between country i and country j is the product of their populations (data: United Nations) divided by their distance squared (data: CEPII [32]): $\frac{P_i P_j}{d_{ij}^2}$. When the actual number of migrants, m_{ij} , falls below this estimate, that may indicate heightened official or unofficial barriers. Thus, we define the raw transnational terrorism barrier between countries i and j as:

$$\widehat{T}_{ij} := \frac{P_i P_j}{d_{ij}^2} / m_{ij} .$$

The data must now be standardized, for several reasons: (1) the barrier data should be comparable with other costs considered by the terrorists (and in the model) by

removing the effects of units for population and distance and (2) since the barrier is a cost and risk, it must be represented by positive number in the activity network. Therefore, the quantity T_{ij} was computed from \widehat{T}_{ij} by determining the minimum ($Min\widehat{T}$) and median ($Med\widehat{T}$). Because of (2) $Min\widehat{T}$ is subtracted from \widehat{T}_{ij} , and for (1) the quantity is divided by the median of the shifted values:

$$T_{ij} = \left(\widehat{T}_{ij} - Min\widehat{T} \right) / \left(Med\widehat{T} - Min\widehat{T} \right).$$

The resulting values are non-negative numbers with a median of 1.0. The more standard procedure of first removing the average and dividing by the standard deviation was rejected because the distribution is visibly non-Gaussian with large positive outliers (hence a skewed mean and large variance). Domestic operations will be assumed to have negligible barriers ($T_{ii} = 0$ for all countries i). Visa-free travel zones such as the European Schengen zone could be incorporated into T_{ij} , but were not because (1) they do not eliminate the considerable linguistic and cultural barriers, and (2) data on terrorism originating in Europe suggests a strong preference for domestic attacks (a catalog is found in [4]). Thus, plotters prefer targets in their homeland even though a neighboring European country might offer more valuable targets.

The OECD data lacks information about migration to non-OECD countries. Therefore set $T_{ij} = \infty$ in all such cases (effectively blocking such paths). While the OECD includes some of the most geopolitically-important nations of the planet, obtaining data on translocation costs to non-OECD countries would be valuable for two reasons. First, only with such data can we estimate the risk of terrorism to those nations (such as the July 11, 2010 bombings in Kampala), and second to estimate the effect of counter-terrorism policies in the OECD on terrorism in other countries. Indeed, in the ITERATE database of terrorist incidents [33], attacks on OECD countries that can be traced to Islamist groups account for only 22% of all Islamist attacks.

3.3 *Estimating the Risk of Interception at Country j , I_j*

The risk of interception can be estimated from OECD data on expenditure on public order and safety as a fraction of GDP. The relevant figure is the fraction of GDP rather than the raw figure because the number of valuable targets is related to the size of the economy, so the fractional figure indicates the level of security vulnerable sites can expect to receive. The GDP also correlates with the population size (in rich countries) and thus to the amount of police resources available to protect any human target. The extreme case of totalitarian police states is suggestive: in such countries internal security expenditures are disproportionately large relative to the GDP, and indeed terrorists have a lot of difficulties operating there [23]. This estimate of course neglects the efficiency of internal security force – a factor that is hard to estimate.

The internal security data is transformed almost exactly like the barrier data and for the same reasons: start with figures for internal security expenditure as a fraction of GDP for country j , SEC_j then compute the minimum ($MinSEC = \min_j SEC_j$) and median ($MedSEC$), and then normalize:

$$I_j = (SEC_j - MinSEC) / (MedSEC - MinSEC).$$

Generally speaking, we find that there is not much variation in the risk of interception in different countries (Table 1), as compared to variation in factors such as yield, discussed next. This suggests that interception risk plays a minor role in target choice.

3.4 Estimating the Yield from Attacks at Country j , Y_j

Transnational terrorist attacks attempt to influence policies. For example, one of al-Qaida's original objectives was to compel the withdrawal of US forces from Arabia, while Hezbollah forced France and the US to withdraw their peacekeepers from Lebanon in the 1980s. The precise value of the targets shifts with time and the political situation, but typically larger richer countries make for more powerful players in the international arena, and hence more important targets. Moreover, their homelands carry more targets of symbolic, political and economic significance. The economic damage from the loss of life and physical assets is also higher in richer countries because they tend to have higher productivity for labor and capital. Thus, it is expected that transnational terrorists would seek to attack larger richer countries. The weight of a country can be estimated from its dollar GDP figures at current exchange rates (data: UN).

Timing or political dynamics does play a role in transnational terrorism but its importance should not be overestimated. For example, the Madrid March 11, 2004 train bombings are often viewed as intending to pressure the Spanish government to withdraw its forces from Iraq, and they were timed with the Spanish elections. But surely an important factor was Spain's geopolitical weight (GDP is ranked 12th in the world) and its large contribution to the 2003 invasion. Otherwise, al-Qaida could have just as well pressured smaller countries such as El Salvador and Mongolia to withdraw their contributions to the invasion.

Here is how the yield Y_j was computed from the GDP figures. Recall that costs (barriers, internal security) are all positive, so yields must be negative. Let the minimum GDP be $MinGDP$, and the median $MedGDP$. The following formula produces negative values with a standardized median:

$$Y_j = (MinGDP - GDP_j) / (MedGDP - MinGDP).$$

The resulting values have a median of -1.0 .

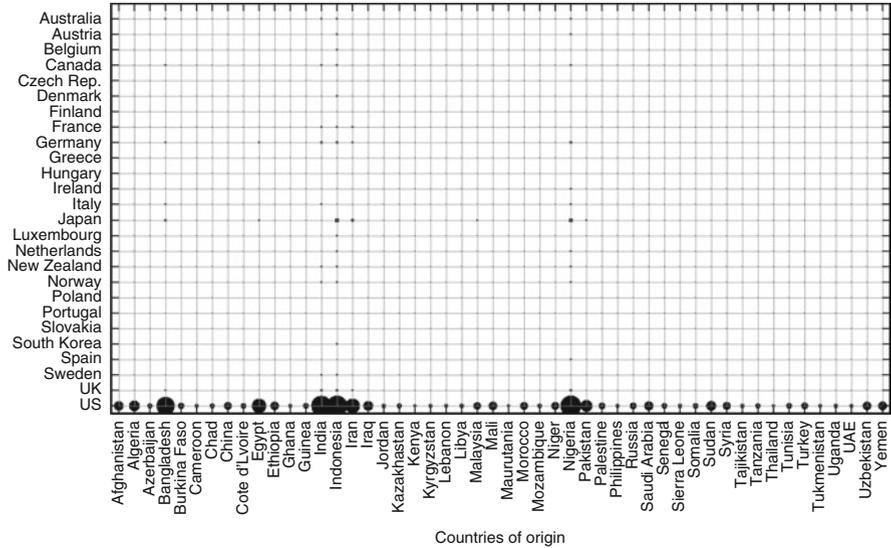


Fig. 3 Predicted attack risk matrix. The area of a circle at coordinates (i, j) is proportional to the number of plots from i to j . The *bottom row* indicates that the vast majority of plots target the US

4 Predictions

One way of representing the solution of the model is through an attack risk matrix, the counterpart of the historical data matrix in Fig. 1. The model predicts (Fig. 3) that the United States would attract the bulk of transnational terrorism – all other countries are almost free of terrorism (small circles). The reason the United States is such a magnet is because of its vast geopolitical weight and relatively open borders.

Examination of the sources for attacks exposes a number of risks. There is a considerable terrorist threat from Bangladesh, India, Indonesia, and Nigeria. They combine a large population and relatively high support for terrorism. It is notable that the 2009 Christmas bomber was Nigerian – one of the first attacks on OECD from that country. The risk from India stems from its large Muslim population (about 160 million) and the relatively large radicalization in the region (although the radicalization might be lower in India than in neighboring countries.)

The high burden of attacks borne by the US is directly related to the rational choice model: if there is a big prize to be won by attacking the US, no rational terrorist would attack other countries. The reasons why non-US attacks do occur (cf. Fig. 1) include: (1) some terrorist groups such as ethno-nationalist groups see as their enemy a particular country and lack a global agenda; (2) global Salafi groups have not yet expanded their recruitment channels in countries such as Nigeria and Bangladesh, so a large fraction of attacks is still carried out by groups with more narrow agendas; and (3) the US has deployed counter-terrorism measures commensurate with the threat it faces, making the US too costly to attack.

One implication of this finding concerns US policy. The matrix justifies in principle outlays by the US government towards countering international terrorism as a whole, without regard to its target. Investments in international counter-terrorism measures, such as nation building in unstable states, if effective in reducing the number of plots, are also efficient from the US perspective: because the US is the target of choice, it will retain most of the benefits from reducing the terror threat [28]. Unfortunately, many policies previously adopted were ineffective or had perverse effects on international terrorism (the so-called “blowback”) (see e.g. [15, 16].)

4.1 National Fortresses

Consider now several alternative scenarios for the future, motivated by strengthening of counter-terrorism defenses, which may make transnational attacks less feasible. Suppose the US was successful in deterring attacks against itself by greatly increasing the barriers to entering US soil. If so, Fig. 4 shows the likely effect.

The protection of US frontiers will significantly increase the attack risk to most other OECD nations because transnational groups should then switch to more accessible targets. Perhaps surprisingly, Japan, now rarely mentioned as a target will see the largest absolute increase in terrorism. This prediction is due to its international profile, Japan being the second largest country in the OECD on

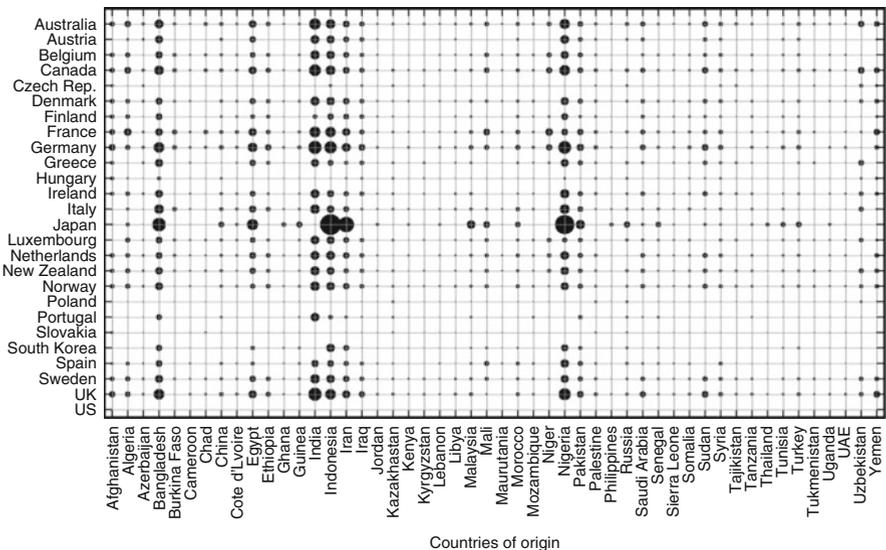
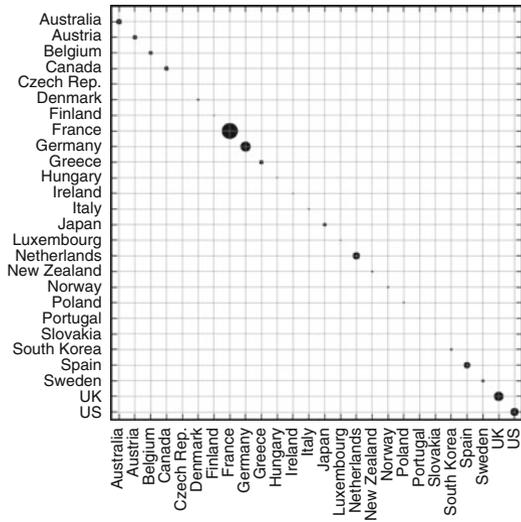


Fig. 4 Attack risk matrix in scenario where US becomes inaccessible to foreign plots. Terrorist plots increase in all other OECD countries

Fig. 5 Attack risk matrix in a scenario where OECD countries cannot be accessed by foreigners (both inside and outside the OECD). Countries with relatively large radicalized Muslim populations (e.g. France) rise in rank relative to their OECD peers. The total number of attacks on OECD countries does decrease significantly because foreign plots are blocked



several measures. Japan’s woes will be shared to some extent by most other major OECD countries, who will also see an increase in attacks (side-by-side numerical comparison with the baseline scenario is found in the tables of Appendix 1.)

Another possible scenario is where the security forces in each country are able to intercept the majority of external plots against their homelands. In other words, the translocation cost becomes very large ($T_{ij} = \infty$ for $i \neq j$). In this world, the dominant form of terrorism is home-grown. As Fig. 5 shows, this materially changes the risk matrix. Countries such as the France, with relatively large and relatively radicalized Muslim communities will see much more terrorism.

The two scenarios point to large conflicts of interest between OECD countries in tackling transnational terrorism. Helping the US intercept plots through advance warning will increase terrorism everywhere else. More broadly, country A will not always benefit from helping country B. Doing so might sometimes increase the chances that A’s enemies, some of which even based in B, will shift to A. This factor may explain part of the difficulty achieving intelligence sharing and international police cooperation. Indeed, B could even come to an understanding with its home-grown terrorists in which they abstain from domestic attacks in return for non-intervention in their activities against A.

4.2 Deterrence

A number of defensive strategies are founded on deterrence. In terrorism, deterrence may involve convincing would-be groups or cells that operations are too risky or that the entire struggle they wage is hopeless. The model can express such conditions on

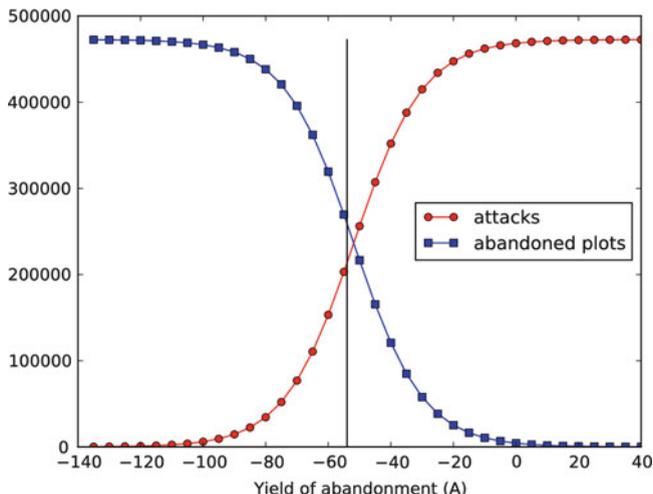


Fig. 6 The number of attacks as a function of the yield from abandoning. Negative values make abandoning more competitive and decrease attacks (*left side*) while positive values indicate that abandoning is costly and encourage attacks (*right side*). The *vertical black line* indicates the yield from attacking the US – the most valuable target. The sigmoid shapes suggest that the effect of deterrence is low until a threshold is reached, but the threshold must be close to the perceived value of attacking the US (*the vertical line*)

a global level by varying the parameter A , the perceived yield from abandoning. Raising this yield is equivalent to raising risks throughout the network. The results are in Fig. 6. The effect of A is non-linear with a threshold at around $A = -35$ beyond which attacks decline. Unfortunately, the threshold lies quite high, indeed nearer to the yield from attacking the US (-54) than countries such as France (-6.8), implying that it would be necessary to create a very large deterrence effect to reduce the number of plots.

If this level of deterrence is somehow achieved, the reduction in attacks will not occur at once in all countries because cells in some countries have lower translocation costs than cells in other countries. As a result, their perceived net benefit and probability of success are higher. Thus plots originating within the developed countries such as the G7 and especially home-grown plots will be the last to experience deterrence because they originate so close to high-value targets.

5 Discussion

The network model draws attention to differences between our past experience with terrorism and its possible future. Populous regions like Nigeria and Bangladesh are predicted to produce many plots although they have not participated significantly

in transnational terrorism yet. If those regions start producing terrorists at a level commensurate with their size and radicalization, the world will see many more attacks. Alternatively, it is possible that those regions have characteristics that hold back violent extremism. If so, future research should identify those characteristics and suggest policies that maintain and encourage them.

The model confirms the significant danger from substitution effects. Perceived successes in reducing the number of attacks against it may be due to a strategic redirection by terrorist groups that increases the risk to other countries. In the scenario where the US deters all attacks by foreign terrorists, many other countries would experience a large increase in threats. To an extent this has already been seen in Europe.

The current model considered the risk from a large-scale Islamist movement. Because such movement is yet to emerge, there is no record of attacks which could serve as validation data – a characteristic problem in risk analysis. However, the model could be re-estimated for extant groups and those variants could then be validated against the historical record. It would be particularly useful if databases such as ITERATE are augmented by the much larger record of attacks that were intercepted.

The model introduced above has limitations where perhaps the most significant is the assumption that a terrorist group's main resource are its human resources. In practice, attacks also require intelligence gathering, training and materials. Future work can develop network-theoretic methods to analyze how terrorist groups would bring those resources together while maintaining secrecy. It would also be possible to consider the risk of attacks by specific groups, including detailed model of their target preferences. Another particularly interesting extension are attacks on foreign representatives of a country (e.g. human representatives such as diplomats or journalists and physical installations such embassies or business offices). Such foreign representatives give terrorist groups high-value targets without the risk of transnational attacks. Similarly, one may consider attack on modes of international transit such as airplanes and ships.

6 Conclusions

The paper introduces a model of transnational terrorist groups that represents operations as a global activity network. It is possible to estimate the parameters of the model, and then predict the number of plots directed at OECD target countries from countries throughout the world. The model highlights the exceptionally high risk of attacks against the US. Yet if the US is successful in deterring attacks against itself without reducing the overall supply of terror then most OECD countries would see sharp increases in attacks because of a substitution effect.

The scale of the substitution effect should alert policy makers to the need to develop and execute multinational defensive strategies. Current strategies, focused on protecting national borders, are both inefficient at reducing the global supply of

plots and increase the threat to allied countries. Ideally, counter-terrorism strategies would reduce terrorism at its places of origin, creating benefits to the entire international community. Abstract solutions to this problem have actually been developed using the methods of graph theory [8, 41], where it is known as network interdiction. Those methods could identify where barriers should be erected in the transnational terrorist network to produce an increase in the costs to the terrorists in such a way that they cannot avoid it by shifting their plots to other countries. If those methods could be implemented as practical counter-terrorism strategies, then the threat of transnational terrorism would be greatly reduced.

Acknowledgements A conversation with Gordon Woo has inspired this work. Matthew Hanson, Michael Genkin and Vadas Gintautas suggested useful improvements. Part of this work was funded by the Department of Energy at the Los Alamos National Laboratory under contract DE-AC52-06NA25396 through the Laboratory Directed Research and Development program, and by the Defense Threat Reduction Agency grant “Robust Network Interdiction Under Uncertainty”. Released as Los Alamos Unclassified Report 10-05689.

Appendix

1 Global Sensitivity Analysis

Considerable uncertainty exists above the values of the model parameters: the supply of plots, translocation costs, interception costs and the yields. Indeed, it is likely that the estimates of those parameters in Sect. 3 are different from the ones used by the terrorist groups. To explore the sensitivity of the predictions to this uncertainty we considered 100 realizations of the model, each with different parameter values. In each realization, each of the original values of the parameters was randomly changed: the value was multiplied by a random number sampled uniformly from $[0.5, 1.5]$. Thus, the values were varied through a range of $\pm 50\%$.

Table 4 shows the sensitivity in the expected number of attacks against various countries. In the majority of cases, the expected number of attacks changes by $\pm 10\%$, often less. The reason for this is that paths in the networks become sums of random quantities, and errors tend to partially cancel each other when summed (central limit theorem). The highest sensitivity was observed in the attacks against the US in the scenario when the US is protected against foreign plots. In such a case, the number of attacks in the US varies exactly as the number of plots that start in the US.

The values of λ (the determinism in the path selection, explained in Appendix 2) was kept at its default value (0.1) since λ directly expresses sensitivity. In the limit of $\lambda \rightarrow 0$, the terrorist groups is completely insensitive to risk or cost while in the limit $\lambda \rightarrow \infty$ the sensitivity is infinite and even small changes in costs can lead to arbitrarily large changes in path choice. The regime $\lambda \rightarrow \infty$ is the case where a decision maker can distinguish arbitrarily small differences in utility and never

Table 4 Expected number of plots and sensitivity to parameter estimates

Country	Plots	Range (%)	Country	Plots	Range (%)
Australia	2804.9	94.5–105.4	Australia	29229.1	96.4–101.5
Austria	1405.9	91.6–109.0	Austria	13691.0	94.5–104.5
Belgium	1817.1	93.4–108.1	Belgium	17954.6	94.6–103.5
Canada	3120.1	93.4–106.0	Canada	32647.7	94.4–102.8
Czech Republic	251.9	91.3–127.2	Czech Republic	2964.1	88.1–122.6
Denmark	1869.2	94.5–106.6	Denmark	18816.7	96.0–102.6
Finland	1183.4	92.4–110.8	Finland	11493.5	94.7–108.0
France	3049.7	94.1–110.2	France	31064.9	95.2–105.3
Germany	4272.6	93.3–107.4	Germany	42340.4	95.3–102.8
Greece	1344.2	93.8–109.7	Greece	14042.7	93.4–106.1
Hungary	281.5	92.4–130.2	Hungary	3035.2	91.3–122.5
Ireland	1694.0	93.9–107.6	Ireland	17422.9	94.6–104.1
Italy	2008.2	92.4–110.0	Italy	19648.6	93.2–109.7
Japan	6563.3	92.9–117.9	Japan	57477.1	92.3–115.1
South Korea	852.2	93.5–115.5	South Korea	7499.1	92.4–114.3
Luxembourg	1590.6	94.6–107.3	Luxembourg	16065.4	94.6–103.4
Netherlands	2015.1	93.2–107.8	Netherlands	20133.1	93.5–104.4
New Zealand	1832.9	91.1–110.1	New Zealand	19131.8	90.4–107.9
Norway	1966.9	95.3–106.3	Norway	20065.9	96.4–102.3
Poland	86.8	90.1–131.9	Poland	1003.9	89.3–131.5
Portugal	598.2	87.0–120.1	Portugal	6008.4	87.3–119.9
Slovakia	80.9	91.0–133.0	Slovakia	882.0	88.4–131.0
Spain	1379.5	93.9–113.3	Spain	13281.8	93.0–111.3
Sweden	2070.0	94.0–106.8	Sweden	21226.0	95.0–102.5
United Kingdom	3467.2	89.9–111.5	United Kingdom	35333.4	91.0–106.1
United States	425091.5	99.3–100.5	United States	238.9	58.8–144.0

When the supply of the plots and the costs on the edges are varied, the expected number of attacks against a country j , Z_j , changes. Shown are Z_j and the relative change coefficients: $[z_{j:\min}, z_{j:\max}]$. Namely, $z_{j:\min} Z_j$ is the number of attacks at the bottom decile; $z_{j:\max} Z_j$ is the number at the top decile. The baseline scenario (*left*). The scenario where the US is protected from foreign plots (*right*).

makes mistakes. Fortunately, clandestine and illicit decision makers like terrorist leaders are far from this omniscient regime.

2 Computation of Probabilities

In the framework of the theory of complex networks, attack plots could be represented as the motion of an adversary through a weighted network (the plot itself is the adversary we wish to stop). The adversary aims to find an attack path or to hide, whichever plan has the lowest cost. To map such a decision to the framework of activity networks, connect the “attack” and “abandon” nodes in Fig. 2 to a node termed “end” with edges of cost 0. Thus, an attack on a country j corresponds

to an adversary that starts at country i and goes through country j and then to the node “attack” and finally to “end”. The decision to abandon corresponds to an adversary that starts at country i then goes to “abandon” and then to “end”. The expected number of attacks on a particular target t can be computed by combining information about path costs with information about the supply of plots from a particular country S_i and the yield of abandonment A . Namely, it is the number of trips from all sources that arrive to the “attack” node from target country t .

The least-cost path corresponds to the optimal choice by the terrorists, but they can make mistakes. An attack plan under uncertainty could be described as a Markov chain [20]. The chain has initial distribution proportional to S_i , and a transition probability matrix \mathbf{M} describing the likelihood of taking a particular edge on the network. The “end” node is the absorbing state of the chain. The \mathbf{M} matrix can be computed using the least-cost guided evader model described in [20]. Briefly, for each edge (u, v) of the network, the transition probability through it is given by the formula

$$M_{uv} = \frac{\exp[-\lambda(c(p_{uv}) - c(p_{u*}))]}{\sum_w \exp[-\lambda(c(p_{uw}) - c(p_{u*}))]},$$

where $c(p_{u*})$ is the cost of the least-cost path from node u to the end node, and $c(p_{uv})$ is the cost of the path through edge (u, v) : $p_{uv} = (u, v) \cup p_{v*}$. The sum in the denominator runs over the neighbors of node u . Thus, the model generalizes the least-cost path model³. The parameter λ was set to 0.1, in the reported data, but its value has a smooth effect on the predictions of the model because of the smoothness of the exponential function. The number of plots against a target country t is now found by taking the probability of a trip to that target multiplied by the total number of plots ($= \sum_i S_i$).

References

1. Abrahms, M.: What terrorists really want: Terrorist motives and counterterrorism strategy. *Int. Secur.* **32**(4), 78–105 (2008). <http://www.mitpressjournals.org/doi/abs/10.1162/isec.2008.32.4.78>
2. Anderton, C.H., Carter, J.R.: On rational choice theory and the study of terrorism. *Def. Peace Econ.* **16**(4), 275–282 (2005)
3. Arquilla, J., Ronfeld, D.: *Networks and Netwars: The Future of Terror, Crime, and Militancy*. RAND Corporation, Santa Monica, CA (2001)
4. Bakker, E.: *Jihadi terrorists in europe*. Tech. rep., Netherlands Institute of International Relations, Dec 2006

³To compute the distances to the “end” node, $c(p_{uv})$, we use the Bellman–Ford algorithm because edge weights are negative for some edges (e.g. yield from attacks). Gutfraind et al. [20] uses the faster algorithm of Dijkstra because it treats only the case of positive weights.

5. Berman, E., Laitin, D.D.: Religion, terrorism and public goods: Testing the club model. *J. Public Econ.* **92**(10–11), 1942–1967 (2008). <http://www.sciencedirect.com/science/article/B6V76-4S4TNTW-1/2/6a0e405748612f6c10b7db12ace22fc1>
6. Bier, V.M., Oliveros, S., Samuelson, L.: Choosing what to protect: Strategic defensive allocation against an unknown attacker. *J. Public Econ. Theory* **9**(4), 563–587 (2007)
7. Caplan, B.: Terrorism: The relevance of the rational choice model. *Public Choice* **128**(1), 91–107 (2006). <http://www.springerlink.com/content/041521274700t406>
8. Corley, H.W., Sha, D.Y.: Most vital links and nodes in weighted networks. *Oper. Res. Lett.* **1**(4), 157–160 (1982)
9. Corman, S.R.: Using activity focus networks to pressure terrorist organizations. *Comput. Math. Organ. Theory* **12**, 35–49 (2006). <http://www.springerlink.com/content/F36M527745172454>
10. Dugan, L., Lafree, G., Piquero, A.R.: Testing a rational choice model of airline hijackings. *Criminology* **43**(4), 1031–1065 (2005). <http://www.blackwell-synergy.com/doi/abs/10.1111/j.1745-9125.2005.00032.x>
11. Enders, W., Sandler, T.: Distribution of transnational terrorism among countries by income classes and geography after 9/11. Report by the Center for Risk and Economic Analysis of Terrorism Events (CREATE) (2005)
12. Enders, W., Sandler, T.: What do we know about the substitution effect in transnational terrorism. In: Silke, A. (ed.) *Researching Terrorism: Trends, Achievements, Failures*, pp. 119–137. Frank Cass, Ilford (2004)
13. Erlander, S., Stewart, N.F.: The gravity model in transportation analysis: theory and extensions, *Topics in transportation*, vol. 3. VSP, Utrecht, The Netherlands (1990)
14. Finbow, A.S., Hartnell, B.L.: On designing a network to defend against random attacks of radius two. *Networks* **19**(7), 771–792 (1989). <http://dx.doi.org/10.1002/net.3230190704>
15. Ganor, B.: *The Counter-Terrorism Puzzle: A Guide for Decision Makers*. Transaction Publishers, Piscataway, NJ (2005)
16. Ganor, B.: Terrorist organization typologies and the probability of a boomerang effect. *Stud. Confl. Terrorism* **31**, 269–283 (2008)
17. Ginsburg, S.: *Countering terrorist mobility: Shaping an operational strategy*. Tech. rep., Migration Policy Institute, Feb 2006
18. Gutfraind, A.: *Mathematical Terrorism*. Ph.D. thesis, Cornell University, Ithaca, New York, USA (2009)
19. Gutfraind, A.: Optimizing topological cascade resilience based on the structure of terrorist networks. *PLoS ONE* **5**(11), e13448 (2010)
20. Gutfraind, A., Hagberg, A.A., Izraelevitz, D., Pan, F.: Interdiction of a Markovian Evader. In: Dell, R., Wood, K. (eds.) *Proceedings of the INFORMS Computing Society Conference*. INFORMS (2011)
21. Hanson, M.A.: *The economics of roadside bombs*. SSRN eLibrary (2008)
22. Harmon, C.C.: *Terrorism Today*, 1 edn. Routledge, Oxford, UK, (2000)
23. Harrison, M.: *Counter-terrorism in a police state : The KGB and codename blaster, 1977*. The Warwick Economics Research Paper Series (TWERPS) 918, University of Warwick, Department of Economics (2009). <http://ideas.repec.org/p/wrk/warvec/918.html>
24. Hoffman, B.: *Inside Terrorism*. Columbia University Press, USA (2006)
25. Jung, W.S., Wang, F., Stanley, H.E.: Gravity model in the Korean highway. *EPL (Europhysics Letters)* **81**(4), 48005 (2008). <http://stacks.iop.org/0295-5075/81/i=4/a=48005>
26. Lake, D.A.: Rational extremism: Understanding terrorism in the twenty-first century. *Dialog-IO*, pp. 15–29. Spring, Berlin (2002)
27. Landes, W.M.: An economic study of U. S. aircraft hijacking, 1961–1976. *The J. Law Econ.* **21**(1), 1 (1978). <http://www.journals.uchicago.edu/doi/abs/10.1086/466909>
28. Lee, D.R.: Free riding and paid riding in the fight against terrorism. *Am. Econ. Rev.* **78**(2), 22–26 (1988). <http://www.jstor.org/stable/1818091>
29. Lindelauf, R.H., Borm, P.E., Hamers, H.: The influence of secrecy on the communication structure of covert networks. *Soc. Netw.* (2009)
30. Lugo, L.: *Mapping the Global Muslim Population*. Pew Research Center, Oct 2009

31. Manningham-Buller, E.: The International Terrorist Threat to the UK. MI5 website (Nov 2006). <http://www.mi5.gov.uk/output/the-international-terrorist-threat-to-the-uk-1.html>
32. Mayer, T., Zignago, S.: Notes on CEPII's distances measures. <http://www.cepii.fr/anglais-graph/bdd/distances.htm> (May 2006), Centre d'Etudes Prospective et d'Informations Internationales
33. Mickolus, E.F.: International Terrorism: Attributes of Terrorist Events (ITERATE). <http://www.icpsr.umich.edu/cocoon/ICPSR/STUDY/07947.xml> (2009)
34. OECD: Immigrants and expatriates: Total population by nationality and country of birth. online (2006), Organisation for Economic Co-Operation and Development
35. Sageman, M.: *Leaderless Jihad – Terror Networks in the Twenty-First Century*. University of Pennsylvania Press, Philadelphia, PA (2008)
36. Sandler, T.: Collective action and transnational terrorism. *World Econ.* **26**(6), 779–802 (2003)
37. Sandler, T., Enders, W.: An economic perspective on transnational terrorism. *Eur. J. Polit. Econ.* **20**(2), 301–316 (2004). <http://ideas.repec.org/a/eee/poleco/v20y2004i2p301-316.html>
38. Shapiro, J.N., Siegel, D.A.: Underfunding in Terrorist Organizations. In: Memon, N., Farley, J.D., Hicks, D.L., Rosenorn, T. (eds.) *Mathematical Methods in Counterterrorism*, pp. 349–382. Springer, New York (2009)
39. Shapiro, J.N., Siegel, D.A.: *The Greedy Terrorist: A Rational Choice Perspective on Terrorist Organizations. Terrorist Financing in Comparative Perspective. Inefficiencies and Vulnerabilities*. Stanford University Press, California (2009)
40. Shughart, W.F. II: Terrorism in rational choice perspective (2009), working Paper
41. Washburn, A., Wood, K.: Two-Person Zero-Sum Games for Network Interdiction. *Oper. Res.* **43**(2), 243–251 (1995). <http://or.journal.informs.org/cgi/content/abstract/43/2/243>
42. Wike, R.: Pew global attitudes project. Pew Research Center (2006-2009)
43. Woo, G.: Understanding terrorism risk. online (2004), report for Risk Management Solutions
44. Woo, G.: Intelligence Constraints on Terrorist Network Plots. In: Memon, N., Farley, J.D., Hicks, D.L., Rosenorn, T. (eds.) *Mathematical Methods in Counterterrorism*, pp. 205–214. Springer, New York (2009)



<http://www.springer.com/978-3-7091-0387-6>

Counterterrorism and Open Source Intelligence

Wiil, U. (Ed.)

2011, XVIII, 458 p. 182 illus., Hardcover

ISBN: 978-3-7091-0387-6