Forecasting the Locational Dynamics of Transnational Terrorism

A Network Analytic Approach

Bruce A. Desmarais
UMass Amherst Political Science

Joint work with Skyler J. Cranmer (UNC Chapel Hill Political Science)
Paper published in the Proceedings of the 2011 European Intelligence and Security Informatics Conference, copyright IEEE Computer Society

February 10, 2011

The Problem

- Forecasting transnational terrorist attacks is important
- Successful forecasting is critical for resource allocation
- Problem: most forecasting techniques rely on country-specific time-series
- Related Problem: need to be able to identify *new* threats

Background 1: Predictors of Terrorism

Much of the empirical research on terrorism focuses on identifying covariates that *explain* the within-country frequency of terrorism.

Terrorism is more likely in

- Countries with **democratic governments** (Li 2005)
- Countries that **grant concessions to terrorists** (Kydd and Walter 2006)
- Countries with **further economic reach** (Li and Schaub 2004)

Problems

- Research is not explicitly focused on forecasting
- Covariates can be costly and time consuming to collect
- No information on the source of terrorism

Background 2: Forecasting Frequency

The line of research that explicitly addresses forecasting focuses on predicting the number of events in a country given the recent history of events.

- Frequency of terrorist attacks exhibit cycling (Enders, Parise and Sandler 1992)
- Extreme increases in attack frequency are unsustainable (Enders and Sandler 2000)
- Series can be accurately forecast using Poisson Changepoint (Brandt and Sandler 2010)

Problems

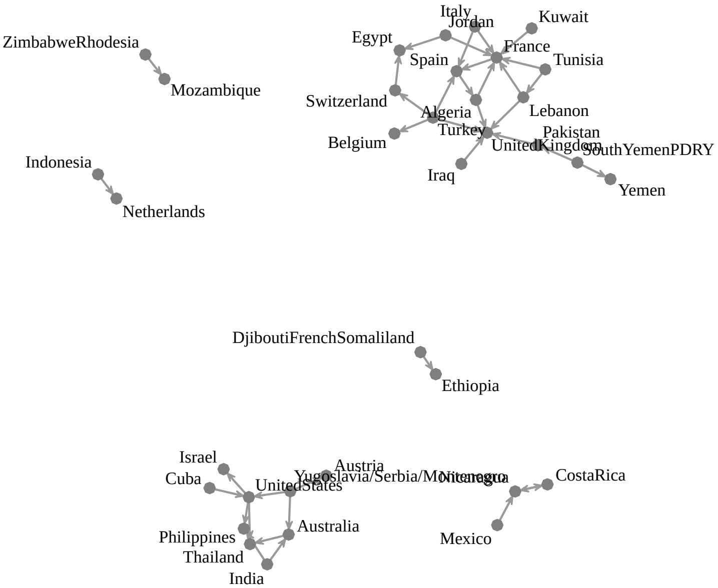
- No information on the source of terrorism
- Without recent series of terrorism, forecasts fail

Data

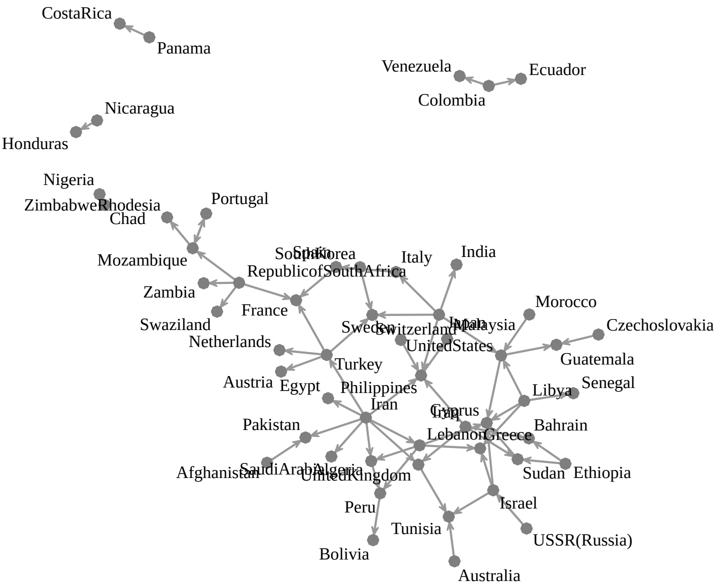
International Terrorism: Attributes of Terrorist Events

- Data from the ITERATE dataset (Mickolus, 2008)
- More than 12,000 transnational terror attacks between 1968 and 2002
- Data codes *known* nationalities of terrorists and the location of their attacks
- Edges exist from a terror producer to a terror target, within a given period
- Networks have a median of 175 vertices over our timespan
- 20-40% are self-ties (i.e., loops)

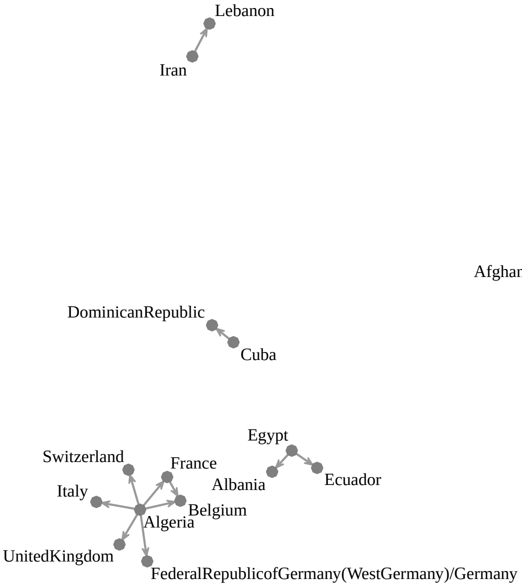
Network: 1978



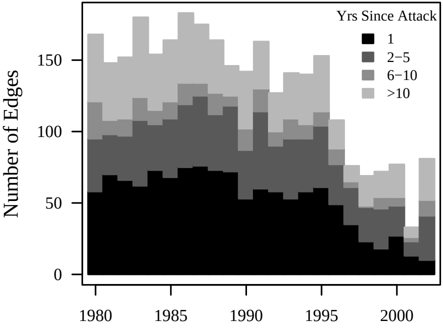
Network: 1988



Network: 1998



Edge Innovation



Low degree of edge recurrence

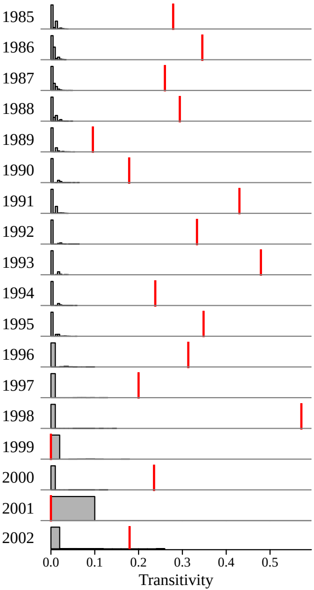
Time series techniques will not work for innovations

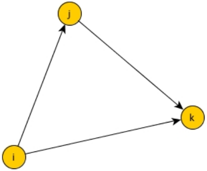
Any information that can be leveraged about indirect ties will be valuable

Our Research Objectives

1. Develop an approach to forecasting the **network** of transnational terrorist attacks in order to **forecast source information**.
2. To overcome the **sparsity** in the network and **lack of innovation** in country-specific time series, we seek to leverage indirect ties to improve prediction.
3. Methodologically, we **improve upon extant proximity-based prediction algorithms**

Transitivity





Transitivity: how important is proximity for edge formation

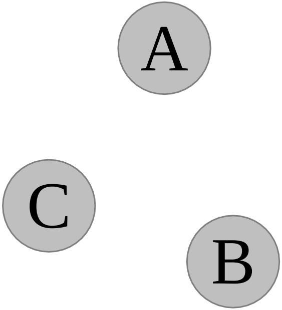
If high transitivity, proximity-based forecasting should be fruitful

CUG test for transitivity

Transitivity indicates that indirect ties will have predictive power w.r.t. edge formation

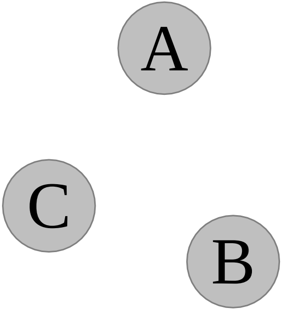
Why Would this Terrorism Network be Transitive?

Consider states A, B and C



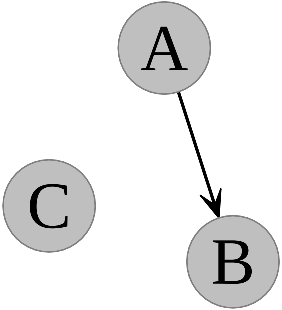
Why Would this Terrorism Network be Transitive?

Suppose group X's recent operations are based in A



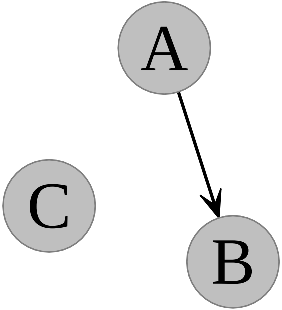
Why Would this Terrorism Network be Transitive?

X launches a campaign in B with recruits from A



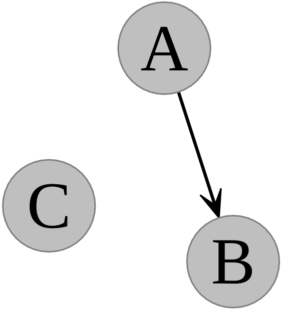
Why Would this Terrorism Network be Transitive?

Up to and throughout the campaign, X recruits in B



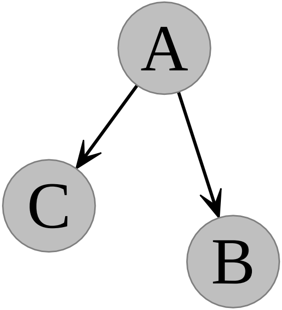
Why Would this Terrorism Network be Transitive?

Or, via the attacks, X gains attention of sympathizers



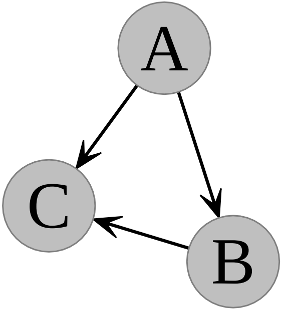
Why Would this Terrorism Network be Transitive?

X launches a campaign in C with recruits from A



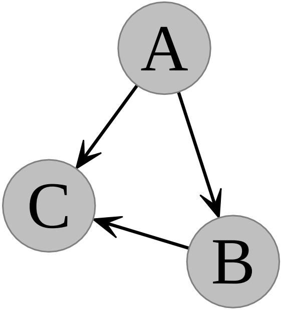
Why Would this Terrorism Network be Transitive?

The new recruits from B join in attacks on C



Why Would this Terrorism Network be Transitive?

The new recruits from B join in attacks on C



Ideological and Nationalist Terrorism

- **Ideological Groups:** organize around sociopolitical, religious, or economic doctrine
  - al-Qaeda
  - Red Army Faction
- **Nationalist Groups:** organize to gain authority or autonomy in a specific country
  - Quebec Liberation Front
  - Ukrainian Insurgent Army

Our argument applies to ideological groups

Proximity-based Link Prediction

Liben-Nowell and Kleinberg (2003): Nodes that are structurally similar are likely to link in the future.

Prediction Process:

1. Define a training network over t_0 to $t-1$, denoted $N^{t_0,t-1}$
2. There is an edge from i to j in $N^{t_0,t-1}$ if i sent an edge to j in the interval t_0 to $t-1$
3. Define dyad-wise proximity scores $\delta(i,j)$
   - Path length from i to j
   - Number of partners shared by i and j
4. Rank dyads based on $\delta(i,j)$
5. Those with higher scores are predicted to tie in the future

Liben-Nowell and Kleinberg (2003)

Strengths:

- Prediction is based solely on graph topology – no covariates
- Can experiment with t_0 to optimize prediction

Weaknesses:

- Does not permit precise probability statements about future edges
- Cannot integrate/combine proximity measures

Our Approach: TERGM

- Developed by Hanneke, Fu, and Xing (2010)
- Let N^t be the observed network at time t
- Can condition N^t on K previous realizations of the network to account for temporal dependencies

$$\mathcal{P}(N^t|K,\boldsymbol{\theta}) = \frac{\exp\{\boldsymbol{\theta}'\,\boldsymbol{\Gamma}(N^t, N^{t-1}, \ldots, N^{t-K})\}}{C(\boldsymbol{\theta}, N^{t-K}, \ldots, N^{t-1})}.$$

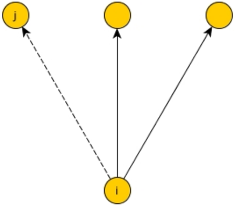
- Each proximity measure δ is integrated into the TERGM by adding

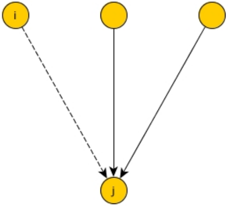
$$\Gamma(N^t, N^{t_0,t-1}) = \sum_{ij} N^t_{ij}\delta(i,j)^{t_0,t-1}.$$

- We estimate a new $\boldsymbol{\theta}$ for each t to account for temporal heterogeneity

Our Proximity Measures: Flow

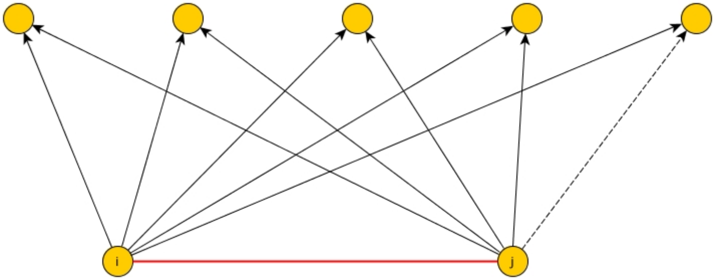
- **Flow**. Generalizes preferential attachment to the directed case
- A process whereby an attack from i to j is likely if i sends many attacks and/or j receives many attacks
- Mathematically: $\delta(i, j) = k_i^o k_j^i$, where k^o and k^i are the out and in-degrees respectively





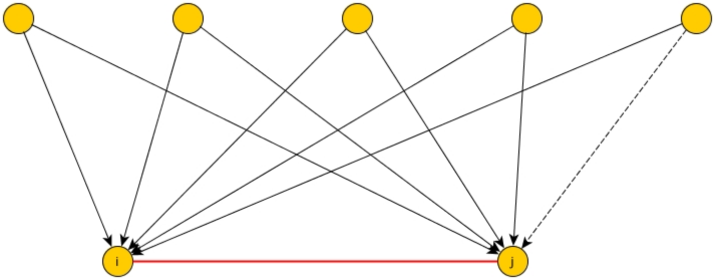
Our Proximity Measures: Common Targets

- **CTarget**. The number of common targets for a dyad
- Mathematically: $\delta(i,j) = \sum_h N_{ih} N_{jh}$.



Our Proximity Measures: Common Attackers

- **CAttacker**. The number of common attackers for a dyad
- Mathematically: $\delta(i, j) = \sum_h N_{hi} N_{hj}$



Our Proximity Measures: Two Similarity Measures

We consider 2 similarity measures

- **JacSim**. The Jaccard similarity between two countries normalizes the measure of common neighbors by the total number of neighbors of the vertices in the dyad

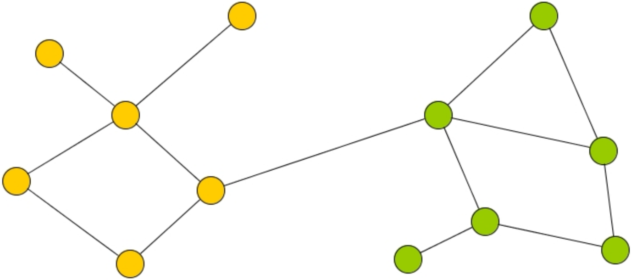
$$\delta(i,j) = [\mathbf{CTarget} + \mathbf{CAttacker}]/[k_i + k_j]$$

- **AASim**. Adamic/Adar similarity adjusts the measure of common neighbors for the rarity of the neighbors to which the two countries tie

$$\delta(i,j) = \sum_h [\ln(k_h)]^{-1} (N_{ih}N_{jh} + N_{hi}N_{ji})$$

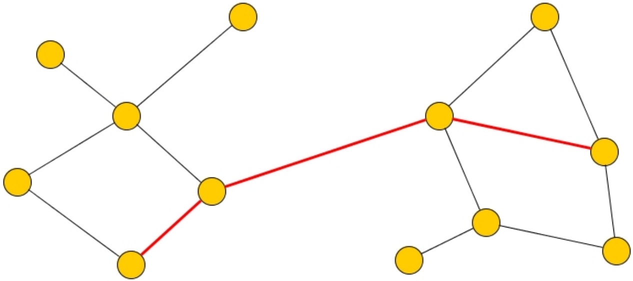
Our Proximity Measures: community membership

- **SameCom**. Common community membership
- We partition the countries into communities using the random walk modularity optimization algorithm "Walktrap" (Pons and Latapy, 2005)
- We then create an indicator, $\delta(i,j) = \mathbf{1}(c_i == c_j)$, of whether i and j are members of the same community.



Our Proximity Measures: Minimum Path Length

- **Distance**. Minimum path length between i and j
- We set $\delta(i, j)$ equal to the number of countries in the network plus one if there is no path from i to j.



Additional Measures

We also include, in each model, the following

- A count of the number of edges in the network to model the network's density
- A memory term (**PrevAttack**) to capture persistence in the ties between the training network and the current network

Mathematically: memory at time t is $\sum_{ij} N_{ij}^{t} N_{ij}^{t_0,t-1} + (1 - N_{ij}^{t})(1 - N_{ij}^{t_0,t-1})$

Specification

- We try each statistic computed on the networks over the intervals $[t-1, t-1]$ and $[t-5, t-1]$
- Our analysis begins at 1980 and ends at 2002
- The memory term and each of the proximity terms is
  - Included computed on the one year training interval
  - Included computed on the five year training interval
  - excluded from the model.
- This leads to a total of $3^8 = 6,561$ models estimated at each t

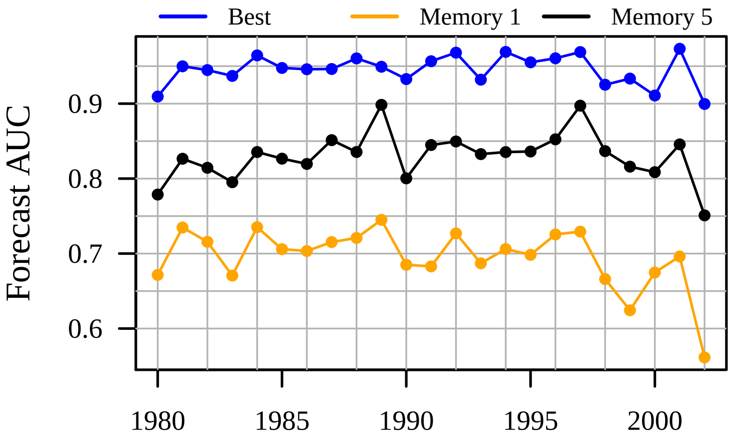
Forecasting

True Forecasting Exercise

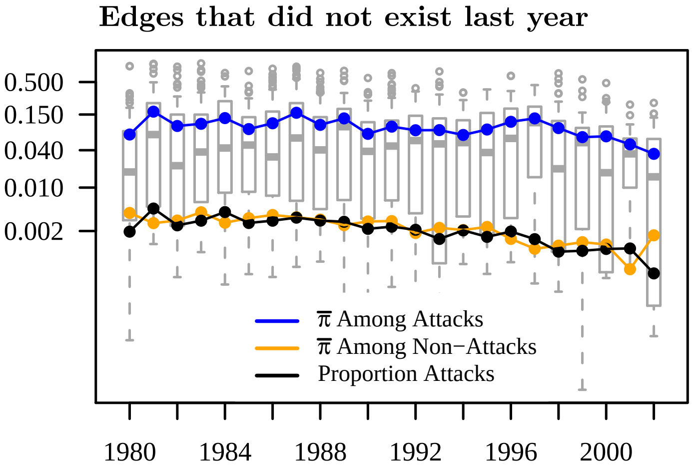
1. Estimate a TERGM for each year up to $t-1$
2. To forecast network in year t, select **best** model up to $t-1$
3. Performance is predictive log score
4. We use $\boldsymbol{\theta}^{t-1}$ to perform the forecast of N^t
5. $\boldsymbol{\theta}^{t-1}$ estimated to fit N^{t-1} based on $N^{t_0-1,t-2}$

Forecast Model for N^t has not been trained on N^t

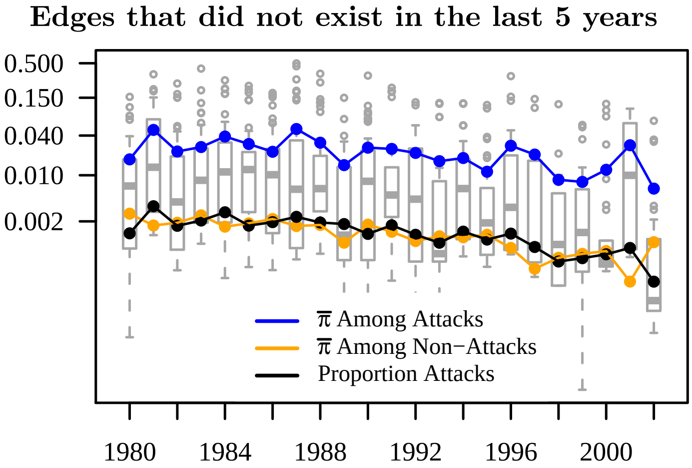
Results: Overal Forecasting Performance



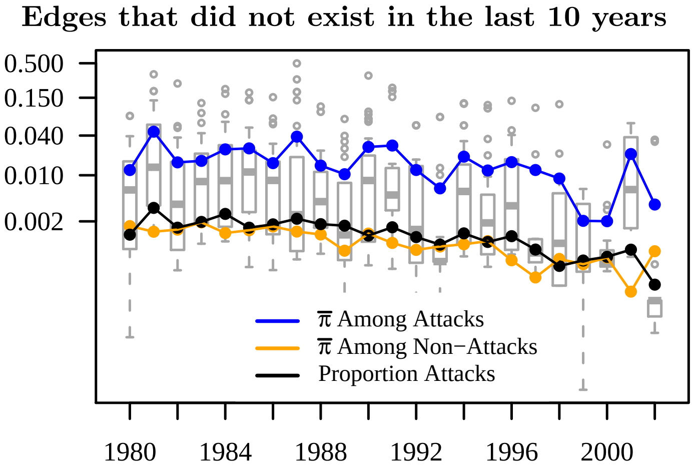
Results: Predicting Edge Innovations



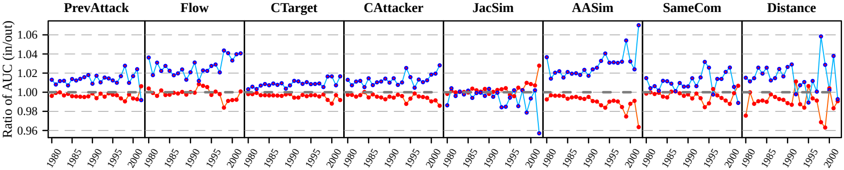
Results: Predicting Edge Innovations



Results: Predicting Edge Innovations



Results: Patterns in the Proximity and Memory Features



- Ratio of mean one-year-ahead forecast AUCs with and without the given measure
- A value greater than one indicates that the average forecast AUC is higher when the respective term is included
- The superior performance of the measures computed with five year memories reinforces idea that the transnational terrorism network exhibits long memory

Terrorism in the U.S. in 2001

Top Ten Forecasted Sources, 2001

Rank	Country	P(Attack)
1	Algeria	0.126
2	Pakistan	0.055
3	Iraq	0.044
4	Jordan	0.037
5	Cuba	0.037
6	Canada	0.029
7	Romania	0.024
8	**Saudi Arabia**	0.012
9	**Egypt**	0.011
10	Iran	0.011

Overall Probability of Attack on the U.S. 0.41

Contributions

- We show that a network-analytic approach can succeed in forecasting transnational terrorism
- We show that indirect ties can be leveraged to forecast innovations in terrorist links
- We advance link forecasting methods by integrating vertex proximity measures into TERGM

Future Research

- Extend methodology such that edges are attack frequency
- Test against Brandt et al's forecasting technology
- Relax linear combination assumption in TERGM
- **Suggestions?**