Repression and Network Science: Tools in Fight against Terrorism

By

Dominick' E. Wright

A dissertation submitted in partial fulfillment
of the requirements for the degree of
Doctor of Philosophy
(Political Science)
In the University of Michigan
2010

Doctoral Committee:

Professor Walter R. Mebane Jr., Co-Chair
Professor James D. Morrow, Co-Chair
Professor Robert J. Franzese Jr.
Assistant Professor Philip B.K. Potter

TABLE OF CONTENTS

List of Figures

List of Tables

List of Appendices

INTRODUCTION

The dissertation, *Repression and Network Science: Tools in Fight against Terrorism*, explores what determines post-terror repression in democracies and what alternative tools network science may ultimately reveal to for compelling authorities to rely on repression less. To do this three papers concentrate on some aspect of the question at hand. The first chapter is empirical, using a panel, cross-section design to evaluate under what conditions democracies use state terror or state repression following terrorism. Chapter 2 takes the opposite view, using high-powered statistics to evaluate a single case. At question is the tool in use more than the terrorist network under inspection. Network science is fascinating, disappointing, and daunting, offering a world of potential with few advances, in the area of theoretical evaluation, and therefore large amount of work ahead. Chapters 2 and 3 explore various aspects of what is needed with 2 focusing on improving methods in network statistics and 3 stressing the need for further development of theories for testing with improved statistical models.

Chapter 1 uses the following observation as its point of departure. Countries can respond to terrorism judicially, extrajudicially, or by doing nothing. Human rights proponents decry extrajudicial responses as repressive and illiberal, but advocates for such countermeasures consider them effective at promoting security and the reason that terrorists rarely attack non-democracies. Amid this controversy, democracies rarely use extrajudicial responses. Why do democracies moderate responses to terrorism? Both sides of the debate claim that it is due to legislative constraints obstructing chief executives. I argue that political ideology motivates use repression and therefore determines its use. To test the theories, I define measures for ideology and legislative constraint and use them on an original dataset covering nearly 20 years of terrorism and repression in approximately 70 countries. Empirical results show that ideology determines repression against terrorism and conditions the effect of legislative opposition. The demonstration that ideology interacts with governmental institutions to determine post-terror repression is the

first step to redefining a theory about which factors influence the way that democracies negotiate security-liberty tradeoffs in the fight against terrorism.

Chapter 2 outlines a set of procedures for using exponential random graph modeling (ERGM) to maximize the fit of network statistics models used to profile the structure of observed networks. The procedures include sweeping the parameter space of exponential parameters when network formulas include statistics that have more parameters than they do sufficient statistics. Another proposal is to use filter and rank methods for evaluating models following estimation. Application of the methods to the analysis of the terrorist network produced by the Jemaah Islamiyah organization in 2000 demonstrates that the procedures perform as described.

Chapter 3 begins with the following observation as its point of departure. News cycles today seemingly produce a consistent stream of reports on how the latest counterterrorism efforts have resulted in the death or arrest of a terrorist "leaders," yet the attacks continue and new "leaders" emerge. Research has shown religiously motivated terrorist groups are less susceptible to decapitation strategies (Jordan, 2004), but the literature has to this point offered little explanation for how this occurs. To argue religiously motivated or other population-based groups benefit from community support does not shed light on how they harness these resources and what happens to make them stop. Filling the void in the literature, this paper provides statistical evaluations of network structure and narrative accounts of how a terrorist group contended with successive counterterrorism efforts that decimated its ranks but largely failed to prevent its attacks. It finds that scale-free theory does not explain the variation in outcomes because the group never exhibited the characteristics. Narrative analysis of the time series focused attention on the dual aspects of dynamically growing networks and the importance of equipping members with skills and resources prior to drawing the attention of authorities.

CHAPTER I

How Executive Ideology and Legislative Opposition Determine Post-Terror Repression in Democracies

I. Introduction

Between 1980 and 2000, one in four months a democracy suffered at least one terrorist attack.[1] Responses to terrorism include acting judicially, extrajudicially, or doing nothing. Judicial responses are legal actions like arresting terrorism suspects and bringing them to trial. Extrajudicial responses are illegal actions like killing terrorism suspects without bringing them to trial and without just cause. Some consider repression illiberal and against norms that protect individual rights, but others see repression as the preferred countermeasure against terrorism.[2] A frequent argument is that non-democracies use repression and that terrorists attack them comparatively less for this reason. Some democracies seem to have incorporated similar approaches, while others have yet to do so.

Recent cases in Western democracies seem to reinforce the argument favoring repression. After 9/11, Spanish and American authorities coordinated efforts to bring down a Spanish cell of radical Islamists associated with Al-Qaeda. Wiretapped conversations recorded members like Imad Barakat Yarkas praising Allah for the eventual strike on the United States, convincing many American authorities that he had prior knowledge of the attack and deserved the highest allowable punishment. Spanish law maximizes life sentences at 40 years but Yarkas

[1] The statistic uses terrorism data from the Global Terrorism Database (GTD) and a composite definition of democracy developed using indices from Polity IV and the Database on Political Institutions.

[2] For example, the debate surrounding extrajudicial killing is the belief that everyone has the right to a fair trial before receiving a death sentence, and the belief that being a terrorist negates such rights.

received far fewer than even that, leaving American authorities to question how democratic policies are supposed to deter future terrorist attacks when their punishments seem so lax. Shortly thereafter, in 2004, remnants of Yarkas's cell participated in the largest terrorist attack in Spanish history and emphasized that the judicial approach proved ineffective. Compare this to democracies like France, which grants the chief executive a considerable amount of autonomy and who uses the equivalent of Special Forces proactively to counter threats in ways that some consider borderline repression. The "new wave" of radical Islamist terrorism saw strikes against the Americans (9/11), English (London Bombings), and Spanish (Madrid Bombings), while the French remained unscathed. Repression, or at least the ability to use it, appears to represent a clear, tactical advantage: deter terrorism with the threat of death or other extreme punishments.

Despite the apparent advantage, democracies rarely use repression against terrorism, which leads to my research question, "What determines the use of post-terror repression?" Extant theory argues that legislative opposition, defined as politically motivated "checks" and "balances," determines when democracies repress. Unopposed leaders repress, while opposed ones do not. My theory claims that ideology—not legislative opposition—determines the use of repression. Chief executives and their beliefs about the acceptability of repression determine whether a state uses it to combat terrorism. Legislative opposition meant to constrain them is ineffective, possibly because actions like oversight and budget control are reactive, *ex post* measures.

Tests of the two theories incorporate measures for ideology, legislative opposition, terrorism, and repression, defined as extrajudicial killings, on an original dataset of behavior by approximately 70 democracies over 18 years to identify what happens following terrorist attacks. The primary finding is that ideology determines the use of repression and legislative opposition is ineffective at stopping it.

The remainder of the paper proceeds in the following manner. First, it reviews the extant theory on legislative opposition and highlights problems with one of its motivating assumptions that the new theory relaxes. An outline of the theory of ideologically influenced counterterrorism follows, providing a basic

description of what ideology is and why it might influence how acceptable repression is to improve security. Next, it describes the research design that evaluates the argument along with the data used to conduct the test. The remaining two sections present the findings and conclude with statements about how they refine extant theory of democratic counterterrorism and what the next steps are for developing the theory further.

II. Literature Review

Two assumptions in the security-liberty tradeoff paradigm motivate extant theory to predict that legislative opposition restricts repression against terrorism. Used in a decision-theoretic model to derive expectations for counterterrorism policy, one assumption states that chief executives (hereafter referenced as executives) or leaders of countries uniformly prefer to suppress terrorist violence with repression. An additional assumption drawn from conjecture is that legislative opposition constrains executives and explains when they do not repress as much theoretically expected. Combined, the assumptions lead to the theoretical prediction that legislative opposition prevents executives from using repression against terrorism.

A decision-theoretic model explains the tradeoff between security and liberty the combined behaviors of three different actors—terrorists, voters, and executives—to explain how the security-liberty tradeoff determines observed behavior (Enders & Sandler, 2006; Viscusi & Zeckhauser, 2003). Terrorists, motivated to attack for a variety of reasons (Schneckener, 2006), do so according to the freedoms a society affords them (Crenshaw, 1981; Farrell, 1982; Wilkinson, 1976). Social networks are the medium that terrorists use to mobilize for attack (Sageman, 2004), which is true even in the case of "lone wolves" (i.e., terrorists that act alone) because of the need to acquire materials like explosives and detonators. Communication, movement, and assembly are all behaviors critical to the growth and mobilization terrorist networks. Distributed training manuals instruct members on how to convene meetings in secret, acquire materials necessary for attack, and

perform other such activities.[3] None of these manuals explicitly calls for action only in democracies, a fact attested to by the presence of terrorist groups in places like Saudi Arabia, Iran and other repressive non-democracies. The difference between democracies and non-democracies is that network growth and function are comparatively easier in countries where national law treats freedoms as inherent rights, rather than centrally controlled freedoms.

Individuals hold political preferences for security and liberty that determine how much repression executives use against terrorism because voter support determines executive political survival. Theorists assume that this is not the case in non-democracies.[4] Although the exact of these preferences is subjective and conditioned on personal rankings for the two outcomes as well as perceptions of terrorist threats (Viscusi & Zeckhauser, 2003),[5] a tradeoff exists as long as voters attribute benefits to security and liberty. *Ceteris paribus,* increasing levels of terrorism at fixed levels of liberty render them dissatisfied, leaving executives with the option of expanding or retracting freedoms. To do the former increases terrorism and makes voters even more dissatisfied; hence, leaders restrict rights at levels that balance security and voter tolerance for repression. Repression occurs in democracies because voters tolerate it. As controversial as the theorized behavior seems, experimental research seems to support it, showing that subjects prefer certain forms of repression when faced with increasing terrorism threats (2003, pp. 4-14).[6]

---

[3] Material referenced includes manuals from the Animal Liberation Front, White Supremacist groups, and Al-Qaeda.

[4] Specifically, security-liberty tradeoff theorists assert that the responsiveness of government to average individuals requires democratic institutions (Enders & Sandler, 2006, pp. 34-35). In non-democracies, the vote does not constrain executives, so their only interest is in maximizing social stability. Alternative theoretical models recognize that even autocratic leaders face constraint, albeit in a different form than the need to respond to mass preferences (Bueno de Mesquita, Smith, Siverson, & Morrow, 2004). One attempt to generalize the relationship in the context of counterterrorism is to use a general responsiveness parameter that characterizes the relationship between mass preferences and political elite action (Denardo, 1985).

[5] An additional influence is historical experiences with repression like those of African Americans and French North Africans.

[6] Specifically, experimental results show that terrorism threats compel individuals to tolerate profiling (e.g., racial, ethnic, religious, national, and so forth) that uses group membership, rather than individual behavior as probable cause for accosting by state authorities.

Applications of the theoretical model include using it to explain differences in terrorism outcomes conditioned on comparisons between regimes and characteristics of regimes. Comparisons between regimes describe why democracies suffer more terrorist attacks than non-democracies, arguing that the differences in repression induced by voter preferences explain why democracies suffer more terrorist attacks for any given level of terrorist threat (Crenshaw, 1981; Eubank & Weinberg, 1994; Farrell, 1982; Wilkinson, 1976).[7] Comparisons between regimes, according to their characteristics seek to identify what it is about certain governmental systems that explain the occurrence of terrorism (Eyerman, 1998; Li, 2005). Quan Li's argument about the effect of legislative opposition to executive behavior is relevant to the discussion in this paper. He argues that institutional constraints, such as legislative opposition, make it comparatively more difficult for leaders to repress against terrorism. In the context of security-liberty tradeoff theory, his argument asserts that certain democratic leaders do not repress as much as others do because legislative opposition obstructs them. He is not alone in this basic assessment (Chalk & Rosenau, 2004; Donohue, 2008). Processes like deliberation and oversight carried out by "veto players," political actors with the capability (e.g., roles like committee chair or floor leader) and the incentive (because of conflicting political interests) to oppose certain policies (Tsbelelis, 2002), are the reason why executives cannot raise repression to the desired increment.[8] He concludes that legislative opposition causes higher terrorism levels, because it prevents executives from using repression to thwart attack. Though empirical results show that measures of executive constraints correspond with higher amounts of terrorism, they do not substantiate the argument that Li

[7] One criticism of this conclusion is that use of event-count data for terrorism from "open source" media like newspapers and other such outlets biases higher counts in favor of democracies because of their "free speech" laws (Drakos K. , 2007; Drakos & Gofas, 2006). Outside of the fact that terrorism levels might also increase because terrorists exploit news reporting to carry their message to wider audiences (Bassiouni, 1981), an empirical problem faced by the literature as a whole is that no one has distinguished terrorism threat from terrorism events. Thus far, the use of event-count data has conflated the two concepts and prevented a veritable, regime-based comparison.

[8] His argument also extends to the formulation of anti-terror policies, which lies beyond the scope of this paper, as it is not information contained, *en masse,* within publicly available sources. Additionally, detailed information is unavailable for certain activities carried out by domestic equivalents to Special Forces units and intelligence agencies.

proposes. Measures of executive constraint share a strong correlation with other measures of democracy and therefore reinforce the original finding that democracies experience more terrorism than non-democracies do; hence, they are inadequate proxies for indicating repression and make Li's point a conjecture worth testing, rather than an empirically verified result.

III. Theory

A growing body of literature significantly differs from extant theory and its reliance upon governmental institutions to explain post-terror repression and its place within the overall understanding of democracies and terrorism. Extant theory assumes that political elites have role-defined counterterrorism preferences, making executives prefer post-terror repression and legislators oppose it. At face, the argument appears satisfactory but quickly unravels when questioned why executives and legislators would differ in counterterrorism preferences according to their institutional roles. A competing theory based upon political ideology argues differently, asserting that political elites have counterterrorism preferences influenced by political ideology. The theory presented here builds upon micro-foundations established in the literature on social psychology and attempts to extend them to counterterrorism behavior.[9]

Political ideology is a term used to describe the beliefs maintained by individuals, which ascribe importance to outcomes according to perceptions of what their constituent events entailed (Rokeach, 1973; Schwartz & Bilsky, 1987, 1990). Observed outcomes occur according to a sequence of events that produce them. Some refer to such sequences as "descriptive histories," but it is important to understand that these are more than just knowledge about what combination of actions and behaviors led to the observed event. Equally as important is the rank ordering of these constituent events by individuals, which is what makes subjectively maintained value systems important. Originally based in psychology and described as values and desired end-states, political scientists have long since

[9] A related approach in the literature compares terrorism rates in countries according to the political ideology of governments (Koch & Cranmer, 2009).

bridged the divide to connect these abstract concepts to the notion of political references, giving rise to the concept of political ideology (Campbell, Converse, Miller, & Stokes, 1960).[10] Research on individual attitudes, collective behaviors, and political outcomes has attempted to demonstrate how a value-based rationality view of political behavior illustrates the connection what psychological and formal theoretic operationalizations of personal motivations (Chong, 2000). The linkage between values as well as beliefs on one hand and core preferences on the other is that both serve as explanations for what systematically determines individual action.

Value-based reasoning, in the context of counterterrorism preferences, argues that the liberal and conservative ideologies differ on principal grounds that influence views about how acceptable post-terror repression is. Research that evaluates the internalization of values as a product of anthropological evolution and refers to them as "virtues," finds that liberals and conservatives differ significantly in their moral foundations. Specifically, liberals internalize the virtues of "harm/care" along with "fairness/reciprocity," while conservatives uphold "ingroup/loyalty, authority/respect, and purity/sanctity," (Graham, Haidt, & Nosek, 2009, pp. 1,032). What matters concerning attitudes toward post-terror repression, I argue, is the contrast between "fairness/reciprocity" and "ingroup/loyalty." Perceptions of individual rights, whether they are public or private goods, distinguish liberal and conservative political ideologies from one another and largely determine opposition and support for the use of repression against terrorism. "Fairness" drives the perception that individual rights are public goods, requiring society to provide them to individuals irrespective of their transgressions. "Ingroup" drives the perception that individual rights are private goods, allocated by the state to those considered deserving and in the "in groups" for whom respect of legal restrictions applies and withheld from "out groups." The result is nearly unconditional support for rights and freedoms by liberals and a conditional view on

[10] Applications of political ideology within political science concentrate on orienting individuals along a single dimension of political preference, which is a practice that began with studies of the American Voter but has since extended to general conceptualizations of politics worldwide (Powell Jr., 2000).

the extension of liberties by conservatives. This is not a matter of "good" versus "bad" but instead an identification of socially constructed difference that social scientists can systematically observe and investigate.

Political elites like executives and legislators are not uniformly motivated to support or oppose use of repression conditioned on the political office they hold or political conflict, as extant theory argues. Instead, what motivates them is the desire to retain office, which they do by satisfying a political constituency. Attaining and retaining office (political survival) requires taking actions deemed desirable within an accepted political ideology for the partisan group. Whether political elites in alternative partisan camps fully internalize the tenets of competing ideologies remains in question but what is clear is that constituents refer in part to political ideologies when evaluating the performance of leaders (Aldrich, Gelpi, Feaver, Reifler, & Sharp, 2006).

What effect does legislative opposition have? One argument is that it is wholly ineffective at moderating repression, because of being reactive and limited in scope to ex-post investigations and budgetary coercion. Independent legislatures formulate law or public policy but repression is extrajudicial or extralegal, which by definition lies outside the official policy process; thus, limiting the influence that legislators can have on restricting its occurrence. Many acts of repression, such as extrajudicial killing and torture, occur at the level of individual agents acting against suspected and alleged terrorists or associates of terrorists. Such behavior does not require explicit instruction from the chief executive to occur. Instead, it can result from a range of actions including ambiguous suggestion (e.g., enunciation of "win at all costs" strategies) and the perception of tacit approval because known violators go unpunished. The opportunity for legislators to act under these circumstances is by hearing about transgressions and responding with investigations that serve as exposés or slashing budgets as punishment for the misuse of governmental resources. Either way, the options left to legislators are reactive and therefore deterrents based on the logic of punishments. Prosecution by a special investigator is an action that makes legislative response credible, but it is also an occurrence with little historical precedent in the anti-terrorism context for democracies. Budget

slashing is another alternative, but it faces opposition when supporters of repressive countermeasures argue that the actions made the country safer and that cutting finances amounts to punishing agencies for doing their jobs.

Another argument about the effect of legislative opposition looks to its intersection with ideology and posits that if there is a constraining effect, it will be most apparent in the case of liberal legislative opposition against conservative executives. The unbounded ideological nature of centrists makes it difficult to declare universally how they feel about equality and whether they may find the conservative argument for repression persuasive during times of crises. For those reasons, the effect of centrist legislative opposition is outside the scope of the ideological theory presented here.

IV. Research Design

The empirical question evaluated in this paper asks, "What determines the use of post-terror repression?" To answer the question I use the following equations:

$$p(R_{ait} = 1 \,|\boldsymbol{\tau}'\boldsymbol{T}_{t-2}, \boldsymbol{\beta}'\boldsymbol{X})$$

Equation 1

$$p(R_{ait} = 1 \,|\boldsymbol{\gamma}'\boldsymbol{I}_{t-1}, \boldsymbol{\tau}'\boldsymbol{T}_{t-2}, \boldsymbol{\lambda}'(\boldsymbol{I}_{t-1}{}'\boldsymbol{T}_{t-2}), \boldsymbol{\beta}'\boldsymbol{X})$$

Equation 2

Repression, R_{atx}, dichotomously measured for repression type *x* and in year *t* can happen under two types of chief executive leadership (*a*): liberal (left) or conservative (right). Evaluation of post-terror repression includes three categories of abuse: extrajudicial killing, disappearances, and political imprisonment.[11] Extrajudicial killing is execution without just cause, such as the threat of death, by state agents or their proxies. Disappearances amount to kidnapping by state agents or their proxies. Torture is unlawful physical abuse of prisoners by state authorities or their proxies. Political imprisonment occurs when state authorities or their proxies detain individuals without charge and for reasons unrelated to the

[11] Torture is not a form of post-terror abuse systematically used by democracies. It does occur, as evidenced in certain American and Israeli cases, but it is not a regular occurrence, at least not according to data contained in the CIRI database.

commission of a crime. Terrorism, $\boldsymbol{\tau}'\mathbf{T}_{t-2}$, is a set of two integer measures. One is an indicator of terrorism level or the total number of monthly attacks in a country. This is the measure used in the interaction terms with legislative opposition. Another is a control variable that indicates terrorism surges or the positive deviation in terrorism events between seasonally adjusted months (see the description for seasonal adjustment in the Data section below). Terrorism surges represent deviations from steady states and amount to crises that are likely to make reporting state abuses less likely in nearly all governments. $\boldsymbol{\beta}'\mathbf{X}$ measures the influence of control variables discussed in the Data section below.

Both regression equations have a lag structure that evaluates repression at time t and terrorism at time $t - 2$ or **L2**. Equation 2 adds the moderating effects of repression measured at time $t - 1$ or **L1**. Archival research into the few publicly documented instances of extrajudicial killing as repression in democracies, such as those cases in Peru and Colombia at the hands of death squads, shows tendencies of a considerable lag between terrorist attacks and reports of repression even when the alleged violations happened shortly thereafter. In an empirical analysis of correlations on repression following terrorism unreported here, findings show a strong, positive correlation between a two-year lag (**L2**); hence, its selection as a covariate for the reported model. The one-year lag (**L1**) on legislative opposition allows time for the legislature to react to undisclosed reports of repression that they may prompt to become public the following year through investigations or other forms of reprimand.[12] The measure for legislative opposition is the result of multiple calculations.

The term $\boldsymbol{\gamma}'\mathbf{I}_{t-1}$ represents the effect of legislative opposition, measured according to political strength and ideological distance from the empowered executive. Opposition to the executive is the combination of ideological distance and

[12] Some might argue that the separation of terrorism events and legislative influence potentially constraints legislative opposition to only having post hoc influence post-terror repression, so the analysis includes an alternative model with jointly observed terrorism and legislative opposition. The results do not qualitatively differ from the lagged sequence; hence, the reported findings contain only the estimates for the lagged model.

vote-based strength.[13] Ideology is a three-category measure, containing values of left, center, and right. Calculation of ideological distance reviews the top four vote-receiving parties in government and assesses the maximum point of difference between the any of these parties and the party of the executive. For example, if an executive is a conservative (on the right), and the most different political party in the top four is centrist, then the ideological distance is coded as centrist. If the most different political party is liberal (or left), then the ideological distance is coded as liberal. Political strength is a measure indicating the total number of votes that a political opposition has in a government. Each government has a total number of votes allocated to legislators, and the political strength indicator tallies the total number of votes held by parties opposed to the executive's party. For coalition governments, the measure includes parties not in the coalition. The final calculation of strength sets the total number of government votes in the denominator and the number of oppositional votes in the numerator, creating a weight that moderates the effect of ideological opposition in a given year. An exception to the rule for constructing these variables is the condition stating that legislative opposition is equal to zero when the party of the executive has majority control of the legislature.[14] Interpretation of the constant term in these models is for an executive-led system without relevant political opposition. The interaction term, $\boldsymbol{\lambda'(I_{t-1}'T_{t-2})}$, is the product of terrorism levels and the two types of legislative opposition (each with its respective interaction).

The two equations use panel-averaged probit to produce estimates.[15] Equation 1 produces estimates used to evaluate the hypothesis that ideology determines post-terror repression. The theory of ideologically motivated repression states that terrorism should elicit repressive responses in conservatively led but not

[13] These two variables are calculated using measures from the Database on Political Institutions (DPI). The ideological distance component of the legislative opposition variable is derivation of the "polarization" variable in DPI.

[14] When there are two legislative houses, legislative opposition is equal to zero when the party of the executive controls the lower and upper houses. Coding for this condition comes from the DPI variable "allhouse."

[15] A technical appendix discussing issues of endogeneity and temporal persistence is available upon request.

liberally led democracies. This means that the marginal effect of terrorism on repression should be positive and statistically significant for conservative-led systems but not liberal-led ones. Equation 2 produces estimates used to evaluate the hypothesis that legislative opposition constrains post-terror repression. Extant theory argues that legislative opposition restricts the use of repression irrespective of ideology. To evaluate the argument it is necessary to calculate the difference in marginal effects, subtracting the marginal effect of terrorism on repression from the marginal effects of terrorism and legislative opposition on repression. To support extant theory, this quantity should be less than zero and statistically significant. A combination of the two theories extends this analysis by saying that liberal legislative opposition should constrain conservative executives and not vice versa. The theoretical challenge to this combination of theories says that legislative opposition to repression is reactive and therefore ineffective.

V. Data

State repression is action taken by an agent of the state in violation of laws protecting individual rights. Data on state repression comes from the Cingranelli-Richards or CIRI dataset (2004), which records state violations of human rights across multiple categories. The categories of interest in this paper are extrajudicial killing, disappearances, and political imprisonment, which studies have shown to share an association with terrorism (Piazza & Walsh, 2009; Wright D. , 2009).[16] Extrajudicial killing occurs when state authorities or their proxies are responsible for the death of an individual, which occurred outside the auspices of law and an official trial. Disappearances occur when agents of the state or their proxies kidnap individuals, rather than lawfully arrest them.[17] Political imprisonment occurs when state authorities or their proxies hold individuals without charge, for example,

[16] The authors found that extrajudicial killing and disappearances correspond with terrorism but not political imprisonment.

[17] Given current debates among policy makers, some might liken the practice to rendition or the kidnapping and transfer of individuals to other countries for interrogation likely to include torture and other abuses meant to coerce information from the suspect. The measure of disappearances used in this paper accounts only for kidnappings that occur by state authorities within their sovereign territories and is therefore not synonymous with rendition.

during mass arrests. All three measures of abuse are dichotomous measure indicating whether there have been any reports of such behavior. Research assistants in the CIRI project derive values for these variables from field reports provided by Amnesty International and country-reports provided by the United States State Department. Data contained in the field reports is the result of an "abuse generating process" carried out by the state and recorded by anonymous observers in the field. Keeping their identity secret is paramount to the ability of Amnesty International being able to collect information that state authorities find highly objectionable. Data collection of this sort is linear in form with a micro-level sampling process and a discrete reporting mechanism (Cingranelli & Richards, 1999).[18]

Data on governmental institutions define the analyzed sample of democracies, measure the effect of legislative opposition, and indicate the ideological stance of executives. The identification of democracies used a combination of indicators, the Polity Index from Polity IV (Marshall & Jaggers, 2009) along with the Legislative and Executive Competitiveness Indices (LIEC and EIEC respectively) from the Database of Political Institutions or DPI (Beck, Clarke, Groff, Keefer, & Walsh, 2001). Use of the three variables enabled a flexible but tractable definition of democracy.[19] The Polity Index is a 21-category variable meant to measure alternative levels of democracy with the lowest values indicating autocracy, middle values indicating anocracy or transitioning regimes, and upper values indicating democracy. It is common to represent the variable on the negative ten to ten number line [-10, 10]. LIEC and EIEC variables are seven-category indicators describing how competitive the government under evaluation is, where

[18] The linear component is a count function that tallies the accumulation of abuses performed by state personnel against identifiable victims. Sampling occurs according to the direct and indirect observation of these abuses by field representatives, which has spatial and sociological components unreported by Amnesty International and the State Department. Spatial components connote the proximity of an observer to the event with the assumption being that the farther the person is away from an incident, the less likely that he or she is to have witnessed it. Sociological components are the social network lines of communication that an observer can use to view events vicariously and therefore dampen the effect of the spatial component.

[19] Criticisms in the literature that find fault with use of the Polity Index as an explanatory variable (Gledistch & Ward, 1997; Treier & Jackman, 2008) do not apply here because it does nothing more than help define the sample in this paper.

competitiveness indirectly represents how well democratic institutions in the country function. A strict "filter" for democracy states that a country must have a Polity Index score of eight or greater and LIEC and EIEC values of six or greater. Results unreported here indicate that legislative opposition does not restrict repression, but an insufficient number of cases of repression under liberal-led regimes made the sample inadequate for testing the effects of ideology. A less restrictive sample for democracies sets the threshold for the Polity Index at six and leaves the LIEC and EIEC values unchanged.

A measure for ideology drawn from DPI distinguishes between types of executive leadership and informs the ideological component in the legislative opposition measure (see the Research Design section for a description of its construction). Economists created the DPI dataset and intended use of the ideology measure to predict alternative economic platforms but there is nothing inherent to the coding that is explicitly economic.[20] Ideology, in DPI, is a three-category measure that identifies left, centrist, and right political orientations. I define liberal ideology as left and conservative ideology as right. Coding of the variable by DPI analysts uses four sources and follows a five-stage process that begins with evaluating party name and concludes with comparing internally coded values to a platform-based measure from an alternative dataset.[21] The first stage evaluates the name of a political party. Those containing the words conservative, Christian-Democratic, or right wing are conservative. Those containing the words communist, socialist, social-democratic, or left wing are liberal. The identification of centrists relied on the description of a government in the referenced sources as centrist according to professed party positions. The next two stages are attempts to reference other sources of information if the party name is insufficient for ascribing an ideological position. The final two include comparing the name-driven assignment with a platform-based measure and reconciling differences between the two.

[20] There is some precedence in the literature for using the DPI ideology variable in terrorism studies (Koch & Cranmer, 2009).
[21] Sources include the *Europa Year Book*, *The Political Handbook of the World*, the PARLINE database from the International Parliamentary Union, and the IFES Election Guide.

Data used to measure terrorism come from the Global Terrorism Database (GTD), which is a measure of domestic and transnational terrorism within countries.[22] The measures for terrorism indicate terrorism levels and changes in levels (or "shocks" of violence). Both measures are count variables that operate at the level of events. Terrorism level measures the absolute number of attacks committed within a sovereign territory during each month. Research has shown that it is necessary to account for seasonal trends in terrorism (Brin, 2006; Drakos & Kutan, 2003; Tournyol du Clos, 2009). The reason for this is that a primary goal associated with the act of terrorism is to use fear as method of coercion, which the culprits achieve through the spread of news about their attacks (Bassiouni, 1981). Irrespective of ideological motivation and goal, many acts of terrorism (especially events targeting people) become more likely and frequent in number during and in places where people are most likely to congregate. To account for this effect, the measure of terrorism used in this paper includes seasonal adjustments that measure terrorism on a monthly scale. Besides de-trending exogenous cycles unrelated to the question of repression and governmental institutions, seasonally adjusted terrorism measures also facilitate analyzing time series data when the outcome variable of interest is annual. Traditional time series analysis restricts evaluation to two months out of twelve in a year (losing more than 90% of available data), but seasonal adjustments prevent such data loss by evaluating change in monthly dyads between years. Figure 1 illustrates this point.

[22] Tests that used the transnational terrorism measures of RWITD (from RAND) and ITERATE did not demonstrate a positive correlation with repression values in democracy. A systematic comparison of these datasets with GTD will reveal whether the difference is because of the domestic terrorism cases in GTD or because of a difference in what accounts for transnational terrorism between the databases.

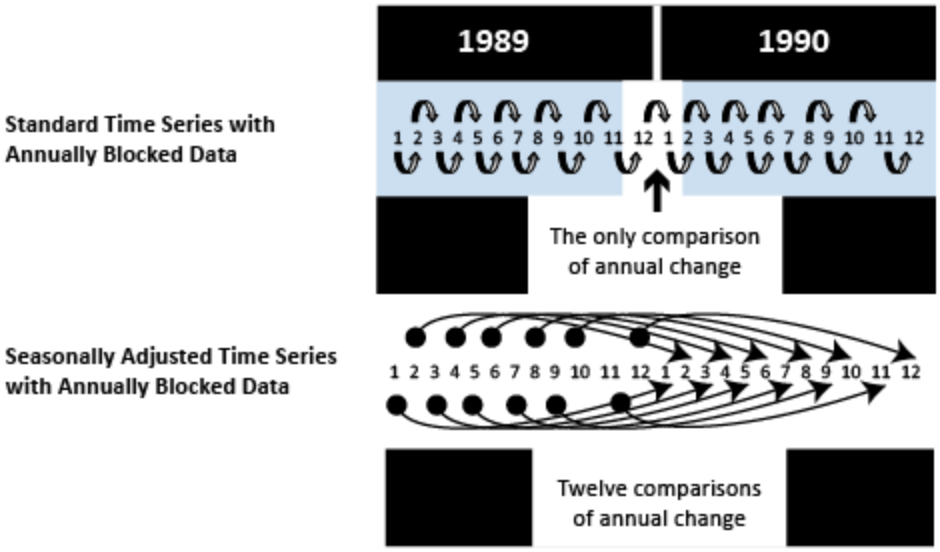

Figure 1 (Seasonally Adjusted Terrorism Levels): Seasonally adjusted terrorism data purge the measure of exogenous cycles at the same time that it preserves data otherwise loss using other time series techniques. The top figure in the panel shows the month-to-month construction of standard time series and the data loss when measuring an annual outcome. The bottom figure shows how seasonal adjustment creates twelve dyad pairs of months.

Control variables in the regression models account for the effects of alternative types of government, civil war, economic downturns, and voter participation on the occurrence of repression. Analysis of repression and legislative opposition implies and evaluation of executive power, which may differ according to the governmental system under consideration. To account for this, presidential systems serve as the reference category in the empirical model that includes measures for parliamentary systems and mixed systems as dummy variables. Repression is more likely to occur during periods of conflict (Davenport, 2008), so the empirical model includes an indication for those countries that have experienced civil war at any point during the period analyzed. Data on the occurrence of civil wars comes from Nicholas Sambanis.[23] Other research has shown that "voice" or voter participation significantly determines whether states repress in general. The theory asserts that activation within the electorate restrains not only political elites but also bureaucrats that carry out state action. More indirectly, voter participation also helps to stimulate the constraining role of other institutional actors like the judiciary. Data on voter participation during the last election (the

[23] His dataset is available at: http://pantheon.yale.edu/~ns237/.

percentage of enfranchised individuals that voted), drawn from Van Haanen is what Davenport used to express this relationship previously; hence, it is suitable here. Lastly, research has shown that wealthier countries are less likely to use repression (Davenport, 2008). If prosperity makes state violence less likely, then it is possible that the opposite will also hold true; economic downturns may spur terrorism levels and other types of social disorder that invite repressive responses. Annualized data on economic contractions provided by William Easterly, Ross Levine, and David Roodman (2003) form the measure, economic contraction. The indicator measure takes on a value of one when the gross domestic product per capita in the current year is less than the previous one, and zero otherwise.

VI. Findings

Two regression models use the panel-averaged probit estimator to answer question, "What determines post-terror repression?" The first model assesses whether the ideology of executives influences the occurrence of post-terror abuses like extrajudicial killing, disappearances, and political imprisonment.

	Extrajudicial Killing		**Disappearances**		**Political Imprisonment**	
	Conservative	*Liberal*	*Conservative*	*Liberal*	*Conservative*	*Liberal*
$Terrorism_{t-2}$	**0.0294****	0.0008	**0.0259****	0.0046	0.0066	0.0002
	(0.0065)	(0.0045)	**(0.0054)**	(0.0047)	(0.0043)	(0.0055)
$Terrorism\ Surge_{t-3:t-2}$	-0.0254**	0.0029	-0.0113	-0.008	-0.0074	-0.0043
	(0.0074)	(0.0053)	(0.0064)	(0.0057)	(0.0052)	(0.0064)
Civil War	1.2897**	1.2187**	0.8784**	--†	0.8294**	1.2747**
	(0.2859)	(0.4107)	(0.2669)	--†	(0.291)	(0.3267)
Voter Participation	0.0017	0.0005	0.001	-0.0056**	0.0072**	0.0094**
	(0.0013)	(0.0013)	(0.0018)	(0.0015)	(0.0013)	(0.0018)
Economic Downturn	-0.1839*	-0.0221	0.1656	-0.7066**	-0.2121**	0.5441**
	(0.0735)	(0.0722)	(0.0879)	(0.152)	(0.0686)	(0.0856)
Constant	-0.7763**	-0.7136**	-1.4143**	-0.8575**	-0.9432**	-1.1788**
	(0.1669)	(0.1904)	(0.1855)	(0.167)	(0.1744)	(0.1771)
Country-Months	4,308	3,528	4,308	3,528	4,308	3,528
Countries	54	42	54	42	54	42
Wald X^2	39.24	10.44	56.91	35.52	42.36	86.55
$p > X^2$	0	0.0636	0	0	0	0

Table 1 (Regression Results): Regression estimates on the occurrence of post-terror repression across three types of abuse and according to the ideology of executive leaders. **indicates that the coefficient is significant at the p < 0.01 confidence level & * indicates statistical significance at the p < 0.05 confidence level †indicates that the variable was dropped for reasons of collinearity.

Table 1 displays the regression results for levels of repression following terrorist attacks, as indicated by coefficient estimates for $Terrorism_{t-2}$, showing that post-terror repression occurs at a statistically significant level in conservative-led democracies but not liberal-led ones. Under conservative-led systems, democracies are likely to encounter post-terror abuses in the areas of extrajudicial killing and disappearances but not political imprisonment.[24] The variable, CIVIL WAR, significantly accounts for all forms of abuse irrespective of executive type, demonstrating that the influence of ideology has its limits. Voter Participation, or "voice," does not have the pacifying effect theorized in the literature, at least not consistently across abuse and executive types. It reduces the occurrence of disappearances in liberal-led regimes but increases political imprisonment irrespective of leadership type and has no statistically significant effect on the occurrence of extrajudicial killing.[25] Economic Downturns do not demonstrate a consistent pattern of influence for abuse in relation to repression or executive type. Surges in terrorism ($Terrorism\ Surge_{t-3:t-2}$) generally have a statistically insignificant effect on the occurrence of repression. Coefficient estimates in categorical choice models are first step to understanding the influence covariates have on outcomes. Marginal effects represent the true influence that terrorism has on repression according to executive type.

[24] A disaggregated measure of political imprisonment shows that conservative-led systems are likely to experience post-terror abuses at moderate but not excessive levels. Other disaggregated results show that conservative-led systems are likely to have excessive post-terror abuses in extrajudicial killing and disappearances.

[25] Other analyses that evaluated "voice" used composite outcome variables comprised of the Political Terrorism Scale and other measures for abuse (Davenport, 2008). Future research should investigate the difference between aggregate measures of abuse like those used by Davenport, disaggregated measures of abuse like those used in this paper, and a portfolio approach to abuse that treats alternative forms of repression as substitutes.

	Extrajudicial Killing	*Disappearances*	*Political Imprisonment*
Conservative Executive	0.0112**	0.0059**	0.0024
	(0.0026)	(0.0015)	(0.0016)
Liberal Executive	0.0003	0.001	0.0001
	(0.0016)	(0.0011)	(0.0018)

Table 2 (Marginal Effects of Terrorism): Changes in the likelihood of observing repression given changes in terrorism levels under alternative ideological leadership contexts. Calculation for the values occurs at the mean for all variables. ** indicates statistical significance at the p < 0.01 level of confidence & * indicates statistical significance at the p < 0.05 confidence level.

Table 2 shows that with respect to instantaneous change, terrorism attacks in conservative-led systems cause the likelihood of extrajudicial killing to raise 0.01 units and the likelihood of disappearances to raise 0.006 units. Both of these effects have high levels of statistical significance. Liberal-led systems demonstrate negligible relationships with post-terror repression, having marginal effects that are relatively small in magnitude and statistically insignificant. The findings support the theory that ideology matters in determining whether democracies use repression. A remaining question is whether legislative opposition has an effect on post-terror repression. Specifically, in the case of conservative-led systems, does the presence of centrist or liberal opposition limit the occurrence of post-terror repression?

Extant theory maintained that legislative opposition prevents repression-wielding executives from abusing rights following terrorist attack. Analysis of post-terror repression conditioned on executive ideology showed that extant theory wrongly assumes all executives abuse rights after attacks. Conservatives repress while liberals do not. The extension of a theory that combines the role of ideology and the controlling effect of legislative opposition uses an empirical test to determine if liberal legislative opposition constrains post-terror repression by conservative executives.

	Extrajudicial Killing	Disappearances
Centrist Opposition	-0.0192**	-0.0128
	(0.0034)	(0.0078)
Liberal Opposition	-0.007**	0.02**
	(0.0014)	(0.0025)
$Terrorism_{t-2}$	0.009	0.0163
	(0.007)	(0.0087)
Centrist Opp. * $Terrorism_{t-2}$	0.0237**	0.0051*
	(0.0063)	(0.0021)
Liberal Opp. * $Terrorism_{t-2}$	0.0001	-0.0003
	(0.0001)	(0.0002)
Terrorism $Surge_{t-3:t-2}$	-0.0069	-0.0072
	(0.0075)	(0.0098)
Civil War	0.3672	0.6077*
	(0.3401)	(0.2732)
Voter Participation	0.0079**	0.0005
	(0.002)	(0.0034)
Economic Downturn	-0.2399*	0.4242**
	(0.1031)	(0.1551)
Constant	0.0005	-1.609**
	(0.2976)	(0.2656)
Country-Months	1,548	1,548
Countries	23	23
Wald X^2	67.56	87.36
$p > X^2$	0	0

Table 3 (Conservative Leaders & Opposition): A comparison of the difference in marginal effects between conservative-led systems dealing with legislative opposition to those that operating without it. Calculation occurs at the variable means. ** indicates statistical significance at the p < 0.01 level of confidence & * indicates statistical significance at the p < 0.05 confidence level.

Table 3 shows the regression estimates for the effects of legislative opposition on post-terror repression in conservative-led systems. The analysis of legislative opposition includes presidential and semi-presidential democracies to the exclusion of parliamentary ones because some argue that opposition parties have no power in these latter systems.[26] Individual coefficients in these regression

[26] That said, the results for extrajudicial killing extend to parliamentary democracies. Centrist and liberal opposition in the legislature, even if not officially empowered, makes it less likely that post-

models do not convey all of the information necessary to evaluate the argument about the effects of legislative opposition (Brambor, Clark, & Gloder, 2006). Assessment of legislative opposition requires calculating the difference of differences in marginal effects (Berry, DeMerritt, & Esarey, 2010).

	Extrajudicial Killing	*Disappearances*
Centrist Opposition	-0.0099** (0.0024)	-0.0034 (0.0023)
Liberal Opposition	-0.0209** (0.0049)	-0.005* (0.0025)

Table 4 (ME of Legislative Opposition): Table showing the difference in marginal effects for legislative opposition conditioned on ideological type. Results show that centrist and liberal legislative opposition tends to limit post-terror repression in conservative-led systems. ** indicates statistical significance at the p < 0.01 level of confidence & * indicates statistical significance at the p < 0.05 confidence level.

To perform difference of differences calculations in this analysis requires calculating the unconditioned marginal effect of terrorism on the alternative types of repression and subtracting it from the marginal effect of terrorism conditioned on the two types of legislative opposition. If the difference is less than zero, the estimated effect is a modifying one. Results presented in Table 4 show that legislative opposition tends to have a statistically significant modifying effect on the occurrence of post-terror repression in conservative-led regimes. Additionally, the magnitude of this marginal effect tends to be larger for liberal opposition than it is for centrist opposition.

VII. Conclusions

What motivated this paper was the question, "What determines post-terror repression in democracies?" Conclusions drawn from the empirical analysis in this paper are that ideology determines the occurrence of post-terror repression in democracies and that ideologically motivated legislative opposition acts to constrain it. Until now, conjecture, rather than empirical findings, motivated the argument that legislative opposition constrains executive leaders and the relationship

terror repression occurs under conservative-led regimes. These results are statistically and substantively significant.

extended to post-terror repression. The contribution of this paper is that it put the argument about legislative opposition on an empirical foundation and showed that the motivation to use post-terror repression has ideological underpinnings. Research in this paper is part of a growing literature considering the role of ideology, terrorism, and counterterrorism within democracies from the bottom-up.

One theory is the "Cheney Hypothesis," which states that terrorists attack liberal-led states, rather than conservative ones, because they know that liberals will refrain from using repressive responses. It is the standard "hawk" versus "dove" argument, claiming the success of conservative-led deterrence through post-terror repression. Empirical results in the literature appear to confirm the argument (Koch & Cranmer, 2009), showing that terrorists target liberal-led regimes more frequently for attack than they do conservative-led ones. Results presented in this paper appear to be the link between the psychological studies cited in the Theory section and the empirical results presented by Koch and Cranmer. At the level of the individual, liberal political ideologies oppose post-terror repression and conservative ones condone them. At the level of the state, liberal executives preside over governments that do not use post-terror repression, while conservative ones engender the opposite. Vís à vís the state and terrorists, the consequence is clear, as terrorists target democracies led by liberals more than they do those led by conservatives. Inclusion of the other theory about the role of legislative opposition leads to the extended conclusion that if democracies want to protect themselves from terrorist violence, they should elect conservative executives and shift the balance of power in favor of the executive relative to the legislature. Such reasoning, however, seems to overlook the fact that 9/11 and the Madrid 2004 Train Bombings (3-11 or M-11), two of the historically largest attacks in their respective countries and the new Millennium, both occurred under the watch of unquestionably conservative governments. Arguably, these attacks by radical Islamists occurred because of the foreign policies of the United States and Spain, not because of who the leadership at the current time was. An interpretation of this sort addresses whether terrorists attack because who their targets are, as the "Cheney Hypothesis" claims, or because of what they do as other works in the literature claim (Potter &

Wright, 2009). Answering the question will require a thoughtful analysis that does more than compare coefficients and thinks hard about to identify what truly amounts to support for either or both of the claims.

Left looming in the background of the analysis on repression has been the related question of what determines legal response to terrorism. Does ideology matter or are other forces at play? When terrorists strike, is it better to counter the tactics that they used to attack or to deter them from being a terrorist in the first place? Legal approaches can act as responses to both of these questions, while repressive ones operate only on the second. After first World Trade Center and the Oklahoma City Bombings, the American Congress enacted laws that sought to give counterterrorism officials a long-term edge over anyone considering acts of terrorism like those used in the two attacks. Exact components to the two sets of bombs differed on various grounds but one aspect they shared was reliance on ammonium nitrate fertilizer, which is appealing because the nitrates in it help to create a forceful blast cycle under the right conditions of heat and pressure. Even more appealing at the time was the fact that fertilizer containing the nitrates was plentiful, relatively cheap, and otherwise easy to acquire, evidenced by the fact that it was as easy for the respective terrorists to acquire it in New York City as it was in the American heartland. Legislative acts taken by Congress and supported by then President Clinton, despite the complaints from farming interests, sought to dilute the fertilizers and make them ineffective resources for bombs. Other measures included adding "taggants" or chemical markers to more conventional explosives like SEMTEX. Taggants are what trigger "sniffer" machines at places like airports, governmental buildings, and other likely targets of terrorism. Countermeasures of these sorts recognize that truly deterring terrorists, especially those willing to commit suicide, is unlikely and therefore it is more important to incapacitate them temporarily in a technologically driven game of "cat and mouse." To understand counterterrorism in democracies and elsewhere, it is necessary to think of the overall set of actions that governments may pursue. An openly available, large-N dataset on legal and repressive counterterrorism is unlikely to arise anytime soon,

but it is this information that researchers require to answer the questions driving debates in the literature and policy circles.

CHAPTER II

Maximizing the Goodness of Fit for Social Networks: An Application of Amended ERGM Procedures to the Analysis of Terrorist Network Data

I. Introduction

Except for some exceptional circumstances, all network-generating processes are latent.[27] Network-generating processes produce social networks by specifying the "rules" individuals must follow when self-organizing into groups. Latency arises because the rules groups tend not to be common knowledge. What researchers observe are the social structures that individuals following these rules form. A technicality about networks makes it extremely difficult to study collective structures as the outcome of interest. Whereas a standard statistical approach to the described estimation problem would be to determine how a proposed set of factors condition the observed social structures, it is computationally impossible to distinguish one network from another definitively. This is known as the *network isomorphism* problem, defined as NP-Hard, because the amount of time it takes to compare how close two networks of even moderate size (e.g., 20 members) is computationally infeasible.

Network science has sought to circumvent the problem by evaluating networks according to their structural signatures or unique characteristics of network emergence. An emergent characteristic is one that arises unexpectedly through simple rules or from the "bottom up" (de Marchi, 2001). Current statistical

[27] Some exceptions include those instances of simulation through computational algorithms or concurrent observation in experimental or natural-experiment settings.

technologies limit the evaluation of network emergence to readily known and easily quantified mathematical distributions like the Power Law and other long-studied quantities. The problem is not every proposed theory exhibits emergence in a form following from the limited repertoire contained in the library of available tests. It is one thing to demand a theory is internally consistent and empirically falsifiable. It is quite another to demand it fit into one of only a few forms. The methodological choice is to continue developing tests from known distributions then to evaluate if the best fitting mold is the one theory predicted (Clauset, Shalizi, & Newman, 2009). An alternative is to develop a flexible tool used to identify network emergence in any form it occurs. Combined with the methods outlined in this paper, exponential random graph modeling (ERGM, also known as *p** statistical modeling) is a network statistics estimator offering researchers a path to evaluating their theories flexibly.

ERGM is a statistical model often misunderstood and misapplied in the literature. The misunderstanding is thinking that the estimates it produces directly test for the determinants of the latent network-generating process. This is not true nor is it the intention of those that developed. At its core, ERGM detects patterns of values in adjacency matrices, commonly restricted to binary entries. One way to represent a network is with an adjacency matrix, clearly demonstrating the applicability of ERGM to characterizing patterns of connections. This is where the misunderstanding occurs. Graph theory has long used algorithms, which are rules, to characterize various types of structural properties in networks also known as graphs (Wasserman & Faust, 1994). ERGM incorporates these algorithms, in the form of network statistics, to characterize structural properties of an evaluated network as a profile. Many ERGM users have conflated the rules of structural characterization with those of structural growth. A metaphor makes clear why this is wrong. Upon observing the complex structure of a tree, someone could diligently record the type of bark it has, the arrangement of its branches, its type of leaves, the presence of stomata on its leaves, and so forth. A reporting of these descriptions would quickly separate trees along lines like deciduous from coniferous, palm from oak, and so forth, but it would not explain the genesis from seed to tree for any one of them. The same observation applies for ERGM as a tool of structural

characterization. Even those who understand this is what ERGM does tend to misapply it, which is what this paper devotes its attention to correcting.

Misapplication of ERGM arises because researchers tend not use it to maximize the fit of a proposed network formula to the evaluated data. A problem that is most egregious when using network statistics that have more parameters than sufficient statistics (e.g., the curved exponential-family of functions) whose undefined values researchers should "sweep" across a well-defined state space in search of a global optimum. Frequently, however, this is not the practice followed. What results is the identification of a local optimum in the parameter space and not the global one. When a network formula contains numerous such terms, the global optimum is a jointly specified quantity users should identify through jointly conducted parameter sweeps.[28] Compounding the estimation problem in ERGM when using these terms are issues with "network degeneracy" and failed MCMC convergence, two issues discussed at length in the technical review below then followed with a set of prescriptions.

This paper proposes and demonstrates methods or procedures for using ERGM to maximize fit of a statistical model to observed network data. Analysis of its results reveals the procedures perform as expected but highlights needs for further considering what it means to maximize fit of structure in a network. Fit maximization captures the most prominent features of network data but not its rarely occurring features. Although expected, given the use of maximum likelihood estimation, it is still a problem. In summary, the paper makes two contributions. It offers a clear path for substantive theorists to test their theories of network emergence without having to restrict them to known mathematical distributions. Additionally, it demonstrates for technical, ERGM users improved methods for best harnessing the estimator, while also highlighting shortcomings in the evaluation of its results.

[28] Middle-of-the-road practices sweep parameters independently then fix their values for estimation in the joint model specification. Future evaluation will compare this to the procedures described here.

Organization of the paper proceeds as follows. After the introduction is a brief presentation of the data used in the analysis. The paper then continues with a review of ERGM. A discussion of problems encountered when using ERGM leads into a description of procedures useful for overcoming them. Deploying the procedures requires focus on maximizing fit of the proposed model to the evaluated data. The next section demonstrates application of the procedures to a single case identifying what network formula best describes the network of the Jemaah Islamiyah terrorist organization in 2000. Final sections of the paper review estimation results of the parameter sweeps and present some concluding thoughts.

II. A Review of the Literature Demonstrating the Need for Improved Network Statistics Methods

An argument made in the introduction is that some theories about network-generating processes produce expectations with network emergence characteristics easily characterized by known mathematical distributions. Others do not. What follows in the sections below are prescribed remedies for this estimation problem. Before engaging in the technical discussion, this section engages in the substantive area of terrorism networks, comparing a theory with easily characterized emergence to one whose expectations do not follow from extant mathematical distributions.

Barabási and co-authors argue that preferential attachment processes produce "scale-free" networks,[29] which have the structural trait of Power Law distributed connections among members when sufficiently matured.[30] There are few members with many connections and many with few connections: hubs and spokes. From a counterterrorism perspective, the prospect of combating networks

[29] See Watts (2004) for a review of the literature on "scale-free" networks and the following works as examples of the original contributions (Barabási & Albert, 1999; Barabási & Bonabeau, 2003; Bianconi & Barabási, 2001).

[30] A "scale-free" network contains a "hub and spoke" membership. Hubs in the network are individuals with many connections and spokes are those with relatively few. Clauset, Shalizi, and Newman (2009) present a series of tests for identifying Power Law distributions in observed data.

of this type is appealing because targeting the hubs structurally dismantles the group.[31]

Enders and Jindapon (2009) build upon a rational framework of terrorist networks (Enders & Su, 2007) to argue that terrorists self-organize under the competing pressures attack maximization and threat minimization. Attack maximization induces a high rate of connections among members for the purposes of exchanging resources and information. Avoiding detection means minimizing the size of a "behavioral footprint" (i.e., actions that authorities can trace, such as correspondences like phone calls and e-mails or direct encounters like meetings) according to the threat level posed by authorities.[32]

The "MinMax" combination makes for an optimizing network formation process. One conclusion is that terrorists operating under similar threat environments and drawing from populations with similar distributions of capabilities should form networks with similar structural features; an interesting hypothesis that excludes ideology and goals as determinants of self-organization. It also excludes a clear structural signature like the Power Law distribution forecasted by "scale-free" theory. Rather than a single characteristic readily identified through comparison against known mathematical distributions, expectations forwarded by "MinMax" theory concern relative similarities and differences in structure. Precisely evaluating this theory and others that are unable to associate their expectations with readily known mathematical distributions requires evaluation with an empirical tool that accurately describes structural properties of an observed network unable to associate their expectations with readily known mathematical distributions. Test availability is not a suitable metric for evaluating proposed theories; hence, the purpose of this paper.

[31] At least as long as the counterterrorism operations also include attempts to prevent the group from continuing to form connections with one another and expanding its membership by recruiting from the surrounding population. If not, the prospects of *breaking* the network are low because failure to stop for the dynamics of flow and continued percolation (tie formation).

[32] Authorities determine a threat level by how vigilant they are at detecting terrorist threats, which is a function of counterterrorism efforts like patrols, data mining, surveillance, informants, and so forth.

III. Introduction to the JJATT Data on Jemaah Islamiyah

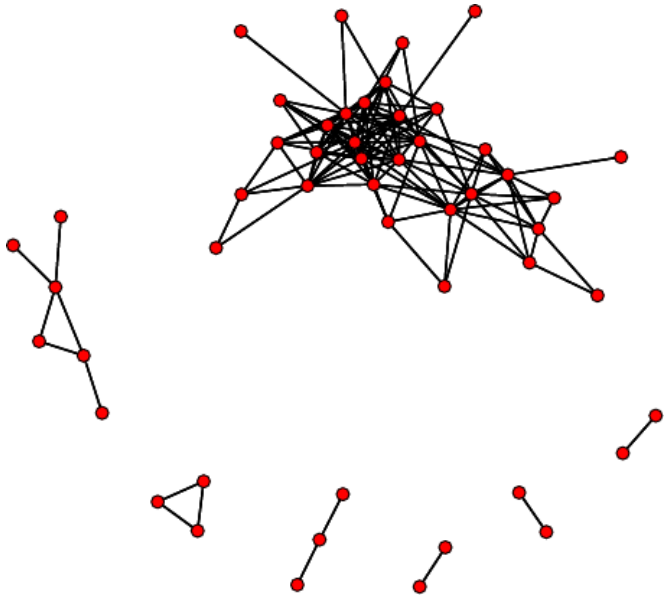

Figure 2 (Jemaah Islamiyah, 2000): A graphical depiction of the binary, undirected data on Jemaah Islamiyah in 2000.

Figure 2 is a network visualization of Jemaah Islamiyah (JI) terrorist organization. The representation comes from the year 2000, a turning point in the evolution of the group. This was the first year its membership organized and executed three terrorist attacks in Indonesia and one in the Philippine's.[33] Data on this group comes from the John Jay & ARTIS Transnational Terrorism (JJATT) project and contain information on the various social linkages between members of the terrorist organization.[34] The graph above is a binary and undirected, capturing the association between individuals along the social dimensions of friendship, family, and mutual participation in terrorist operations.[35] Data collection for JJATT included field-based interviews of individuals associated with JI or members of JI, secondary materials (e.g., police interrogation reports, court discovery material, and court transcriptions), and tertiary or "open source" materials (e.g., newspaper

[33] These attacks were the Philippine Ambassador's Residence Bombing, the Jakarta Stock Exchange Bombing, the Christmas Eve Bombings, and the Metro Manila Bombings.
[34] These data are available at: http://doitapps.jjay.cuny.edu/jjatt/index.php.
[35] This is the most basic representation of the data, which compounds alternate social networks into a single network. One interpretation of such a network is that it is the meta-network or composite set of all social relations linking individuals within a group (Carley, 2006, p. 55). The methods described and applied in this paper are appropriate for the characterization of meta-networks and any other sub-network suitable for ERGM analysis.

articles, governmental white papers, and non-governmental organization reports). The working assumption for the methods presented in this paper is that Indonesian, Malaysian, and Filipino authorities correctly identified the membership of JI in 2000 but may have been wrong about the connections they drew between members. A section in the Conclusion of the paper addresses ways forward for weakening the assumption about correctly identified membership within the framework presented here.

IV. Reviewing Exponential-Family Random Graph Models (ERGM) and Problems with Using It

$\boldsymbol{\Upsilon}$ is the infinite space defining all possible networks with distinct partitions in $\boldsymbol{\Upsilon}$ made according to membership size (N). N is a discrete variable, such that $\underline{N} = 3$ (according to the standard definition in sociology that the smallest unit of analysis is a triad) and $\overline{N} = \infty$. Furthermore, let $n_{\cdot} \geq 3$ be an element in N. $\Upsilon_{\cdot}$ represents the partitions or slices in $\boldsymbol{\Upsilon}$ that describes the distribution of all networks in each partition. A mass density function defines the distribution in $\Upsilon_{\cdot}$ and varies according to the ratio of the total number of members with connections to those with possible connections.

$$D = \frac{\sum \sum_{j=1}^{n_{\cdot}-1} x_{i,j \neq i}}{n_{\cdot}^2 - n_{\cdot}}$$

Equation 3

Equation 3 shows that for a network dyad containing members i and j, network density (D) is equal to the total number of connected dyads ($x_{ij} = 1$) divided by the difference between network membership (r) raised to the second power and network membership. Subtracting r from the square of itself indicates that a member i cannot have a connection to itself ($i \nleftrightarrow i$).[36] So, every Υ_n rises from the single network that represents D = 0% or no connectivity, maximizing at D = 50% density, and then decreasing again to the concluding point at D = 100% or full connectivity for any network of size $n_{\cdot}$. Density varies from $D = 0$, indicating no

[36] This is also the reason why the first summation runs from $j = 1$ to $r - 1$.

connections, to D = 1, indicating that all possible connections in the network have been realized.

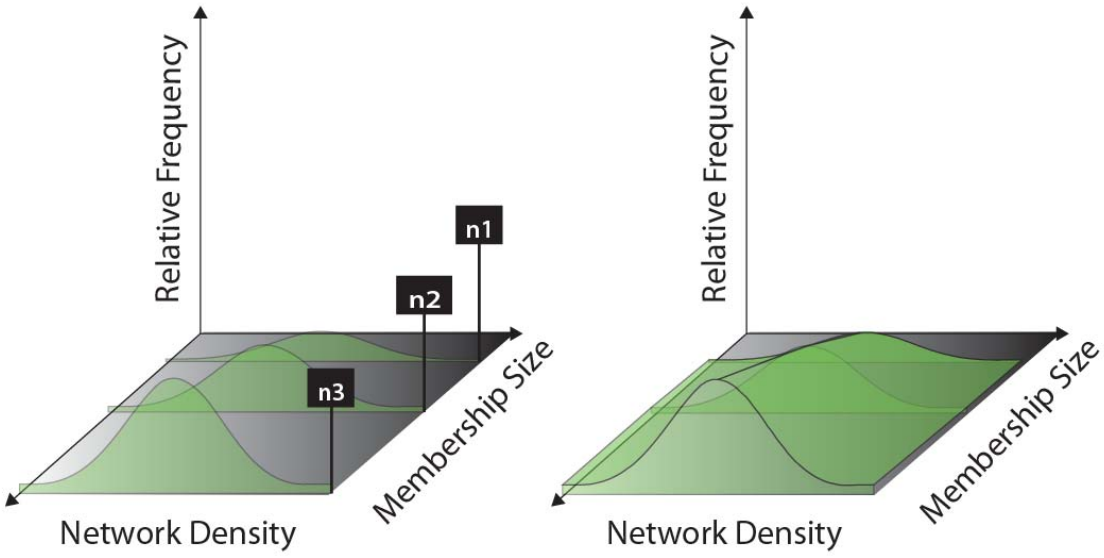

Figure 3 (Network Space): A visual representation of the theoretically infinite set, ϒ that contains all possible network combinations. A three dimensional representation of ϒ maintains that networks can vary by membership size and density. A third dimension captures the relative frequency of networks for each value of density. The boundary value for each slice is one, indicating that only one network apiece describes the empty and full sets.

Figure 3 is a visual representation of an interval in **ϒ**, displaying its three dimensions according to $Y_{n=1}$, $Y_{n=2}$, and $Y_{n=3}$. Defining the three-dimensional space are the quantities network density (D) along the X-axis, membership size (N) along the Y-axis, and relative frequency (C) along the Z-axis. From the figure it is clear that density acts as a standardized measure. The graphic on the right places a sheet over the slices and uses it to convey that **ϒ** is approximately continuous for all integers in $\mathbb{R}^+$. A combinations function specifies the value of the mass density function and produces the height of each slice in **ϒ** according to the total possible number of possible networks formed according to the number of members having at least one connection.

$$C_{Y_n}(r|n) = \frac{n!}{r!\,(n-r)!}$$

Equation 4

Equation 4 defines the count (C_{Y_n}) for the alternate number of ways to create connections between r members of a network with membership sized to n. C is non-monotonic but symmetric with respect to r. When r = 0 or r = n, C = 1, indicating

"empty" and "full" networks respectively. This relationship is true for any Υ_n. Equation 5 shows that Ξ_{Υ_n} is the cumulative density function, representing the aggregate number of networks in Υ_n as *r* increases.

$$\Xi_{\Upsilon_n}(r|n) = \int_{r=0}^{r=n} \frac{\sum\sum_{j=1}^{n-1} x_{i,j\neq i}}{r^2 - r} d(r)$$

Equation 5

The graphic on the right of Figure 3, shows that the maximum value of Ξ_{Υ} continuously increases as membership size increases. This results in a cumulative density of $\boldsymbol{\Upsilon}$ being:

$$\Gamma_{\boldsymbol{\Upsilon}}(r, N) = \int_{N=3}^{N=\infty} \int_{r=0}^{r=n} \frac{\sum\sum_{j=1}^{n-1} x_{i,j\neq i}}{r^2 - r} d(r)d(N)$$

Equation 6

Casual inspection of Equation 6 shows $\Gamma_{\boldsymbol{\Upsilon}}$ quickly transitions from being an easily manageable quantity when *N* = 3 to sub-infinite but extremely large number at even moderate values of *N* like *N* = 20. In other words, it is not necessary to for a network to have anywhere near an infinite number of members for it to have a near-infinite number of alternate forms that it could take. Understanding this general quality about networks is important for comprehending some of the challenges faced when attempting to estimate the likelihood that a given set of network statistics accurately summarizes the structural properties of an observed network.

Exponential-family random graph modeling (ERGM) is an estimation technique used to identify determinants of network structure (Robins, Pattison, Kalish, & Lusher, 2007; Snijders, 2002; Wasserman & Robins, 2005). It aims to describe how likely an observed network, y_{kn}, is relative to all possible networks in Υ_n, conditioned on network statistics in the vector **g** and their sufficient statistics contained in the vector $\boldsymbol{\theta}$. Equation 5 depicts this relationship.

$$p_{\boldsymbol{\theta}}(\Upsilon_n = y_{kn}|\mathbf{g}) = \kappa^{-1}\exp\{\boldsymbol{\theta} f(y_{kn}, \mathbf{g})\}$$

Equation 7

In Equation 7, κ is a normalizing constant, such that $\kappa \equiv \Upsilon_n(\boldsymbol{\theta}(\mathbf{g}))$, representing the evaluation of y_{kn} as a function of the statistics **g** relative to all networks in Υ_n produced according to **g**.

$$\kappa = \sum_{k=1}^{K} \exp\{\boldsymbol{\theta} f(w_{kn}, \mathbf{g})\}$$

Equation 8

Let y_{kn} be the k$^{\text{th}}$ network with membership size n in an ordered subset of networks in Υ_{n}, **w**. Equation 8 makes clear that the evaluation in Equation 7 is in fact the likelihood that network formula $\boldsymbol{\theta}'\mathbf{g}$ accounts for the structure of $y_{k\text{n}}$ relative to all of the other networks in **w** produced by the formula. Another way of stating this is that for the subset of Υ_{n} or **w** produced according to $\boldsymbol{\theta}'\mathbf{g}$, what are the odds of observing $y_{k\text{n}}$? The purpose of estimation with ERGM is to maximize this quantity.

The network formula $f(y_{k\text{n}}, \mathbf{g})$ attempts to describe the pattern of connections throughout the network, $y_{k\text{n}}$. Consider the representation of a network with an adjacency matrix. The rows represent each i^{th} member and the columns represent their possible *j* connections. Recall that $\boldsymbol{\theta}$ is a vector of change coefficients and **g** is a vector of network statistics functions. A network statistic is a function valued according to the application of an algorithm to the network in question. $\boldsymbol{\theta}$ captures the overall effect that network statistics have on the rate of connections in a network. Each element in $\boldsymbol{\theta}$ is a measure of effect relative to random chance, defined as the odds 50:50. Any θ_{q} valued less than zero indicates that the statistic in question accounts for connections at a rate less than random chance. Any θ_{q} valued greater than zero indicates the opposite. Network statistics can be structural, pertaining to connections between members, or personal, describing the individual characteristics of members and dyads.

This paper restricts analysis to elements in **g** that are structural determinants.[37] An additional restriction is to a certain type of network, the

[37] The author is not convinced that popular ERGM software like "ergm" or SIENA properly account for individual attributes when performing the Markov Chain Monte Carlo simulation of replicate networks discussed below. To do so, these programs would have to construct multi-variate correlation matrices for structural factors and attributes as well as between structural factors and attributes. Inspection of the source code for "ergm" offers no indication that the MCMC process is uses employs such a multi-variate covariance structure; hence, the skepticism offered by the author. This does not mean that attributes will not explain patterns of connections in an observed network. Just that there is no way to determine what this really means in the context of a larger undefined population. Note that even if estimation must approximate Υ_{n} through simulation, the population of networks is a theoretically known quantity. The same is rarely true for characteristics observed in a sample of individuals that form a network.

undirected or dichotomous graph. These networks are such that for members *i* and *j*, a connection from *i* to *j* implies a connection from *j* to *i* ($i \leftrightarrow j$). For the analysis conducted in this paper, a formula of network statistics effectively describes the pattern of 1's and 0's in the upper triangle of the adjacency matrix.[38]

ERGM calculates values in $\boldsymbol{\theta}$ in one of two ways. If the proposed formula $f(\boldsymbol{\theta},\mathbf{g})$ contains terms in $\mathbf{g}$ that demonstrate "dyadic independence," then estimation of $\boldsymbol{\theta}$ uses what the literature calls *maximum pseudo likelihood* (Hunter, Goodreau, & Handcock, 2008, p. 250). A term is dyadically independent when it acts as a co-variate of the node in question and does not change conditioned on a change made to any other node in the network. Terms like individual attributes and descriptions of aggregate structural properties (e.g., network density) have dyadic independence. Equation 9 shows that the maximum pseudo likelihood calculation of $\boldsymbol{\theta}$ under these circumstances is a logit model with the state of a dyad (x_{ij} = 0 or x_{ij} =1) being the outcome variable and terms in $\mathbf{g}$ acting as the regressors.

$$p(x_{ij} = 1 | y_{kn}) = \frac{e^{\boldsymbol{\theta}'\mathbf{g}}}{1 + e^{\boldsymbol{\theta}'\mathbf{g}}}$$

Equation 9

As a maximum pseudo likelihood estimator, the logit function in Equation 9 accounts for variation in structure for elements in $\mathbf{g}$ with respect to y_{kn} but in no way accounts for the likelihood sought for maximization in Equation 7 because it makes no account for the denominator represented in Equation 8. Rather than being a pseudo likelihood, Equation 9 amounts to a biased representation of the estimates for all cases other than when the specification of $\mathbf{g}$ is such that y_{kn} is at the center of the distribution in w. The literature has largely concluded that use of this estimator is inappropriate (Wasserman & Robins, 2005, pp. 157-159).

Terms that demonstrate "dyadic dependence" compel ERGM calculation of $\boldsymbol{\theta}$ that uses a maximum likelihood estimator for the logit function. What distinguishes it from the pseudo likelihood calculation is use of a Markov Chain Monte Carlo process to generate a sample population of networks that approximates the

[38] Evaluating only half of the adjacency matrix is sufficient the $i \leftrightarrow j$ relationship makes it a symmetric matrix. Additionally, analysis does not include "self-ties" or $i \leftrightarrow i$ connections, so estimation also excludes the diagonal.

calculation of Equations 1 and 2.[39] Altogether, the calculation is known as Markov Chain Monte Carlo maximum likelihood estimation, hereafter referred to as MCMCMLE. Calculation of $\boldsymbol{\theta}$ evaluates the distribution of values supplied by the application of toggling to the dyads in y_{kn} and the replicate sample. Calculation of each θ_q in $\boldsymbol{\theta}$ consists of evaluating changes in the value of a statistic according to "toggles" of network dyads. To toggle a dyad means to turn a 1 to 0 or a 0 to 1. ERGM determines preliminary estimates of values for $\boldsymbol{\theta}$ then uses these values to generate replicate networks.

Generation of network replicates uses the preliminary estimates of $\boldsymbol{\theta}$ from y_{kn} and user-set specifications for simulation to generate a sample of replicates.[40] One simulation parameter is sample size, which indicates the total number of replicates it is necessary to generate to complete estimation. Two other parameters are *burn-in* and *interval*. ERGM uses a Markov Chain Monte Carlo (MCMC) process to generate replicate networks. Recall that estimation begins with just one network. To generate replicates, ERGM randomly selects dyads in the observed network and alters their states according to the specified network formula. Network sampling in this manner returns to the view that $y_{n\mathrm{k}}$ is a random variable drawn from Υ_n and that any different configuration of $y_{n\mathrm{k}}$ represents another draw from the subset of Υ_n, $\mathbf{w}$. The parameter *burn-in* defines how many replicate networks the generator will simulate before initiating construction of the sample. *Burn* is an appropriate description because the parameter determines how many changes to $y_{n\mathrm{k}}$ will ensue before populating the sample. The literature prescribes using a relatively large value for *burn-in* to distinguish members in the sample of $\mathbf{w}$ from $y_{k\mathrm{n}}$ as much as possible. Once sampling has begun, the parameter *interval* states how many changes must ensue between evaluations of replicates potentially added to the sample. As a step-length, *interval* specifies how distinct from one another sampled members in $\mathbf{w}$ are from one another. Replicate evaluation uses the measure of density to determine

[39] Calculation of the true likelihood would require evaluating a network formula across all of the networks in Υ_n, which is computationally infeasible for even moderate sized networks. This is because of the permutation function described above.

[40] All of the parameters have default settings, so it is unnecessary for users to input values unless they want to customize the estimation runs.

where a proposal lies in Υ_n according to network density and how different it is from $y_{n\mathrm{k}}$. Rejection of a network occurs when a replicate falls outside a density bandwidth of $\mathrm{D}(y_{k\mathrm{n}}) \pm \varepsilon$.[41]

Largely unrecognized in the literature is the fact that the replicate evaluation mechanism in ERGM incorporates a certain type of measurement error into the estimates. Random selection of replicates with a density that varies according to the $\mathrm{D}(y_{k\mathrm{n}}) \pm \varepsilon$ threshold accounts for differences in the absolute number of connections recorded in the data. Narrowing the threshold inserts, perhaps falsely, an increasing level of confidence in having recorded the correct number of connections within the network. The extreme specification is $\varepsilon = 0$, which imposes the assumption that the data contain the correct number of connections and that all comparisons should have only that number. Users should set $\varepsilon = 0$ only when they are 100% confident that the data contain the right number of connections.

Evaluation of ERGM estimates determines whether the MCMC process converged and—if it has—which of the formula terms are statistically significant along with what the magnitude of their effects are. MCMC convergence occurs when the sufficient statistics estimated from the replicate sample form a uni-modal distribution. A uni-modal distribution of coefficients indicates that only one regime of networks exists for the formula **g**. Statistical significance and coefficient magnitude combine to reveal whether the term in question accounts for connections in $y_{k\mathrm{n}}$ at a rate greater or less than random chance (i.e., $\theta = 0$) at a specified level of statistical significance. Beyond these two points of assessment, the literature also advises that users evaluate "goodness of fit" for the specified model (Hunter, Goodreau, & Handcock, 2008). To do this, users are to evaluate how much the replicate networks that an accepted formula produces resemble $y_{k\mathrm{n}}$. Direct comparison of even moderately sized networks (i.e., nine or more members) is an NP-Hard problem (or non-polynomial time "hard" problem) and therefore

[41] Users have a limited choice on how to alter this sampling parameter. For example, they can choose to make all replicates have the same density as $y_{k\mathrm{n}}$, to make the replicates have the same relative distribution of degree as $y_{k\mathrm{n}}$, to make all replicates have a maximum or minimum number of connections, and so forth. For more details on the options, see the software documentation. Specification of the bandwidth parameter requires users to state the minimum and maximum number of connections members can possess, which is not always the easiest calculation to make.

computationally infeasible for most networks (e.g., n > 4). An alternative is to define the same structural properties for at least two networks then determine how close, in terms of the properties, the two are to one another. Here, this evaluation amounts to determining whether the property in question of the observed network falls within the confidence interval produced by the formula replicates (Morris, 2003). Commonly analyzed structural properties include degree distribution (i.e., the relative frequency of connections in y_{nk}), shared partner distribution (i.e., relative frequency of the number of mutual partners actors in y_{nk} share), and geodesic distribution (i.e., the relative frequency of path-lengths describing the minimal distances between members of y_{nk}). Altogether, calculation of ERGM and evaluation of its estimates roughly consists of five steps.

1.	Specify a formula of network statistics and calculate coefficients for the observed network.
2.	Use the specified formula along with the calculated coefficients to generate alternate networks also known as replicates.
3.	Produce a sample of replicates according to a set of simulation parameters.
4.	Estimate new coefficient values for the specified formula by evaluating the replicates, determining whether estimates in the sample converge.
5.	Analyze the coefficients and the "goodness of fit" diagnostics for the estimates.

Table 5 (ERGM in 5 Steps): A five-step description of Markov Chain Monte Carlo maximum likelihood estimation using ERGM.

V. Estimation Problems with ERGM

As many in the literature have come to find, it is difficult to achieve good estimates with ERGM by following the five steps outlined in Table 5. Two major hindrances encountered are network degeneracy and failed convergence of the MCMC process. When a $\boldsymbol{\theta}$ for a formula produces a network sample, $\mathbf{w}$, whose

members occur at or near the extremes of Υ_n, estimation encounters the problem of degeneracy. Unless y_{kn} is obviously near the boundaries of Υ_n, there is little reason to consider the generated replicates useful. This has not prevented a debate from ensuing in the literature with some contending there is theoretical merit to identifying degenerate and near degenerate formula specifications is useful (Wasserman & Robins, 2005, pp. 156-157). This is true for theoretical explorations for the $f(y_{.n}, \mathbf{g})$ specifications that produce networks at or near the boundaries, but it is not true for characterizing y_{kn} not lying in either extreme. For this reason, standard ERGM estimation simply halts when it encounters network degeneracy. The literature has treated degeneracy as a problem that arises because of the formula $f(y_{.n}, \mathbf{g})$, highlighting the need to for improved model specification.

A favored approach to improving model specification replaces static, dyadically dependent terms in **g** (e.g.**,** triangulation, node degree, k-star, and so forth) with more complex ones. One such class of terms comes from the curved exponential family of functions (Hunter D. , 2007).[42] Curved exponential functions have more parameters than they do sufficient statistics (Efron, 1975). In the context of a network statistics formula, this means that the estimator calculates a value for not only the associated θ but the exponential parameter as well.

$$\text{GW Degree}\,(y_{nk}) = \mathrm{e}^{\alpha}\sum_{l=1}^{n-1}\{1-(1-\mathrm{e}^{-\alpha})^{l}\}D_l(y_{nk})$$

Equation 10

Equation 10 defines the curved exponential function known in the literature as geometrically weighted degree. Geometrically weighted degree as a function of y_{nk} compresses the frequency distribution of connections among members into a single value. The exponent, α, indicates the weight placed on a given category of connections or l. The index of the summation operator runs from $l = 1$ to $l = n - 1$, because that is the most connections a member in the network can have without

[42] Other candidates include "alternating k-stars" and other similar functions. Procedures outlined in this paper extend to all network statistical terms containing exponential parameters in addition to the change statistics calculated in the network formula. That means that they include "alternating k-stars," which the paper has excluded from the analysis for the purpose of brevity.

counting a connection to itself. The term D_l designates the number of members in the network with l connections. When $\alpha = 0$, no transformation of the degree distribution occurs. However, when $\alpha > 0$ members with higher numbers of connections receive lower weights and the opposite when $\alpha < 0$.

Curved exponential functions like geometrically weighted degree are flexible, meaning that users can vary values of the exponent in search of a $\boldsymbol{\theta}$ that maximizes goodness of fit (Hunter, 2007, p. 228; Hunter, Gooderau, & Handcock, 2005, p. 27). Exponents can take on any values in the set of real numbers, $\mathbb{R}$. This means an expanded parameter space, the range of values specified as in the domain of the function, for identifying the fit maximizing value. Locating such values entails sweeping through this space in some way. Such a search casts aside notions of substantive inquiry[43]; a point alluded to at the outset of this paper. The stated need for parameter sweeping is not without precedence. In a brief, concluding, note on how to identify exponent values that best fit the data, Hunter and Handcock write, "Naturally, however, data-driven estimation of θ_5 **[the exponent]** is to be preferred unless θ_5 can be pre-set based on theoretical considerations," (2004, p. 20). Under what conditions, other than simulation, will a researcher know the value of a generative exponent? Very few circumstances —if any—are likely. The best conclusion one should draw from this statement is that it is necessary to sweep the parameter space when specifying a network formula containing one or more of the curved exponential-family terms.

Parameter sweeping to avoid degeneracy and to maximize fit does not automatically resolve all of the estimation problems. Failed MCMCMLE convergence is another issue bemoaned for some time in the literature (Snijders, 2002). No convergence in the estimates of sufficient statistics implies an underlying multi-modal distribution of values that indicate alternate regimes of networks. Fully appreciating what it means to have alternate regimes generated by a single set of

[43] Substantively, positive values of α indicate anti-preferential attachment processes, while negative values indicate preferential ones. Recall the theory of "scale-free" networks and the argument that preferential attachment produces networks with Power Law distributions. Reported findings in the literature tend to place substantive weight on the interpretation of these values within a variety of social network settings. For an example, see Goodreau, Kitts, and Morris (2009).

initial estimates is important. Remember that the purpose of ERGM is to identify the MLE for y_{kn}. A situation characterized by multiple network regime differs from a single regime, because of separate one of Failure to converge reflects a lack of agreement among alternate modes that represent different regimes of networks produced by the sampling process (10). Rather than there being too few networks in a low density probability mass of Y_n, as encountered in degeneracy, there are too many networks with distinct differences. The resulting estimate is the original pseudo likelihood estimate that users should have little confidence in regarding estimation of Equation 7. The estimates will fit the observed network (i.e., have a desirable AIC) but will not include an evaluation of the other networks in **w**. Since it is the approximate likelihood evaluation for the performance of the parameter estimates in **w** that ERGM aims to achieve, this is not an acceptable estimation result.

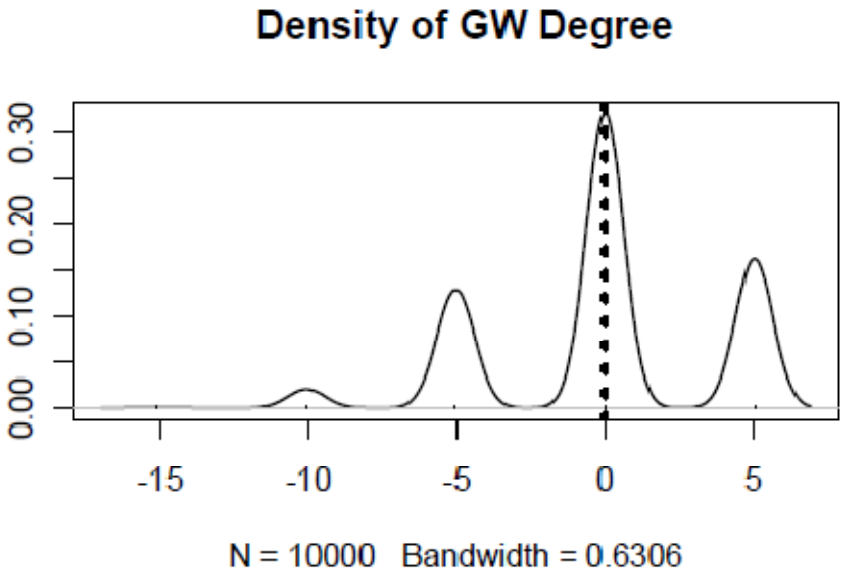

Figure 4 (Failed MCMC Convergence): An example of a multi-modal degree distribution produced in the analysis of a five-member, "toy network" using an ERGM formula containing the geometrically weighted degree distribution terms for a directed network.

Figure 4 displays the MCMC distribution of the geometrically weighted degree distribution term applied to a five-member network used for the purpose of

exposition.[44] Four regimes are apparent in the data, making estimation of a single estimate along the dashed line somewhat meaningless for all but one regime of the sample. Snijders offers a number of techniques for coercing the network-generating sampler into producing network replicates with convergent statistics (14-29). Two of the discussed strategies include increasing sample size and using a alternate sampling algorithm. Increasing sample size aspires to use the "law of large numbers" as leverage against the underlying inherent multi-modality, but its shortcomings should be apparent. To ignore the estimates drawn from the alternate modes means to waste information about what estimates may maximize the fit for the y_{kn}. Unnecessarily discarding information is rarely a boon to estimation.

The other option of altering the sampling algorithm appeals to the standard MCMC dictum of achieving convergence, but it may also serve as a more sophisticated way of unnecessarily discarding information. MCMC convergence works upon the idea that a sufficiently tuned Marko Chain will reach equilibrium and that failure to do so means to evaluate the model under disequilibrium. Sorting through this matter convincingly is beyond the scope of this paper, but it is possible that the multi-modal distribution represents multiple equilibria that have varying probabilities of realization. If this is true, then estimation should include the pair-wise combination of these values and evaluate them accordingly. To perform such an assessment requires rewriting code in the software then comparing the strategy to those that Snijders proposes. The endeavor constitutes a point of future research but not something to implement currently. Given the disagreement on the matter, this paper treats regions of the parameter space as "dead zones" and looks to reassess the matter in the future.

[44] Simulation of the network used the terms "edges" and "triangle" with $\theta_E = 0.3$ and $\theta_T = 0.05$. The ERGM estimation used included the "edges" and "geometrically weighted degree" terms, including a parameter sweep of the α exponent that ran from -1 to 1. Regions of failed MCMC convergence occurred in the range $\alpha = -0.3$ to $\alpha = 1$.

VI. Procedures for Maximizing fit with ERGM and Evaluating Their Application

Procedures proposed in this paper amend steps outlined in Table 5 to include sweeping the parameter space of network formulas that contain curved exponential-family terms and filtering estimation results according to various statistics that indicate how well the model performed. As indicated above, sweeping the parameter space of the specified model is not controversial according to the discussion in the literature. Rather, it is a process that the literature has not been clear regarding how to do it. This paper presents two separate procedures that users can follow; only one of rich the demonstration applies.

Ideally, parameter sweeping consists of two, iterative phases: broad search and drill-down or narrow search. Broad search specifies a very wide interval in the state space in a series of integers and their median points, for example, the series 0, 0.5, 1, 1.5, 2, 2.5 and so forth. Evaluation of these intervals does not "fix" the exponents as constants but instead uses them as initial conditions then allows the MLE to perform as it should by estimating the most likely combination of exponential values along with the sufficient statistics for the data networks in the sample. Analysis of the results collected during the first phase identifies which regions of the parameter space have the highest likelihoods, treating each of them as candidates for the MLE estimates. The second phase of narrow search establishes intervals around each candidate and applies a more granular search around in the space, meaning smaller increments than 0.5 steps. Although time consuming, this is the ideal procedure. The less time consuming procedure establishes the interval for narrow search, *ex ante*. This paper implements the second procedure of narrow search only but future research will evaluate it in comparison to the broad-narrow combination. It is possible that which type of sweep is best depends upon the structure of the network in question. Ultimately, the goal will be to specify a diagnostic test for helping users make an informed decision.

Parameter sweeping strategies assist in the identification of possible solutions for maximizing model fit but do not make the evaluation themselves.

Recall the estimation problem posed by Equation 7: estimate $\boldsymbol{\theta}$ for $\mathbf{g}$ such that it makes the network $y_{k\mathrm{n}}$ most likely in Y_{n}. Recall that the literature advised "goodness of fit" statistics to make the evaluation. These effectively compare structural properties of $y_{k\mathrm{n}}$ to those exhibited by the rest of the networks in $\mathbf{w}$ on condition of $\boldsymbol{\theta}'\mathbf{g}$. To do this is an easy task for a few evaluations but extremely time consuming following even the shorter version of the outlined parameter sweeps. What makes the process difficult is the fact that ERGM does not automatically generate these statistics following its simulations. It requires a post-estimation step of simulating large numbers of replicate networks from $\mathbf{w}$ to form the confidence interval used to assess fit with $y_{k\mathrm{n}}$.

Research results on a simulated, 5-member network shows that "goodness of fit" performance parallels three results retrieved directly from the estimation results. The three results are whether the formula parameterization avoided degeneracy, whether estimates demonstrated MCMC convergence, and whether the formula identified statistically significant values for all of the included terms at a confidence level of $p < 0.05$. It may seem odd at first that all of the values for included terms must have statistically significant values, since this seems to force the term upon the model unnecessarily. The assessment would be valid if the empirical question was theoretical, but it is not. Instead, it is about identifying the best description. From that perspective, researchers must determine whether they want to include or exclude a term. The point made here is that the terms researchers include must have estimates relevant to the formula; otherwise they act as noise that distorts estimates that the model makes. Having filtered the results according to these three criteria, the *Akaike information criterion* (Akaike, 1973) or AIC score ranking mirrored that produced using the traditional "goodness of fit" measures.[45] A claim that this makes is that the proposed combination of filtering

[45] The formula for AIC is: $\mathrm{AIC}(\mathrm{M}) = -2\big(\ln\mathrm{LL}(\mathrm{M})\big) + 2\mathrm{x}_{\mathrm{M}}$. The equation says that AIC is a function of the evaluated model, M. It is the difference between two times the number of terms in the model (x_{m}) and two times the log likelihood (LL) of the model. LL is approximated in the case of ERGM. To see why AIC scores produced during a parameter sweep track LL, it is only necessary to realize that x_{m} becomes a constant, since the formula does not change regarding the number of evaluated terms. So, the only change that occurs is in the performance of LL as a function of M. Since everything in the

and ranking sufficiently approximates evaluations made using "goodness of fit" statistics. An assessment of this claim concludes the section that analyzes estimates produced from the case study of the Jemaah Islamiyah terrorist network.

Review of ERGM and problems encountered when using it has led to an outlining of procedures in this section that extend as well as revise current practices in the literature. The extension consists of recognizing that estimations using network statistics possessing more parameters than sufficient statistics should include parameter sweeps that attempt to identify the likelihood maximizing parameter value within a defined parameter space. When a network formula consists of more than one of these terms, then the parameter sweep should occur jointly across a grid for the combination of two terms, a cube for the combination of three, and so forth. The revision to current practice amends calculation of the "goodness of fit" statistics for incorporation within the time-consuming parameter sweep procedure. A claim that the paper makes is that filtering then sorting estimation results approximates evaluations made using "goodness of fit" simulation and confidence interval evaluation procedures. Filtering requires sequentially establishing non-degeneracy for a given parameter space, demonstrating MCMC convergence, and identifying parameter and sufficient statistic estimates that are statistically significant. Ranking entails sorting estimates by their AIC scores from lowest to highest. Discussion in the paper has led to the corollary argument that estimation should occur for the parameters as well as the sufficient statistics, which is something that has yet to become common practice in the literature.

Assessment of the proposed procedures involves demonstrating them in a case study and evaluating the core and secondary arguments made about their use. The core argument is that these procedures are useful for maximizing the fit of a proposed model. Testing this proposition involves applying the filtering and ranking steps then assessing the "goodness of fit" for the highest and lowest ranked estimates. If the procedures do what the paper claims, then the model fit for the

formula remains constant except for the fit of the model, the AIC effectively subsumes the BIC (which includes an account of sample size) within this type of parameter sweep analysis.

highest ranked model specification (i.e., the one with the lowest AIC) should be better than that of the lowest ranked one. Importantly, this is a conservative test biased against finding support for the proposed procedures. Filtering excludes all specifications that have not converged and do not contain parameterizations for network statistics terms that are statistically significant. The comparison then is one at the margins, distinguishing the best from the best and not merely comparing the best against the worst.

The secondary argument is that ERGM estimation should occur for sufficient statistics for formula terms in **g** in addition to the exponents of the terms also contained in **g**. Two types of visual analysis evaluate this proposition. One consists of rendering the likelihood surface in its "fixed" state, displaying performance of the estimates according to the height throughout the parameter space. Comparison of this "fixed" condition to a graphic that illustrates where the final estimates settled establishes support for estimating the exponents if the MLE shows that the final exponent values differ considerably from those specified in the initial conditions. If the estimated landscape differs significantly from the "fixed" one, then there is support for the argument. A second evaluation of the argument evaluates the phase portrait of the estimation sequence. Phase portraits illustrate with vectors the trajectories and distance of change between the initial conditions (or starting values) and the final estimates. Support for the argument rests in a portrait that exhibits a high degree of movement during the sequence of estimations.

VII. The Best fit Description of Jemaah Islamiyah, 2000: A Case Study

The statistical model used to characterize the Jemaah Islamiyah network consists of three terms, one dyadically independent term and two curved exponential family terms that are dyadically dependent. The equation for the model is:

$$p(x_{ij} = 1 | y_{kn}) = \frac{e^{\boldsymbol{\theta}'\mathbf{g}(D,\alpha,\lambda)}}{1 + e^{\boldsymbol{\theta}'\mathbf{g}(D,\alpha,\lambda)}}$$

Equation 11

The full expression of $\mathbf{g}(\mathrm{D}, \alpha, \lambda)$ is:

$$\theta_1\left(\frac{\sum\sum_{j=1}^{r-1} x_{i,j\neq i}}{r^2 - r}\right) + \theta_2\left[e^{\alpha}\sum_{l=1}^{n-1}\{1-(1-e^{-\alpha})^l\}D_l(y)\right] + \theta_3\left[e^{\lambda}\sum_{l=1}^{n-1}\left\{1-\left(1-e^{-\lambda}\right)^l\right\}D_l(y)\right]$$

Equation 12

Equation 12 presents a formula that characterizes structure of the terrorist network as a function of network density, a geometrically weighted degree distribution, and a geometrically weighted shared partner distribution. The terms network density and geometrically weighted degree have been discussed, respectively in Equation 3 and Equation 10 above. The geometrically weighted shared partner distribution is similar in form to the geometrically weighted degree distribution, but its interpretation differs considerably. The exponent, λ, resembles α by assigning a weight to *l* but now *l* represents the number of mutual partners that members *i* and *j* share. *l* still has a range from *l* = 1 to *l* = n – 1, but it now serves as an indicator for clustering in the network, rather than just the central connectivity of member *i*. The term D_l indicates the total number of dyads in the network with a total of *l* shared partners.

Equation 12 contains two exponential parameters that require evaluation with a parameter sweep. This paper demonstrates the drill-down or narrow version of the sweep by evaluating both of the parameters throughout the interval [-1, 1]. Increments used to cover this space are steps of 0.05.

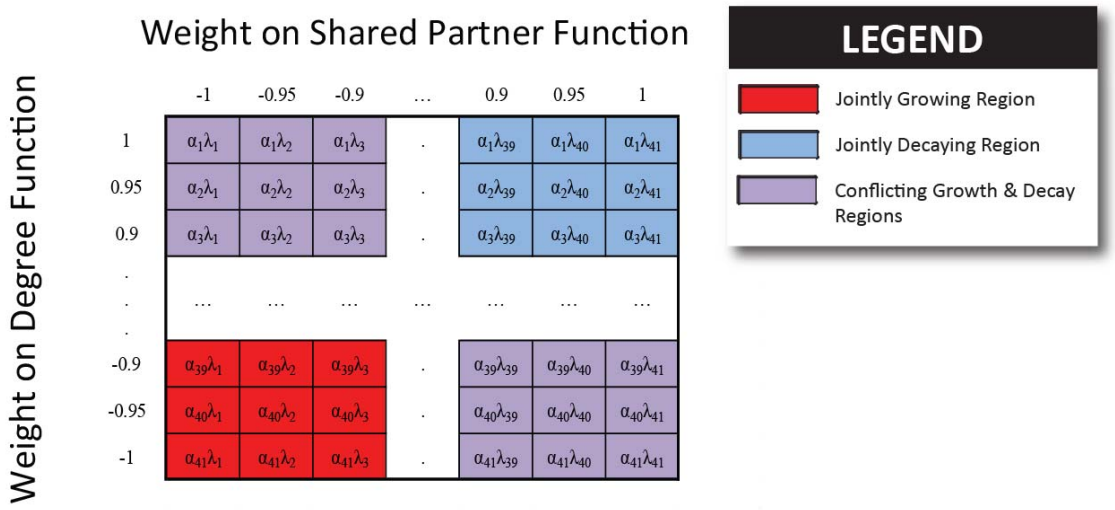

Figure 5 (Joint Parameter Sweep): A graphic displaying the joint-parameter space analyzed along with a categorization of the alternate regions.

Figure 5 summarizes the joint parameter space and the sequence of parameter values used for the exponents for estimation. Alternately colored regions indicate what combined effects the parameters have on their respective distributions. Counting counter-clockwise, Quadrant I indicates joint decay for the parameters, since they are both positive. Quadrant II indicates growth in λ but decay in α. Quadrant III indicates growth, since both are negative. Quadrant IV indicates decay in λ but growth in α. Steps with length 0.05 across the parameter space make for a total of 41 increments along the two axes. Combined, this produces a total of 1,681 ERGM estimations. Estimation set the MCMC simulation parameters as the following:

Sample Size	10,000
Burn-In	4,000
Interval	100
Maximum Iterations	5

Table 6 (MCMCMLE Specifications): Table outlining the simulation parameters used during the 1,681 estimations.

Table 6 shows that the sample sizes generated contained a total of 10,000 replicates, that *burn-in* culled 4,000 replicates before initiating sampling, that 100 changes occurred between sample evaluations began, and that the estimator had 5 attempts to identify the maximum likelihood estimates for each step in the sequence. Snijders (2002) suggested users take at least 1,000,000 steps away from y_{kn} when selecting replicates from the Y_n sample space. The product of sample size, *burn-in*, and interval is 4,000,000,000 or 4 x 10^9, well beyond the prescribed threshold.

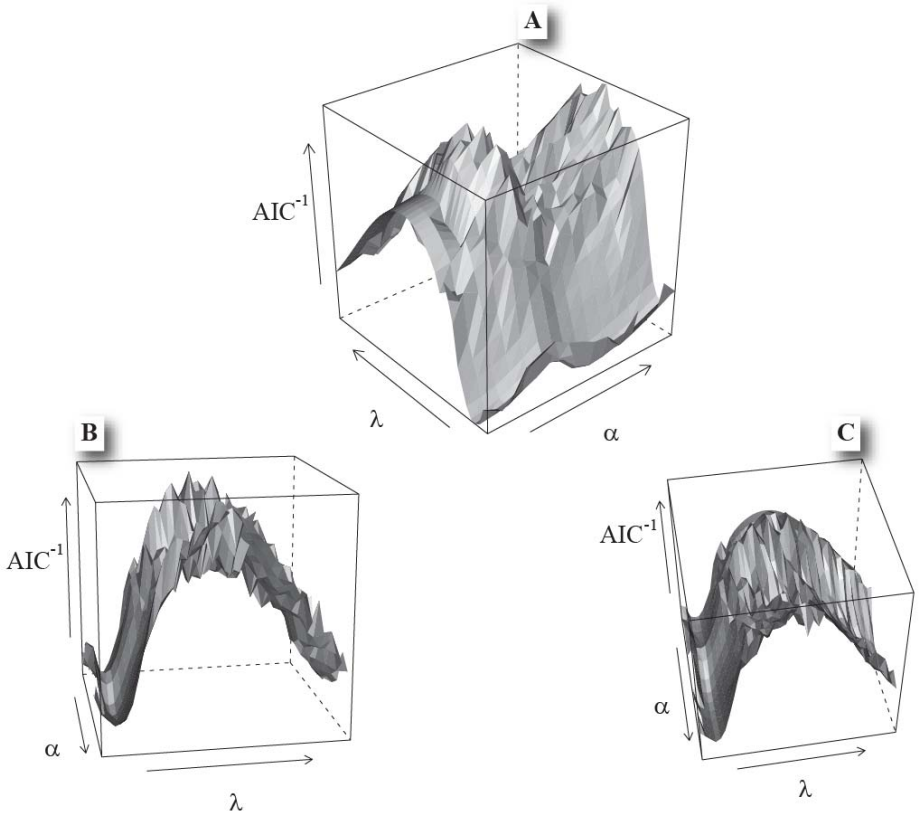

Figure 6 (JI 2000 Likelihood Surface): A visualization of the likelihood surface for the Jemaah Islamiyah terrorist organization in the year 2000.

Figure 6 displays alternate renderings of the likelihood surface produced from approximately 1,000 of it 1,681 estimations. It visually represents the exponents α and λ as "fixed," rather that estimated quantities. AIC^{-1} along the Z-axis proxies representation of the log-likelihood in Equation 7, which is suitable given

the fixed number of parameters (see 45 for further elaboration). Two features in Figure 6 are prominent. First, there appears to be a convergence in estimates for λ, indicated by a single mode. Alternately, estimates in α appear bimodal.

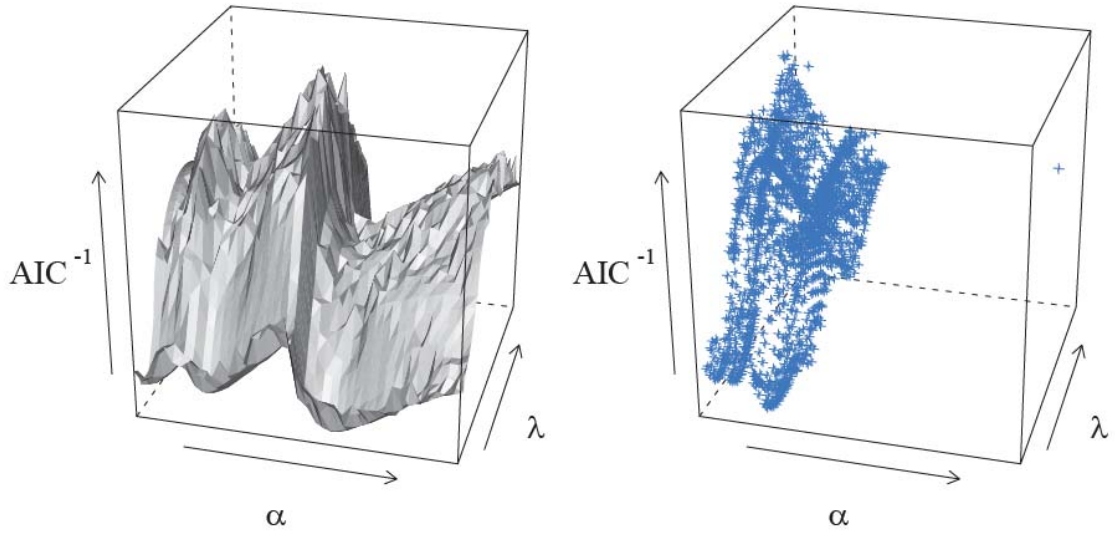

Figure 7 (Comparison between "Fixed" and Varying Renderings of the Exponents): Contrasting renderings of the estimates in the parameter space between artificially "fixed" and varying depictions. Compression in α and the indication of a good candidate for a converging mode support the argument for estimating, rather than fixing parameters for terms with exponents.

Figure 7 contrasts the artificially "fixed" rendering of the complete surface containing all 1,681 estimates with a cloud plot of the final exponential estimates. Compression in α, the reduction from a reasonably spread set of different modes, is significant and clear. Clearly, the initially specified values rarely turned out to be the MLEs, a point that the phase portrait summarizes.

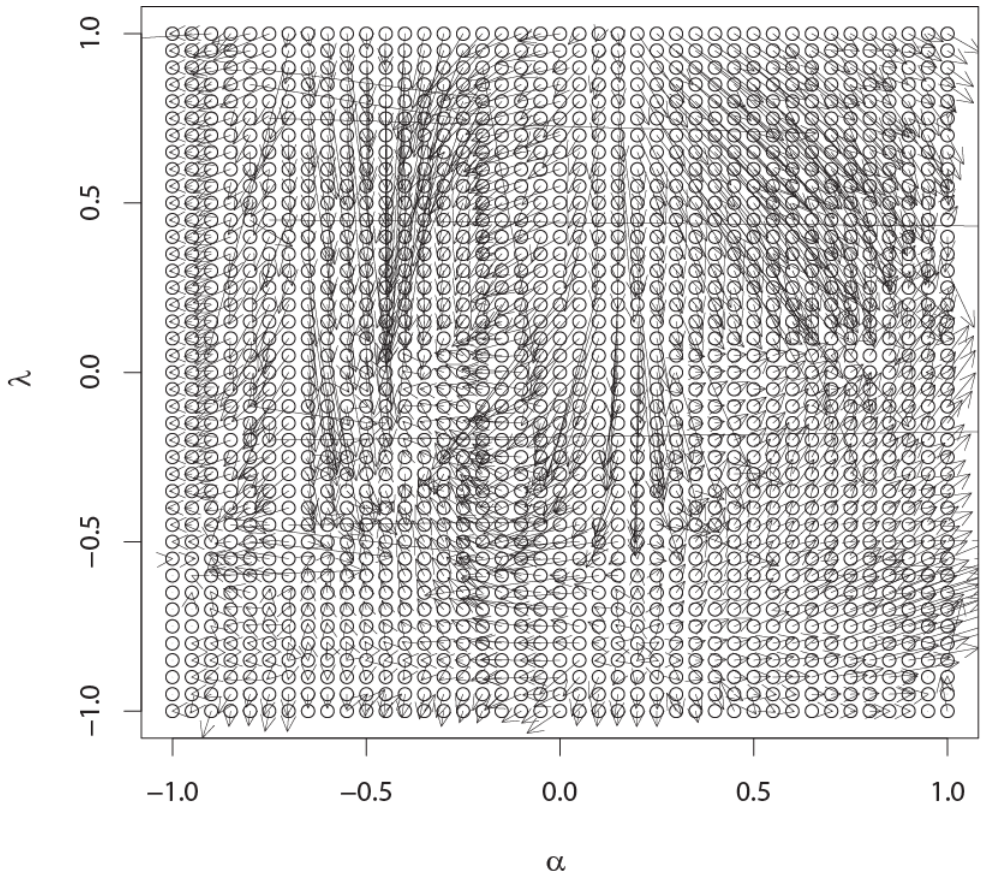

Figure 8 (Parameter Sweep Phase Portrait): A phase portrait graphic of the changes in value that frequently occurred for the exponents, clearly distinguishing the "initial conditions" from the MLEs.

Figure 8 presents the phase portrait of changed values for the exponents, highlighting the frequent difference between their "initial conditions" and their MLEs. Regions in the plot that look like nearly empty dots represent points in the parameter space where the MLE differed insignificantly from the initially specified values. Darker regions show the contrary, indicating with vectors of alternate lengths regions not only differed from the original specifications but also tended to converge in the calculation of a new estimate. Sometimes the distance traveled proved considerable (i.e., characterized by very lengthy arrows). In light of the earlier discussion about using "fixed" exponent values, such an approach would not have led to the same convergence by construction. The estimator would not have had the opportunity. This points up the importance of at least considering regular inclusion of parameter sweeps in analyses that include curved exponential family

terms. Otherwise, users seem to be relying on sheer luck of the draw (or specification) when attempting to identify the MLE for such network formulas.

Network Statistics	Highest Ranked	Lowest Ranked
Density	0.033**	-1.898****
S.E.	(0.014)	(0.082)
GW Degree	30.654****	0.767****
S.E.	(0.442)	(0.255)
α	-0.064****	-0.601****
S.E.	(0.014)	(0.097)
GW Shared Partner	-0.455****	-0.075****
S.E.	(0.013)	(0.013)
λ	-0.205****	-0.851****
S.E.	(0.033)	(0.155)
AIC	542.51	804.82
BIC	568.06	830.37
MCMC Sample Size	10,000	10,000
Burn-In	4,000	4,000
Interval	100	100
Maximum Iterations	5	5

Table 7 (Highest and Lowest Filtered Estimates): Estimated sufficient statistics and parameter values for the highest and lowest ranked, filtered estimates from the joint-parameter sweep.

Estimation using the joint-parameter sweep produced 1,681 records of results. Out of these, only eight sections or less than 0.4% of the parameter space faltered because of degeneracy. The fact that about 12.8% of the estimates failed to demonstrate MCMC convergence emphasizes that degeneracy and convergence are separate estimation problems with their own unique solutions.[46] Including curved exponential family terms in the formula largely resolved any concerns there might have been with degeneracy, but the problem of multi-modality within certain sections of the parameter space remain largely unresolved. Applying the filter that removed degenerate regions, MCMC "dead zones," and set a minimum *p*-value of 0.05 preserved approximately 14.2% of the sample (i.e., 238 entries).Minus the

[46] Specifically, about 13% or 218 sections in the parameter space had one or more of the estimated values fail to converge, while about 12.6% or 212 sections had all of the values fail to converge.

invalid entries, this amounts to a 83.7% reduction in the evaluated parameter space by selecting the best of the best estimates for a formula used to describe the structure in y_{kn}. Table 7 displays estimates for the highest and lowest filtered and AIC-ranked entries.[47] Inspection of the results shows that a difference in sign emerged for only one of the network statistics, Density. For the remainder of the statistics, including the parameter estimates for the exponents, there is a very big difference in magnitude, despite the consistency in sign. To appreciate how different the filtered estimates are requires comparing their "goodness of fit" statistics.

[47] Table 7 also reports the BIC values for the ranked entries. The fact that factors like sample size and the number of terms remained constant throughout the estimation makes the AIC and BIC values differ by a constant value of 262.31.

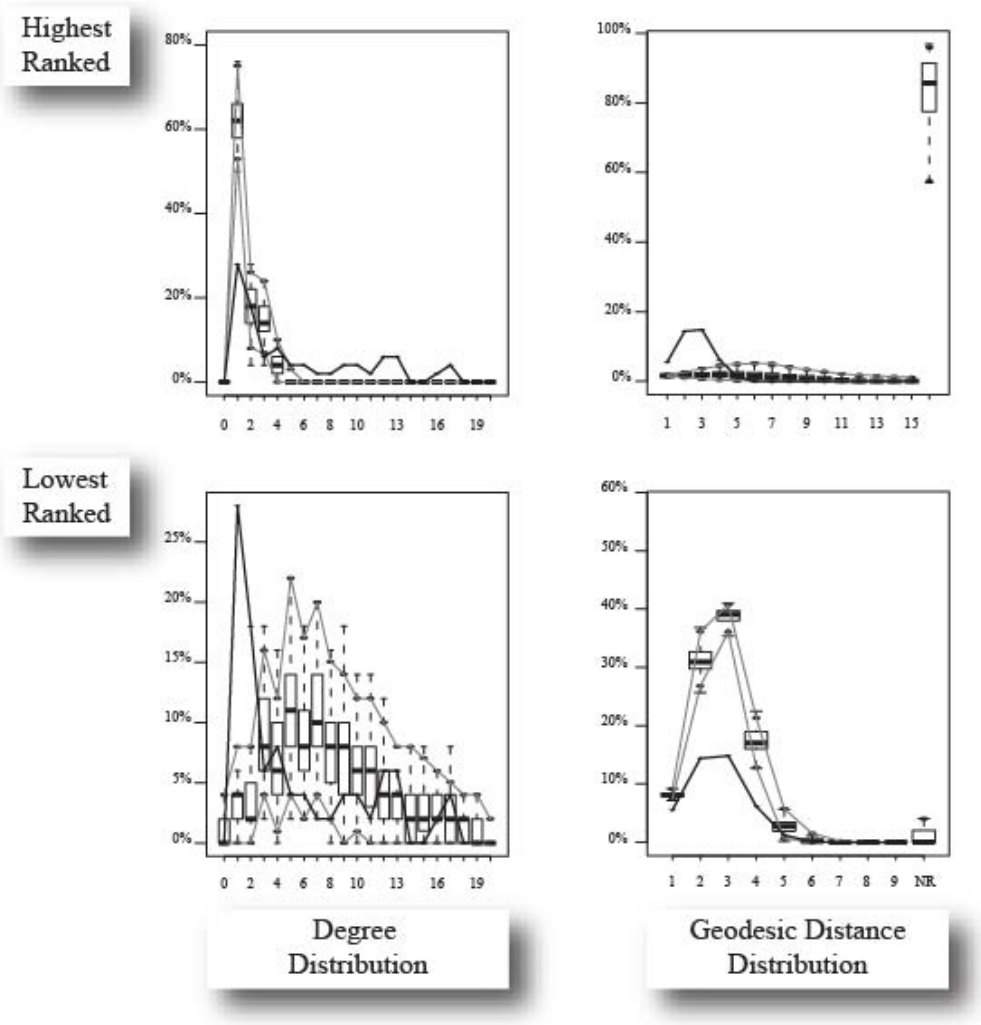

Figure 9 ("Goodness of Fit" between Best and Worst Performing Network Formulas): Comparison of two structural characteristics, degree distribution and geodesic distribution, in terms of the "goodness of fit" producing by the *best* and *worst* performing filtered estimates for the network formula.

Calculating "goodness of fit" statistics was computationally infeasible for all 1,463 of the viable regressions, but easily achieved for comparing the two, alternately ranked entries. Figure 9 displays results of the comparison with visual plots for two of the three structural properties commonly evaluated in the literature.[48] The two distributions evaluated are the degree distribution and the

[48] Near identically perfect matches for both entries on the calculation of the edgewise shared partner distribution made including that figure meaningless for comparison. They both did equally well at accounting for clustering. This is interesting, though, given their considerably different values for the GW Shared Partner θ and λ.

geodesic distance distribution. A degree distribution is a relative frequency of the number of connections members have and the total number of members with that amount. A geodesic distribution is somewhat more global for the network in general, describing relative frequency for the numbers of path lengths apart members are from one another. In the figures, the bold line depicts values for the quantity in question, and the light grey line depicts the standard deviation confidence interval for the simulated population. The Box-and-Whisker plots are another way to represent the distribution with dark dashes in the middle of boxes indicating the medians for respective categories. The vertical axis reports the relative frequency of plots in the graph.

A review of the plots shows that the higher ranked model made better predictions for a majority of the sample in the category of degree distribution, while both models fared poorly in the prediction of geodesic distributions. The higher ranked model over predicts the number of members with only one connection but does a good job predicting the number of members with between two and four connections. The lower ranked model, on the other hand, does a good job of predicting members with three or more connections. Despite doing a better job throughout most of the range of possible values, the lower ranked model did worse in the area of accurately predicting values for a majority of the sample. Most of the members have one or two connections, categories where the lower ranked model fared the poorest. Using the absolute number of accurate predictions as a metric, neither model did well in the category of geodesic distribution. This result could be because of exploring too small a portion of the parameter space by using only the narrow search or from not including the appropriate network statistic in the model specification. Performing well for a majority of the sample is commendable but there is also something to predicting lower probability occurrences, which the lower ranked model did in for the degree distribution.

Not much of this paper has dealt explicitly with the structural modeling of networks and the use of these techniques to study and counter terrorist networks, but a review of the model results points to the need for bridging the two. Analysts and authorities must contend with the fact that terrorist networks not only have

latent social processes that generate them,[49] but that they are also clandestine or "dark." Sometimes the terrorists with the least likely attributes prove to be the most dangerous, making it important for authorities to have tools that balance between getting most of the data right most of the time and making accurate predictions for the rarely occurring events that are infrequent but important. Whereas this paper originally set out to propose a way to identify the best fitting results, it has concluded that, at least in the context of terrorist networks, a slightly different goal is necessary. Rather than further developing methods for models that are right most of the time but make no account for rare events, future developments should look to combine the two. Bayesian model averaging offers one path to developing and implementing these methods in network science. Another possibility is to run "goodness of fit" statistics for the filtered results then to rank them according to their ability to combine accurate mapping for a majority of the network at the same time that they account for rarely occurring events as well.

VIII. Conclusion

Opening discussion in this paper described how most theories about the generation of networks do not have emergence characteristics easily identified by known mathematical distributions. This leaves many of them untested or poorly tested. The paper then sought out to describe methods for identifying a flexible statistical test researchers can use to test proposed any proposed theory. It then forwarded prescriptions for use of the exponential random graph estimator, emphasizing using it to maximize fit, as its original authors intended. After applying the procedures to analysis of an empirically observed terrorism network, the paper concluded that the methods identify the most likely components of a structure but not its rarely occurring ones. This is less of a problem for testing theories than it is for using simulation of estimated network properties to a population of networks known to exist but difficult to detect. Immediate examples like terrorist networks,

[49] No matter what the narrative of a person identified as a terrorist after an attack or failed plot is, authorities rarely capture someone before they set down the path to become a terrorist.

crime syndicates, and other clandestine groups come to mind when thinking about how this problem of partial characterization limits the application.

Some concluding remarks are in order, regarding the testing of theory with the methods proposed in this paper. Maximizing fit of a model to the data is the first and sometimes the only step to comparing observed data to proposed theory. Enders and Su assert that networks generated under the same condition will display similar properties. Assessing this theory amounts to observing a number of terrorist networks produced from the same or comparable security environment as well as source population (i.e., those who can become members) then determining how close their MLEs are. Other theories require multiple steps. Any theory specifying micro-foundations it asserts leads to unique outcomes for the data requires empirically-driven simulation then comparison against the observed network. The closer a simulated network is in the parameter space to the MLE of an observed network, the more likely it is to explain its occurrence. Thus far, this is conjecture. The Postscript will describe an example of a future analysis used to determine where this logic holds and falters.

CHAPTER III

The Fallacy of "Decapitation": A Case Study of Mantiqi I and a Failed Counterterrorism Strategy

I. Introduction

News cycles today seemingly produce a consistent stream of reports on how the latest counterterrorism efforts have resulted in the death or arrest of a terrorist "leaders," yet the attacks continue and new "leaders" emerge. Research has shown religiously motivated terrorist groups are less susceptible to *decapitation* strategies (Jordan, 2004), but the literature has to this point offered little explanation for how this occurs. To argue religiously motivated or other population-based groups benefit from community support does not shed light on how they harness these resources and what happens to make them stop.

Network science is a framework premised on the importance of connections, so an explaining intact groups sustain action is not a unique proposition. Scale-free networks are patterns of social organization where few members act as "hubs" for large numbers of otherwise unconnected members in the network (Bianconi & Barabási, 2001). Scale-free network theory argues that networks formed by preferential attachment processes have "hub and spoke" patterns of structure, which make them resilient to attacks that do not target their leaders (Barabási & Bonabeau, 2003). The reason for this is "hubs" serve as the significant bond in the group, holding it together and sustaining flows of resources and information between even disparate members.

Mantiqi I, a splinter group of the terrorist organization, Jemaah Islamiyah, led in the radicalization of Southeast Asia through waves of attacks lasting from 2000 to 2005. Bali I in 2002, which killed 88 vacationing Australians, sent shudders throughout the post-9/11 world and quickly led a dragnet by the authorities causing the group leader, Hambali, to flee. Despite his eventual arrest, the group developed a new leader in Noordin Top and continued its rash of bombings. When the killings finally stopped in 2005, the group was responsible for hundreds of deaths and many more wounded.

Filling the void in the literature, this paper provides statistical evaluations of network structure and narrative accounts of how a terrorist group contended with successive counterterrorism efforts that decimated its ranks but largely failed to prevent its attacks.

A unique proposition scale-free theory does not make is Power Law distributions of connections, "hub and spoke" patterns of connections among members, are signature characteristics of groups formed preferentially. The theory section develops these thoughts further and proposes a test for examining whether changes to scale-free state explains how Mantiqi I continued attacking.

The narrative tells a rich, but slightly different story, which focuses less on leaders alone and more on the harnessing of resources from members and the surrounding public. It provides no verbal evidence of the *coup de grâce* in 2005 being the final elimination of the last network "hub." Instead, it shows attacks stopped after counterterrorism efforts killed someone other than the leader Noordin Top. Further emphasizing how the empirics contradict the theory, recent events show attacks have begun anew in Indonesia, despite the recent assassination of Noording Top by authorities.

A comparison of empirical findings and descriptive narrative do not support the application of scale-free theory. At no time during the period did Mantiqi display a Power Law distribution, making it impossible to conclude a transition from being scale-free to not being scale-free explains why it stopped attacking. Closer inspection of the narrative points to an alternative answer, observing the group

stopped attacking when it no longer had the ability to do so. This was not because it lost its leader but because it lost its remaining bomb maker, Azhari Husin.

Organization of the paper is as follows. The next section introduces the data used in the analysis with a brief background on Mantiqi I then a description of methods for data collection. Next is a description of scale-free network theory according to its descriptions of behavior and expectations of network structure. The research design section describes the semi-parametric test used to test scale-free network theory, followed by a presentation of the findings. A narrative describing the terror-counterterror interaction between Mantiqi I and authorities fills the gap left by the negative finding for scale-free theory. The paper then concludes with final remarks.

II. Data on Mantiqi I

This paper evaluates whether during the period 2000-2006 the radically violent, Jemaah Islamiyah (JI) splinter group, Mantiqi I, exhibited a Power Law distribution of connections among members. Demonstration of the characteristics during a period would provide support for the argument that the group was scale-free and provide some grounds for using a "decapitation" counterterrorism strategy against it. This section summarizes the history of Mantiqi I then describes the data collection and coding procedures that produced the network data as part of Department of Defense-sponsored data collection project that the author took part in from 2006 to 2009.

Abdullah Sungkar and Abu Bakar Ba'asyir formed JI in 1993 after they split with the leadership of Darul Islam, a jihadist movement in Indonesia. Sungkar was the central figure and the source of vision, inspiration, and direction for JI until he died in 1999. His death left a leadership vacuum within JI that no one ever truly be filled. Many expected Ba'aysir, a long time confidant of Sungkar, to lead successfully following Sungkar's passing his death, but he proved a disappointment.

Allegedly taking over as amir (or the spiritual leader of the group), Ba'aysir was an ineffective leader of operations, prompting group members to criticize him for being full of lofty rhetoric but no action. Discontent grew then initiated a change

in organizational structure drastically breaking from Sungkar era. Centralized and hierarchical since its inception, the organization fractured into mantiqis (or regional sub-organizations throughout Southeast Asia) under Ba'aysir. What resulted were two factions, composed of moderates and violent radicals.

Mantiqis II (Indonesia), III (Philippines), and IV (Australia) all had relatively moderate leaderhip. Mantiqi I (Malaysia and Singapore), on the other hand, contained the radical minority wing. Mantiqi I leaders included Hambali, the regional head, and Zulkarnaen, the head of military affairs for JI's Central Command council. Ba'asyir put the confirmed his ineptitude as a leader by deferring to Hambali who then radicalized the organization by pursuing a violent jihad supported by funds and resources received from al-Qa'ida.

Ultimately, the Hambali-led militant minority engineered all JI terrorist attacks from 2000-2003, including the devastating Bali I bombings in 2002. As the attacks mounted, Southeast Asian authorities continuously tightened the security environment. On the run, Hambali fled to Thailand in 2003 but did not escape arrest. Noordin Top, former headmaster of Lukmanul Hakiem, one of the two most radical JI madrassahs, took advantage of the power vacuum and ascended to the informal role of attack leader. He led attacks on the Marriott Hotel in Jakarta (2003), the Australian Embassy in Jakarta (2004), and three restaurants and clubs in Bali (2005) before attacks stopped when authorities gunned down his accomplice, Azhari, at a makeshift bomb making facility.

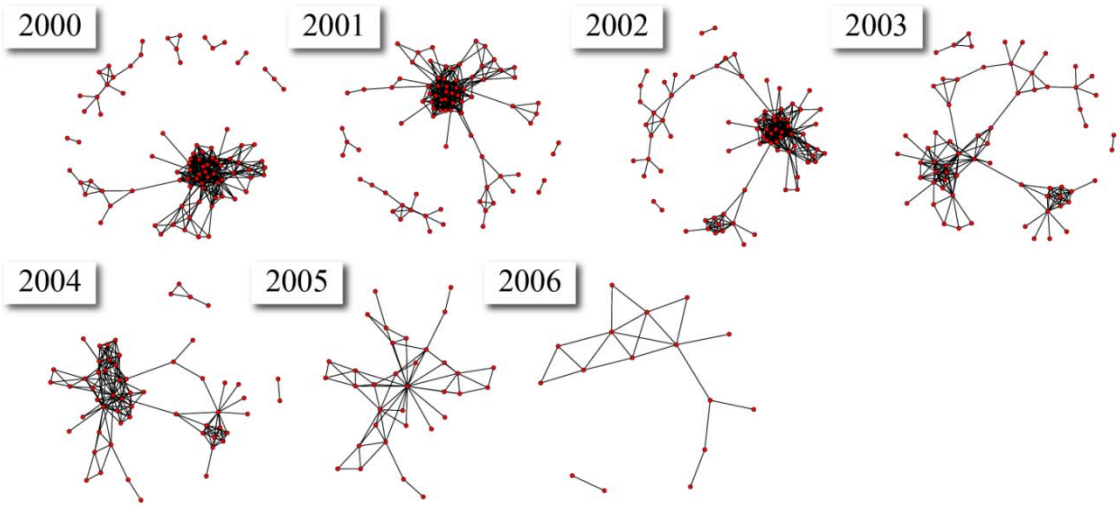

Figure 10 (Mantiqi I, 2000-2006): A graphical depiction of the Mantiqi I faction of Jemaah Islamiyah time series from when it first began attacking in 2000 to when the attacks stopped following culmination of counterterrorism efforts in 2006.

Figure 10Figure 2 is a network visualization of Mantiqi I, assembled according to the connections among members associated with attacks from 2000-2006. Data on this group comes from the John Jay & ARTIS Transnational Terrorism (JJATT) project and contain information on the various social linkages between members of the terrorist organization.50 The binary, undirected graphs in the figure show the effect counterterrorism operations had on its membership, increasingly thinning it throughout the period.

Data collection for JJATT included field-based interviews of individuals associated with JI or members of JI, secondary materials (e.g., police interrogation reports, court discovery material, and court transcriptions), and tertiary or "open source" materials (e.g., newspaper articles, governmental white papers, and non-governmental organization reports). Coded connections capture the association between individuals along the social dimensions of friendship, family, and mutual participation in terrorist operations.

---

[50] Between 2006 and 2009, the Air Force Office of Scientific Research funded the collection and recording of data on individuals associated with jihadist terrorism in a variety of locales across the world. Of particular interest to the JJATT project was further expanding the database on terrorist networks built by Marc Sageman (2004). To that end, the project produced largest source of publicly available data on terrorist attack networks. Such groups are those whose members were directly involved with committing a terrorist attack or had a direct association with someone that did. These data are available at: http://doitapps.jjay.cuny.edu/jjatt/index.php.

Coders for the project defined relationships as being in place when individuals would meet or otherwise contact one another (e.g., via telephone or courier).[51] The resulting coding methodology focused on relationships between two or more individuals and changes in them over time. The source materials used to compile this data included reports from field-based investigations (e.g., interviews with the associates of terrorists, members from the surrounding community, and on rare occasions the terrorists themselves), court transcripts, case discovery materials, and "open sources" (e.g., governmental and non-governmental reports as well as journalistic accounts). The exact coding of relationships defined a relationship as being in place once the researcher established that intentional contact between two or members occurred. Once in place, researchers did not consider a relationship dissolved unless there was a clear account of a dispute between individuals (and therefore a severance in relations) or a significant change in personal circumstances (such as imprisonment, arrest, or exile).

III. Scale-Free Networks

Scale-free networks arise because members connect with one another preferentially; choosing more often to connect with highly connected members than other. The literature does not validate, at the individual level through surveys or other data, why this should happen but conjectures it occurs because of a desire to move information and resources efficiently by connecting to a larger group, despite some constraint on the ability to form relations. This is plausible but underspecified in the proposed micro-foundations, since the only systematic component regularly depicted is a Power Law generative function, which also serves as the means for testing it. The expectation that scale-free networks follow a Power Law distribution is less interesting as a theoretical proposition than it is as an empirical observation. A wide variety of social and biological networks are scale-free, an outcome with little chance of happening randomly (Barabási & Bonabeau, 2003). As stated earlier,

[51] This type of data differs considerably from recording detailed accounts of the interactions themselves, the ideal foundation to network data.

the Power Law distribution is a reliable test for determining whether a network is scale free, given the expectation of "hub and spoke" distributed connections.

Before moving to a discussion of the methods used to evaluate whether the Mantiqi I network was ever scale-free from 2000 to 2006, it is important to re-emphasize why identifying such networks is important from a counterterrorism perspective. These networks are of interest in counterterrorism because targeting the "hubs" effectively breaks the networks. For counterterrorism officials, arguments that terrorist networks may be scale-free offers some currency, since the proposed strategy for stopping them is clear and not complicated.

IV. Power Law Distribution Test and a Robustness Check

Discussion of scale-free network theory closed stating the expectation of a Power Law distribution characterizing degree distributions of mature networks. Newman (2005) originally sketched out a semi-parametric test eventually formalized in Clauset, Shalizi, and Newman (2009). Maximum likelihood estimation (MLE) and bootstrap simulation form the primary mechanics of the test. It uses MLE to estimate the most likely parameter value in a Power Law generating function to have produced the observed distribution. Bootstrap simulation produces replicates conditioned on the MLE estimates and compares them to the observed distribution using the non-parametric Kolmogorov-Smirnov Test. The remainder of this section augments the verbal description provided thus far then moves to a discussion of the robustness check performed on one of the cases in the series.

$$p(x) \propto x^{-\alpha}$$

Equation 13

Equation 13 describes the probability distribution of x as a function its value raised to the parameter $-\alpha$ ($\alpha > 0$). This is a standard representation of the Power Law distribution. Negative values in the exponent act downward weights that grow in proportion to the value transform. This means the larger x is the larger the downward weight. What results is a decreasing probability of large values occurring. Steepness of result depends upon the size of α, as displayed in Figure 11.

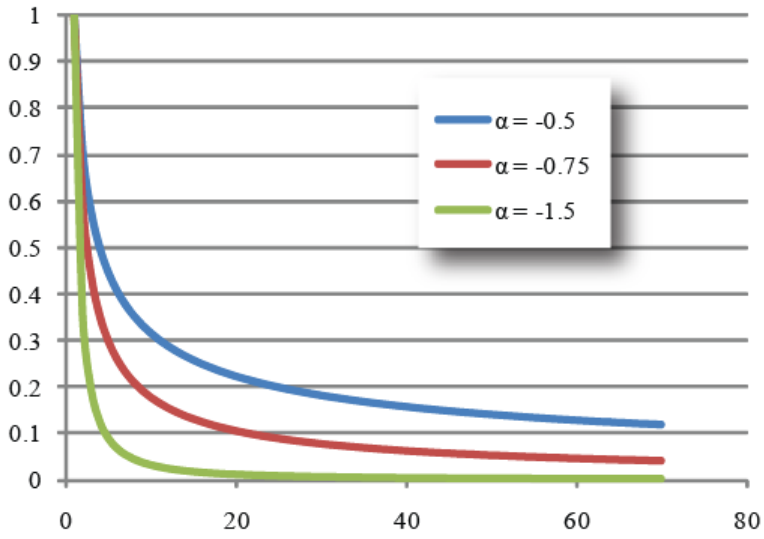

Figure 11 (Power Law Plot): Graphic displaying Power Law distribution plots for three values of α.

Empirical examples from the natural world demonstrating the dictum "big things happens in small numbers" abound, ranging from the magnitude of earthquakes to links between servers forming the World Wide Web. The question in this paper is whether the Mantiqi I terrorist network continues the trend.

Graphics like that pictured in Figure 11, when applied to empirical data, can prove illustrative, but not demonstrate. Visual analysis alone does validate a Power Law distribution. Furthermore, the authors note that few empirically observed display a Power Law throughout the entire range of their values (i.e., x1, x2,…, xN). Known in the literature as an "exponential cutoff" model, the observation implies that detecting a Power Law just became more difficult. Not only is the line plot like the one above insufficient, establishing what part of the distribution to include for analysis is not as clear-cut as one would hope. Clauset, Shalizi, and Newman remedy this issue by treating identification of the cutoff as a maximum likelihood estimation problem that sequentially identifies likelihood maximizing values of x (i.e., "x min") and α. The sequence involves iteratively identifying the likelihood maximizing value of $\hat{\alpha}$ with a constant x_{min} and choosing the value for x_{min} along with its associated $\hat{\alpha}$ that provides the best fit in comparison to a Power Law distribution.

$$\frac{\xi'(\hat{\alpha}, x_{min})}{\xi(\hat{\alpha}, x_{min})} = -\frac{1}{n}\sum_{i=1}^{n} \ln x_i$$

Equation 14

Equation 14 is a representation of the MLE used to estimate $\hat{\alpha}$. This equation is for discrete values of x.[52] It specifies $\hat{\alpha}$ as the solution to the ratio of a zeta function differentiated according to $\hat{\alpha}$ and the zeta function as function of $\hat{\alpha}$, where in both cases the proposed value of $x_{\min}$ is constant. In Equation 15, $\hat{\alpha}$ has no exact, closed-form expression, prompting the authors to identify an alternate function for estimation.

$$\hat{\alpha} \simeq 1 + n\left[\sum_{i=1}^{n} \ln \frac{x_i}{x_{min} - \frac{1}{2}}\right]^{-1}$$

Equation 15

Equation 15 is the function evaluated as an approximation of Equation 14, which treats $\hat{\alpha}$ as if it were continuous. Correcting for indiscrete solutions produced from Equation 15, the authors round results up to the nearest integer and state that unreported analyses demonstrate the approach works well. Having identified the MLE for $\hat{\alpha}$ conditioned on a fixed $x_{\min}$, the next step is to evaluate how a the distribution of observed data compare to a Power Law when transformed by the $\hat{\alpha}$ and $x_{\min}$ values.

$$D = \max_{x \geq x_{min}} |S(x) - P(x)|$$

Equation 16

Equation 16 shows that a distance statistic (D) is the maximum result in absolute distance between a cumulative probability function defined by the estimates (S (x)) and the cumulative probability distribution defined by a Power Law (P(x)). This is the Kolmogorov-Smirnov or KS, non-parametric statistic, considered useful for assessing comparisons in non-normal data (Press, Teukolosky, Vetterling, & Flannery, 1992).

A review of the procedures by the authors evaluated how well the estimator performed when detecting parameter estimates for the Power Law distribution in

[52] Only the discrete MLE receives attention here because *x* cannot take on indiscrete values when depicting network connections. Individuals cannot share a partial social relation in this dataset nor can they share a relation with a partial person.

controlled experiments. The setup specified $\hat{\alpha}$ and $x_{\min}$ values then ran the procedures to retrieve them. They identified the threshold for acceptable performance at $x_{\min} > 6$. Below this point, the estimates became unreliable. Another conclusion drawn from the evaluations was the sample size (the number of x values) needed to exceed 50. Sample size restrictions limit analysis of the Mantiqi I time series to the years 2000 to 2004, each of which had $x_{\min}$ estimates larger than the minimum threshold. Estimation of the most likely Power Law parameter values for an evaluated distribution is phase one of a two-phased test. Next is the comparison of these estimates to those produced from replicates simulated as a counterfactual depicting what the observed data would like when generated by a Power Law process.

Simulation of the replicates uses estimates from the observed data to structure the counterfactual assessment. Prescription of these procedures rests on the observation that simulating values only from a Power Law would result in an uneven comparison, since the procedures model the observed data as resulting from an exponential cutoff. Generation of the replicates effectively performs bootstrap sampling of two distributions, populating values for the first sample with draws from values in the observed distribution below the $x_{\min}$. The strategy ensures that replicates resemble observed data, concentrating attention on differences in the fit with a Power Law. Replicate generation draws from a Power Law with exponent set to $\hat{\alpha}$. For each of the sub-distributions, replicates have the same number of entries as observed data. Comparison of the replicates first applies the procedures for Equation 15 and Equation 16 then evaluates whether the resulting KS statistic is larger than that of the observed data. For the authors, a replicate KS statistic larger than the evaluated distribution indicates an instance of the observed value falling within the counterfactual Power Law distribution. The question is if, with respect to the observed distribution, the ratio between replicates with larger KS values to those with values smaller than or equal to a are statistically significant. If so, evidence suggests support for the hypothesis the observed values came from a Power Law distribution. Failure contests this conclusion. A statistical *p*-value describes significant support by the number of replicates with larger values to the

total number in the sample. The quotient determines how statistically significant the findings are with a threshold for significance specified by the user.

Analysis in this paper uses computer code the authors provide for calculating the MLEs original code written by the author in line with the procedures specified above (see **Error! Reference source not found.**).53 Parameter estimations and the imulations used the random number generator seed 1,000. Additionally, simulations specified replicate sample sizes at 1,000.

V. Results of the Scale-Free Analysis

Empirical analysis of the Mantiqi I network sequentially led by Hambali then Top shows reveals no evidence that the group self-organized according to the expectations of scale-free theory. Application of the semi-parametric test outlined by Clauset, Shalizi, and Newman that identifies the MLE for parameter values in a Power Law distribution consistently rejected the hypothesis the group exhibited the signature trait of scale-free network emergence. Specifically, the observed data did not demonstrate a smaller difference between its cumulative distribution and that of a Power Law than replicate distributions drawn from a counterfactual representation of it did.

Year	α	x_{min}	D	p-value	Membership Size
2000	2.749	16	0.131	0.794	87
2001	2.730	16	0.152	0.881	83
2002	2.578	12	0.126	0.861	79
2003	3.414	14	0.157	0.458	66
2004	3.222	20	0.131	0.015	57
Random Seed:	1,000				
Sample Size:	1,000				

Table 8 (Power Law Test Results): Results showing that from 2000 to 2004, the period when Mantiqi I had data suitable for the semi-parametric analysis, the group did not exhibit a Power Law distribution.

Table 8 shows the results of applying the test for a Power Law distribution with a lenient requirement for statistical significance set at $p < 0.1$ or the 90%

[53] R code provided by the authors is available at: http://tuvalu.santafe.edu/~aaronc/powerlaws/.

confidence level. This means a reported value must exceed 90% to support the hypothesis the network displayed a Power Law distribution for the investigated year. As the results show, none of the years satisfied this threshold and only two of the years (2001 and 2002) came close. Recall that the *p*-value evaluates how many replicates from the simulation had distance values greater than the observed network. The assessment asks whether the network falls cleanly within the confidence interval established through bootstrap simulation. Most of the time, it is not close.

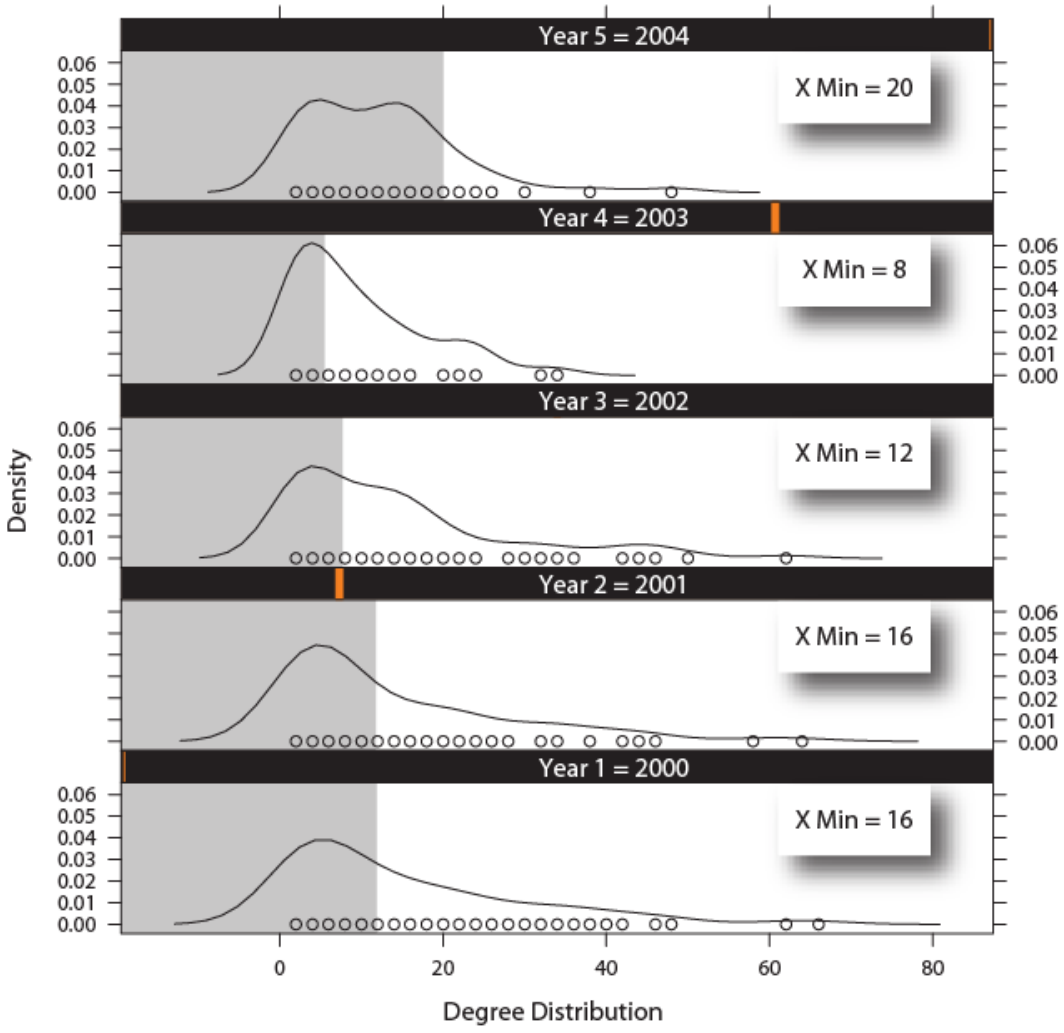

Figure 12 (Mantiqi I Kernel Density Plot): Kernel plots depicting a Gaussian transformation of the distribution data that works to smooth its appearance. Dots at the bottom of the graphic indicate where the data are in the distribution, while the "*x* min" panels indicate the MLE estimates for each plot. Grey zones indicate the region of the data treated as below "*x* min."

Figure 12 displays kernel density plots of the degree distributions throughout the analyzed period. Although these are not "test" of the Power Law distribution, they do provide some insight into the results. The grey region indicates values below the "x min" threshold excluded by the MLE. White regions of the curves indicate active regions used for evaluation. Estimations results designated 2001, 2002, and 2003 as the most likely Mantiqi I had a Power Law distribution. Although not statistically significant, long tails in these distributions illustrate the group sometimes came near demonstrating the expected scale-free characteristic. Regardless, however, this trend clearly disappeared by 2004, yet the group continued attacking for two more years. Even under severely relaxed evaluation, the observed change from scale-free to not scale-free would not explain the cessation in attacks.

VI. Case Study Narrative

The narrative about Mantiqi I and the greater Jemaah Islamiyah organization from 2000 to 2005 is a detailed record of what events transpired during each period. Unlike the description provided earlier, it is more abstract, not recounting names other than those already listed in the preliminary description, choosing instead to summarize what changes occurred overall. The first category of "attacking" details how many attacks the group performed and what they were. Attacking presents terrorists with the ability to recruit but also raises the stakes of arrest. The amassing of monetary and physical resources is important for the purchasing of weapons, among other materials for the group. Improvement of human capital resources is occurs through the training of existing members or forming new connections with others. Last, the category of suffering attack, a negative feedback loop resulting from authorities hunting those responsible down for arrest and assassination.

2000 to 2002

Attacking

2000 to 2002 Attacks
2000 Medan Church Bombings
2000 Jalan Kenanga / Sitorus Bombing
2000 Philippines Ambassador Residence Bombing
2000 Jalan Sudirman bombing
2000 Indonesian Communion of Churches Bombing
2000 Rizal Day Bombing
2000 Christmas Eve Bombings
2001 HKBP / Santa Ana Bombing
2001 Atrium Mall Bombing
2001 Singapore Plots
2002 Bali I Bombing

Amassing monetary and other physical resources

As leader, Hambali used his connections to central members of the al-Qa'ida membership, whom he first met during the 1990s, to obtain funding for all of the JI attacks he orchestrated (Conboy, 2006).

Improving human capital resources

Besides funding attacks, the al-Qa'ida connections enabled Hambali to send certain network members away for training and technical skills. Most important among these was as Azhari Husin, a formally trained mathematician that went onto become an expert bomb maker (International Crisis Group, 2003). In addition to sending members off for training, he worked with the rest of the JI leadership to establish training camps in the Southern Philippines (International Crisis Group, 2004).

Getting Attacked

After the 2000 Christmas Eve bombings, the 2001 Atrium Mall bombings, and the 2001 Singapore Plots, JI suffered a series of arrests. Increased pressure from the authorities forced Hambali and his leadership team (including Noordin Top and Azhari Husin) into hiding.

2003

Attacking

2003 Attack

Marriott Hotel Bombing

Amassing resources

Hambali, no longer in official power and control of the group because of fleeing, can still access channels for funds from al-Qa'ida, tapping them to help fund the Marriott Hotel Bombing.

Azhari and Top begin their ascent to strong leadership positions they use to acquire financial resources to help finance the bombings as well as gain access to previously hidden, from him at least, caches of explosives (International Crisis Group, 2006).

Improving Human Capital

The new mantle of leadership enabled Top to expand his recruitment base through new connections drawn from places like radical madrassah, al-Mukmin or by mobilizing existing but previously untapped connections like Lukmanual Hakiem (where he had served as headmaster) along with co-conspirators in previous attacks (International Crisis Group, 2006).

Getting Attacked

Top's search to expand his recruitment bases was as much out of a desire to increase relationship as it was a necessity. Authorities arrested 19 of 22 made three other important members flee to the point of effective exile. Out of the original network that began in 2000, only 15% remained. Although recruitment occurred, membership change was a net loss.

2004

Attacking

2004 Attack

Australian Embassy Bombing

Amassing resources

Top mobilized his personal network for funds, establishing his first state of independence from Hambali, regarding everything from the funding to logistical.

Improving Human Capital

Just as in 2003, Top reached out to his previously existing and newly acquired connections, appealing to some of the terrorist organizations in the regions (Kompak and Ring Banten) for assistance. This was necessary because of the way the authorities had largely dismantled the entire JI organization.

At this time, Azhari attempts to train new members in the art of bomb making. Two students ultimately proved promising.

Getting Attacked

Authorities arrested a Mantiqi I leader who had previously provided Top and Azhari with accommodations and explosives. Authorities also arrested members of the other terrorist groups who contributed members in previous attacks.

By this time, nearly 79% of the entire network, not just the original network, but the entire network, is either dead or arrested.

2005

Attacking

2005 Attack

Bali II Attacks

Amassing resources

Nothing occurred.

Improving Human Capital

Nothing occurred.

Getting Attacked

With no new recruitment to replenish the massive manhunt following attacks, remaining membership sustains devastating losses. Key among these losses are Azhari, the bomb maker along with one of his prized students. Authorities killed these two and a number of others in raids following the attacks.

One of the remaining members, however, was Top.

This would be last of terrorist attacks in the country until 2009.

VII. Conclusion

This paper sought to improve understanding of how a terrorist group suffering attacks to its leaders sustains the ability to not only survive but also persist in its ability to attack. Scale-free network theory proposed that action continued because authorities failed to remove the major "hubs" in networks presupposed to have arisen from preferential attachment. Being a generalized theory, this is the view imposed on nearly all empirically observed networks. A test to verify a structural key to evaluating the theory, however, rejected the scale-free network hypothesis. Additionally, for those cases in the time series that were somewhat close in value, their change in state occurred too far in advance of stops in attacks to have "predicted" them. An alternative evaluation approach presented a narrative on patterns of outcomes experienced throughout the time series.

Review of the events made clear that a key feature to sustaining capability by Mantiqi I and its remnant relied on a continued ability to mobilize past and new connections within the population for contributions to membership and material resources. Although the group consistently suffered net losses in the size of its membership, the ability to mobilize connections made this value smaller than it would have been. Lastly, although removed early on from leadership, actions Hambali took as a leader had ongoing effects on the ability of the group in terms of human capital and physical resources. While the authorities were unaware of the virulent presence growing in their midst, Hambali took advantage of the

opportunity (unlike Ba'aysir) and built a terrorist foundation that would last for years.

CONCLUSION

The dissertation set out to explore what determines the use of repression against terrorism and how to improve understanding of a tool, network science, in the hopes providing authorities with a suitable alternative. It found that in democracies post-terror repressions works the one would think, conservative-led states favor its use, while liberal and centrist legislatures help oppose it. It is wrong to presuppose the micro-foundations downward to the level of the voter just because of these findings. Instead of doing that, future research should explore the two different but associated outcomes. The first being whether conservative and liberal ideologies act the same way at the individual level, as they did at the state level. Next, would be an exploration of whether adherence to the ideologically defined strategy determined political survival. The rest of the Conclusion serves as a postscript and sketches descriptions of alternate ways forward for some of the network science topics addressed in the dissertation.

I. Using ERGM for Theoretical Evaluation

Chapter 2 and Appendi distinguished between identifying the best formula for describing a network and testing a theoretical argument about what processes generated it. Recall a structural formula is useful for reproducing networks with structural characteristics similar to the network under investigation. At heart, the formula is data-intensive and a-theoretical but with its uses. A network generation process is the opposite. It offers a theory about why members join a network and what determines connections formed between them. Supposition about what drives these two processes can be right or wrong and appropriate application of ERGM can serve as a tool for theory assessment.

Future model validation using ERGM will assume two things. First, it assumes a network-generating process operating under fixed conditions produces networks recognizable as having arisen from those conditions. Next, it posits these networks, though different in appearance, will resemble one another in the structural characteristics they exhibit. With these assumptions in hand, model evaluation with

ERGM exploits the fact that the estimator maximizes formula fit, using it to compare MLEs between two or more networks. What exact networks should serve as comparison depends upon the proposed theory.

Theories hypothesizing about what process gave rise to an observed network should follow a two-phase procedure, while those asserting only that certain networks should resemble one another should follow just one phase. The two-phase procedure combines empirically founded simulation followed by ERGM analysis. Using empirical data to motivate generation of replicates is important for evaluating the counterfactual, "Had this process taken place, this is how the network would have turned out." The only data requirement in this situation is that theorists have data on the connections.[54] Theorists should not restrict parameters and hence the richness of theory according to available data, but they should be aware of the need to sweep the parameter space of parameters not anchored by empirical data. Not doing so will bias inference in a way few can imagine and none can dismiss. Simulation should include the generation of numerous networks under the hypothesized conditions.

One way to conduct the secondary phase of analysis is to run ERGM on each of these networks, categorizing results according to changes in theorized conditions of interest. Evaluation would then consist of identifying which sample produces estimates closest to those of the original network. Another option is more direct, using the theorized model as the sample replicator for ERGM, rather than randomly perturbing the observed network. This should be more efficient and will give a more direct answer. Assessment will determine which generating condition produced fit with the highest MLE. Comparing multiple models means using different theoretical devices as the engine for replicate generation. It is straightforward, conceptually, but requires some changes to software and will inevitably prove time consuming to

[54] A technical note on data collection is that the format for the data should be as granular as possible, meaning it should code what network data indicate, such as interactions between individuals, for the duration that they occur. Subsequent data analysis can transform these interactions into binary relations if the researcher likes, but the data collector should afford them this opportunity.

execute.[55] Model evaluation under the alternate scenario requires only the estimation step.

Available software like SIENA works toward this two-pronged approach, reflecting the spirit but not the mechanics of the description above. Where the proposed approach differs from SIENA is its emphasis on allowing any theory to be expressed and compared relative to the network under investigation. SIENA, on the other hand, restricts the parameters for theoretical assessment at the same time that it claims openness to theoretical evaluation. Why does it fail here? Failure occurs because SIENA concentrates on using "canned" theoretical terms to predict whether a tie occurs and how long it exists between members of a network. Many theoretical models do not include such parameterizations, making it necessary to transform these theoretical models into expectations of values for the terms included in SIENA before truly evaluating the models relative to theory. Otherwise coefficients for the generative terms are without context and little better than the ERGM structural estimates. When transforming proposed theory into SIENA terms is easy, comparative evaluation should make use of SIENA. When such transformation is difficult, comparative evaluation should follow the less-constrained methods outlined here that make use of ERGM.

II. Chapter 3 Extension: An Analysis of Target-Driven Measurement Error

Target-driven measurement error in network analysis arises when observed data for a network incorrectly includes or omits individuals as well as connections between individuals because of intentional behavior by the individuals under surveillance. A simplification of the matter is to think of the issue as one-sided, meaning that terrorists meant for all of the observed data to remain hidden and that its observation is a failure on the part of terrorists to keep it concealed.[56] Assuming

[55] Current functionality of "ergm" and packages like it allow for the indirect testing method. The other described method, which replaces the MC replicator, will require introducing new code.

[56] Two-sided analysis would consider the possibility that some observed connections are misleading, meaning that they are irrelevant to the conduction of terrorist action, portrayed instead in the attempt to throw investigators off onto dead-end leads.

that observed data results from a failure to conceal it and that some members of a network have done a better job than others of remaining hidden and/or concealing their connections implies that individuals in the group have a distribution of capabilities. Latent network analysis first assumes a theoretical model about the process governing network structure. It then presumes some understanding of the composition of people associated with the dynamic network generation process. An important detail of the composition assumption is that it consists of knowledge about what attributes the individuals possess. Individual attribute information is useful (although unnecessary) for identifying determinants of what enables members to keep their connections along with themselves concealed. The section below describes how to think about methods that assume the number of network members is known but the true pattern of connections between members remains unknown.

III. Random versus Behavior-Driven Errors in Network Analysis

Some recent work in the application of network science to the study of clandestine networks has sought to weigh results against the possibility of measurement error. One concerns random or input error. Input error applied to a network means stochastically "flipping on" or "flipping off" connections between individuals in a group. Randomly select a dyad, evaluate its state (connection or no connection), then change that state. In the context of data collection, "random error" presumes that mistakes in coding relations arise randomly; hence the name *input error*. What other types of error might there be? Clandestine networks contain individuals that strive to throw authorities off in their surveillance of members and their activities. From a network connections perspective, active attempts at throwing authorities off the "scent" is likely to have a success rate conditioned on some characteristic of the individual making the attempt. Capability defined according to the successful incorporation of terrorist tradecraft is a latent characteristic. No one takes the equivalent of a tradecraft IQ test or some other type

of aptitude exam, making it necessary to recognize that the quantity of interest is latent and deserving of treatment becoming of latent variable analysis.

Appendices

Appendix A

A Primer for Exponential Random Graph Modeling (ERGM)

I. Introduction

Networks consist of members (or nodes) and connections between members (the lines in images of networks). Social network have nodes that are individuals and connections that represent a value for a social relationship between individuals.[57] Binary, undirected networks are the simplest representation of a social network. Binary assignment indicates that a relationship exists or it does not. "Undirected" is a graph theory characteristic stating that a connection from member A to B ($A \longrightarrow B$) implies a connection from B to A ($B \longrightarrow A$) or more simply $A \longleftrightarrow B$. Discussion in this paper focuses on binary, undirected networks.

Exponential random graph (ERG) or p^* modeling (hereafter referred to as ERGM) is a class of network estimator that statistically profiles an observed network. A statistical profile of a network is its description within an agreed-upon language used in network science. The "words" of this language are network summary statistics calculated by algorithms describing alternate characterizations of a structure. For example, one summary statistic, *triangle* uses an algorithm to identify how many triplets of nodes in a network share mutual relates. A completed or *transitive* triangle is one where all three of the members share mutual connections. For members *A, B, C,* this means $A \longleftrightarrow B$, $B \longleftrightarrow C$, and $A \longleftrightarrow C$.

A series of summary statistics, in a sense, form a sentence describing the evaluated network. An issue users of network science on contend with is that the number of possible networks is infinite, meaning that a poorly crafted sentence of

[57] It is possible to have a single network comprised of multiple social relations. These are multiplex networks. Sometimes researchers treat each relationship type individually and other times they separate them. The networks analyzed in this paper have a single, social dimension that describes whether two individuals have a direct social relationship with one another.

network statistics could describe any number of possible networks. If the goal is to describe the network in question as accurately and uniquely as possible, then the requirement is to identify a sentence structure accomplishing this goal; hence, ERGM. Although this is what the estimator attempts to do, arcane and otherwise inaccessible descriptions of its mechanics and purpose in the literature do not convey the point adequately. To see this, one need only note many who use ERGM think they have described what processes produced a network, which is like thinking an accurate description of what something looks like automatically conveys information about how it came to be, its genesis. Technical users of network science recognize the fallacy of such thinking, noting the difference between network generation and network description and developing separate literatures around the two topics. This appendix serves as an attempt to persuade those who conflate network genesis and network description to stop doing so. The hope is that an accessible outlining of what ERGM does will prove persuasive through the provision of accepted and understandable information.

II. A Description of Exponential Random Graph Modeling

Statistical profiling of a network produces a formula describing patterns of connections in it. Components of the formula contains are structural characteristics (i.e., network statistics) and individual attributes (characteristics of the individual members) associated with the network.[58] Together the structural and individual components comprise network functions. A complete statistical profile contains network functions with their associated logit coefficients, which state the odds of the component in question generating a connection relative to random chance.[59] Conceptually, one can use the formula to create alternate networks that resemble

[58] ERGM formulae can evaluate attributes individually or dyadically. Individual assessments consist of determining whether certain personal traits determine the degree or number of connections for that node. Dyadic assessments determine whether certain matching (homophily) or opposing (mixing) patterns for values of a trait make a connection between two nodes more or less likely.

[59] *Generation* is a term appropriate for the post-hoc analysis of the network in question and not the evolutionary process that created it. It is possible that the function in question was part of the latent data generating process for growing the network (i.e., the percolation function or algorithm), but it is inappropriate to assume that this is the case without further tests.

the original network. The process ERGM follows to derive estimates for the coefficients is that of Markov Chain Monte Carlo Maximum Likelihood Estimation (MCMCMLE).

The MCMCMLE process in ERGM performs a few primary steps to produce coefficient estimates. The first step is a conceptual one. Let Υ be an infinitely large set containing all possible networks for all possible membership sizes. One way to conceptualize Υ is as three-dimensional space partitioned by network density (D), membership size (n), and relative frequency. Density is the total number of realized connections between members relative to the total number possible. Formally, this quantity is:

$$D = \frac{\sum_{i=1}^{n} x_{i,j\neq i}}{n^2 - n}$$

Equation 17

Equation 17 shows that network density, D includes the interval [0, 1]. $D = 0$ indicates no connections and $D = 1$ indicates all possible connections in the network have been realized. Membership size, n is the total number of individuals within the network. Each alternate membership size represents a slice in Υ.

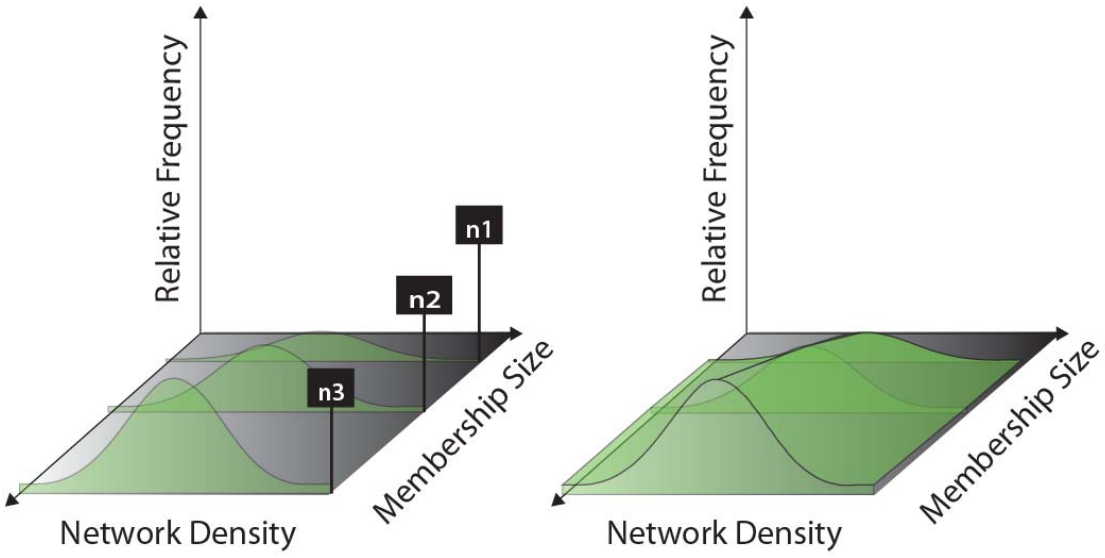

Figure 13 (Network Space): A visual representation of the theoretically infinite set, Υ that contains all possible network combinations. A three dimensional representation of Υ maintains that networks can vary by membership size and density. A third dimension captures the relative frequency of networks for each value of density. The boundary value for each slice is one, indicating that only one network apiece describes the empty and full sets.

Figure 13 is a visual representation of the three-dimensional partitioning of $\boldsymbol{\Upsilon}$. The graphic on the left displays three density plots or "slices" of $\boldsymbol{\Upsilon}$ with each indicating a different family of networks according to membership size. The graphic on the right places a sheet over the slices and uses it to convey that $\boldsymbol{\Upsilon}$ is approximately continuous for all integers in $\mathbb{R}^{+}$. A combinations function defines the height of each slice in $\boldsymbol{\Upsilon}$ according to the total possible number of ways to distribute a specified number of connections among members. A formal representation combination is:

$$\frac{n!}{r!\,(n-r)!}$$

Equation 18

Equation 18 defines the alternate number of ways to create connections between *r* members of a network with membership sized to *n*. It is non-monotonic with respect to *r*, rising from the single network that represents $D = 0\%$ connectivity, maximizing at $D = 50\%$ density, and then decreasing again to the concluding point at $D = 100\%$ for any network of size *n.* The figure to the right shows that the value of D at its maximum steadily increases as membership increases, so $\mathrm{V}(D_{n3}) > \mathrm{V}(D_{n2}) > \mathrm{V}(D_{n1})$. All of this is useful for understanding that $\boldsymbol{\Upsilon}$ is an infinite but readily defined space with discernible characteristics.

The next step in ERGM recognizes that an observed network is a "draw" from the appropriate slice in Figure 13, meaning that it is a random variable. This perspective is important for understanding the MCMC process that ERGM uses but unimportant in terms of generalization. Let y_{ind} be the observed network that is the i^{th} member of the *n*-family drawn from $\boldsymbol{\Upsilon}$ with *d* density.

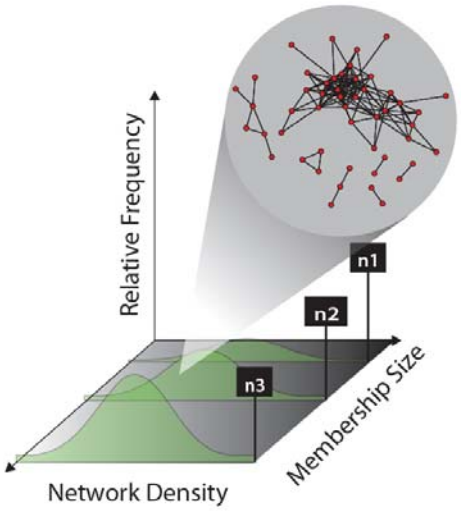

Figure 14 (Networks as Random Variables): An illustration of how an observed network is conceptually a "draw" from a slice of Y according to membership size, *n*, and density, *d*.

To derive coefficient estimates on the network functions that make up the statistical profile for y_{ind} requires calculating change statistics of it as well as other comparable networks from the same family. These networks are replicates, indicated individually by $\tilde{y}_{j\neq i,n}$ and as a set with $\tilde{\boldsymbol{y}}$. A change statistic is the aggregate calculation of differences in value of a network statistic under evaluation elicited by "toggling" connections observed in y_{ind} and $\tilde{\boldsymbol{y}}$. To toggle a binary connection between members a and b in any network (x_{ab}) means to change $x_{ab} = 0$ to $x_{ab} = 1$. The coefficient of change, θ, places the aggregation of these changes within a logit function. The vector of these coefficients is $\boldsymbol{\theta}$.

The MCMC process of ERGM uses y_{ind} to generate the replicate set, $\tilde{\boldsymbol{y}}$**,** and then calculates the convergent coefficient of change value for this entire sample population. Determination of this sample population value uses Maximum Likelihood Estimation (MLE). Final estimates for coefficient estimates and their variation is in the form of a sample estimate, making them externally valid, in theory, but also requiring extra work for evaluating the observed network within the context of the estimates. One procedure contained within the "ergm" package is goodness-of-fit statistics. Calculation and plotting of "first-moments" like degree distribution, shared partner statistics, and path-length statistics are useful for determining whether the observed network falls within the 95% confidence interval

established by estimates for the population. This is a type of model “fit” diagnostics in the broad sense but not a systematic one that provides definitive results other than the interval determination.

Appendix B

R-Script for the Producing Bootstrap Estimates of the Power Law Distribution Fit Semi-Parametric Test

I. Introduction

Clauset, Shalizi, and Newman present a semi-parametric test for estimating the parameter values of an evaluated distribution if a Power Law distribution produced it. The parameter estimates themselves convey nothing. To interpret them statistically requires comparing them to a sample population. One way to do this would be to determine if parameter estimates for the observed network are within the confidence interval of a simulated population. Such a test is not what the authors prescribe, and it is unclear why they do not consider, especially given their focus on specifying a statistical test. The alternate test the authors opt for outlines evaluating how many of the sample replicates have distance or KS statistics greater than the KS statistic of the evaluated network. They provide code for deriving the parameter estimates but not for assessing these relative to a replicate sample. The code (written in R-script) listed below is an implementation of what they specify. It presumes the user has extracted the original parameter estimates after running the "pl fit" function the authors have published online.

II. Power Law Distribution Fit Test in R-Script

```
plfit.test<-function(d,sim.length,seed){
set.seed(seed)

#Get Alpha Estimates
alpha.model<-plfit.alpha(d,finite=TRUE)

#Get Xmin Estimates
xmin.model<-plfit.xmin(d,finite=TRUE)

#D Object Code
D.model<-plfit.d(d,finite=TRUE)
```

```
	#Code for Sub Xmin Count
	model.locount<-length(d[d<xmin.model])

	#Code for Xmin & Over Xmin Count
	model.hicount<-length(d[d>=xmin.model])

	#Code for Sub Xmin Subset
	model.loset<-d[d<xmin.model]

	#Code for Custom Power Law Sequence
	model.pl<-
	sample(xmin.model:max(d),100,replace=TRUE,prob=(xmin.model:max(d))^-
	alpha.model)

	tally<-list(1,sim.length,1)
	# Simulation
	for (t in 1:sim.length){
		x1.model<-
		ifelse(model.loset==0,NULL,sample(model.loset,model.locount))
		#sample from the non PL region of the evaluated model
		x2.model<-ifelse(model.pl==0,NULL,sample(model.pl,model.hicount))
		#sample from the PL region of the evaluated model
		x3.model<-c(x1.model,x2.model)
		#combine the two samples
		tally[[t]]<-plfit.d(x3.model,finite=TRUE)
			#retrieve the D-score from the simulated sample
	}
	p.value<-1-(length(tally[tally>D.model])/sim.length)
	ls<-c(alpha.model,xmin.model,D.model,p.value)
	ls
}
```

Works Cited

Akaike, H. (1973). Information Theory and an Extension of the Maximum Likelihood Principle. In N. Petrov, & F. Csaki (Ed.), *Second International Symposium on Information Theory* (pp. 267-281). Budapest: Akademiai Kaidó.

Aldrich, J., Gelpi, C., Feaver, P., Reifler, J., & Sharp, K. (2006). Foreign Policy and the Electoral Connection. *Annual Review of Political Science , 9*, 477-502.

Barabási, A., & Albert, R. (1999). Emergence of Scaling in Random Networks. *Science , 286*, 509-512.

Barabási, A., & Bonabeau, E. (2003, May). Scale-Free Networks. *Scientific American* , 50-59.

Bassiouni, M. (1981). Terrorism, Law Enforcement, and the Mass Media: Perspectives, Problems, Proposals. *The Journal of Criminal Law and Criminology , 72* (1), 1-51.

Beck, T., Clarke, G., Groff, A., Keefer, P., & Walsh, P. (2001). New Tools in Comparative Political Economy: The Database of Political Institutions. *The World Bank Economic Review , 15* (1), 165-176.

Berry, W. D., DeMerritt, J. H., & Esarey, J. (2010). Testing for Interaction in Binary Logit and Probit Models: Is a Product Term Essential. *American Journal of Political Science* .

Bianconi, G., & Barabási, A.-L. (2001). Competition and Multiscaling in Evolving Networks. *Europhysics Letters , 54* (4), 436-442.

Brambor, T., Clark, W. R., & Gloder, M. (2006). Understanding Interaction Models: Improving Empirical Analyses. *Political Analysis , 14*, 63-82.

Brin, E. (2006). Politically-Oriented Tourism in Jerusalem. *Tourist Studies , 6* (3), 215-243.

Bueno de Mesquita, B., Smith, A., Siverson, R., & Morrow, J. (2004). *The Logic of Political Survival.* Boston: MIT Press.

Butts, C. (2003). Network Inference, Error, and Informant (In)Accuracy: A Bayesian Approach. *Social Networks , 25*, 103-140.

Campbell, A., Converse, P., Miller, W., & Stokes, D. (1960). *The American Voter.* New York: Wiley.

Carley, K. (2006). Destabilization of Covert Networks. *Computational and Mathematical and Organizational Theory , 12*, 51-66.

Carley, K., Dombroski, M., Tsvetovat, M., Reminga, J., & Kamneva, N. (2003). Destabilizing Dynamic Covert Networks. *Eighth International Command and Control Research and Technology Symposium.* Washington, DC.

Chalk, P., & Rosenau, W. (2004). *Confronting the Enemy Within: Security Intelligence, the Police, and Counterterrorism in Four Democracies.* Santa Monica: The RAND Corporation.

Chong, D. (2000). *Rational Lives: Norms and Values in Politics and Society.* Chicago: University of Chicago Press.

Cingranelli, D. L., & Richards, D. L. (2004). *The Cingranelli-Richards (CIRI) Human Rights Dataset* . Available at http://www.humanrightsdata.org.

Cingranelli, D. L., & Richards, D. L. (1999). Measuring the Level, Pattern, and Sequence of Government Respect for Physical Integrity Rights. *International Studies Quarterly , 43* (2), 407-417.

Clauset, A., Shalizi, C., & Newman, M. (2009). Power-law Distributions in Empirical Data. *SIAM Review , 51* (4), 661-703.

Conboy, K. (2006). *The Second Front.* Jakarta: Equinox Publishing.

Conway, D. (2009, November 16). *Structurally Induced Random Graph Model of Social Networks.* Retrieved April 20, 2010, from Zero Intelligence Agents (ZIA): http://www.drewconway.com/zia/wp-content/uploads/2009/11/SIRG_Conway_elstemp.pdf

Crenshaw, M. (1981). The Causes of Terrorism. *Comparative Politics , 13* (4), 379-399.

Davenport, C. (2008). *State Repression and the Domestic Democratic Peace.* New York: Cambridge University Press.

de Marchi, S. (2001). *Computational and Mathematical Modeling in the Social Sciences.* New York: Cambridge University Press.

Denardo, J. (1985). *Power in Numbers: The Political Strategy of Protest and Rebellion.* Princeton: Princeton University Press.

Dombroski, M., & Carley, K. (2002). NETEST: Estimating a Terrorist Network's Structure. *Computational and Mathematical Organizational Theory , 8*, 235-241.

Donohue, L. (2008). *The Cost of Counterterrorism: Power, Politics, and Liberty.* New York: Cambridge.

Drakos, K. (2007). The Size of Under-Reporting Bias in Recorded Transnational Terrorist Activity. *Journal of Royal Statistical Society , 170* (4), 990-21.

Drakos, K., & Gofas, A. (2006). The Devil You Know but Are Afraid to Face: Underreporting Bias and Its Distorting Effects on the Study of Terrorism. *Journal of Conflict Resolution , 50* (5), 714-735.

Drakos, K., & Kutan, A. M. (2003). Regional Effects of Terrorism on Tourism in Three Mediterranean Countries. *The Journal of Conflict Resolution , 47* (5), 621-641.

Easterly, W., Levine, R., & Roodman, D. (2003). New Data, New Doubts: Revisiting "Aid, Policies and Growth". *World Bank Working Paper Series , #26*.

Efron, B. (1975). Defining the Curvature of a Statistical Problem (with Applications to Second Order Efficiency). *The Annals of Statistics , 3* (6), 1189-1242.

Enders, W., & Jindapon, P. (2009). Network Externalities and the Structure of Terror Networks. *Journal of Conflict Resolution* , 1-19.

Enders, W., & Sandler, T. (2006). *The Political Economy of Terrorism.* New York: Cambridge University Press.

Enders, W., & Su, X. (2007). Rational Terrorists and Optimal Network Structure. *Journal of Conflict Resoltion , 51* (1), 33-57.

Epstein, J., & Axtell, R. (1996). *Growing Artificial Societies: Social Sciences from the Bottom Up.* Washington, D.C.; Cambridge, MA: Brookings Institution Press; The MIT Press.

Eubank, W., & Weinberg, L. (1994). Does Democracy Encourage Terrorism. *Terrorism and Political Violence , 6* (4), 417-443.

Eyerman, J. (1998). Terrorism and Democratic States: Soft Targets or Accessible Systems. *International Interactions , 24* (2), 151-170.

Farrell, W. R. (1982). *The U.S. Government Response to Terrorism: In Search of an Effective Strategy.* Boulder: Westview Press.

Gledistch, K., & Ward, M. (1997). Double Take: A Reexamination of Democracy and Autocracy in Modern Politics. *Journal of Conflict Resolution , 41* (3), 361-383.

Goodreau, S., Kitts, J., & Morris, M. (2009). Birds of a Feather, or Friend of a Friend? Using Exponential Random Graph Models to Investigate Adolescent Social Networks. *Demography , 46* (1), 103-125.

Graham, J., Haidt, J., & Nosek, B. (2009). Liberals and Conservatives Rely on Different Sets of Moral Foundations. *Journal of Personality and Social Psychology* , 1,029-1046.

Hu, D., Kaza, S., & Chen, H. (2009). Identifying Significant Facilitators of Dark Network Evolution. *Journal of the American Society for Information Science and Technology , 60* (4), 655-665.

Hunter, D. (2007). Curved Exponential Family Models for Social Networks. *Social Networks , 29*, 216-230.

Hunter, D. (2007). Curved Exponential Family Models for Social Networks. *Social Networks , 29*, 216-230.

Hunter, D., & Handcock, M. (2004). *Inference in Curved Exponential Family Models for Networks.* State College: Penn State Department of Statistics.

Hunter, D., Gooderau, S., & Handcock, M. (2005). *Goodness of Fit of Social Network Models (TNR: 05-02).* Technical Report, Penn State, Statistics, College Park.

Hunter, D., Goodreau, S., & Handcock, M. (2008). Goodness of Fit for Social Network Models. *Journal of the American Statistical Association , 103* (481), 248-258.

Hunter, D., Handcock, M., Butts, C., Goodreau, S., & Morris, M. (2008). ergm: A Package to Fit, Simulate and Diagnose Exponential-Family Models for Networks. *Journal of Statistical Software , 24* (3).

International Crisis Group. (2003). *Jemaah Islamiyah in Southeast Asia: Damaged but Still Dangerous.*

International Crisis Group. (2004). *Southern Philippines Background: Terrorism and the Peace Process.*

International Crisis Group. (2006). *Terrorism in Indonesia: Noordin's Networks.*

Jordan, J. (2004). Leadership Decapitation of Terrorist Organizations. *International Studies Association.* Montreal: www.allacademic.com.

Koch, M., & Cranmer, S. (2009). Do Governments of the Left Attract more Terrorism than Governments of the Right? *Conflict Management and Peace Science* .

Li, Q. (2005). Does Democracy Promote or Reduce Transnational Terrorist Incidents. *Journal of Conflict Resolution , 49* (2), 278-297.

Marshall, M., & Jaggers, K. (2009). POLITY IV PROJECT. *Political Regime Characteristics and Transitions, 1800-2007* . Fairfax, VA.

Ministry of Home Affairs. (2003). *The Jemaah Islamiyah Arrests and the Threat of Terrorism, White Paper.* New Phoenix Park: Ministry of Home Affairs, Republic of Singapore.

Morris, M. (2003). Local Rules and Global Properties: Modeling the Emergence of Network Structure. In R. Breiger, K. Carley, & P. Pattison (Eds.), *Dynamic Social Network Modeling the Emergence of Network Structure* (pp. 174-186). Washington, DC: National Academy Press.

Newman, M. (2005). Power Laws, Pareto Distributions and Zipf's Law. *Contemporary Physics , 46* (5), 323-351.

Piazza, J., & Walsh, J. (2009). Transnational Terror and Human Rights. *International Studies Quarterly , 53*, 125-148.

Potter, P., & Wright, D. (2009). Does Soft Foreign Intervention Trigger Terrorist Attack? *International Studies Association.* New York.

Powell Jr., B. G. (2000). *Elections as Instruments of Democracy: Majoritarian and Proportional Visions.* New Haven: Yale University Press.

Press, W., Teukolosky, S., Vetterling, W., & Flannery, B. (1992). *Numerical Recipes in C: The Art of Scientific Computing* (2 ed.). Cambridge, England: Cambridge University Press.

Price, D. d. (1980). A General Theory of Bibliometric and Other Cumulative Advantage Processes. *Journal of the American Society for Information Science , 27*, 292-306.

Robins, G., Pattison, P., Kalish, Y., & Lusher, D. (2007). An Introduction to Exponential Random Graph (p*) Models for Social Networks. *Social Networks , 29*, 173-191.

Sageman, M. (2004). *Understanding Terror Networks.* Philadelphia: University of Pennsylvania Press.

Schneckener, U. (2006). Germany. In Y. Alexander (Ed.), *Counterterrorism Strategies: Successes and Failures of Six Nations.* Washington D.C.: Potomac Books, Inc.

Simon, H. (1955). On a Class of Skew Distribution Functions. *Biometrika , 42*, 425-440.

Snijders, T. (2002). Markov Chain Monte Carlo Estimation of Exponential Random Graph Models. *Journal of Social Structure , 3* (2), 1-40.

Snijders, T., Steglich, C., & van de Bunt, G. (2010). Introduction to Actor-Based Models for Network Dynamics. *Social Networks , 32*, 44-60.

Tournyol du Clos, L. (2009). French Terrorism: The Clues of a Descriptive Analysis. *Annual Meeting of the International Society of Political Psychology.* Paris.

Treier, S., & Jackman, S. (2008). Democracy as a Latent Variable. *American Journal of Political Science , 52* (1), 201-217.

Tsbelelis, G. (2002). *Veto Players: How Political Institutions Work.* Princeton, NJ: Princeton University Press.

Tsvetovat, M., & Carley, K. (2007). On Effectiveness of Wiretap Programs in Mapping Social Networks. *Computational and Mathematical Organizational Theory , 13*, 63-87.

Viscusi, W. K., & Zeckhauser, R. J. (2003). Sacrificing Civil Liberties to Reduce Terrorism Risks. *Journal of Risk and Uncertainty , 26* (2-3), 99-120.

Wasserman, S., & Faust, K. (1994). *Social Network Analysis: Methods and Applications.* New York: Cambridge University Press.

Wasserman, S., & Robins, G. (2005). An Introduction to Random Graphs, Dependence Graphs, and p*. In P. Carrington, J. Scott, & S. Wasserman (Eds.), *Models and Methods in Social Networks Analysis* (pp. 148-161). New York: Cambridge University Press.

Watts, D. J. (2004). The "New" Science of Networks. *Annual Review of Sociology , 30*, 243-270.

Watts, D., & Strogaz, S. (1998). Collective Dynamics of "Small-World" Networks. *Nature , 393*, 440-442.

Wilkinson, P. (1976). Terrorism versus Liberal Democracy: The Problems of Response. *Contemporary Terrorism* .

Wright, D. (2010). Indirect Network Comparison Methodology (IncM): Theoretically Motivated Hypothesis Testing for the Determinants of Network Structure. *International Studies Association.* New Orleans.

Wright, D. (2009). Which Repressive Counterterrorism Strategies do Democracies Use? *International Studies Association.* New York.