

## ABSTRACT

Title of Dissertation:     FORMALIZING THE INFORMAL: A NETWORK  
                                  ANALYSIS OF AN INSURGENCY

Brian Joseph Reed, Doctor of Philosophy, 2006

Dissertation directed by: Professor David R. Segal  
                                  Department of Sociology

This research project applies Social Network Analysis to Saddam Hussein's network and demonstrates how network analysis techniques uncovered a web of family and tribal linkages that resulted in the ousted dictator's capture. I use Simmel's approach to affiliations and interactions among consensual actors as the frame in which to view why and how warfare operates the way it does in the present context of an insurgency, and what difference it makes for states (and non-states) that war is waged in this particular manner. This project adds to the emerging sociology of war that is not primarily concerned with why wars start or why some states wage war against others, but rather with how wars work once opponents are engaged.

I used two mapping networks and six associated sub-networks – trust (immediate family, extended family, close friendships, bodyguards) and strategy and goals (money and resources, insurgent operations) – to identify the structural and relational characteristics of the network. Network concepts allowed me to highlight the structure of the previously unobserved associations by focusing on the pre-existing relationships and ties that bind together such a group. By focusing on the

roles, organizational positions, and those actors who are prominent and/or influential, I was able to get a sense of how the associations were structured and how the group functioned, how members were influenced and power was exerted, and how resources were exchanged.

I found that insurgent members co-opted pre-existing ties to facilitate their operations. Roles are defined according to these pre-existing ties – primarily familial ties, but also those linked by previous political, tribal, or organizational association. Key individuals are connected to one another, thus forming a domain for each that gives them a high status in terms of prestige and influence. Those that are not part of this core group and who sit on the periphery of these critical task relationships extend the network and allow it to operate at a far greater distance. In short, social network analysis allowed me to formalize the informality of the insurgent network by visualizing the structure of one that we did not readily observe.

FORMALIZING THE INFORMAL:  
A NETWORK ANALYSIS OF AN INSURGENCY

by

Brian Joseph Reed

Dissertation submitted to the Faculty of the Graduate School of the  
University of Maryland, College Park in partial fulfillment  
of the requirements for the degree of  
Doctor of Philosophy  
2006

Advisory Committee:

Professor David R. Segal, Chair  
Professor Mady Wechsler Segal  
Associate Professor Meyer Kestnbaum  
Associate Professor Alan Neustadt  
Professor George Quester

©Copyright by  
Brian Joseph Reed  
2006

## DEDICATION

This work is dedicated to the memory of the Soldiers of the 1<sup>st</sup> Brigade Combat Team, 4<sup>th</sup> Infantry Division who died in the service of their country while deployed to Iraq in support of Operation Iraqi Freedom (March 2003 – March 2004), and to the memory of CPT Ian Weikel, killed in action on 18 April 2006 in Balad, Iraq.

## ACKNOWLEDGEMENTS

While this work would not have been possible without the varied assistance and contributions of many people, there are several I want to specifically acknowledge. First, I owe a special thanks to Dr. David R. Segal. I consider myself extremely fortunate to have had the opportunity to work with him throughout my academic career, and his mentorship and guidance have been invaluable. When I was a cadet at the United States Military Academy, it was Dr. Segal who first impressed upon me the importance of studying sociology and its place in my development as an Army officer.

Second, I am grateful to the United States Army for giving me the opportunity to complete this course of study and the chance to lead and educate Soldiers in this great Army. I am especially grateful to the officers, non-commissioned officers, and Soldiers who allowed me to succeed and to reach this point in my career.

Finally, and most importantly, I owe a special debt of gratitude to my wife, Kirsten, and my children, Stephanie, Kaelin, and Brandon. Without your patience, understanding, and encouragement, this would not have been possible.

## TABLE OF CONTENTS

List of Figures	vi
List of Tables	vii
1. Introduction	1
- Project Overview	4
2. Social Network Analysis	8
- Social Network Analysis...not Net-Centric Warfare	19
- The Social Network Fit with the Current Problem	22
3. Social Network Analysis and Resistance Networks	24
- Summarized Propositions	45
4. Insurgent Warfare	48
- State Failure	50
- Guerrilla Insurgency	51
- External Power	53
- Iraq...and Others	55
- Conclusion	59
5. Methods	62
6. The Case Study – The Network of Saddam Hussein	72
- The Background and Rise to Power of Saddam Hussein	74
- Operation Iraqi Freedom	80
- Operation Red Dawn	81
- Identifying and Specifying the Network	86

7. General Network Measures	89
- The Network of Saddam Hussein	94
- Trust Mapping Networks	97
- Strategy and Goals Mapping Networks	100
- Discussion	101
8. Actor Measures	108
- The Network of Saddam Hussein	108
- Trust Mapping Networks	114
- Strategy and Goals Mapping Networks	122
- Discussion	127
9. Role Analysis	132
- The Network of Saddam Hussein	132
- Trust Mapping Networks	133
- Strategy and Goals Mapping Networks	141
- Discussion	147
10. Conclusion	151
References	162

## LIST OF FIGURES

1. The Network Analysis and Warfare Relationship	5
2. A Model for Insurgent Warfare	50
3. Network of Saddam Hussein	91
4. Saddam Hussein's 23 Direct Ties	92
5. Personal Secretary Sub-Network	103
6. Chief of Staff Sub-Network	110
7. Chief of Operations Sub-Network	125
8. Chief of Operations & Personal Security Sub-Networks	126
9. Other Sub-Networks	128
10. Immediate Family Multiplexity	135
11. Extended Family Multiplexity	138
12. Close Friend Multiplexity	139
13. Bodyguard Multiplexity	141
14. Money and Resources Multiplexity	144
15. Insurgent Operations Multiplexity	146

## LIST OF TABLES

1. Mapping Networks	64
2. Direct Ties to Saddam Hussein	90
3. Clique-by-Clique Co-Membership Matrix	96
4. Hierarchical Clustering of Equivalence Matrix	96
5. Summary of General Network Measures	102
6. Main Network Degree Centrality Measures	109
7. Main Network Eigenvalues	113
8. Immediate Family Degree Centrality Measures	114
9. Immediate Family Eigenvalues	115
10. Extended Family Degree Centrality Measures	116
11. Extended Family Eigenvector Centralities	118
12. Close Friend Degree Centrality Measures	119
13. Close Friend Eigenvector Centralities	120
14. Bodyguard Degree Centrality Measures	120
15. Bodyguard Eigenvector Centralities	121
16. Money and Resources Degree Centrality Measures	122
17. Money and Resources Eigenvector Centralities	123
18. Insurgent Operations Degree Centrality Measures	124
19. Immediate Family Structural Equivalence	133
20. Immediate Family Automorphic Equivalence	134
21. Extended Family Structural Equivalence	137

22. Extended Family Automorphic Equivalence	137
23. Money and Resources Structural Equivalence	142
24. Money and Resources Automorphic Equivalence	142
25. Insurgent Operations Structural Equivalence	145
26. Insurgent Operations Automorphic Equivalence	145

## CHAPTER 1

### INTRODUCTION<sup>1</sup>

The study of networks, interactions, and relationships has a long history in academia. The different forms and methods of study have varied over the years and the ideas pertaining to such a study have been shaped by scholars from many fields. However, from a sociological standpoint, it is Georg Simmel who has made perhaps the greatest contributions to our understanding of the patterns, or forms, of social interaction (Ritzer 1996). One of his primary interests was interaction (or association) among conscious actors and his intent was to look at a wide range of interactions that may seem trivial at some times but crucially important at others. In short, Simmel's sociology was always concerned with relationships, especially interaction, and his work was shaped by the belief that everything interacts in some way with everything else (p. 268).

It was in his seminal work, *The Web of Group Affiliations*, that Simmel (1908/1955) outlined his thoughts related to his interest in the sociological components of interpersonal relationships. In developing such a relationship, an individual at first sees oneself in an environment that is relatively indifferent to individuality, but which has implicated the individual in a web of circumstances. These circumstances impose on the person a close co-existence with those whom the accident of birth has placed next to him/her. As the development of society

---

<sup>1</sup> Note: All thoughts and expressions contained within this presentation are solely those of the author and are not the official position of the Department of Defense or the United States Army.

progresses, each individual establishes for oneself contacts with persons who stand outside of this original group affiliation, but who are related or connected to him/her by virtue of some similarity or interest. This association based on such external factors (i.e., the similarity or interest) becomes superceded over time by association in accordance with internal relationships, or a genuine attachment between persons that is more powerful than the external factor(s) that brought them together in the first place.

The number of different social groups in which the individual participates is one of the hallmarks of culture – that is, it will vary based on one’s place in time, history, and/or society. Regardless, if one does belong to more than one group, some of these groups may be integrated. Other groups, however, may be so arranged that one group appears as the original focus of an individual’s affiliation, from which he/she then turns toward affiliation with other, quite different groups on the basis of the person’s special skills or qualities, which distinguish him/her from the primary group. The groups with which the individual is affiliated constitute a “system of coordinates” such that each new group with which one becomes affiliated circumscribes the person more exactly and more unambiguously (p. 140).

As a person becomes affiliated with a social group, one surrenders to the group. However, the individual retains some individuality because one’s pattern of participation is unique. Multiple group affiliations can strengthen the individual and reinforce the integration of one’s personality. An infinite range of individualizing combinations is made possible by the fact that the individual belongs to a multiplicity

of groups and, therefore, it is the case that one feels and acts with others, but also against others (p. 155). This results in individuals having to negotiate conflicting loyalties.

The extent to which associations form a tightly-knit group may be gauged on the basis of whether and to what extent such a group has developed a special code of “honor.” (p. 163). Such a code would imply that every member of the group would feel that his/her honor was diminished whenever any member suffered an insult or deprivation of one’s honor. In this sense, the association possesses a collective sense of honor. Groups make certain that the conduct of their members will be appropriate through the establishment of a specific concept of honor, such as family honor, professional honor, reputation, etc. However, whether it is honor or coercive actions, no matter how extensive, severe, and all pervasive the control of such group sanctions over the individual may be, there will remain relationships in one’s life that will escape it, thus allowing one to maintain one’s freedom of action.

From Simmel’s point of view, the real world is composed of innumerable events, actions, interactions, and so forth (Ritzer 1996). To cope with this maze of reality, people order it by imposing patterns, or forms, on it. The sociologist’s task, Simmel argued, is to impose a limited number of forms on social reality, on interaction in particular, so that it may be better analyzed. Such an interactional approach involves selecting some bounded, finite phenomenon from the world of flux; to examine the multiplicity of elements that compose it; and to ascertain the

cause of their coherence by disclosing its form. Forms are the patterns exhibited by the associations of people (p. 272). In other words, they are social networks.

### Project Overview

Simmel's work on affiliations is particularly relevant to my interest in resistance networks, a type of social networks. The purpose of my project is to apply Social Network Analysis to resistance network organizations within the context of insurgent warfare, with the intent of providing an evaluation of those concepts and methods that prove to be useful when applied to an insurgency. The phrase "social network" refers to the set of actors and the ties among them. The network analyst seeks to model these relationships in order to depict the structure of a group (Wasserman and Faust 1994). My sociological question of interest is as follows:

- Given that even formal organizations have informal associations (for example, student groups in academic departments), how does one understand the properties of these informal (and often unobserved) social structural environments, and then understand the impact of this structure on the functioning of the group and/or the influence of this structure on the individuals in the group? What role do social networks play in providing enough information to infer an organization in the absence of a formal, visible structure?

More specifically, my research question centers on the juxtaposition of Social Network Analysis and resistance networks:

- How does Social Network Analysis inform our understanding of “informal” networks that are characterized by secrecy, stealth, and covertness?

This project is set within the context of insurgent warfare. It is my position that this type of warfare has resulted in a change in military organization in the United States.<sup>2</sup> Likewise, there has been a resulting shift in how we view and understand the enemy, and how we now fight that enemy. The relationship between the military organization and how we see and fight the enemy is reciprocal – that, is, one affects the other. Figure 1 depicts this relationship and also demonstrates how social network analysis contributes to our understanding of the enemy.

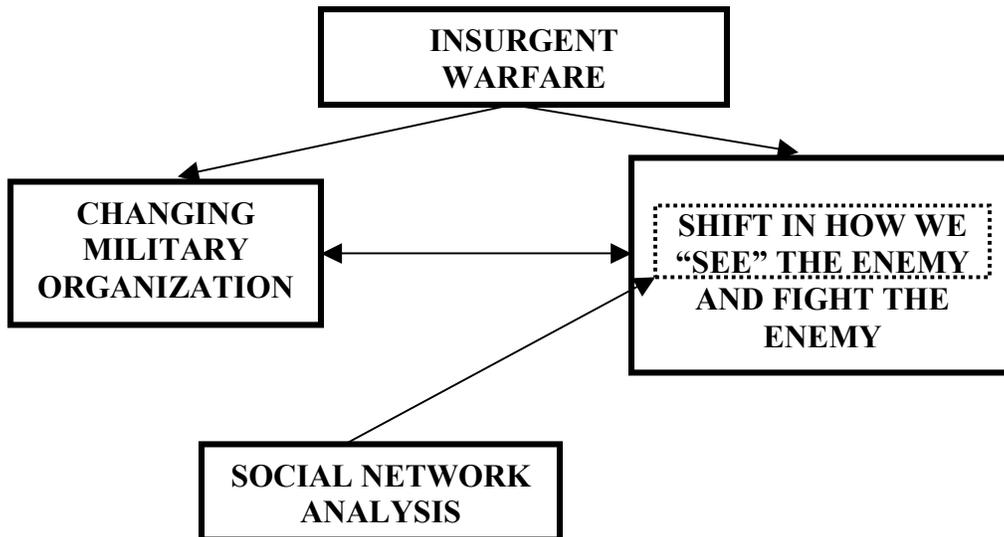


Figure 1: The Network Analysis and Warfare Relationship

---

<sup>2</sup> A discussion about the scope of the changes within the U.S. military is beyond the purpose of this project. Suffice it to say that the military (and the Army in particular) is undergoing fundamental changes in how it is organized to fight the enemy. “Transformation” is the word often associated with these changes.

In order to analyze this problem, I will first outline the theory and literature on social networks and some of the existing research on resistance networks from a network analysis perspective. I will then discuss insurgent warfare and will introduce a model that I believe contributes to our understanding of such warfare. Methodologically, I will apply traditional Social Network Analysis (SNA) to the network of Saddam Hussein. I will demonstrate how Social Network Analysis techniques combined with military thinking about organizational structure uncovered a web of family and tribal linkages that resulted in the successful capture of Saddam Hussein on 13 December 2003.

I believe this work is important for two primary reasons. First, while anthropologists, sociologists, and political scientists who are studying the growing roles of organizational networks in social movements are making good progress, the work is somewhat limited. Therefore, from a sociological perspective, this project is important because it expands on the limited research in the arena of social networks, specifically as it applies to resistance networks. This work will combine not only the “how to” of inferring relationships, but also an analysis of the relationships themselves, both grounded in social network concepts. Additionally, the results of this project will add to the emerging sociology of war – a body of work that is not primarily concerned with why wars start or why some states wage war against others, but rather with how wars work once opponents are engaged (Kestnbaum 2005).

Secondly, from a policy perspective, if insurgent warfare is the principal threat – as seems increasingly likely – then it may prove useful to view it through the

perspective offered by Social Network Analysis. With this project, I hope to merge the academic with the operational by taking one idea, trying to provide a clear definition for it, and then applying this idea to other situations. The usefulness of this type of approach – taking a definition/concept from one area and moving it to another – is revealed in the number of new insights that one obtains in the “perceptions of aspects of reality” that were there, but had not been apprehended without the concept and its definition (Hage 2004). Therefore, what makes this work uniquely different from previous research involving social networks is the application of the sociological skills offered by a network theory approach to a complex and previously uninvestigated problem, thereby resulting in a systematic, network approach for understanding an insurgent network.

A network analysis of war and insurgency differs from more conventional approaches, and this might lead us to rethink some of our more conventional analyses. An insurgency is a subset of war (Department of the Army 2006). At its core, war is a violent struggle between hostile, independent, and irreconcilable wills attempting to impose their intent on another. As an extension of both policy and politics with the addition of military force, war takes different forms across the spectrum of conflict. It is within this spectrum that an insurgency exists (p. 1-1). Each insurgency will be unique. Few fit neatly into any rigid classification. However, interconnectedness is a new aspect of the contemporary wave of insurgencies (p. 1-4). Insurgents can now link with other groups throughout the state, world, or region, joining in loose organizations with a common objective.

Breaking up these networks can be difficult. Defeating such an enemy requires a response that deals with the array of linked resources that sustain it. Conventional military thinking and approaches do not always allow for such a response. Commanders facing an insurgency are dealing with an enemy organized as a network. No longer can analysts use just an organizational chart to describe the enemy configuration. It is much more difficult for a commander to readily differentiate the enemy from members of the population. The commander can no longer expect to face a single, consistent leader running a large subordinate organization. It is increasingly unlikely that we can expect the enemy to exhibit a coherent pattern of activity that would result from a single leader.

Therefore, what a network analysis approach affords us is a different way of thinking. Such a shift in thinking can be difficult. The characteristics of network analysis may be counter-intuitive to traditionalist military thinking, which is rooted in the efficiency of a hierarchy with a strong set of baseline norms and subordination (p. E-1). Instead of a hierarchical perspective as in more conventional military thinking, we now need to consider linkages across people, groups, units, etc.

## CHAPTER 2

### SOCIAL NETWORK ANALYSIS

Network analysts start with the simple yet powerful notion that the primary business of sociologists is to study social structure. They believe that the most direct way to study a social structure is to analyze the patterns of ties linking its members (Wellman 1983). The fundamental difference between a social network explanation and a non-network explanation of a process is the inclusion of concepts and information on relationships among units in a study. Network analysis operationalizes structures in terms of network linkages among units. Regularities or patterns in interactions give rise to “structures.” The social network perspective views characteristics of the social units as arising out of structural or relational processes or focuses on properties of the relational systems themselves. The task is to understand properties of the social (or economic, political, etc.) structural environment and how these structural properties influence observed characteristics and associations among characteristics. Standard social science perspectives usually ignore the relational information (Wasserman and Faust 1994, pp. 6-7).

Social network analysis traces many of its modern roots back to efforts, decades ago, to developing sociograms and directed graphs to chart the ties among different actors in particular contexts - what gradually became known as a network (Ronfeldt and Arquilla 2001). A sociogram is a picture in which people (or social units) are represented as points in a two dimensional space, and relationships among pairs of people are represented by lines linking the corresponding points (Wasserman

and Faust 1994, p. 12). Studies of sociograms developed mainly by social psychologists took such phenomena as clique formation, leadership, or task performance as their main problems. In these analyses they related the structure of friendship choices in a group to leadership or the performance of tasks. Out of these studies developed the identification of a particular pattern of linkages which could be used in the explanation of how test subjects performed the tasks they were given and in understanding the chains of linkage along which information flows (Mitchell 1969, p. 4).

It was sociometry that first tied together the studies of sociograms, interpersonal relationships, and patterns of linkages into a coherent, theoretical and methodological framework, and it is from this that Social Network Analysis evolved. Sociometry dealt with the mathematical study of psychological properties of populations (the theoretical), undertaken through methods that inquire into the evolution and organization of groups and the position of individuals within them (the methodological). Thus, it is a framework for a process of classification which is calculated to bring individuals together who are capable of harmonious interpersonal relationships, and so creating a social group which can function at a maximum efficiency and with the minimum of disruptive tendencies and processes (Moreno 1978).

In its infancy, the central question that the sociometrist asked was “Who shall survive?” Which are the social laws of natural selection? By sociometric methods, one was able to gain direct evidence as to how natural selection took place

continuously in the very society of which it was a part, every second, in millions of places (Moreno 1978). Individuals and groups are pushed out from the anchorages in social aggregates to which they belong, from material resources which they need, from love and reproduction, from jobs and homes. It is in the billions of small groups, therefore, in which the process of natural, social selection comes to the awareness of the sociometrist. It is in sociograms that these minute processes are brought to visibility (p. 7).

Sociometry starts as soon as one is in a position to study social structure as a whole, and its parts at the same time (Moreno 1978). This was impossible as long as the individual was still a main concern, as with an individual's relation and adjustment to the group. Once the full social structure could be seen as a totality it could be studied in its minute detail, via sociograms. We thus become able to describe sociometric facts (descriptive sociometry) and to consider the function of specific structures and the effects of some parts on the others (dynamic sociometry) (p. 52).

Recognition that sociometry shares with sociology the tendency towards elaborated social systems, coupled with the recognition that sociograms could be used to study social structure, led to a rapid introduction of analytic techniques and the inspiration for other researchers to incorporate network ideas in their research (Moreno 1978; Wasserman and Faust 1994). While anthropologists had long used network concepts as partial, indirect descriptions of social structure, several analysts started developing these concepts more self-consciously and systematically, defining

a network as a set of ties linking social system members across social categories and bounded groups. Researchers began using network concepts to study Third World migrants from rural areas to cities (Wellman 1983, p. 158). In the past twenty years, many sociologists have worked to expand network concepts into a comprehensive structural formulation, thus greatly increasing the scope and claims of network analysis by treating all social structures as social networks (Wellman 1983).

The diversity of contemporary research is a result of sociologists linking network concepts with a variety of technical and substantive concerns (Wellman 1983). The network perspective has proved fruitful in a wide range of social and behavioral science disciplines. Many topics that have traditionally interested social scientists can be thought of in relational or social network analytical terms (Wasserman and Faust 1994). Such applications are important for problems concerned with devising more effective schemes, for example, of marketing products or promoting ideas, exerting influence in organizations, defining the representativeness of political bodies, or even searching for a job (Watts 1999). These are certainly important ideas and appropriate for social science research, but my interest here is focused primarily on how systems behave and how that behavior is affected by their connectivity.

Given that Social Network Analysis is an approach to analyzing social structure focusing on a network-based view of the relationships between actors, it is important that the unit of analysis is not the individual, but an entity consisting of a collection of relationships among them – similar to the approach of its sociometry

predecessor (Wasserman and Faust 1994, p. 5). In social systems, for example, it is quite possible for person A to be well acquainted with both person B and person C, yet for B and C to be not even remotely familiar with each other. On the other hand, it is possible that B and C are connected via some relationship. Regardless, a normal part of life is that each of us belongs not to a single group of acquaintances but to many, within each of which everyone pretty much knows everyone else but between which little interaction occurs (Watts 1999, p. 12). Along these same lines, Wellman (1983) proposes six analytic principles when trying to make sense of structured connectivity:

1. *Ties often are asymmetrically reciprocal, differing in content and intensity*: There is rarely a one-to-one correspondence between what two persons give to each other. However, while ties are rarely symmetric, they are usually reciprocated in a generalized way.
2. *Ties link network members indirectly as well as directly; hence ties must be analyzed within the context of larger network structures*: The very nature of a tie is defined by the larger networks in which it fits. It is the overall structural context of network members that defines the specific ties.
3. *The structuring of social ties creates nonrandom networks; hence network clusters, boundaries, and cross linkages arise*: Because of transitivity<sup>3</sup>, two linked network members often draw others with whom they are linked

---

<sup>3</sup> Ties in networks are often *transitive*. If there is a tie between A and B and a tie between B and C, then there is an increased probability of a direct tie between A and C.

into a cluster of ties in which most members are directly linked with each other. Finite limits<sup>4</sup> operate so that involvement in such densely knit clusters entails the loss of other ties. Jointly, these structural processes encourage many ties within a cluster's boundary and few ties across its boundary. However, because transitivity and finite limits are weak assumptions, individuals are usually members of multiple social networks and their ties (cross-linkages) can connect clusters.

4. *Cross-linkages connect clusters as well as individuals*: The nodes of a network do not have to be individual persons. They can be clusters, groups, or other discrete units. Ties between such nodes may occur because some persons are members of several clusters or because certain persons have "foreign relations" with other portions of the network.
5. *Asymmetric ties and complex networks distribute scarce resources differentially*: The density of clusters, the tightness of cluster boundaries, and the patterns of ties with and between clusters all structure resource flow. Because of their structural location, members of a social system differ greatly in their access to resources. Also, people as well as resources flow through network positions as they change structural positions. Indeed, positions themselves may be subject to social mobility as people with different resources occupy them.

---

<sup>4</sup> There are finite limits to the amount and intensity of ties an individual can maintain. Consequently, most cannot add many new ties without giving up all or part of their existing ties.

6. *Networks structure collaborative and competitive activities to secure scarce resources:* In a system with finite resources, interest groups compete for access to them. In a nonrandom hierarchical network with asymmetric ties, members must use collaborative or complementary ties to gain access to these resources. Clustering within a network organizes these ties into more or less bounded factions and coalitions. Competition for resources may lead to social structural change. Coalitions and factions shift in time, and network realignments can have broad systematic consequences.

From the view of Social Network Analysis, the social environment can be expressed as patterns or regularities in relationships among interacting units (Wasserman and Faust 1994), and there are several goals related to this (Dekker 2002). The first goal of Social Network Analysis is to visualize relationships between actors and to uncover structure. Second is to study the factors that influence relationships (for example, the age, cultural background, and previous training of the people involved) and also to study the strength of the relationships. Third is to draw out implications of the relational data, including bottlenecks where multiple information flows funnel through one person or section, situations where information flow does not match formal group structure, and individuals who carry out key roles that may not be formally recognized by the organization. Finally, the fourth goal is to make recommendations to improve communication and workflow in an organization (Dekker 2002).

Those who have used the notion of social networks in understanding relationships and linkages have found it necessary to distinguish certain features of or characteristics of these networks as being germane to the explanation of the behavior they have sought. Mitchell (1969) proposes several morphological and interactional characteristics which are likely to be appropriate in any attempt to define social behavior adequately. The morphological characteristics of personal networks – *anchorage, density, reachability, and range* – refer to the “shape of the individual’s network”. They may be equated with the structural aspects of social behavior – that is, the relationship or patterning of the links in the network in respect to one another.

1. *anchorage*: The point of anchorage of a network is usually taken to be some specified individual whose behavior the observer wishes to interpret. Saddam Hussein is the point of anchorage in this study.
2. *density*: The extent to which links which could possibly exist among persons do in fact exist. I will make significant use of this concept.
3. *reachability*: The degree to which a person’s behavior is influenced by his or her relationships with others often depends on the extent to which one can use these relationships to contact people who are important to him/her or alternatively, the extent to which people can contact the individual through these relationships. We used this concept in an applied sense to find Saddam.
4. *range*: Some people have many direct contacts while others have few.

The interactional criteria refer to the nature of the links themselves – the behavior of individuals vis-à-vis one another – and are the *content, directedness, durability, intensity, and frequency* of the interaction in the links. I use these concepts to describe the network.

1. *content*: The meanings which the persons in the network attribute to their relationship.
2. *directedness*: Whether the relationship between people in the network is considered as either oriented from one to the other, or reciprocal.
3. *durability*: Sets of obligations and rights associated with the recognized relationship resulting from kinship, duration of group membership, etc.
4. *intensity*: The ability of a person to exert influence over others.
5. *frequency*: The regularity of contact between nodes in the network.

As evidenced by the preceding discussion, social network analysis provides a precise way to define important social concepts, a theoretical alternative to the assumption of independent social actors, and a framework for testing theories about structured social relationships (Wasserman and Faust 1994). Equally relevant is the understanding of a social network approach to assessing power and power distribution in organizations.

Structural perspectives on power argue that power is derived from where each person stands in the division of labor and the communication system of the organization. The division of labor in an organization creates subunits and differentiated roles, and each subunit and position develops specialized interests and

responsibilities. Further, each subunit or position makes claims on the organization's resources. In the contest for resources, those who do well succeed on the basis of the resources they possess or control as well as the ties they can form with people who influence allocations. Control over resources, and the importance of the unit in the organization, are derived from the division of labor, which gives some positions or groups more control over critical tasks than others. Power, then, comes from the control over resources, from the ties one has to powerful others, and from the formal authority one obtains because of one's position in the hierarchy (Pfeffer 1992).

The knowledge that produces power in organizations is not only technical knowledge about the work process itself, but also the knowledge of the organization's social system (Pfeffer 1992). People who are well placed in the communication network also tend to be the central players in terms of power and influence. Consequently, we can say that power is a function of one's position in the network of communications and social relations, where this position is assessed not only simply in terms of structural centrality, but also in terms of the power of the people with whom one is connected.

A *central* actor is one involved in many ties (Wasserman and Faust 1994). Actors who are the most important or the most prominent are usually located in strategic locations within the network. An actor is considered to be *prominent* if the ties of the actor make the actor particularly visible to the other actors in the network. Prominence is measured by looking not only at direct or adjacent ties, but also at indirect paths involving intermediaries. Therefore, to determine which of the actors

in a group are prominent, one needs to examine not only all choices made by an actor and all choices received, but indirect ties as well. As we will see, Saddam Hussein's prominence is indicated more by his indirect than direct ties.

Many different measures of network centrality have been developed over the years. Freeman (1979) has described three related conceptualizations of centrality: betweenness, connectedness, and proximity or closeness. Betweenness is a particularly useful indicator of information control; it assesses the extent to which a person falls between pairs of other individuals on the communication paths that link them. Connectedness simply describes the number of others with whom one has contact and it is more a measure of communication activity than of one's centrality in the network. Finally, closeness measures the distance between the focal individual and all other individuals in the communication network, using the shortest communication paths that exist between them. Closeness indexes which of a group of people can reach all reachable others in the fewest number of steps, and as such it serves as an indicator of independence, because one who is close to all the others in the communication network cannot as readily have his or her access to those others controlled by someone else.

#### Social Network Analysis...not Net-Centric Warfare

Social Network Analysis is not Net-Centric Warfare.<sup>5</sup> While the two are compatible – an argument that I will make later – Network Centric Warfare (NCW) is very different – different not in the core idea of almost any network approach of

---

<sup>5</sup> Net-Centric Warfare and Network Centric Warfare are used interchangeably.

relationships and links, but different in its focus. While Social Network Analysis is concerned with understanding the relationships and ties between people and groups, NCW is a technology-based concept. More specifically, NCW is “an information superiority-enabled concept of operations that generates increased combat power by networking sensors, decision makers, and shooters to achieve standard awareness, increased speed of command, higher tempo of operations, greater lethality, increased survivability, and a degree of self-synchronization” (Czarniawska 2005. p. 63). In essence, Net-Centric Warfare translates information superiority into combat power by effectively linking knowledgeable entities in the battlespace.

In 1998, Vice Admiral Arthur K. Cebrowski<sup>6</sup> argued that the United States was in the midst of a revolution in military affairs (Cebrowski and Garstka 1998). For nearly 200 years, the tools and tactics of how we fight have evolved with military technologies. Cebrowski argued that fundamental changes had affected the very character of war. Who can make war has changed as a result of weapons proliferation and the fact that the tools of war increasingly are marketplace commodities. By extension, these affect the where, the when, and the how of war. Network-centric warfare and all of its associated revolutions in military affairs grew out of, and drew their power from, these changes and fundamental changes in American society. These changes were dominated by the co-evolution of economics, information technology, and business processes and organizations (Cebrowski and Garstka 1998).

---

<sup>6</sup> In many military and defense circles, Vice Admiral Cebrowski is often referred to as the “father” of the Net-Centric Warfare concept.

Network Centric operations deliver to the United States military the same powerful dynamics as they produce in American business. At the strategic level, the critical element for both is a detailed understanding of the appropriate competitive space. Operationally, the close linkage among actors in business ecosystems is mirrored in the military by the linkages and interactions among units and the operating environment. Tactically, speed is critical. Net-Centric Warfare, where battle time plays a critical role, is analogous to the new economic model, with potentially increasing returns on investment. Very high and accelerating rates of change have a profound impact on the outcome, "locking-out" alternative enemy strategies and "locking-in" success. Network Centric Warfare enables a shift from attrition-style warfare to a much faster and more effective warfighting style characterized by the concepts of speed of command and self-synchronization. In the end, Network Centric Warfare is applicable to all levels of warfare and contributes to the coalescence of strategy, operations, and tactics. It is transparent to mission, force size and composition, and geography (Cebrowski and Garstka 1998).

While Social Network Analysis is not Network Centric Warfare, it does enable the utilization of a network centric approach. Continued exploration of the relationships between information and combat power requires both new analytic tools and new cognitive models. The ability to increase combat power at the tactical level provides operational commanders with increased flexibility to employ their forces to generate desired effects across the spectrum of operations. Emerging evidence highlights that Network Centric Warfare can provide commanders with an improved

capability for dictating the sequence of battle and the nature of engagements, controlling force ratios and rates of closure, and rapidly foreclosing enemy courses of action (Garstka 2000).

A network analysis approach contributes directly to this capability. Defining elements of Social Network Analysis allow commanders to see military operations as a process beginning with the development of knowledge of the adversary, viewed as a complex adaptive system, the environment, and one's own assets and capabilities (Egnell 2005). Knowledge of the enemy will enable a commander to determine the effects he or she needs to achieve in order to convince or compel the enemy to change his/her behavior – a knowledge that is informed via a social network lens.

#### The Social Network Fit with the Current Problem

When considering the current Global War on Terrorism (and most specifically those operations in Afghanistan and Iraq), the deep dynamic guiding my analysis is that present-day warfare favors the rise of network forms of organization. It is a great challenge to fight a counterinsurgency in a traditionally networked society.<sup>7</sup> Fighting a counterinsurgency implies defeating the insurgency's main, regional, and local fighters. It means disrupting the underground and auxiliary support apparatus. It requires finding and arresting its leaders and shadow government cadre. Finally, counterinsurgency forces must dislocate the recruitment and indoctrination processes

---

<sup>7</sup> This analysis considers the perspective of the United States. Therefore, the U.S. military is fighting a "counterinsurgency" against an insurgent enemy force. The enemy in places like Iraq, Afghanistan, and the Philippines is waging an insurgent war.

that mobilize the individuals and resources to overthrow a constituted government (McCallister 2005).

A network analysis approach allows for a more complete understanding of how such network based “enemy” systems behave and how that behavior is affected by their connectivity. The intelligence and information work that my unit did in Iraq is known as the “Intelligence Preparation of the Battlefield” and from it one can infer the relationship between this process and sociological research. The intelligence background and link diagrams that we built were rooted in the concepts of network analysis.

The Intelligence Preparation of the Battlefield – or IPB - is a vital command and staff function for successful counterinsurgency operations. It begins with the commander’s estimate of how the enemy is fighting as well as the enemy’s strengths and weaknesses. It is complimented by a staff estimate. It becomes an hypothesis confirmed or denied by daily reconnaissance, surveillance, reporting, and command assessments. It thus evolves. The purpose is to assist the commander in identifying targets, objectives, and friendly tactics. Its value is that it allows commanders to direct operations against the enemy. An IPB at brigade level will have many components based on the threat the commander sees. Link diagramming of various enemy cells/nodes is a key component to the IPB process. Terrain analysis is absolutely vital as is an understanding of the diverse population. The enemy and people are not monolithic. The understanding of the terrain and population at large gives the commander an understanding of how to choose the time and location of

future operations as well as tactics. This supported offensive operations that kept the enemy reacting to our will.

Nowadays, many writings about terrorists, criminals, and activists observe that one grouping or another is organized as a network. However, the analyst should be able to specify more than simply that. Among other things, assessment at this level should include showing exactly what type of network design is being used, whether and how members may act autonomously, where leadership resides and/or is distributed, and whether and how hierarchical dynamics may be mixed in with the network dynamics. Social network analysts should be able to identify and portray the details of a network's structure - as well as they traditionally do when charting an adversary's leadership structures, especially for analyzing terrorist and criminal groups (Ronfeldt and Arquilla 2001).

A requirement on today's battlefield is to make an assessment of the political and social architecture of the operating environment, from both the friendly and enemy perspective; to successfully accomplish this requires more than a reading of field manuals, but also an understanding of the complexity of the nature of warfare. At least as it applies to understanding how the enemy operates, I believe that there is a value-added to a network approach to analyzing what that enemy looks like and how that enemy fights. Resistance networks often do not behave like other social networks, but by asking what kind of social network is a resistance network, one is afforded a window into the network, thereby understanding what that network looks like, how it is connected, and how best to destabilize it.

## CHAPTER 3

### SOCIAL NETWORK ANALYSIS AND RESISTANCE NETWORKS

When dealing with resistance networks, how do you “discover” a network that focuses on secrecy and stealth? How does one understand the properties and relationships that depict the structure of a group that does not want to be known? There has been some work done in this area. In 1960, Philip Selznick published *The Organizational Weapon* with an eye to developing a theory of institutional assessment, and the intent of offering a special key to the understanding of communism. His premise was that one needs to view the structure one is studying as an instance of a class of objects whose general features are to be explored via the question: what kind of social system is a communist network? The task of interpretation is to identify significant patterns of motivation, interest, and need around which characteristic types of action are organized (Selznick 1960, p. 12). Whether interpretation is focused on a single personality or on a “resistance elite,” the problem is one of isolating a set of interdependent variables forming a unique system. When we have identified the system, we can tell something about the way the behavior is summoned and constrained. This helps us make predictions concerning certain likely responses.

Sparrow (1991) provides an excellent overview of the application of social network analysis to terrorist activity, and describes three problems in analyzing resistance networks:

1. *Incompleteness* – the inevitability of missing nodes and links that the investigators will not uncover.
2. *Fuzzy boundaries* – the difficulty in deciding who to include and who not to include.
3. *Dynamic* – these networks are not static, they are always changing. Instead of looking at the presence or absence of a tie between two individuals, Sparrow suggests looking at the waxing and waning strength of a tie depending upon the time and the task at hand.

With respect to deriving “data” about resistance networks, Baker and Faulkner (1993) suggest looking at archival data to derive relationship information. The data they used to analyze illegal price-fixing networks were mostly court documents and sworn testimony. These data included accounts of observed interpersonal relationships from various witnesses. The researchers’ fundamental position is that such information was not to be acquired via conventional means – for example, surveys, interviews, etc. Mitchell (1969) makes a similar point in his discussion of the use of archival data as one means to “piece together” the network.

Krebs (2002) looked at the difficulty in mapping covert networks by using the hijacker network associated with the events of 11 September 2001. To draw an accurate picture of a covert network, he proposed that one first needs to identify task and trust ties between the conspirators. The same relationships we map in business organizations would tell us much about illegal organizations. These data are occasionally difficult to unearth with cooperating clients. However, with covert

criminals, the task is enormous, and may be impossible to complete. The six mapping networks are below. I will use these concepts to map Saddam's network.

1. *trust* - prior contacts in family, neighborhood, school, military, club, and organization;
2. *family and kin* - tribal linkages, previous associates (not family), etc;
3. *task* - logs and records of phone calls, electronic mail, travel records, etc;
4. *observation of meetings and attendance* - how messages were disseminated and by whom, attendees at meetings and gatherings, etc;
5. *money & resources* - bank account and money transfer records, where the money came from, who delivered it;
6. *strategy & goals* – statements in the media, videos and encrypted disks delivered by courier, who was making public statements, confiscated multimedia.

The best solution for network identification may be to discover possible suspects and then, via snowball sampling, map their ego networks – see to whom else they lead, and where they overlap. To find these suspects it appears that the best method is for diverse intelligence agencies to aggregate their information – their individual pieces to the puzzle – into a larger emergent map. By sharing information and knowledge, a more complete picture of possible danger can be drawn (Krebs 2002).

The 9/11 hijackers' network had a hidden strength – massive redundancy through trusted prior contacts. The ties forged in school, through kinship, and

training/fighting in Afghanistan made this network very resilient. These ties were solidly in place as the hijackers made their way to the United States. While here, these strong ties were rarely active – used only for planning and coordination (Krebs 2002). In effect these underlying strong ties were mostly invisible during their stay in the United States.

Strong ties, which were frequently formed years ago in school and training camps, keep the cells interconnected. Yet, unlike normal social networks, these strong ties remain mostly dormant and therefore hidden. They are only activated when absolutely necessary. Amongst the 9/11 hijacker network, for example, weak ties were almost non-existent between members. Minimizing the weak ties reduces the visibility into the network, and lowers the chance of leaks out of the network. In a normal social network, strong ties reveal the cluster of network players – it is easy to see who is in the group and who is not. In a covert network, because of their low frequency of activation, strong ties may appear to be weak ties. The less active the network, the more difficult it is to discover. However, the covert network has a goal to accomplish. Network members must balance the need for secrecy and stealth with the need for frequent and intense task-based communication. The covert network must be active at times. It is during these periods of activity that they may be most vulnerable to discovery (Krebs 2002).

Similarly, using the 9/11 hijacker network, Rothenberg (2002) developed some general descriptions of the network features of the terrorist organization – about what a terrorist network, either local or global, might look like, and the characteristics

that define it. I will return to these descriptions in my analysis of Saddam Hussein's network.

1. *The entire global network is a connected component:* Estimates of the size of the network are as varied as estimates of the size of personal networks. If it numbers in the thousands, as the information on training camp attendees suggests, then it is unlikely that everyone knows everyone else. It is, however, likely that anyone in the network can be reached in some way by anyone else. Moreover, it is likely that on the local level, individual ties are very strong: the two persons know each other very well and they know dozens or even scores of persons in common. On a higher level (regional, national, international), individual ties are likely to be weaker but the strength of association (the people who are known in common) is likely to remain high.
2. *The network is redundant on every level:* Each person can reach other people by a multiplicity of routes. Information and material can travel along multiple routes with the same destination. Though there will be some variation in degree of centrality (the number of persons with whom an individual is in active contact), this variation will be small, so that the loss of one person cannot interrupt transmission. The redundancy in communication channels will be mirrored in the redundancy of active groups (provide for many so that a few make it through to the end).

Finally, there is a redundancy in the leadership; that is, numerous persons can play a pivotal role.

3. *On the local level, the network is small and dynamic:* It is likely that small cells (e.g., 4 to 6 people) operate with relative independence and little oversight in the intermediate term. It is likely that there is some turnover in personnel, particularly in light of a long lead-up time. Such dynamics are aided by the considerable structural equivalence of roles in the network so that persons can be deployed in different locations with ease, or eliminated if need be.
4. *The network has formidable barriers to entry and exit:* Exit is not tolerated. Entry is only possible through having led an entire life that becomes the individual's credential. New recruits are sought, but the screening process is arduous, training endless, selectivity high, and the waiting process after training can be long. Entry is a process that takes years, so that rapid penetration of the network is very difficult.
5. *The network is not managed:* Management implies record keeping. One of the more mysterious aspects of the 9/11 network is the way it kept track of people, of money, or of activities. Perhaps it did not. There were limited computers, no paper, no records, no remains. A system built on trust is untraceable. Such trust is built on the beliefs and loyalty, the shared experience of living and training in a world of no prospects, and a shared language (Arabic, for the most part) plus many other dialects that

provide individuals with an almost unbreakable code as well as evidence of their trustworthiness.

6. *The structural characteristics of the network give it operational flexibility:*

Small, multi-potential groups, with considerable internal discipline but considerable local decision making, adherence to a common cause, few direct contacts but a connection to a larger whole, and an unshakable belief structure has shown itself capable of performing multiple tasks with agility and audacity. Even in the face of some individual bungling that has become evident, the operation can rest its successes on its network characteristics.

Carley et al. (2002) utilized social network analysis and multi-agent models to discuss how to destabilize networks. Network dynamics are a function of not just the social network, but a meta-matrix of networks – not the least of which are the knowledge network (who knows what), the information network (what ideas are related to what), and the assignment network (who is doing what). To track and understand network dynamics, to be truly able to determine how to destabilize networks, we must consider the position of individuals and groups as they are embedded in the overall meta-network. We must move beyond embeddedness in the social network to overall embeddedness in the meta-network.

There are at least two fundamental ways in which network statistics and measures can be applied to address issues at the heart of destabilizing networks (and which will be inherent in my analysis) (Carley et al. 2002):

1. *Location of critical individuals, groups, technologies*: Given any network, such as a communication network, or alliance structure, or monetary flow, where the nodes are individuals, groups, computers, etc., a number of network measures such as centrality or cut-points can be used to locate critical nodes.
2. *Pattern location*: This involves locating patterns such as interaction or communication networks, monetary networks, inter-organizational alliances, mental models, texts, web pages, who was present at what event, and story lines.

Similarly, the authors maintain that there are at least three indicators of destabilization. One is where the rate of information flow through the network has been seriously reduced, possibly to zero. A second is that the network, as a decision making body, can no longer reach consensus, or takes much longer to do so. A third is that the network, as an organization, is less effective; that is, its accuracy at doing tasks or interpreting information has been impaired.

Friedman (2003) makes the argument that there were indicators pointing to the events of 11 September 2001, but they were by no means so unambiguous that they could easily have been deciphered. He maintains that the sheer extent of al Qaeda ambitions, and its practice of selecting from among many operations proposed by lower-level terrorists, made (and makes) predictions of future actions very difficult. Arrests and financial attacks may well preclude attacks, but it will probably always be difficult to be sure of just what plots have been prevented. At least some of

the past reported success against al Qaeda, therefore, may well refer to abortive proposals rather than to plots close to fruition; others were more obviously realistic. None of this means that it is pointless to deal with al Qaeda (and other resistance/terrorist organizations), only that the most profitable targets are probably the sources of money and the central command (which implies a division of labor) rather than the deployed terrorist cells, which may well live independently of al Qaeda itself (p. 42).

Along these same lines, Friedman implies that a social network approach may be useful to understanding such networks and preventing future attacks. His focus becomes one of identification and then disruption. First, one must ask if there is anything that loosely connected terrorist cells share, any center that can be attacked? One answer might be information – not so much information about their mutual enemy (which is easy to gather) as information allowing them to distinguish ally from enemy. In recent years, defense analysts have become increasingly interested in the effect of attacking an enemy's information as a way of crippling him. The cells survive because they are largely invisible to the authorities hunting them. How do they recognize each other? How can a cell member be sure that when he approaches a potential ally, he is not committing suicide? In a large organization, there is some central registry of accredited friends. The key guarantee of legitimacy is the myriad of checks that the surrounding organization routinely carries out. The system fails from time to time, but usually the bureaucracy protects it. A heavily decentralized international terrorist network lacks any such protective bureaucracy. It is, therefore,

inherently vulnerable to attacks which begin with deception – with the destruction of the limited information each cell has about who its friends really are (pp. 101-102).

In the area of criminology, there is evidence of a network approach being used to understand criminal networks, especially those associated with organized crime. In an important historical study of organized crime in New York, Alan Block (1979) discovered that contrary to the traditional paradigm of criminal organizations as hierarchical or pyramidal structures, they were not only more fragmented and chaotic than believed, but these organizations also involved “webs of influence,” linking criminals with those in positions of power in the political and economic world. These patterns of affiliation and influence were far more important than any formal structure and allowed criminals to maximize many opportunities.

More recently, McIlwain (1999) proposes that three major paradigms are used to define and comprehend organized crime. The first proposes that organized crime is best understood as a viable organization, a reflection of the institutional approaches that dominated sociology and business departments during the 1960s. The second rejects the formality of the institutional approach in favor of one based on exchange relationships between those in power and those who need access to that power. The third de-emphasizes that actors engage in organized crime and focuses instead on the business of organized crime. While proponents each make arguments for their own point of view and disclaimers about the others, one central issue at hand is whether or not there is a common underpinning to all three paradigms that can assist scholars in assessing the essence of organized crime.

It is from this central position that McIlwaine advances an organized crime theory based on a social network perspective. He argues that “the least common denominator of organized crime is human relationships engaged in the process of social networking for the provision of illicit goods and services as well as the protection, regulation, and extortion of those engaged in the provision or consumption of these goods and services” (p. 304). He goes on to note that such social networks are not bound by a foundation of culture of local level social systems, but rather individual actors from different cultural backgrounds and distinct social systems share a common understanding of the value of the network with actors from a different cultural background or social system. These social network processes transcend culture and allow for new networks to be created, and similarly, existing networks can be expanded across geographical space due to social mobility and migration. In time, these processes allow local level networks to expand to larger domestic and international networks.

In the same vein, Williams (2001) analyzes the trend that many old-school criminal hierarchies (for example, the Italian Mafia) are reorganizing into sprawling transnational networks. He advances the position that organized crime often operates through fluid networks rather than through more formal hierarchies. However, whatever their precise characteristics, networks provide criminals with diversity, flexibility, low visibility, durability, and the like (p. 71):

1. *Networks can often operate clandestinely:* The more visible a criminal enterprise the more likely it is to be attacked by law enforcement. One of

the most significant points about networks, however, is that they are not immediately and obviously visible. Criminal networks can hide behind various licit activities, can operate with a lower degree of formality than other types of organization, and can maintain a profile that does not bring them to the attention of law enforcement.

2. *Even when they are targeted by law enforcement, many criminal networks are inherently dispersed, with the result that they do not provide obvious centers of gravity or loci for law enforcement attacks:* Lacking a physical infrastructure or a large investment of sunk costs that would add significantly to their vulnerability, networks can also migrate easily from areas where risks from law enforcement are high to areas where the risks are much lower.
3. *Networks also offer opportunities for both redundancy and resilience.* In network structures, it is easier to create redundancies than it is in more formal and rigid organizations – therefore, even if part of the network is destroyed it can still operate. Furthermore, degradation of a network does not necessarily lead to its demise. Networks are very resilient and can easily be rebuilt.

Critical to Williams' work on criminal organizations as network systems is his analysis of the typical characteristics of criminal networks and the roles in criminal networks. My analysis of the Hussein network incorporates these characteristics and roles. With respect to the former, the main characteristics of criminal networks are

those that help make them extremely difficult to combat. Criminal networks provide moving and elusive targets that operate across enemy lines, infiltrating law enforcement agencies and governments, avoiding confrontation in favor of co-option and corruption. They are resistant – although not impervious – to damage and have qualities that facilitate recuperation and regeneration.

1. *Network Cores*: Networks of any substantial size will generally have both a core and a periphery, thereby reflecting asymmetries of power, influence, and status within the network. The core is characterized by dense connections among individuals who provide the steering mechanism for the network as a whole. The core members' relationship is often underpinned by bonding mechanisms that help to create high degrees of trust and cohesion.
2. *Network Peripheries*: This zone features less dense patterns of interaction and looser relationships than the core. Yet, these characteristics play a critical role in networks, exhibiting and exploiting “the strength of weak ties.” In effect, the periphery allows the network to operate at a far greater distance – both geographically and socially – than would otherwise be the case, thus facilitating more extensive operations, more diverse activities, and the capacity to carry out effective intelligence collection.
3. *Criminal Networks as Defensive Structures*: For the most part, networks are very good at self-protection. While it is possible for law enforcement to infiltrate the periphery of the network, getting into the core is much

more difficult partly because entry is dependent on a high level of trust that is based on bonding mechanisms rather than functional utility. Moreover, there are usually several nodes in the network which act as built-in insulators between core and periphery, thus distancing the core leaders from operations and making it very difficult for law enforcement to strike at the center of gravity.

4. *Criminal Networks as Facilitators of Cooperation:* Criminal networks come together with one another when it is convenient or beneficial for them to do so without this being a threat to their identity. Some criminal networks develop steady supplier relationships with one another, while others develop contract relationships for the provision of certain kinds of services. Criminal networks are also able to draw on a whole set of support structures, whether through acts of paternalism in the community or through more strictly financial considerations.
5. *Criminal Networks as Boundary Spanners:* Another closely related advantage of criminal networks is their capacity to flow around physical barriers and across legal or geographical boundaries. Networks transcend borders.
6. *Criminal Networks as Creators and Exploiters of Corruption:* Criminal organizations extend their reach by co-opting individuals and organizations in ways that facilitate, enhance, or protect. The corruption

networks they create are dynamic rather than static, increasing in significance as corrupted officials become more senior.

7. *Criminal Networks as Robust and Resilient Organizations*: Networks are highly resilient, partly because of what might be termed loose coupling. Even if some parts of the network are destroyed, the effects are limited since other parts are left intact. In a loosely coupled network, cascading effects are limited and damage to one part of the network does not undermine the network as a whole. Resiliency also stems from the capacity to limit the damage that is inflicted by developing certain forms of redundancy that facilitate recovery if part of the network is degraded or damaged.

Networks feature a considerable division of labor among members. Indeed, it is possible to identify a series of critical roles, some of which occur in all networks, and others that are found in specific types of “business” in which criminal networks are involved. In some networks, the tasks will be implicit and intuitive; in others, they are explicit and formal. In most criminal networks, the following roles are likely to be discernible (pp. 82-83):

1. *Organizers*: Those core individuals and groups that provide the steering mechanism for the network. These organizers will generally determine the scale and scope of activities and provide guidance and impetus for their execution.

2. *Insulators*: Individuals or groups whose role is essentially to insulate the core from the danger posed by infiltration and compromise. These individuals transmit directives and guidance from the core to the periphery of the network. They also ensure that communication flows from the periphery do nothing to compromise the core.
3. *Communicators*: Individuals who ensure that communication flows effectively from one node to another across the network as a whole. Their responsibility is to transmit directives from the core group and provide feedback. In some cases, insulators and communicators will be at odds because of competing impulses inherent in their differing responsibilities.
4. *Guardians*: Enforcers concerned with the security of the network who take measures to minimize vulnerability to external attack or infiltration. Precautions about who is recruited to the network combine with measures to ensure loyalty through a mix of ritual oaths and latent coercion directed against the new members or their families. Guardians act to prevent defections from the network, or in the event that such defections take place to ensure that the damage is minimized.
5. *Extenders*: Those whose role is to extend the network by recruiting new members, by negotiating with other networks regarding collaboration, and by encouraging defectors from the world of business, government, and law enforcement. Among the tactics that extenders typically use are voluntary recruitment through bribery and corruption and involuntary recruitment

through coercion, sometimes leavened by the addition of rewards or inducements. Their targets typically include important and powerful politicians who can provide a high degree of protection, bureaucrats in particularly sensitive or pivotal positions, and financial managers who provide access to legitimate financial institutions.

6. *Monitors*: Those who ensure the effectiveness of the network and whose responsibilities include reporting weaknesses and problems to the core organizers, who can then initiate remedial action. These network members are particularly crucial in ensuring implementation and providing guidance on appropriate corrective measures where necessary. They ensure that the network is able to adjust to new circumstances and maintain the high degree of flexibility that is critical to the capacity to circumvent law enforcement.
7. *Crossovers*: People who have been recruited into a criminal network but who continue to operate in legal institutions, whether governmental, financial, or commercial. By operating in a different sphere from most of the network, they are able to provide invaluable information and protection.

When confronting criminal networks, Williams offers several alternatives. First, it is important to recognize that although criminal networks are resistant to disruption and have high levels of redundancy and resilience, they are not impervious to attack by law enforcement. The nature of these networks, however, suggests that

the attacks need to be carefully orchestrated, finely calibrated, and implemented in a comprehensive and systematic fashion. Indeed, there are several important prerequisites for initiating effective attacks on networks, especially clear delineation of objectives and enhanced intelligence assessments.

In attacking criminal networks, it is vitally important to determine the major objectives: Are they to destroy the network, simply to degrade its capacity to carry out criminal actions, or to detach the network from its support apparatus in the licit world? The objectives can range from making operations more difficult for the network through creating instability in the environment to more direct attacks on the network itself that are aimed at disruption of its activities, dislocation or degradation of its capabilities, or even its complete destruction. While all are legitimate objectives, it is essential that there is clarity about precisely which of them is being chosen (p. 91).

Understanding network structures and operations makes it easier to identify vulnerabilities against which concentrated attacks should be directed. Particularly important in this connection is the identification of critical nodes. A critical node in a network is one that generally has a high level of importance and a low level of redundancy. The importance can reflect the existence of certain specialized skills or the position of the node within the network. The low level of redundancy stems from the lack of adequate substitutes for those with these skills. In addition to those nodes that are obviously critical, there are those that can become critical because of more general damage inflicted on the network. These nodes - the ones that are important

but highly redundant - can become critical if they are attacked simultaneously or in close succession to one another. While this requires effective coordination, it is certainly an option that needs to be considered (pp. 93-94).

The other obvious target for attack is the network core. If the network is functioning effectively, however, and the insulation processes are working as intended, then this will prove extremely difficult. If the core figures are identified and removed, one of two results is possible. The first is that the network is so well-established that it can continue to function. A variation on this is that some of the figures who have been close to the core, but not necessarily part of it, can substitute for those removed from the steering group. The second possibility is that attacking the core group will significantly degrade the network and along with other measures, such as an attack on the gateways, will either force it to cease operating or, at the very least, significantly degrade its capacity and reach.

In the area of trust and criminal networks, several researchers have made considerable efforts to come to a better understanding of the importance of trust in the context of organized crime. Von Lampe and Ole Johansen (2003) argue that the most appropriate frame of reference for discussing trust in the context of organized crime is a network approach. According to a widely held notion, criminal relations in general and within illegal enterprises in particular tend to be embedded in kinship ties. This view is supported by general assumptions about the link between family and trust. However, the link between kinship ties and criminal relations may not be as easily established as one commonly assumes. First, there is the aspect of inner family

conflicts. The assumption of family based trust hinges on a somewhat romantic notion of family harmony that does not always live up to reality (von Lampe and Ole Johansen 2003). In his analysis of Southern Italian Mafia families, Pino Arlacchi (1986) has observed that often relations between families of brothers are marked more by disagreement and impulses toward mutual conflict and less by cooperation and solidarity.

A second issue is that of “borrowed loyalty” – that is, under what circumstances do long-term relations with no illegal connotation, as is the case with familial ties, become a basis of trust for criminal cooperation? In their research on alcohol smugglers in Norway, von Lampe and Ole Johansen found no indication of a dominant role of kinship structures in the black market (p. 11). So, just because a “blood” relationship existed, the implication was not that there was criminal behavior associated with this tie. In fact, in the case of the illegal alcohol market, close-knit, local communities in rural Norway appeared to be a more significant trust factor than the immediate family. In these communities, black market alcohol operations are widespread and disloyal behavior would be directed not only against a business partner, but against the entire community. Under such conditions, family ties, to the extent that they are criminally relevant at all, provided no value-added in trust relations and, therefore, were not a prominent feature of the cooperative structures (p. 12).

### Summarized Propositions

The review of the literature and research pertaining to resistance networks, and the theoretical offerings of Simmel and Social Network Analysis, lead to some of the central propositions formulating this research:

1. Resistance networks often do not behave like normal social networks.
  - a) Resistance networks are both coercive and covert.
  - b) In a normal social network, strong ties reveal the cluster of network players – it is easy to see who is in the group and who is not. In a resistance network, because of their low frequency of activation, strong ties may appear to be weak ties. The less active the network, the more difficult it is to discover.
  - c) Resistance networks are inherently dispersed, with the result that they do not provide obvious centers of gravity or loci.
    - i. Resistance networks are characterized by incompleteness in data collection methods – the inevitability of missing nodes and links.
    - ii. Resistance networks are characterized by ambiguous boundaries – the difficulty in deciding whom to include and whom not to include.
    - iii. Resistance networks are dynamic – these networks are not static, they are always changing.

- d) In resistance networks, it is easier to create redundancies than it is in more formal and rigid organizations – therefore, even if part of the network is destroyed, it can still operate.
  - i. Resistance networks are very resilient and can easily be rebuilt.
- 2. A network analysis approach to understanding resistance networks allows for predictions concerning certain likely future behavior of the network, thereby allowing for a focus on prevention, rather than only prosecution, of coercive behavior.
  - a) The best solution for network identification may be to discover possible suspects and then map their ego networks – see to whom else they lead, and where they overlap.
  - b) Power is a function of one's position in the network of communications and social relations, where this position is assessed not only simply in terms of structural centrality, but also in terms of the power of the people with whom one is connected. People who are well placed in the communication network also tend to be the central players in terms of power and influence. Disruption occurs by focusing on the connections.
  - c) There is a clear division of labor within the network – for example, financiers, logisticians, operators, decision makers, etc. Control over resources, and the importance of the node in the network, is

derived from the division of labor, which gives some positions or groups more control over critical tasks than others. Power, then, comes from the control over resources (Pfeffer 1992). Disruption occurs when this “power node” is eliminated.

- d) A resistance network lacks a “protective bureaucracy” thereby omitting some checks and balances to guarantee secrecy and covertness, and thus making it more vulnerable to infiltration.
- e) To be able to determine how to destabilize resistance networks, we need to consider the position of individuals and groups as they are embedded in the overall meta-network – that is, the knowledge network (who knows what), the information network (what ideas are related to what), and the assignment network (who is doing what).
- f) Kinship/familial ties do not guarantee a relationship that may be associated with resistance behavior.

## CHAPTER 4

### INSURGENT WARFARE

Low intensity conflict, or guerrilla warfare, has been more common throughout the history of warfare than has conflict between nations represented by armies on the conventional battlefield (Nagl 2002). The essential features of guerrilla warfare – avoiding the enemy’s strengths, clever use of the terrain, and striking at outposts and logistical support centers from unexpected locations – have barely changed since the days of the Romans and the Persians. However, what has changed, and thus made guerrilla warfare a more potent form of conflict for the accomplishment of political objectives, is the addition of revolutionary thinking (Nagl 2002).

Present day standard views of insurgency are based on our interpretation of the classic texts of insurgency warfare and our experiences dealing with wars of national liberation in the late 20<sup>th</sup> Century (McCallister 2005). The basic tenets for this form of warfare are found in the writings of past practitioners such as Mao Tse–Tung. Mao saw revolutionary war as protracted and organized into three phases: a phase of organization, consolidation, and preservation by which the insurgents build political strength; a second phase of progressive expansion as the insurgents gain strength and consolidate control of base areas; and the final decisive phase whereby the insurgents commit regular forces (which have been carefully husbanded up to this point) culminating in the destruction of the enemy (Hammes 2004; Nagl 2002, p. 23). Mao also called for clearly defined political goals and firmly established political

responsibility. As the first practitioner to define insurgency, Mao understood that war is fundamentally a political undertaking and that political mobilization was the most fundamental ingredient for winning the war (Hammes 2004).

The question arises, then, as to whether or not this view of insurgency is in line with our expectations of 21<sup>st</sup> Century insurgent warfare. As we look at the existing operations in Iraq and Afghanistan and the overall Global War on Terrorism, does the classical understanding of revolutionary warfare square with the present-day dilemmas? I believe that the past and the present are not so different. Features of historical insurgencies are evident in the modern conceptions of an insurgency, most notably the concentration on defeating the political will of one's enemy rather than defeating the enemy's army on the battlefield. Like those that came before them, the insurgent leaders in Iraq, Afghanistan, the Philippines, and other places where the United States' war on terrorism is being waged, are in this for the long haul.

There is a distinctiveness, however, to what we are witnessing in Iraq, Afghanistan, and in other areas. Such a model is not a rejection of the past, but instead a revision of what we have witnessed in previous insurgent warfare experiences. Precipitated by state failure, we see non-state actors organized in non-state form, organized (albeit loosely) across territorial boundaries, operating along pre-existing structural linkages that are adapted to wage insurgent warfare. In addition, there is the presence of an external foreign power attempting to restore order and governance in a country that is not its former colony. This phenomenon can be captured in the following manner:

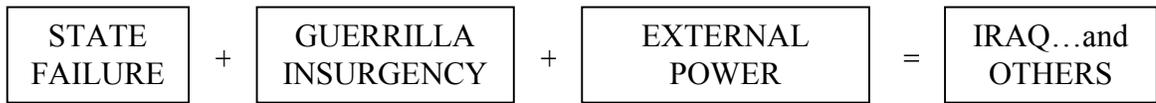


Figure 2: A Model for Insurgent Warfare

### State Failure

Potentially, one of the primary centers of disorder in the 21<sup>st</sup> Century will be failed states - areas where the state has either disappeared or become simply one more criminal gang among many (Lind 2004). These areas represent the future for much of the world. Just as some cultures are likely to be centers of order, others will be centers or sources of disorder. Insurgent networks thrive on disorder.

State failure is “a process by which the state loses the capacity and/or the will to perform its fundamental governance and security functions” (Manwaring 2005, p. 27). Failing or failed state status is the breeding ground for instability, criminality, insurgency, regional conflict, and terrorism. Such conditions can host destructive networks of all kinds and/or various forms of ideological insurgency. The contemporary, chaotic global security environment reflects a general lack of legitimate governance and civil-military cooperation in many parts of the world. Instability thrives under these conditions (Manwaring 2005).

As important as instability might be in a national or transnational threat environment, one important consideration is that it is only a symptom – not the threat itself. Rather, the ultimate threat is “state failure” (Manwaring 2005, p. 30). Along these lines, probably the most insidious security problem facing the nations of the world today centers on the threat to a given nation-state’s ability and willingness to

control its national territory, and the non-state actors who are seeking violent change within the borders of that nation-state (Manwaring 2005).

The overarching point of the preceding discussion is that the greatest security challenges of today and the near future consist of failing states and regional insecurity, which has worldwide repercussions, and the rise of terrorism, which thrives in areas lacking political control. The essence, then, of contemporary warfare is asymmetry – an asymmetry of will and means.<sup>8</sup> The “enemy” adjusts itself by employing unconventional strategies like insurgencies and terrorist attacks. The enemy of contemporary conflicts is network based, flexible, and transnational in scope (Egnell 2005). One could make the argument that the beginning of this nature of warfare lies with the fall of the Berlin Wall and the collapse of the Soviet Union, thereby allowing more sub-national and regional organizations to have a national and/or international voice.

### Guerrilla Insurgency<sup>9</sup>

My conception of the modern insurgency is one characterized by non-state actors organized in non-state form, linked by pre-existing ties (as an example, religion, family, tribe) that are adapted to conducted insurgent warfare. Such actors are intent not on just short-term gains and goals, but with the inclination to make a long-term difference. Thus, the aims these non-state actors adopt, and the resources

---

<sup>8</sup> Of note, however, is that asymmetry is not something new. The Bolshevik revolution in Russia was an insurgency structured as a network of cells, and, in that tradition, so was the Viet Cong in Viet Nam. Additionally, we have seen evidence of U.S. asymmetrical tactics in our own history, beginning with the American Revolution.

<sup>9</sup> This is guerrilla warfare “on steroids.” A guerrilla insurgency is the strategic employment of guerrilla tactics (most commonly hit and run tactics) combined with terrorist-type acts (e.g., car bombs) to achieve a particular political and/or ideological end.

they employ, are governed not only by the particular characteristics of their own positions, but they also conform to the spirit of the age and to its general character (Clausewitz 1832/1984) – a spirit and character defined by an unorthodox and asymmetric, networked approach aimed not at attempting to win by only defeating one's enemy's armed forces, but rather, directly attacking the minds of decision makers to destroy their enemy's political will. Thus, such conflicts will be lengthy, measured in decades rather than months or years.

Revolutionary coalitions tend to form around pre-existing nationalist, populist, or religious discourses that are capable of aggregating a broad array of social classes and strata. Such organizations may also offer selective incentives to encourage participation in various sorts of activities, particularly dangerous ones like guerilla warfare. It is the ongoing provision of collective and selective goods, not ideological conversion in the abstract, which has played a principal role in solidifying social support for insurgent groups (Skocpol 1994).

While pre-existing ties are the foundation, it is a common interest plus the institutional means to pursue it that are the catalysts in making plausible a collective identity that allows a group to embrace collective action (Gould 1995). Collective identities draw conceptual boundaries around the set of people who are similarly affected by specific circumstances. However, these conceptual maps have no consequence in the absence of pre-existing social ties. The dual role of these social relations – as a means for assessing the validity of a collective identity, and as a means for acting on it, or pushing others to do so – accounts for the fact that formal

and informal ties act together in the mobilization and unity of effort (p. 202). In places such as Iraq or Afghanistan (and others), kinship historically has provided a vehicle for political organization. It has delineated conditions for individuals to come together and cooperate. In particular, kinship ties have served as a basis for political action and collective defense (Charrad 2001).

While not necessarily unique, my model is distinctive because it takes into consideration a networked enemy organized across territorial boundaries and borders. While the organization on the surface appears to be loose, there is a connection (at least an ideological connection) between al Qaeda operations in Afghanistan, Iraq, Yemen, and the Philippines, as an example. To date, it is uncertain as to how many insurgent groups actually exist in the Iraq Theater of Operations. Are the groups united and working together, or are they fractured and purely focused on individual goals and objectives? Regardless, a common theme of all these groups appears to be centered on the ouster of the United States-led coalition and the failure of a democratically based Iraqi Government. Arguably, such a theme is consistent with the objectives of other insurgent groups waging a revolutionary war in other places against U.S. forces.

#### External Power

Within the current insurgency model, a key variable is the presence of an external power and its efforts to restore order and governance that have resulted from state failure, either created from within or the result of a military intervention. In the

case of Iraq, arguably what we are witnessing is a social revolution,<sup>10</sup> one that could not have happened without a breakdown of the administrative and coercive powers of the old regime.<sup>11</sup> The transformation and reconstitution of the state is being overseen by the coalition forces, with the United States as the primary engineer of this undertaking. Such a transformation is unlike classical examples of social revolutions where the reconstitution of coercive and administrative state organizations is driven from within – for example, France, Russia, China, and Iran (Skocpol 1994).

The basic condition for the occurrence of a revolution is the emergence from society or a people of a deliberate effort, tying together leaders and followers, aimed at overthrowing the existing political or social order (Skocpol 1994). Revolutions by nature are complex and multidimensional. The insurgency we see in Iraq is the *result* of a social revolution, precipitated by an external power. In any revolutionary crisis, differentially situated and motivated groups become participants in a complex unfolding of multiple conflicts that ultimately give rise to outcomes not originally foreseen or intended by any of the particular groups involved (p. 111). Hence, witness the rise of the insurgent resistance that came to the forefront after the fall of Baghdad. However, like the classic cases mentioned above, success in Iraq and other places today will depend on the leaderships (i.e., the U.S. sponsored Iraqi government) that do not necessarily have the most coherent or innovative ideologies,

---

<sup>10</sup> I have adopted Skocpol's (1994) conceptualization of social revolutions as the "breakdown of old regimes, processes of conflict among elites and between dominant and subordinate classes, and the reconstitution of new regimes that embody fundamental political, social, and ideological changes" (p. 6).

<sup>11</sup> The intent here is not to debate how or why such a breakdown occurred, only that it occurred. To pursue this argument would mean a debate on U.S. policy toward Iraq, which is not within the scope of this project.

but instead most successfully use popular political mobilizations for state-building purposes: to create armies, systems of governance, and administrative oversight (p. 9).

Along the same lines, historical-comparative analysis of directly ruled colonies and indirectly ruled colonies has shown that the latter have been much less vulnerable to actual defeat and displacement by revolutionary guerrillas (Goodwin 1988). Indirectly ruled colonies are those where an external power sponsors indigenous elites to whom it can later gradually hand power without disrupting administrative-military institutions. After World War II, in Malaya and the Philippines, as examples, restored British and American rulers governed in conjunction with indigenous elites to whom national sovereignty was eventually ceded. During and after the transition to independence, the governments of Malaya and the Philippines were able to use military force and limited reforms to crush or contain marginalized communist guerrillas (Skocpol 1994). In similar fashion, this is generally the route the United States is taking in present-day Iraq. The transfer of sovereignty and national elections have already occurred with the goal of eventually being able to withdraw U.S. military and coalition forces once the fledgling Iraqi government and military are able to defeat or contain the insurgency.

#### Iraq...and Others

In attempting to explain the situation in Iraq, one must consider the fact that a tribal society already has at its disposal affiliated social, economic, and military networks easily adapted to warfighting. The ways in which the insurgents are

exploiting the tribal network does not represent an evolved form of insurgency but the expression of inherent cultural and social customs (McCallister 2005). The social dynamic that sustains the on-going fighting in Iraq is best understood when considered in tribal terms, from the perspective of a traditionally networked society. It is the traditional tribal network that offers insurgents a ready made insurrectionary infrastructure to draw on (McCallister 2005).

The full functioning of a network depends on how well, and in what ways, the members are personally known and connected to each other. This is the classic level of social network analysis, where strong personal ties, often ones that rest on friendship and bonding experiences, ensure high degrees of trust and loyalty (Ronfeldt and Arquilla 2001). To function well, networks may require higher degrees of interpersonal trust than do other approaches to organization, like hierarchies. Kinship ties, be they of blood or brotherhood, are a fundamental aspect of many terrorist, criminal, and gang organizations. For example, news about Osama bin Laden and his al Qaeda network reveal his, and its, dependence on personal relationships he formed over the years with "Afghan Arabs" from Egypt and elsewhere who were committed to anti-United States terrorism and Islamic fundamentalism (Ronfeldt and Arquilla 2001).

This last point raises the issue about the link between Saddam Hussein and al Qaeda. In the minds of many Americans, Saddam and al Qaeda are coupled. This is also the view of many service members serving in Iraq. In a recent poll, 85 % of surveyed military members presently in Iraq said the U.S. mission is mainly "to

retaliate for Saddam's role in the 9-11 attacks," and 77 % said they also believe the main or a major reason for the war was "to stop Saddam from protecting al Qaeda in Iraq" (Zogby International 2006). From my own standpoint, it is certainly apparent that Saddam Hussein and al Qaeda were linked by a common orientation – that is, a hatred and disdain for the West and Israel. Beyond that, I know of nothing one way or the other about how the two are linked.

The relationship between Saddam Hussein and al Qaeda aside, the rise of networks means that power is migrating to non-state actors, because such actors are able to organize into sprawling multi-organizational networks more readily than can traditional, hierarchical, state actors. There is a new realm of sovereignty-free actors (Burk 1998). Multinational corporations, ethnic groups, bureaucratic agencies, ideologies, transnational societies, political parties, international organizations, and even sub-national social movements inhabit this realm. Such entities are not bound by the traditional concerns of states, yet they have sufficient resources to initiate global action on their own authority, and have enough power to affect the course of global affairs (p. 28).

A series of networked enclaves could, then, become a dominant political actor within a state, or group of states. Thus, rather than violently and directly competing with a nation-state, an unconventional non-state actor can indirectly and criminally co-opt and seize control of the state (Manwaring 2005, p. 17). This occurs if the unconventional attacker – terrorists, drug cartels, criminal gangs, or a combination of such actors – blends crime, terrorism, and war thus extending its already significant

influence. This problem becomes compounded if the attacker is able to embrace advanced technology along with more common weapon systems. The attacker can then transcend drug running, robbery, kidnapping, and murder and pose a significant challenge to the nation-state and its institutions. Using complicity, intimidation, corruption, and indifference, the unconventional attacker can quietly and subtly co-opt individual politicians and government officials to gain political control of a given geographical area or political enclave. In the end, such corruption can lead to the emergence of a virtual criminal state or political entity (Manwaring 2005).

A truly non-state actor like al Qaeda cannot, in theory, be deterred because it has no easily located headquarters. Without the possibility of deterrence there is not, in theory, anything that can limit its action. Such actors are an abhorrence to governments simply because they cannot be controlled, at least not by the usual tools that governments have at their disposal. Nor are terrorists generally responsible to those they claim to represent, because they often operate on a criminal or extortionist basis. Thus, they are not controllable within the international system (Friedman 2003).

As a consequence, there are no formal declarations of or terminations of conflict; no specific territory to take and hold; no single credible government or political actor with which to deal; and no guarantee that any agreement between or among contending groups will be honored. In short, the battle space is everywhere, and includes everything and everyone (Manwaring 2005, p. 5). Consequently, power is no longer only combat firepower or police power. These unconventional non-state

wars can be identified by their ultimate objectives or by their results. They are the organized application of coercive military or non-military illicit methods – lethal or non-lethal, direct or indirect, or a mix of both – intended to resist, oppose, gain control of, or overthrow an existing government or symbol of power and bring about fundamental political change (p. 8).

### Conclusion

The fight for the future makes daily headlines. Its battles are not between the armies of leading states, nor are its weapons the large, expensive tanks, planes and fleets of regular armed forces. Rather, the combatants come from violent terrorist networks like Osama bin Laden's al Qaeda, Abu Musab al Zarqawi's insurgents, and drug cartels like those in Colombia and Mexico. Other protagonists - ones who often benefit U.S. interests - are networked civil-society activists fighting for democracy and human rights around the world (Ronfeldt and Arquilla 2001). They prefer to rely on tactics of indirect irregular or guerilla warfare or on episodic acts of terrorism, counting on these to wear down the will and strength of their adversaries (Burk 1998).

In our own history, the United States operated in a similar fashion during the American Revolution. We also faced it in the Indian Wars and the Philippine Insurrection. While we have preferred, prepared for, and celebrated linear war, we also have a history characterized by “unconventional non-state wars.” George Washington was foremost among those Americans who sought to import European, linear models of war, and he modeled his Continental Army as closely as possible

after the rival British armies. However, since Washington's army was limited in personnel, resources, and the time to train up, he soon realized that committing his troops to open battle against the British would invite disaster (Cassidy 2004). Acknowledging these limitations, Washington adopted an indirect strategy of attrition, whereby he avoided general actions against the British main body, but instead concentrated what forces he had against weak enemy outposts and piecemeal detachments. Thus, he employed an unorthodox and asymmetric approach because of incongruous strategic realities (p. 87).

In the Global War on Terrorism, one of the greater challenges for the United States is that it is opposed by a fully mobilized, traditionally networked, very tribalized enemy. What the insurgency possesses is an unassailable base guarded against direct attack. This unassailable base is the social network itself, merging and diverging as the situation dictates (McCallister 2005). The answers to what motivates and sustains such an insurgency are not readily found in traditional insurgency literature. Much better answers can be found by reexamining the dynamics of traditionally networked tribes and clans, or within the sociological prescriptions offered by social network analysis and the theory of Georg Simmel. It is in Simmel's treatment of affiliations that we find the core concepts of networks and linkages – i.e., the crux of the non-linear organization that characterizes present insurgency conceptions. It is by identifying patterns in the non-linear that we begin to understand the organization at hand. Related, with respect to clan-like organizations,

it is Simmel who profoundly outlined a conceptual understanding of how such familial associations impact an individual:

In primitive clan-organizations the individual would participate in several groups in such a way that he belonged to the kinship or totemic group of his mother, but also to the narrower, familial, or local association of his father...With peculiar purposefulness these two kinds of association are therefore so differently arranged that they do not encroach upon each other. Relationships on the maternal side have a more ideal, spiritual nature, whereas on the paternal side they are real, material, and directly effective (Simmel 1908/1955, p. 142).

The modern insurgency represents an evolved form of warfare that takes into consideration the fact that tribal societies have at their disposal pre-existing affiliated social, economic, and military networks easily adapted to warfighting, and these extend across traditional boundaries and borders. This is a trend for the future.

## CHAPTER 5

### METHODS

This project uses the intelligence data that were gathered in Iraq that led to the capture of Saddam Hussein on the basis of an intuitive and informal analysis of Saddam's social networks. In order to gather relevant data for analysis, I have several sources/archival records available to me. First is the 1<sup>st</sup> Brigade Combat Team, 4<sup>th</sup> Infantry Division After Action Review.<sup>12</sup> This document contains pages of details outlining the information and intelligence collection gathering efforts, as well as relevant operational details, resulting in a description of the family and tribal linkages that led to the ultimate capture of the ousted Iraqi dictator. The second source available to me is the Saddam Hussein Link Diagram. This diagram has been declassified (thereby omitting some names and relationships). However, this is the original link diagram that shows the enormous network that surrounded Saddam, thus allowing for analysis of ties and other network properties. The final source of "data" available to me is open source data, specifically the history of the 4<sup>th</sup> Infantry Division's combat operations in Operation Iraqi Freedom, as well as media reporting (print, video, and web) on the events leading up to and surrounding the capture of Saddam Hussein.

Most network analyses are based on obvious sources of data regarding the nodes of the network, frequently by simply asking the network participants with whom they associate. However, we cannot do this with, for example, the resistance

---

<sup>12</sup> I will use only declassified information from this document.

in Iraq or al Qaeda in Afghanistan. In this sense, my work is unique because of the complexity of identifying a network and depicting network relationships of a group or organization that is not prone to a simple survey or interview. Such an approach, however, lends itself to data gathering effects in the findings. In other words, information gathering focused on a particular individual, or individuals, may result in findings skewed in favor of one's importance, and the lack of importance of others, when in reality this may not be completely true.

The intended result of this project is a description of those concepts and methods that are useful, and those that are not, for analyzing the Saddam Hussein network. The endstate is a systematic, network approach for understanding an insurgent network. Procedurally, my analysis consists of four steps:

1. Disaggregate the relationships.
2. Analyze the general network measures for each relationship.
3. Analyze measures for each actor in each relationship.
4. Conduct a role analysis for each relationship.

For the first step, I disaggregated the network according to the relationships outlined in Table 1. I adapted these from Krebs' (2002) work on the 9/11 hijacker network. With the 9/11 hijackers, in order to impose some degree of order on the covert network, one first needed to identify the trust and task ties between the conspirators. Likewise, I take a similar approach in order to formalize the informal relationships of Saddam Hussein's network. The trust ties include those defined by

CODE	RELATIONSHIP	MEANING	DATA SOURCES
	<i>TRUST</i>	<i>These are relationships forged over time via family, tribe, or village. These also include time spent together in the military, school, or various organizations (both social and political).</i>	<i>Prior contacts in family, neighborhood, school, military, club or organization.</i>
<b>10-19</b>	<b>Immediate Family</b>		
10	Father		
12	Mother		
13	Husband		
14	Wife		
15	Son		
16	Daughter		
17	Brother		
18	Half-Brother		
19	Sister		
<b>20-29</b>	<b>Extended Family</b>		
20	Father-in-law		
21	Mother-in-law		
22	Sister-in-law		
23	Brother-in-law		
24	Cousin		
25	Niece		
26	Nephew		
27	Aunt		
28	Uncle		
29	Son-in-law		
<b>30-39</b>	<b>Close Friend</b>		
30	Former Regime Official		
31	Tribe or village association		
32	School, military, or political association		
<b>40</b>	<b>Bodyguard</b>		
	<i>STRATEGY AND GOALS</i>	<i>These are relationships forged by active resistance and support against the current Iraqi government and its coalition sponsor.</i>	<i>Logs and records of phone calls, electronic mail, chat rooms, instant messages, web site visits; travel records; observation of meetings and attendance at common events; bank account and money transfer records; pattern and location of credit card use; videos and encrypted disks delivered by courier; travel records; observation of meetings and attendance at common events.</i>
<b>50</b>	<b>Money and Resources:</b> Provides money, weapons, transportation, housing, communication assets; provides information on coalition forces; recruits attackers.		
<b>60</b>	<b>Insurgent Operations:</b> Plan and execute attacks/activities, decision maker, leadership.		

Table 1: Mapping Networks

immediate family, extended family, close friendships, and bodyguards. The task ties I broadly renamed as strategy and goals to reflect the more insurgent orientation of the network. These ties include money and resources and insurgent operations.

I coded each depicted relationship – designated by a tie, or line, from one node to another – in accordance with one of these relationships. Additionally, the relationships are not mutually exclusive. In other words, while two actors may be linked by trust (they are brothers), they may also be linked via strategy and goals (they are both active in insurgent operations).

Next, I analyzed each relationship along four general network measures: network size, density, transitivity, and cliques. Since actors and the connections among them define a network, it is useful to begin a description of networks by examining these very simple properties. Focusing first on the network as a whole, one might be interested in the number of actors, the number of connections that are possible, and the number of connections that are actually present. Differences among individuals in how connected they are can be extremely consequential for understanding their attributes and behavior (Hanneman and Riddle 2005). More connections often mean that individuals are exposed to more diverse information. Highly connected individuals may be more influential, and may be more influenced by others. Thus, there are good theoretical reasons to believe that these basic properties of social networks have very important consequences.

The size of a network is often very important. It is the number of direct ties involving individual units (Marsden 1990). The size is critical for the structure of

social relations because of the limited resources and capacities that each actor has for building and maintaining ties (Hanneman and Riddle 2005). Density is the extent to which links that could possibly exist among persons do in fact exist (Mitchell 1969). It is the proportion of possible lines actually present in the graph, or the ratio of the number of lines present to the maximum possible. Measuring the density of the network gives us a ready index of the degree of dyadic connection in a population.

Transitivity is a key structural property in social network data (Wasserman and Faust 1994). Because of transitivity, two linked network members often draw others with whom they are linked into a cluster of ties in which most members are linked with each other (Wellman 1983). For the triad involving actors  $i$ ,  $j$ , and  $k$ , it is transitive if whenever  $i$  is to  $j$  and  $j$  is to  $k$ , then  $i$  is to  $k$ . Some small group theorists argue that many of the most interesting and basic questions of social structure arise with regard to triads (Hanneman and Riddle 2005). Triads allow for a much wider range of possible sets of relations. Some also argue that transitive or balanced triads are the "equilibrium" or natural state toward which triadic relationships tend (Hanneman and Riddle 2005). The existence of the third element may directly start or strengthen the union of the other two thereby serving as a mediator or arbitrator wishing to save the group from the danger of splitting up (Simmel 1950).

On the other hand, Simmel also suggests that triads are the most unstable social units and that the appearance of a third party (to a dyad) indicates transition, conciliation, and abandonment of absolute contrast (p. 145). A third party allows for the potential exploitation of the others for one's own purposes and gives rise to shifts

in power and influence. The advantage of the third may result, for example, from the fact that the remaining two hold each other in check, and the third can then make a gain in which one of the other two might deny him/her. In the social life of well-consolidated groups, this may happen merely as one event among others. However, in forming groups or groups with a new member – that is, elements that have never formed an interactional unit – conflict may arise. A third element, which before was equally unconnected to the other two, may spontaneously seize upon an opportunity and thus an entirely unstable interaction will result (p. 154).

The idea of a clique is relatively simple. At the most general level, it is a subset of a network in which the actors are more closely and intensely tied to one another than they are to other members of the network (Hanneman and Riddle 2005). A clique is a collection of actors all of whom “choose” each other, and there is no other actor in the larger population who also “chooses” and “is chosen” by all of the members of the clique. Networks based on cliques, or the mutuality of ties, require that all pairs of members “choose” each other (or are adjacent).

In the third step, I analyzed the actors in each relationship in accordance with four measures: degree centrality, betweenness, eigenvector, and structural holes. I derived these actor measures from network research conducted on ego networks and centrality and power. With respect to the former, it is by studying ego networks that one gains an understanding of the variation in the behavior of individuals by taking a close look at their local circumstances. Describing and indexing the variation across individuals in the way they are embedded in "local" social structures is the goal of the

analysis of ego networks (Hanneman and Riddle 2005). When considering centrality and power, the network approach emphasizes that power is inherently relational. An individual does not have power in the abstract, but instead one has power because he/she can control others. Because power is a consequence of patterns of relations, the amount of power in social structures can vary.

In order to find the most important actors, we need to look for measures reflecting which actors are at the “center” of the set of actors. Central actors must be the most active in the sense that they have the most ties to other actors in the network. The degree of a node is the number of lines that are incident with it. It is a count that ranges from a minimum of 0, if no nodes are adjacent to a given node, to a maximum of  $g-1$ , if a given node is adjacent to all other nodes in the network. An actor with a high centrality level, as measured by its degree, is “where the action is” in the network. Thus, this measure focuses on the most visible actors in the network. An actor with a large degree is in direct contact or is adjacent to many other actors. This actor should then begin to be recognized by others as a major channel of relational information – a crucial cog in the network, occupying a central location. In contrast, actors with low degrees are clearly peripheral in the network. Such actors are not active in the relational process (Wasserman and Faust 1994, pp. 179-180).

Betweenness involves the idea that interactions between two nonadjacent actors might depend on the other actors in the set of actors, especially the actors who lie on the paths between the two. These “other actors” potentially might have some control over the interactions between the two nonadjacent actors. An actor is central

if he/she lies between other actors on their geodesics, implying that to have a large “betweenness” centrality, the actor must be between many of the actors via their geodesics (pp. 188-189).

The eigenvector describes a certain aspect of centrality or status that is not captured by other measures. The eigenvector is an appropriate measure when one believes that an actor’s status is determined by those with whom they are in contact (Bonacich and Lloyd 2001). Eigenvector centrality is best understood as a variant of simple degree. It is not just how many people a person knows that counts, but how many people the people that they know knows (Alexander 1963).

Finally, structural holes separate non-redundant sources of information. These holes in social structure create a competitive advantage for an individual whose relationships span the hole(s). The structural hole between two groups does not mean that people in the groups are unaware of one another. It only means that the people are focused on their own activities such that they do not attend to the activities of people in the other group. People on either side of a structural hole circulate in different flows of information. Structural holes are thus an opportunity to broker the flow of information between people and control the activities that bring together people from opposite sides of the hole (Burt 2001).

My last analytical procedure is a role analysis for each relationship. This consists of three measures: structural equivalence, automorphic equivalence, and multiplexity. In contrast to most social network methods that focus on the properties of actors or the subsets of actors, network role analysis focuses on associations among

relations. Beginning with a set of network data consisting of a collection of relations, the ultimate goals are to “group” actors into positions based on their relational similarity, and simultaneously to describe the association among relations based on how they combine to link actors or positions (Wasserman and Faust 1994).

With structural equivalence, two actors are structurally equivalent if they have identical ties to and from all other actors in the network (p. 356). In terms of the structural information in a network, if two (or more) actors are structurally equivalent, then there is no structural (i.e., network) information pertaining to one actor and not to the other. Automorphic equivalence is based on the idea that equivalent actors occupy indistinguishable structural locations in a network (p. 469). Two actors are automorphically equivalent if and only if there is some automorphism that maps one of the actors to the other. Two nodes that are automorphically equivalent have the same in-degree, the same out-degree, the same centrality on every possible measure, belong to the same number and size of cliques, and so on. The only thing that can differ between automorphically equivalent nodes is the “names” or “labels” attached to them. Nodes that are automorphically equivalent are structurally indistinguishable when labels are removed from the graph (p. 472). In other words, the positions are interchangeable. Automorphic equivalence is more general than structural equivalence. Actors that are structurally equivalent are also automorphically equivalent, but the reverse is not necessarily true.

Multiplexity is the extent to which two actors are linked together by more than one relationship. Ties between actors can be assessed by the number of different

types of exchanges they engage in, and by the type of exchange. Studies of multiplexity in mediated environments suggest three combinations of ties and exchange relations that may be important in work environments: diffuse, weak ties oriented toward general group communication and instrumental exchange; specific, stronger task-focused ties oriented toward production; and specific, emotional support ties oriented toward interpersonal contact (Haythornthwaite 1999).

## CHAPTER 6

### THE CASE STUDY – THE NETWORK OF SADDAM HUSSEIN

Why have the members of the insurgency assumed a network form? Why do they remain in that form? Networks, like other forms of organization, are held together by the narratives, or stories, that people tell (Ronfeldt and Arquilla 2001). These narratives provide a grounded expression of people's experiences, interests, and values. They express a sense of identity and belonging - of who "we" are, why we have come together, and what makes "us" different from "them." These narratives communicate a sense of cause, purpose, and mission. They express aims and methods as well as cultural dispositions - what "we" believe in, and what we mean to do, and how. The right story can thus help keep people connected in a network whose looseness makes it difficult to prevent defection. The right story line also can help create bridges across different networks. The right story also can generate a perception that a movement has a winning momentum – that time is on its side (Ronfeldt and Arquilla 2001).

The tribal ethos influences all aspects of life in modern Iraqi society. The fundamental aspect of tribal identity is extended kinship. The tribe is the largest unit whose associated clan claims a common lineage or descent. But the tribe is more than just a number of descent-based groups, for an individual's stated membership in a particular genealogical heritage can be partly a political act. Much of tribal genealogy is often based on fictive kinship ties. In claiming a particular ancestry, individuals may align themselves with a given political position and strategy which

cannot simply be glossed over as kinship. Tribes exist in a perpetual state of flux. Associations and alliances shift and individuals may move across permeable boundaries. In this sense, tribal identity is flexible since it incorporates an invented quality that provides a context for political and social action (McCallister 2005).

The clan is the second level of organization in Iraq and derives its unity of purpose from its Sheikh, his family lineage, and the territorial proximity of the various sub-clan affiliates of which it is composed. Sub-clans are a composite of patrilineal groups and extended families. These in turn are composed of kinship groups and divided into households. The tribe and clan perform a political and military function, sub-clans and households an economic one. Leadership is traditionally reserved to the outstanding patrilineal lineage of the strongest sub-clan, with the strongest clan providing the leadership of the tribe. In the case of a pan-tribal confederation, the strongest tribe holds the Sheikh of Sheikh position. In a world of perpetual conflict, weaker tribes will seek security through alliances with larger, stronger ones (McCallister 2005).

Marriage is an important community event in Iraq in that it unites two kin groups. Islamic law makes marriage essentially a private agreement between two families and it does not require any ceremony, either religious or civil, for the marriage contract to be valid. Additionally, there is no registration of marriage either with civil or religious authorities. Thus, marriage is essentially a social and familial matter in which the state has no jurisdiction (Charrad 2001). Important, however, is

the impact that marriage has on uniting tribes, clans, and/or households that allows for present and future alliances.

As a process of group formation driven by an issue at hand, members of a tribe, or members of one of its segment, would join together for collective action. Which segments of the tribe unite depends on the subject and context of conflict. Different issues require different political alignments and, therefore, call for the coming together of different parts of the tribe. The operational group might be restricted to a clan within the tribe, or a lineage within the clan, while at other times it might involve several clans or lineages. All the clans that constitute a tribe usually unite in matters that concern the whole tribe. Some tribes might form tribal confederations for specific purposes, usually to enhance their ability to oppose a common enemy (Charrad 2001).

#### The Background and Rise to Power of Saddam Hussein<sup>13</sup>

The death of President Gamal Abdel Nasser of Egypt in 1971 marked the beginning of a new era in contemporary Arab politics, exemplified by men like Hafez al-Assad in Syria and Saddam Hussein in Iraq (Musallam 1996). While they paid lip service to party slogans, these leaders abandoned any serious pretence of an ideological crusade, assuming a realist position as they came to understand how much their countries (and they themselves) might gain by pursuing their own narrow political and national interests. Saddam Hussein has been at the center of politics in

---

<sup>13</sup> The purpose of this section is not to outline in detail the life and political rise to power of Saddam Hussein, but rather to provide background and highlight some of the intricacies of his family lineage and ties. A more detailed analysis of Saddam's relationships takes place in subsequent chapters of this project.

Iraq for a quarter of a century. For eleven years, he was the country's second highest official, and until his ouster in 2003, he was Iraq's undisputed leader. Saddam's rise to power was remarkable. It was characterized by tenacious perseverance, skillful manipulation, and merciless elimination of rivals (Karsh and Rautsi 1991). How he succeeded as long as he did is a tale of patient hard work, unprincipled manipulation of allies and enemies alike, and, surprisingly, genuine support from colleagues and many ordinary people in Iraq who admired his abilities (Henderson 1991).

Saddam was born on 28 April 1937 in the village of al-Ouja near the town of Tikrit, which lies on the banks of the Tigris River, about 100 miles north of Baghdad. Saddam's mother, Subha Talfah, was a member of the local Talfah family. His father, whom Saddam never knew, was Hussein Addul Majid, from the local al-Majid family. On his mother's side, and perhaps on his father's as well, Saddam was part of the local Begat clan of the Albu Nasser tribe (Henderson 1991).

He had a fatherless childhood. Some reports claim that his father died before his son was born, while others allege that the father simply abandoned his wife and child (Musallam 1996). In either case, Saddam's mother re-married. Her new husband was the already married Ibrahim al-Hussan (he was known locally as "Hassan the Liar"), a crude, brutal, and illiterate peasant who resented Saddam and abused him both physically and psychologically. Eventually, Saddam's relationship with his stepfather had deteriorated to the point where the young boy was either thrown out of the house or simply ran away. His relations with some members of his extended family were better, and he chose to move in with his uncle, Khairallah,

where life, although better, remained less than ideal. Khairallah often sent Saddam out to steal for him from the villagers – a habit that eventually landed Saddam, albeit briefly, in a juvenile detention facility.

The name *Saddam* comes from the Arabic meaning “to punch” or “to strike.” Saddam took his biological father’s first name as his own second name. However, instead of taking on the family name of al-Majid, he chose instead to call himself Saddam Hussein al-Tikriti, meaning “from the town of Tikrit.” Thus, other people using the name al-Tikriti are not necessarily direct relatives of Saddam (Henderson 1991). To be sure, however, there was nothing remarkable about the Tikrit into which he was born. The town’s residents, Sunni Arabs, earned their modest living by manufacturing round rafts made of inflated animal skins. Not only did the town lack paved roads, electricity, or running water, but the appalling health and sanitary conditions made physical survival a demanding task. The survival of the fittest was, literally, a reality for Saddam from the first moment of his life (Karsh and Rautsi 1991).

Despite this impoverished upbringing, Saddam Hussein waged a ceaseless campaign of self-improvement, despite tremendous difficulties and challenges (Musallam 1996). Even the very first years of his schooling were achieved in the face of his family’s objections, and despite a long distance between his home and his school. However, according to Saddam Hussein himself, the most important decision in his life was the one in 1955 that took him to Baghdad. It was here that he began his early career in the Ba’th party as one of its leading assassins. When the Ba’th

party lost control of Iraq and fell out of power, Saddam went underground and was imprisoned for a period of time. In 1968, the Ba'th party regained power and introduced a new leader, President al-Bakr, a fellow Tikriti and a relative of Saddam Hussein. The new president entrusted Saddam with the task of ensuring at all costs that the Ba'th party stayed in control this time, thereby giving him one of the highest positions in the party.

While the exact events surrounding his take-over of power remain unclear, Saddam Hussein became the President of the Republic of Iraq on 16 July 1979 when President al-Bakr made a televised speech in which he announced his retirement from the presidency for reasons of health. Once his *de facto* presidency became official, Saddam wasted no time before openly and decisively taking steps to annihilate his few remaining rivals. Using allegations of a plot as the impetus, Saddam violently began to purge remnants of the previous government, thus taking revenge on old enemies, ridding himself of high-ranking party members who were not unreservedly his supporters, and at the same time rallying the country around him in a show of unity that served to consolidate his power (Musallam 1996). The purges were accompanied by organizational changes aimed at further tightening Saddam's grip on the reins of power. On the day he assumed power he merged several cabinet ministries, replaced eight ministers, and created the post of First Deputy Premier and five posts of Deputy Premier (Karsh and Rautsi 1991). All were filled by family members and relatives, or close friends and associates who had risen through the Ba'th party ranks with him.

Before his fall from power, when writing about Saddam's family, one had to exercise extreme caution as such an undertaking could cause more fallout than writing about Iraqi military secrets (Henderson 1991). While the web of rivalry and secrecy was rooted in years of distrust and discord, much of the complexity surrounding Saddam and his family can be traced to 18 October 1988. It was on this date that his oldest son, Udai, killed one of Saddam's most trusted bodyguards. While accounts vary, one thing is definite – Saddam was furious about the attack. The dead man, like many presidential bodyguards at the time, was from one of Iraq's small Christian sects, the Chaldeans, and the president was perhaps fearful that his other bodyguards would be resentful to the point of mutiny unless Udai was punished (Henderson 1991). Again reports vary, but it is widely accepted that Saddam had roundly condemned his son for the killing, and perhaps also had beat his son. Likewise, Saddam's wife, Sajida, intervening on her son's side, was also reported to have been beaten.

Rumors aside, the death of the bodyguard affected power relationships among Saddam's close relatives, all of whom owed their positions of authority to kinship. Particularly sensitive was the situation of Adnan Khairallah, the minister of defense and Saddam's cousin and brother-in-law. Adnan had taken the side of his sister, Sajida, when Saddam had beaten her in his fury over Udai. Whether or not this was true, Saddam knew that Adnan would, in Arab tradition, stand by and defend his blood relatives. Could he now trust Adnan to fulfill both aspects of his duty: to make sure the military was prepared to defend the country, and to make sure the military

was not a threat to the regime (Henderson 1991, p. 85)? Apparently not. In May 1989, Adnan Khairallah, along with several others, was killed in a mysterious helicopter crash.

After Adnan's death, two other arms of Saddam's family renewed their competition for influence: his cousins, the al-Majids, and his half-brothers, the Ibrahims. Of the various branches of Saddam's family tree, the Khairallah branch had been rather short, and he clearly could no longer rely on them. The al-Majid and the Ibrahim branches were longer, and Saddam could play rival members off against each other. In fact, both arms had already become rivals in 1983 when Hussein Kamel al-Majid, then head of the presidential bodyguard, married Saddam's oldest daughter, Raghad. This was a match of which the Ibrahims disapproved, and thus began their fall from grace. Another reason for this fall may have been their increasing greediness, especially that of Barzan. Although Iraqi law strictly prohibits bribe taking by officials, Saddam had to tolerate a large measure of corruption from those in his closest circles as a way of maintaining their loyalty (Henderson 1991, p. 86). Eventually, the three Ibrahim brothers vanished from the public eye.

Once the Ibrahims were out of the capital, the al-Majids had a relatively wide-open field in which to advance. Hussein Kamel's brother, also named Saddam, married the president's other daughter, Rina.<sup>14</sup> Another cousin, Ali Hassan al-

---

<sup>14</sup> For unknown reasons, Hussein Kamel and his wife, Raghad, defected along with his brother, Saddam Kamel, and his wife, Rina. Jordan granted them asylum, and there they began to cooperate with the United Nations Special Commission and the International Atomic Energy Agency. In 1996, after intermediaries for Saddam Hussein had assured them that all would be forgiven, Hussein Kamel and Saddam Kamel were convinced to return to Iraq with their wives. Reportedly (again, accounts

Majid<sup>15</sup>, was promoted to the head of the Ba'th party's northern bureau, which gave him wide party, military, and security powers. However, by 1998, Saddam decided that some of the al-Majids had become too prominent and thus began the rehabilitation of the Ibrahim brothers. Likewise, Saddam had to cope with the aspirations of his two sons, Uday and Qusai. As they matured, the issue of who would be heir apparent introduced further tensions in the family.

### Operation Iraqi Freedom

*Saddam Hussein and his sons must leave Iraq within 48 hours. Their refusal to do so will result in military conflict.*

*President George W. Bush  
17 March 2003*

The success of the United States-led coalition against Saddam Hussein's invasion of Kuwait in 1990 seemed certain in retrospect. The conditions of war that brought the coalition together and carried through the conflict were firm. The threat to regional stability, the global economy, and environmental security, as well as Saddam's desire for Kuwaiti and Saudi oil fields, solidified the clear and present danger of the moment (Fontenot et al. 2004). The result was an unambiguous charter for swift, staunch, and severe collective action against Iraq, culminating in the 100 hours of ground combat that expelled Iraqi forces from Kuwait and loosened Hussein's stranglehold on the Middle East.

During the 12 years following Operation Desert Storm, the deliberate preparation for operations against Iraq focused primarily on defensive preparations in

---

vary), upon their return, they were ordered to divorce their wives and were denounced as traitors. They refused to surrender to Saddam's security forces and were killed in a firefight at a safe house.

<sup>15</sup> Later, he was dubbed "Chemical Ali" for his use of poisonous gas against the Kurds in the late 1980s.

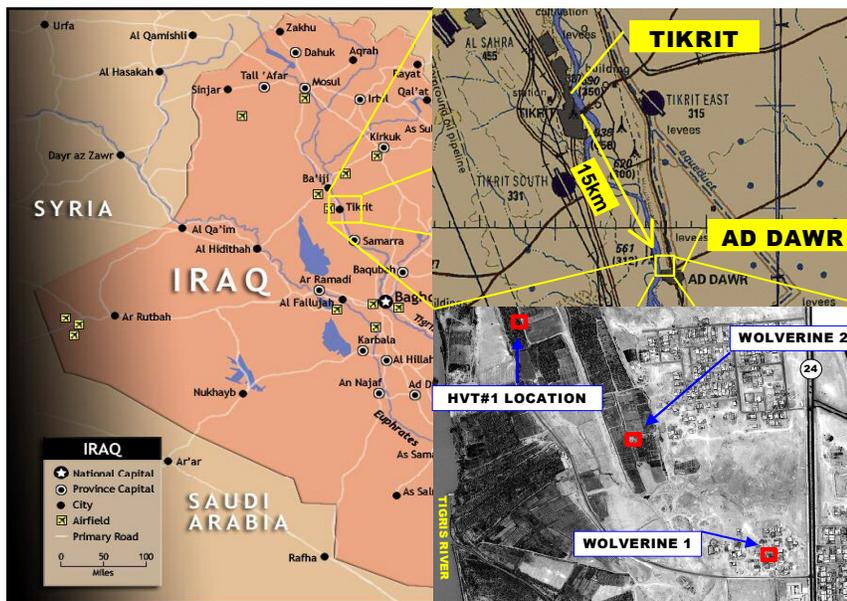
the event of a second Iraqi invasion of Kuwait, and operation of the northern and southern no-fly zones. The U.S. led coalition maintained a presence in the region to serve as a deterrent and to confirm U.S. commitment to the Kuwaiti people. When President Bush named Iraq as part of the “axis of evil” after the events of 9/11, it rekindled speculation about another war with Iraq. Slowly yet steadily, the nation moved ever closer to its second war of the 21<sup>st</sup> Century. Although U.S. forces remained engaged in combat operations in Afghanistan, the focus began to shift toward a possible offensive campaign to remove Saddam’s regime (Fontenot et al. 2004).

President Bush made the decision to launch Operation Iraqi Freedom on 16 March 2003 and issued an ultimatum with a 48-hour deadline on the 17<sup>th</sup>. That decision was the beginning of the end for Saddam Hussein and his regime. America’s strategic goal was embedded in the President’s numerous addresses – establish a free, democratic, prosperous, and non-threatening Iraqi state (Fontenot et al. 2004, p. 86). The first step in achieving that goal was removing Saddam Hussein’s Ba’thist regime, by force if necessary. The path from 17 March to Iraq’s new future started along the Kuwait-Iraq border, included the fall of Baghdad, the regime’s seat of power, and culminated with the capture of Saddam Hussein.

#### Operation Red Dawn

“We got him.” With those words, Ambassador Paul Bremer announced to the world that coalition forces had captured Saddam Hussein. This marked the culmination of months of intensive intelligence and operational work. In reality, the

raid to capture Hussein was nothing particularly spectacular. It was not marked by a great gun-battle between two opposing forces. There was no one dramatic event to mark the operation. When the sun came up on 13 December 2003, there was nothing particularly unique about that day. However, that evening, at approximately 8:26 local time, the enemy was caught off guard by an aggressive, determined and agile combined force. The climactic point of Operation Iraqi Freedom, Operation Red Dawn, was a textbook raid with all forces executing flawlessly and swiftly (Babcock 2005).



A general map of the region showing western Iraq, Tikrit, and Ad Dawr where coalition forces captured Saddam Hussein.

The operation took place in the vicinity of the town of Ad Dawr, just southeast of Tikrit and al-Ouja, the childhood home of Saddam Hussein. In the months leading up to the raid, a combination of human intelligence tips, detainee interrogations, and exceptional intelligence and analytical efforts narrowed down the activities of Saddam Hussein (DoD News Transcript 2003). This effort led the coalition to conduct the raid on 13 December on the rural farmhouse where Saddam was

ultimately apprehended. At about 10:50 that morning, coalition forces received intelligence on the possible whereabouts of the ousted dictator. Two likely locations were identified near the town of Ad Dawr – for operational purposes these locations were identified as Wolverine 1 and Wolverine 2. The 1<sup>st</sup> Brigade Combat Team,<sup>16</sup> 4<sup>th</sup> Infantry Division, in conjunction with Special Operations Forces, was assigned the mission to kill or capture Hussein.<sup>17</sup> At approximately 6:00 PM, under the cover of darkness and with lightening speed, the Raider Brigade forces were positioned and began movement toward the objective northwest of Ad Dawr (DoD News Transcript 2003). Time and surprise were vital. Experience taught that rapid exploitation of information about the enemy was important. Any window of opportunity between the moment the information was received and the time that the operation was executed could be just enough for the target of the raid to escape.

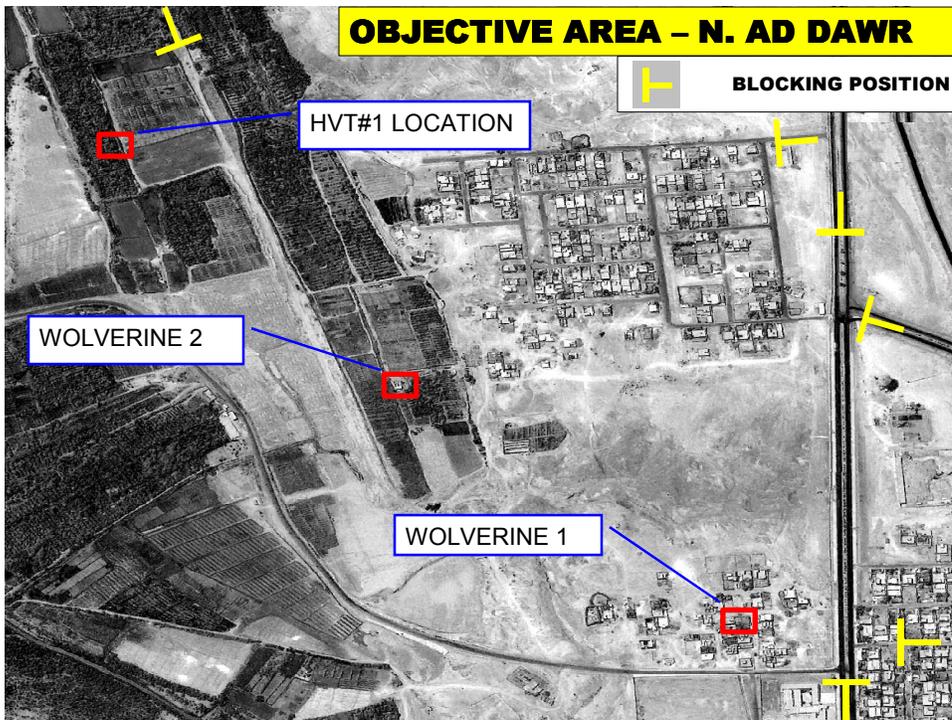
At approximately 7:45 that same evening, a coincidental, but extremely fortuitous power outage resulted in all of the lights going out in Ad Dawr and the surrounding area. With moonrise not until later, the city was completely dark, which aided in concealing the task force's movement as they entered the city. There was no civilian traffic along the main road into town. The force entered the objective area at 7:55 and had forces on Objectives Wolverine 1 and Wolverine 2 by 8:00 PM (Babcock 2005). There was nothing significant to report on either objective. As a result, commanders on the ground decided to cordon (i.e., seal-off) the area and begin an intensive search in the immediate locale. Subsequently, the forces on the ground

---

<sup>16</sup> This unit was also known as the Raider Brigade.

<sup>17</sup> Approximately 600 soldiers were involved in the operation.

identified a suspicious location to the northwest of Wolverine 2.<sup>18</sup> The area was a small walled compound with a metal lean-to structure, and a mud hut. During the search, a spider hole was detected. The spider hole's entrance was camouflaged with brick and dirt<sup>19</sup> (DoD News Transcript 2003).



Imagery of the objective area depicting Wolverine 1 and Wolverine 2. Saddam Hussein was captured at the site marked, "HVT#1 Location."

The assault team cleared the entrance to the hole of dirt, debris, and mats, and removed a styrofoam insert. The person inside of the hole put his hands in the air and responded to the question, "Who are you?" with "I am Saddam Hussein, the President of Iraq, and I am willing to negotiate." With that, a Soldier from the assault team

<sup>18</sup> The discovery of the location was largely due to a source. The source was a key member of Saddam Hussein's inner circle who was captured that morning in an un-related operation. The source led the assault team to a mud hut. One of the occupants at the location attempted to flee, but was detained. Another occupant vehemently denied knowing anything about Saddam Hussein and attempted to lead the assault team away from the objective. However, before he could do so, the source identified and pointed out the location of a potential hiding position near the edge of an orchard (Babcock 2005).

<sup>19</sup> The spider hole was about six to eight feet deep, and allowed enough space for a person to lie down inside of it.

responded with, “President Bush sends his regards,” and Saddam Hussein was pulled from the hole. After a search of the area, a helicopter landed and evacuated Saddam Hussein. By 8:15 PM, initial reports of “JACKPOT”<sup>20</sup> were sent to the Brigade Commander. At 8:26 “JACKPOT” was confirmed.

With the capture accomplished, much excitement and many challenges lay ahead, and while the capture of Saddam Hussein was certainly a significant event, it did not occur by happenstance or luck. It was the result of hard work and excellent intelligence gathering on the part of many people (Babcock 2005). It began when coalition forces realized that the key lay in figuring out the former Iraqi president's clan and family support structures in and around his home city of Tikrit (Loeb 2003). It was only through time and effort that a web of links and ties emerged. A pattern would form which would eventually allow coalition forces to launch Operation Red Dawn, and to be successful.



Photographs showing the mud hut and spider hole where Saddam Hussein was captured.

<sup>20</sup> This was the code-word indicating that Saddam Hussein was in custody.

## Identifying and Specifying the Network<sup>21</sup>

The capture of Saddam Hussein was the result of hard work and excellent intelligence gathering. Since its arrival in Iraq, the 1<sup>st</sup> Brigade Combat Team, 4<sup>th</sup> Infantry Division,<sup>22</sup> had been developing intelligence designed to find not only the Top 55<sup>23</sup> most wanted individuals, but to locate and kill or capture those providing the funding, coordinating opposition, and encouraging operations against coalition forces. Each day another piece of the puzzle fell into place, which led to more of the key players – both highly visible ones like Saddam Hussein, and lesser ones who did the daily work against coalition forces – being identified and located. Further, the Brigade began to build highly visual “link diagrams” that showed the structure of Saddam Hussein’s personal security apparatus and the relationships among the persons identified:

Maj. Gen. Raymond T. Odierno [Commander, 4<sup>th</sup> Infantry Division] said his analysts and commanders spent the summer building "link diagrams," graphics showing everyone related to Hussein by blood or tribe...Odierno said those family diagrams led his forces to lower-level, but nonetheless highly trusted, relatives and clan members harboring Hussein and helping him move around the countryside. The circle of bodyguards and mid-level military officers, drivers and gardeners protecting Hussein...was "kind of like a Mafia

---

<sup>21</sup> This section is an unclassified summary of how the 1<sup>st</sup> Brigade Combat Team, 4<sup>th</sup> Infantry Division “built” the Saddam Hussein network – that is, the series of link diagrams that literally connected the dots between Saddam and associates. Unless otherwise cited, this is an extract from Babcock’s work on the history of the division in Iraq – a compilation of interviews with those most closely involved in “piecing together the puzzle.”

<sup>22</sup> It is important to note that this was a team effort between the 4<sup>th</sup> Infantry Division Headquarters, Special Operations Forces, and the 1<sup>st</sup> Brigade Combat Team. The purpose of this section is not so much to highlight this effort, but rather the general process of how the network was pieced together. The Brigade’s Intelligence Officer, MAJ Stan Murphy, had oversight for this. That is why I often just mention the “Brigade” when describing this process, but, again, it was clearly a team effort and a great example of the utility of information sharing and cooperation.

<sup>23</sup> At the start of Operation Iraqi Freedom, the Department of Defense published a list of the Top 55 most wanted members of the Saddam Hussein regime, of which Saddam Hussein was Number 1 with his sons right behind him at Number 2 and Number 3.

organization -- it's built on hierarchy and who has access to the top man. It's not so much rank-oriented" (Loeb 2003).

In early July, the Brigade, having operated in the Tikrit area since April 2003, had a mountain of data in its database pertaining to Saddam Hussein, family members, close associates, and unrelated insurgents. It was a database that would increase ten-fold prior to the capture of Saddam. As the amount of information and intelligence increased, so did the analysis. Before long, the Brigade received a number of interrogation reports on one of the Top 55. From these reports, four names kept coming up and seemed to be linked. The Brigade's Intelligence Section took those names and compared them to what they already had and started making links out of them. In less than a week, those four names had grown to more than a hundred. In a month, the names and families filled a 36-inch by 36-inch sheet of paper and were difficult to understand at first glance. However, over time, the Brigade began to understand how each name was connected to the next.

This included "assigning" roles and positions to certain people within the network – for example, chief of staff, chief of operations, personal secretary, etc. These were not necessarily positions the individuals occupied prior to the fall of Hussein, but instead were based on our understanding of the role they were filling in support of the insurgency or Saddam's "underground" operations. We assigned these roles from our assessments of various personalities and recent intelligence and information reports. Such a process helped us focus our efforts in determining those who were closest to Hussein and their importance.

Over the days and months, our unit continued to track how the enemy operated. We tracked his trends and patterns, examined the tactics the enemy employed, and started to connect the enemy tendencies with the names and groups on our tracking charts. However, it was the capture of two key associates of Saddam Hussein on 7 November 2003 that confirmed for the Brigade that our template was accurate and that by continuing with the current operational focus, we would eventually succeed in capturing the ousted dictator. Meanwhile, the Brigade made minor adjustments to the template and kept looking at all of the critical data points to find what we may have missed.

Unfortunately, shortly after the apprehension of these key individuals, the information flow seemed to slow down. However, while staying aggressive, the Brigade kept looking for the one piece of missing information – no matter how big, or small – that could lead to breaking the enemy’s ability to continue the fight. Then, toward the end of November 2003, after several weeks of little to no new information relevant to Saddam and his network, a series of operational events led to an abundance of information and new intelligence about the resistance and the whereabouts of Saddam Hussein. The result of this latest intelligence was a series of raids, all designed to capture key individuals and /or leaders of the former regime that could eventually lead to the capture of Saddam. Each raid resulted in more information that led to the next raid. This cycle continued as a number of mid-level leaders of the former regime were caught eventually leading into the inner circle of those most trusted by Saddam.

## CHAPTER 7

### GENERAL NETWORK MEASURES

In this chapter I provide analysis and interpretation of Saddam Hussein's network using four general network measures: size, density, transitivity, and cliques. I do this first for the network as a whole, then for each of the mapping networks: trust (immediate family, extended family, close friend, bodyguard) and strategy and goals (money and resources, insurgent operations). Subsequent chapters provide the analysis and interpretation for the actor measures and the role measures.

Figure 3 depicts the Network of Saddam Hussein (also known as the Link Diagram). There are 214 nodes in the network.<sup>24</sup> I amended this document from the original, unclassified format by further deleting names, units, certain dates, and other information that I felt should not be made public. However, I did not delete or add lines between actors in order to amend relationships. All relationships are depicted as we originally identified them.

Prior to disaggregating the relationships in the Link Diagram, I first identified those actors with a direct tie to Saddam Hussein. My first substantive empirical finding is that there are only 23 actors with direct ties (see Table 2). Since our unit's objective was to locate Saddam Hussein, it follows that one of these 23 actors would be the most likely to know his location. Therefore, I plotted the networks of the 23 with direct ties to Saddam Hussein. In total, I defined 388 relationships. Figure 4

---

<sup>24</sup> Saddam Hussein is node A214 ("A" connotes "actor").

depicts Saddam’s 23 direct ties. Later figures present depictions of the network for each of the 23.<sup>25</sup>

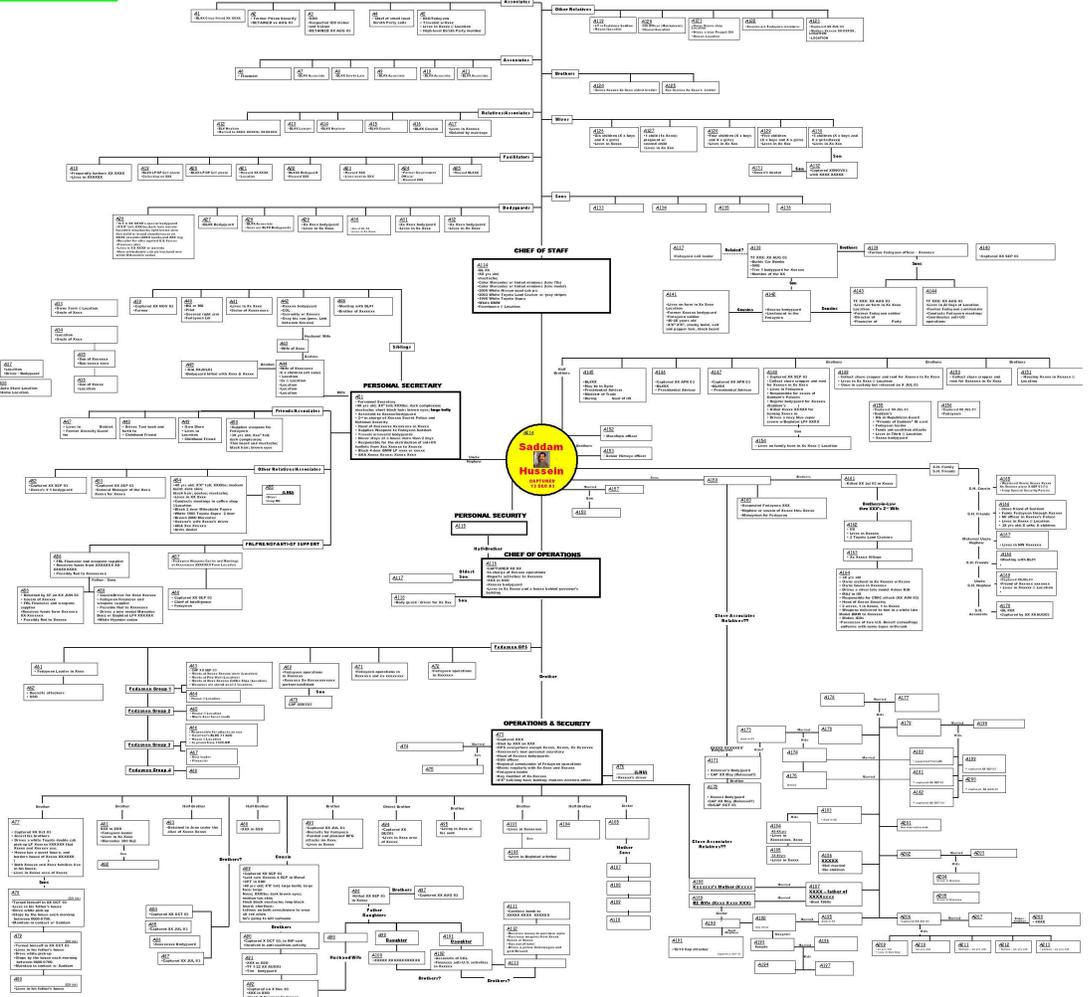
<b>NODE</b>	<b>RELATIONSHIP</b>	<b>NODE</b>	<b>RELATIONSHIP</b>
A114	Former Regime Official and Insurgent Operations	A51	Nephew and Insurgent Operations
A115	Tribe or Village Association and Insurgent Operations	A116	Tribe or Village Association and Insurgent Operations
A145	Half-brother and Insurgent Operations	A146	Half-brother and Insurgent Operations
A147	Half-brother and Insurgent Operations	A148	Half-brother and Insurgent Operations
A149	Half-brother and Money & Resources	A150	Half-brother and Money & Resources
A151	Half-brother and Money & Resources	A152	Half-brother and Bodyguard
A153	Half-brother and Insurgent Operations	A165	Cousin and Insurgent Operations
A166	Former Regime Official and Money & Resources	A167	Nephew
A168	School, Military, or Political Association and Money & Resources	A169	Nephew and Insurgent Operations
A170	School, Military, or Political Association and Insurgent Operations	A159	Son and Insurgent Operations
A161	Son and Insurgent Operations	A157	Wife
A158	Son		

Table 2: Direct Ties to Saddam Hussein

This analysis does not include all of the actors in the diagram since there are some without ties to the networks of the 23. There are seventeen actors to whom this applies. In some cases, these nodes are connected and have formed their own sub-networks. Most likely these represent insurgent groups that we obviously thought were important to track (for example, nodes A137 – A144). However, since the objective for this analysis is the capture of Hussein and they are not tied directly to his network, I did not define relationships for them.

<sup>25</sup> For all of these sub-networks, Saddam Hussein (A214) is depicted in green and the actor with the direct tie is depicted in blue.

UNCLASSIFIED



UNCLASSIFIED

Figure 3: Network of Saddam Hussein

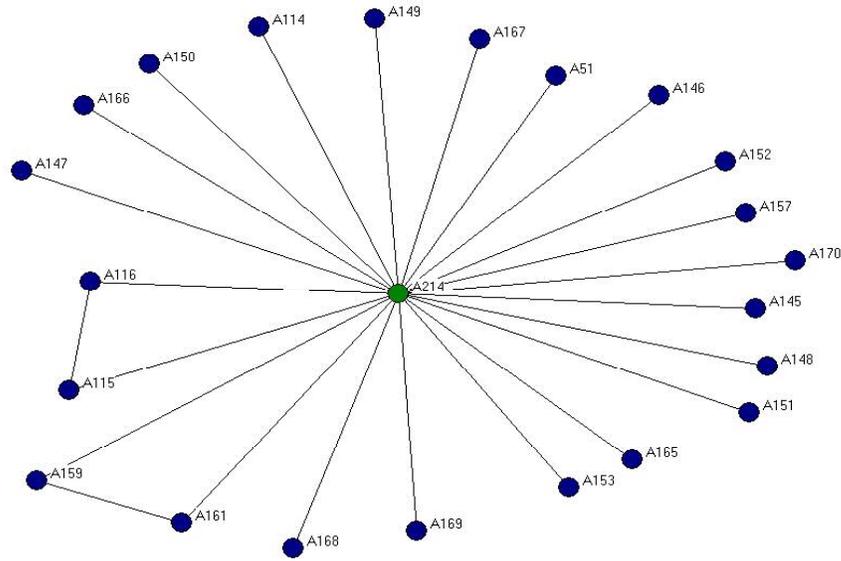


Figure 4: Saddam Hussein's 23 Direct Ties

I used UCINET 6 for Windows (Version 6.59) for all of my statistical analyses. Prior to any procedures, I coded the data in accordance with the relationships in Table 1. The codes in the table are additive and not mutually exclusive. Therefore, if *A* is related to *B* because *B* is the brother of *A*, and *B* is a leader in the insurgency, then the code depicting this relationship is 1760 where 17 is the code for “brother” and 60 is the code for “insurgency operations.”

Additionally, I reciprocated every trust relationship. For example, for a father-son relationship where *A* is the father of *B*, in addition to coding the data to reflect this stated relationship, I also coded the data to reflect the reciprocated relationship – that is, *B* is the son of *A*. The only exception to this rule is the “bodyguard” relationship since this is a one-way relationship (*A* is the bodyguard for *B*; *B* cannot be the bodyguard for *A*).

I entered my data into UCINET using the “EDGELIST1” format. This format is used to read in data forming a matrix in which the rows and columns refer to the same kinds of objects (for example, an illness-by-illness proximity matrix, or a person-by-person network). The 1-mode matrix  $X$  is built from pairs of indices (a row and a column indicator). Pairs are typed one to a line, with indices separated by spaces or commas. The presence of a pair  $i,j$  indicates that there is a link from  $i$  to  $j$ , which is to say a non-zero value in  $x_{ij}$ . Optionally, the pair may be followed by a value representing an attribute of the link, such as its strength or quality, or, in my case, by a category (Borgatti et al. 2002).

EDGELIST means that I specify a beginning and ending point for an arc or a line. Looking at the example from an extract of my data input, there is a trust link between A214 and A51 since A214 is the uncle of A51 (code 28). The second data line indicates the reciprocal link where A51 is the nephew of A214 (code 26).

```
dl n=388 format=edgelist1
labels embedded
data:
.
.
.
"A51" "A214" 28
"A214" "A51" 26
```

My coding procedure affords me flexibility in the analysis. Most importantly, I can be very precise in terms of the relationships I want to analyze. Equally, for the trust relationships, I can collapse the narrow categories into the more general categories under which each falls – that is, immediate family, extended family, and close friend. For the analysis that follows, I used this latter approach.

## The Network of Saddam Hussein

Focusing first on the network as a whole, there are 214 actors. Of these, 17 do not have ties to Saddam's immediate network: A33, A34, A35, A36, A37, A38, A137, A138, A139, A140, A141, A142, A143, A144, A155, A156, and A205. As a result, there are 197 nodes with defined relationships. The measure of a graph's components is a common statistical procedure in network analysis and a good starting point when establishing a frame of reference. Component analysis locates parts of the graph that are disconnected and gives us a sense of the fragmentation of the network. Components of a graph are sub-graphs that are connected within, but disconnected between sub-graphs (Hanneman and Riddle 1995). In this network, there is only one component. Thus, all considered nodes are connected, regardless of the direction of ties.

Density is used to quantify network "knittedness" (Wasserman and Faust 1994). The density of the overall network is 0.0100 – that is, 1 % of all the possible ties are present. Like other findings, this may be a result of how we collected and pieced together the information. Nonetheless, given the existing data, this is not a very dense network – a second important finding.

Transitivity gives us an idea as to the extent to which two linked network members draw others with whom they are linked into a cluster of ties. For this network, there are 59 cases where if  $AB$  and  $BC$  are present, then  $AC$  is also present. Considered another way, less than 2 % (1.89 %) of all relations that easily could be transitive are transitive. There are 3126 triples where  $AB$  and  $BC$  exist. Of these,

there are 3067 cases where one link could complete the triad *AC*. This indicates that most of the individuals in this network are not members of multiple social networks and, as a result, there are a minimum number of cross-linkages. This observation of low transitivity is my third important finding.

Formally, a clique is the maximum number of actors who have all possible ties present among themselves. In this case, there are two substantive empirical findings. First, in the Link Diagram, there are 11 cliques – a small number (see below). Second, there are no cliques with more than three members, which may indicate that a core group of individuals dominates the activities of and within the network. In fact, further analysis will show that most are family relationships.

1. A115 - A116 - A214
2. A159 - A161 - A214
3. A159 - A171 - A172
4. A174 - A175 - A178
5. A177 - A195 - A206
6. A187 - A188 - A73
7. A193 - A194 - A196
8. A193 - A196 - A197
9. A44 - A45 - A51
10. A56 - A58 - A59
11. A73 - A74 - A75

Recalling Simmel's perspective on triads and the potential for instability with the introduction of a third member, the triads above are less likely to undergo significant shifts in power and influence. These are not newly forming triads, but are rooted in a trust/family relationship. In other words, these triads are previously existing interactional units and are thus less likely to experience the exploitation of the others for one's own purposes.

	1	2	3	4	5	6	7	8	9	10	11
1	3	1	0	0	0	0	0	0	0	0	0
2	1	3	1	0	0	0	0	0	0	0	0
3	0	1	3	0	0	0	0	0	0	0	0
4	0	0	0	3	0	0	0	0	0	0	0
5	0	0	0	0	3	0	0	0	0	0	0
6	0	0	0	0	0	3	0	0	0	0	1
7	0	0	0	0	0	0	3	2	0	0	0
8	0	0	0	0	0	0	2	3	0	0	0
9	0	0	0	0	0	0	0	0	3	0	0
10	0	0	0	0	0	0	0	0	0	3	0
11	0	0	0	0	0	1	0	0	0	0	3

Table 3: Clique-by-Clique Co-Membership Matrix

Also, we can look at the extent to which the cliques overlap with one another. The UCINET output above (Table 3) reveals the number of actors that each clique has in common: for example, cliques 1 and 2 have one actor in common, cliques 7 and 8 have two actors in common, and so forth. Equally useful is a cluster analysis of the closeness of the cliques. The UCINET output below shows that cliques 7 and 8 are “tighter” than the others. Considered with the above, this is due to them having 2 actors in common (A193 and A196). However, this is additional evidence that the structure of the total network is very loose.

Level	1	2	3	4	5	8	7	9	0	6	1
2.000	.	.	.	.	.	XXX	.	.	.	.	.
1.000	XXX	.	.	.	.	XXX	.	.	XXX	.	.
0.667	XXXXXX	.	.	.	.	XXX	.	.	XXX	.	.
0.000	XXXXXXXXXXXXXXXXXXXXXXXXXXXX										

Table 4: Hierarchical Clustering of Equivalence Matrix

## Trust Mapping Networks

### Immediate Family Relationships

In the case of immediate family relationships, the previous section highlights the importance of family networks as resources that might be adapted to insurgent operations. Considering those relationships exclusively defined by a link between two actors due to an immediate family tie, there are 127 actors and 213 relationships. In this network, there are six components, or six sub-graphs that are connected within, but disconnected between sub-graphs. The density of the overall network is 0.0133 – that is, 1.33 % of all the possible ties are present.

For transitivity, there are 32 cases where if  $AB$  and  $BC$  are present, then  $AC$  is also present. In other words, 5.27 % of all relations that easily could be transitive are transitive. There are 607 triples in which  $AB$  and  $BC$  exist. Of these, there are 575 cases where one link could complete the triad  $AC$ . This indicates that most of the individuals in this network are not members of multiple social networks and, as a result, there are a minimum number of cross-linkages.

There are 7 cliques in this network (see below). All seven appear in the previous group of eleven. This indicates that immediate family relationships closely and intensely tie a central group of actors to one another, and that family relationships account for much of the previously identified clique structure – my sixth important finding.

1. A187 - A188 - A73 (clique 6 previously)
2. A73 - A74 - A75 (clique 11 previously)
3. A159 - A161 - A214 (clique 2 previously)
4. A174 - A175 - A178 (clique 4 previously)

5. A193 - A194 - A196 (clique 7 previously)
6. A193 - A196 - A197 (clique 8 previously)
7. A56 - A58 - A59 (clique 10 previously)

For this analysis, I also examined “inclusive” relationships – that is, those defined by immediate family and any other relationship (for example, money and resources or insurgent operations). There are 127 nodes and 266 defined relationships. The density of the overall network is 0.0166 – that is, 1.66 % of all the possible ties are present.

For transitivity, there are 42 cases where if  $AB$  and  $BC$  are present, then  $AC$  is also present. Thus, 4.13 % of all relations that easily could be transitive are transitive. There are 1018 triples where  $AB$  and  $BC$  exist. Of these, there are 976 cases where one link could complete the triad  $AC$ . Again, this indicates that most of the individuals in this network are not members of multiple social networks and, as a result, there are a minimum number of cross-linkages. Finally, the number of cliques for these “inclusive” relationships, and shared actors, is exactly the same as the “exclusive” immediate family. This is due to both subsets containing the same actors.

#### Extended Family Relationships

For those relationships exclusively defined by a link between two actors due to an extended family tie, there are 22 actors and 24 relationships. There are six components, or six sub-graphs that are connected within, but disconnected between one another. The density of the overall network is 0.0519 – that is, 5.19 % of all the possible ties are present. Additionally, this network is not transitive; none of the individuals in this network are members of multiple social networks; that is, there are

0 cases where if  $AB$  and  $BC$  are present, then  $AC$  is also present. Finally, there are no cliques in this network. Thus, the extended family is not woven very tightly.

I also examined those relationships that are “inclusive” – that is, those defined by extended family and any other relationship. In this case, there are 22 actors and 33 relationships. The density of the overall network is 0.0693 – 6.93 % of all the possible ties are present. Similar to the “exclusive” extended family relationship, this network is not transitive, and there are no cliques, again due to both groups containing the same actors.

#### Close Friend Relationships

For those relationships exclusively defined by a link between two actors due to a close friend tie, there are 29 actors and 38 relationships. There are three components, or three sub-graphs that are connected within, but disconnected between sub-graphs. The density of the overall network is 0.0503 – that is, 5.03 % of all the possible ties are present. Additionally, this network is not transitive; none of the individuals in this network are members of multiple social networks. In other words, there are 0 cases where if  $AB$  and  $BC$  are present, then  $AC$  is also present. Finally, there are no cliques in this network.

I also examined those relationships that are “inclusive” – that is, those defined by a close friendship and any other relationship. There are 29 actors and 50 relationships. The density of the overall network is 0.0616 – 6.16 % of all the possible ties are present. Finally, due to having the same actors as the exclusive relationship, this network also is not transitive, and there are no cliques.

### Bodyguard Relationships

Given the small number of total cases, I included all bodyguard relationships in this analysis. There are 13 actors and 13 relationships. Of these 13 relationships, 4 are inclusive – that is, the bodyguard relationship and some other relationship. There are three components, or three sub-graphs that are connected within, but disconnected between one another. The density of the overall network is 0.0641; 6.41 % of all the possible ties are present. Finally, as can be expected with such a small network, it is not transitive, nor are there any cliques.

### Strategy and Goals Mapping Networks

#### Money and Resources Relationships

For this network, there are 28 actors. In addition, there are only 28 total relationships defined by a money and resources link. Of the 28 relationships, money and resources exclusively define 12 of them. Given this small number of relationships, I included all of them in my analysis.

There are six components, or six sub-graphs that are connected within, but disconnected between sub-graphs. The density of the overall network is 0.0304 – that is, 3.04 % of all the possible ties are present. For transitivity, there is 1 case where if *AB* and *BC* are present, then *AC* is also present. Additionally, 25 % of all relations that easily could be transitive are transitive (there are 4 triples in which *AB* and *BC* are present; of these, there are 3 cases where one link could complete the triad, *AC*). Finally, there is one clique: A56 - A58 - A59. This is one of the immediate family triads identified earlier.

### Insurgent Operations Relationships

There are 71 actors and 71 relationships defined by insurgent operations. Of these 71, only 14 are exclusive to this relationship. Given this small number of exclusive cases, I analyzed all of the cases together. There are eight components, or eight sub-graphs that are connected within, but disconnected between one another. The density of the overall network is 0.0131 – that is, 1.31 % of all the possible ties are present. For transitivity, there are 2 cases where if  $AB$  and  $BC$  are present, then  $AC$  is also present. Additionally, 3.64 % of all relations that easily could be transitive are transitive (there are 55 triples in which  $AB$  and  $BC$  are present; of these, there are 53 cases where one link could complete the triad,  $AC$ ). Finally, there are 2 cliques: A115 - A116 - A214 and A159 - A161 - A214 (this also is one of the immediate family triads identified earlier). These cliques have A214 in common.

### Discussion

Table 5 summarizes the general network measures for the main network and each of the relationships.<sup>26</sup> In general, the network is not dense, nor transitive.<sup>27</sup> Of the sub-networks, the insurgent operations category is the most fragmented (8 components) and the least dense (1.31 density). There are 8 sub-graphs in which there is a path between all pairs of nodes in the sub-graph and there is no path between a node in the sub-graph and any node not in the sub-graph (Wasserman and Faust 1994). This validates what we know about resistance networks. Namely, these

---

<sup>26</sup> All categories depict the inclusive findings.

<sup>27</sup> The lack of density and transitivity in this network is not surprising given that this is a covert network. Members will only establish ties that are necessary.

networks are inherently dispersed with the result that they do not provide obvious centers of gravity. Likewise, from an information-gathering standpoint, resistance networks are characterized by incompleteness. There is an inevitability of missing nodes and links. The network may be more dense and less fragmented, but due to possible shortcomings in our data collection methodology we may not know this because of gaps in our construction of the network.

	<b># of Actors</b>	<b># of Relationships</b>	<b># of Components</b>	<b>Density (% of possible ties present)</b>	<b># of Transitive Cases</b>	<b>% of Possible Transitive Cases</b>	<b># of Cliques</b>
<b>Main Network</b>	197	388	1	1	59	1.89	11
<b>Immediate Family</b>	127	213	6	1.33	32	5.27	7
<b>Extended Family</b>	22	33	6	6.93	0	0	0
<b>Close Friend</b>	29	50	3	6.16	0	0	0
<b>Bodyguard</b>	13	13	3	6.41	0	0	0
<b>Money &amp; Resources</b>	28	28	6	3.04	1	25	1
<b>Insurgent Operations</b>	71	71	8	1.31	2	3.64	2

Table 5: Summary of General Network Measures

Of the trust relationships (discounting the bodyguard relationship due to the relatively small number of cases), the immediate family relationship is the least connected, within the limitations of our data. It has the most components (6) and the lowest density (1.33 %). The number of components is not surprising given the number of sub-categories along which membership can be linked – that is, father, mother, brother, sister, etc. Likewise, the low density of the network reflects the exclusiveness of the categories. A tie between a father and a son can only exist if one

is a father and the other is his son. On the other hand, the relatively high density of the close friend relationship highlights the broadness of the sub-categories in this network – that is, former regime official; tribe or village association; school, military, or political association. These categories are more inclusive and allow for more ties to form, or for the interpretation of a tie during the information gathering process.

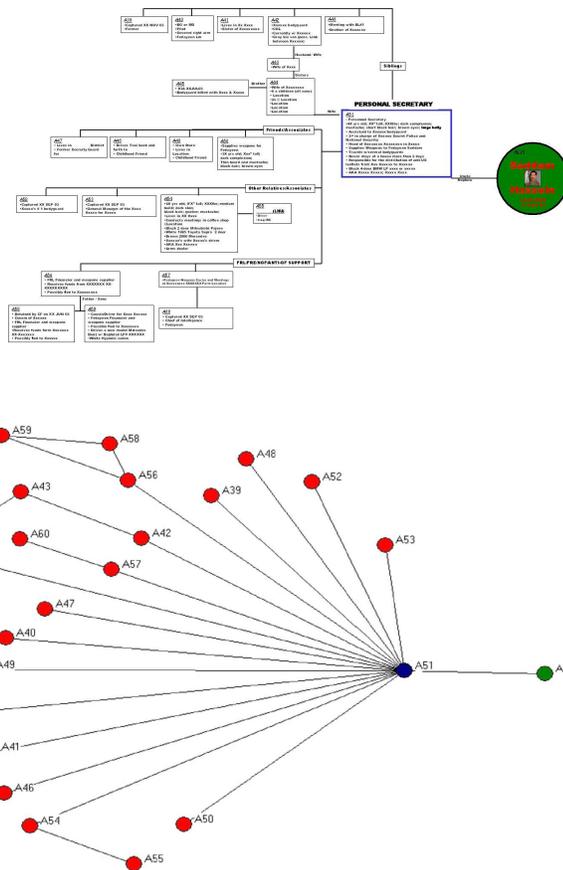


Figure 5: Personal Secretary (A51) Sub-Network

Two general network measures were very useful. First is the concept of transitivity. A normal part of life is that each of us belongs not to a single group of acquaintances but to many, within each of which everyone pretty much knows everyone else, but between which little interaction occurs (Watts 1999). Transitivity tells us that Saddam Hussein (A214) has ties with his personal secretary (A51). The personal secretary has ties with a Fedayeen weapons' supplier (A50). However, Saddam Hussein does not have a direct relationship with the weapons' supplier (see Figure 5 above). Therefore, in this case, when the objective is to capture Saddam Hussein, it is unlikely that the weapons' supplier will be able to provide any specific information as to the location of Hussein. Useful, however, is the location of the personal secretary, which the weapons' supplier may be able to provide due to the direct relationship between the two.

Of note is that 25 % of all possible relations that could be transitive are transitive for the money and resources relationship, while there are single digit percentages of possible transitive cases for everything else. One explanation for this is the smaller number of actors (28) for the money and resources relationship as compared to the other relationships with transitive cases: immediate family (127) and insurgent operations (71). A second reason pertains to the nature of the money and resources relationship itself. When supporting insurgent operations there exists a network of task ties where those providing resources have reason to know of one another and likely interact in order to sustain the resistance. A final reason may be

attributed to the data and how we collected and constructed the network. Again, when collecting information on a covert network, there are likely to be missing nodes.

Equally helpful is the idea of cliques. Looking at the network as a whole, there are 11 cliques of 3 members each. Five of these cliques are purely the result of immediate family relationships, one is due to money and resources and an immediate family relationship, one is due to insurgent operations and an immediate family relationship, and one is solely the result of ties involving insurgent operations.

Not only do cliques tell us which actors are closely tied to other actors, we also are able to discern which actors are in multiple cliques. Take, for example, the following two cliques:

1. A159 - A161 - A214
2. A159 - A171 - A172

With the capture of Saddam Hussein (A214) as our objective, it is sensible to focus on the clique of which he is a part. This clique includes his two sons (A159 and A161). One son, A159, is a member of another clique. By focusing on the two members of this other clique, we may be able to gather information as to the location of A159, which could lead to the capture of Hussein. However, after the death of the two sons in July 2003, this was no longer an option. Therefore, we would have to turn our attention to the only other clique of which Saddam is a part: A115 - A116 - A214. In this case, neither A115 (personal security) nor A116 (chief of operations) are part of multiple cliques. As a result, we would have to use other measures, such as transitivity, to locate a link to one of these actors in order to garner their assistance in determining the location of Saddam Hussein.

Another consideration when discussing cliques is that the strict clique definition (maximal fully-connected sub-graph) may be too strong for many purposes. It insists that every member or a sub-group have a direct tie with each and every other member. One alternative is to define an actor as a member of a clique if they are connected to every other member of the group at a distance greater than one. Usually, the path distance two is used. This corresponds to being "a friend of a friend." This approach to defining sub-structures is called  $N$ -clique, where  $N$  stands for the length of the path allowed to make a connection to all other members (Hanneman and Riddle 2005). Using this relaxed criteria, where  $N=2$ , there are 49 2-cliques for the entire network. Of these 49, only 7 contain Saddam Hussein (A214). When the objective is the capture of Saddam Hussein, such a measure is useful because it is more inclusive. However, the standard, more restrictive clique measure highlights those most closely tied to him.

In summary, there are six major substantive findings when analyzing the network using the general network measures. First, of the 214 actors in the total network, there are only 23 actors with direct ties to Saddam Hussein. Second is that the overall network is not very dense. Third is the low transitivity of the total network. Fourth, there are a small number of cliques, and fifth, no clique is larger than three actors. The last important finding is that family relationships account for much of the identified clique structure.

Finally, one finding of interest is the mean degree of separation for the actors in the network. The distances among actors in a network may be an important

characteristic of the network as a whole. Where distances are great, it may take a long time for information to diffuse across a population. It may also be that some actors are quite unaware of, and influenced by others – even if they are technically reachable, the costs may be too high to conduct exchanges (Hanneman and Riddle 2005).

In the case of the Network of Saddam Hussein, less the 17 without ties to main network – since they cannot lead to Hussein – the mean degree of separation, or average distance between actors, is 5.365. This means that the average distance between any pair of nodes is about 5 paths.<sup>28</sup> Thus, any one actor in the total network is connected to Saddam Hussein by on average 5 other distinct connections. Equally revealing is the percentage of actors who can reach Hussein in one step, two steps, etc.: 1 step – 12 %; 2 steps – 36 %; 3 steps – 38 %; 4 steps – 48 %; 5 steps – 58 %; 6 steps – 64 %; 7 steps – 72 %; 8 steps – 77 %; 9 or more steps – 80 %. Thus, almost half of the other network members are within four degrees of separation of Saddam Hussein, and about two-thirds are within six.<sup>29</sup>

---

<sup>28</sup> A path is a distinct sequence of nodes and lines, starting and ending with nodes, in which each node is incident with the lines following and preceding it in the sequence. For example, a path through a communication network means no actor is informed more than once. The length of a path is the number of lines in it. The shortest path between two nodes is referred to as a geodesic. The geodesic distance, or simply the distance, between two nodes is defined as the length of the geodesic between them (Wasserman and Faust 1994).

<sup>29</sup> A more complete analysis of the degrees of separation of network members from Saddam Hussein should include just the nodes that provided useful information in the capture. However, the classification of this information precludes such an analysis.

## CHAPTER 8

### ACTOR MEASURES

In order to find the most important actors, we need to look for measures reflecting which actors are at the “center” of the set of actors. The general network measures tell us about the overall demographics of the set of actors. The actor measures, on the other hand, give us insight into the most active actors by looking at the number and type of ties to others in the network. For this chapter, I provide the analysis and interpretation for the total network and each of the mapping networks using four actor measures: degree centrality, betweenness, eigenvector, and structural holes.

#### The Network of Saddam Hussein

With directed data it can be important to distinguish centrality based on in-degree from centrality based on out-degree. The in-degree of a node is the number of nodes that are adjacent to  $n$ , while the out-degree of a node is the number of nodes adjacent from  $n$  (Wasserman and Faust 1994). If an actor receives many ties (i.e., in-degree), he/she is often said to be prominent, or to have high prestige. That is, many other actors seek to direct ties to him/her, and this may indicate one’s importance. Actors who have an unusually high out-degree are actors who are able to exchange with many others, or make many others aware of their views. Actors who display a high out-degree centrality are often said to be influential actors (Hanneman and Riddle 2005).

My analysis of degree centrality shows that actor A114 clearly has the greatest out-degrees, and might be regarded as the most influential.<sup>30</sup> Actor A114 also has the largest in-degree. Given A114’s operational position in the overall network – he is the chief of staff – these findings are not surprising, but noteworthy. Figure 6 depicts A114’s network. Actor A214 (Saddam Hussein) has the same in-degree and out-degree and is second in ranking.<sup>31</sup> Intuitively, one might expect Saddam to be the most prominent and/or influential, but from what we know about organizations, the importance of the chief of staff is clear, and thus his influence in this case is not unexpected. This demonstrates the utility of in-and-out centrality in specifying prestige and influence and thus is my first substantive finding when considering the actor measures.

	OutDegree	InDegree
	-----	-----
A114	49.000	32.000
A214	23.000	23.000
A73	21.000	20.000
A51	17.000	11.000
A116	15.000	5.000
A177	10.000	10.000
A206	8.000	8.000
A198	6.000	6.000
A161	5.000	5.000
A96	5.000	5.000
A159	5.000	3.000
A105	5.000	5.000
A89	4.000	4.000
A187	4.000	4.000
A178	4.000	4.000
A77	4.000	4.000

Table 6: Main Network Degree Centrality Measures<sup>32</sup>

<sup>30</sup> It might matter to whom they are sending information. This measure does not take that into account.

<sup>31</sup> The positions of the other double-digit actors are: A73 – operations and security; A51 – personal secretary; A116 – chief of operations; A177 – not identified.

<sup>32</sup> For presentation purposes, I did not show the degrees of all nodes. The remaining nodes have in-degrees and out-degrees from 0 to 3.



marginally important actors, then the status of each would be lower (Wasserman and Faust 1994).

On the average, actors have a degree of 1.964. The range (minimum and maximum) of the out-degree (0 – 49) is larger than that of the in-degree (1 – 32), and there is more variability (standard deviation and variance) across the actors in out-degree (4.405 and 19.405) than in-degree (3.241 and 10.501).<sup>33</sup> The range and variability of degree are important because they describe whether the population is homogeneous or heterogeneous in structural positions. In this case, the population is more homogeneous with regard to in-degree (prominence) than to out-degree (influence).

With binary data, betweenness centrality views an actor as being in a favored position to the extent that the actor falls on the geodesic paths between other pairs of actors in the network. If we add up, for each actor, the proportion of times that they are "between" other actors, we get a measure of actor centrality. We can norm this measure by expressing it as a percentage of the maximum possible betweenness that an actor could have had (Hanneman and Riddle 2005). For this network, actor A214 (Saddam Hussein) has the highest betweenness, followed by A73 (operations and security), A116 (chief of operations), A114 (chief of staff), and A187 (not identified). Of these remaining four, A73, A116, and A114 have a direct connection to A214. Using this data, in conjunction with the link diagram (see Figure 3), the meaning of

---

<sup>33</sup> There are 33 nodes with an out-degree of 0, but they have an in-degree of 1. This means that they are not influential in the network, but have some very limited prominence.

A187's position becomes clear. While not having an identified position in the insurgency, his relationships link two family sub-networks.

The eigenvector approach is an effort to find the most central actors in terms of the "global" structure of the network, and to pay less attention to patterns that are more "local." Consider two actors, *A* and *B*. Actor *A* is quite close to a small and fairly closed group within a larger network, and rather distant from many of the members of the population. Actor *B* is at a moderate distance from all of the members of the population. In a sense, however, actor *B* is really more "central" than actor *A* in this example because *B* is able to reach more of the network with the same amount of effort.

The extract of the UCINET output below tells us how much of the overall pattern of distances among actors can be seen as reflecting the global pattern (the first eigenvalue), and more local, or additional patterns.<sup>34</sup> We are interested in the percentage of the overall variation in distances that is accounted for by the first factor. Here, this percentage is 9.5 %. This means that less than 10 % of all of the distances among actors are reflective of the main dimension or pattern.

In addition, the first eigenvalue should also be considerably larger than the second (here, the ratio of the first eigenvalue to the second is about 1.3 to 1). This means that the dominant pattern is, in a sense, 1.3 times as "important" as the secondary pattern. In short, this is a localized network where those on the periphery

---

<sup>34</sup> The first dimension captures the "global" aspects of distances among actors; second and further dimensions capture more specific and local sub-structures.

are “less connected” – that is, there are great inequalities in actor centrality.<sup>35</sup> This is an additional demonstration of what the initial analysis suggests.

FACTOR	VALUE	PERCENT	CUM %	RATIO
1	7.072	9.5	9.5	1.346
2	5.253	7.0	16.5	1.095
3	4.799	6.4	23.0	1.197
4	4.008	5.4	28.4	1.085
5	3.695	5.0	33.3	1.096
6	3.373	4.5	37.8	1.219
7	2.767	3.7	41.6	1.027
8	2.696	3.6	45.2	1.116
9	2.415	3.2	48.4	1.035
10	2.333	3.1	51.5	1.043

Table 7: Main Network Eigenvalues

When considering structural holes, one of the more useful measurements for this analysis is dyadic redundancy. This means that an actor’s tie to another is "redundant." If *A* is tied to both *B* and *C*, and *B* is tied to *C* then *A*'s tie to *B* is redundant, because *A* can influence *B* by way of *C*.<sup>36</sup> The dyadic redundancy measure calculates, for each actor in ego's network, how many of the other actors in the network are also tied to the other. The larger the proportion of others in the neighborhood who are tied to a given "alter," the more "redundant" is ego's direct tie (Hanneman and Riddle 2005). Actors who display high dyadic redundancy (about 0.7 and above) are actors who are embedded in local networks where there are few structural holes. Unfortunately, due to the large size of this network, the UCINET

<sup>35</sup> Approximately 70 % of the variation should be accounted for by the first factor for the network to be not localized (Hanneman and Riddle 2005).

<sup>36</sup> This also is a transitive relationship. However, transitivity is more concerned with triadic connections while dyadic redundancy refers to aspects of positional advantage/disadvantage. Conceptually and statistically, these measures are different.

automatically suppressed the display of the dyadic redundancy matrix. It is useful, though, for some of the follow-on relationships.

### Trust Mapping Networks

#### Immediate Family Relationships<sup>37</sup>

The extract of the UCINET output below lists those 5 immediate family actors with the highest degree centrality. This shows that A73 (Operations and Security) has the greatest out-degrees, and might be regarded as the most influential. Actor A73 also has the largest in-degree. As I alluded to previously, it is not only the number of connections that is important, but also the status or rank of the actors involved. In this case, A73, as the operations and security officer, has a domain that contains several prestigious actors (see Figure 7 later in this chapter). He is directly tied to the chief of operations, in addition to several individuals directly involved in the insurgency. As a result, he is a person with relatively high status prestige and influence.

	OutDegree	InDegree
	-----	-----
A73	19.000	19.000
A214	13.000	13.000
A114	11.000	11.000
A177	10.000	10.000
A206	7.000	7.000

Table 8: Immediate Family Degree Centrality Measures

On the average, actors have a degree of 2.094. The range (minimum and maximum) of the out-degree (1 – 19) and that of the in-degree (1 – 19) are the same,

---

<sup>37</sup> Given the small variations in the exclusive and inclusive analyses for the general network measures, I used the inclusive categories in the remaining analyses for all relationships.

and the variability is also equal. This means that the network is relatively equivalent in terms of prominence and influence.

When examining the betweenness centrality of these relationships, actor A73 has the highest betweenness, followed by A177, A187, A96, and A200. This means that actor A73 is in a favored position to the extent that the actor falls on the geodesic paths between other pairs of actors in the network. Thus, the more people depend on this actor to make connections with other people, the more power he has. Given A73's identified position in the link diagram as the operations and security officer, this measure confirms that he is an influential person (and he has an immediate family relationship with Saddam Hussein).

FACTOR	VALUE	PERCENT	CUM %	RATIO
1	4.612	7.6	7.6	1.241
2	3.717	6.1	13.6	1.062
3	3.501	5.7	19.4	1.050
4	3.333	5.5	24.8	1.218
5	2.738	4.5	29.3	1.027
6	2.666	4.4	33.7	1.001
7	2.663	4.4	38.0	1.136
8	2.344	3.8	41.9	1.032
9	2.271	3.7	45.6	1.076
10	2.111	3.5	49.0	1.055

Table 9: Immediate Family Eigenvalues

Looking at the eigenvalues in the UCINET output above (Table 9), the percentage of the overall variation in distances that is accounted for by the first factor is 7.6 %. Likewise, the ratio of the first eigenvalue to the second is about 1.2 to 1. In short, this is a localized network where those on the periphery are “less connected.”<sup>38</sup> Thus, if what is important is not how many people a person knows, but how many

---

<sup>38</sup> Some of this may be due to the focus on Saddam Hussein in the information gathering process.

people the people that they know knows, not many people know who is connected to whom! This is the second substantive finding in this chapter. Quite simply, those connected due to immediate family relationships form an elite, tight, close-knit group.

Finally, when considering structural holes and the measure of dyadic redundancy, there were no actors who displayed a dyadic redundancy greater than 0.7. However, A196's tie to A193 is somewhat redundant as 67 % (or 0.67) of A196's other neighbors (or connections) also have ties with A193. Thus, A196 is embedded in a local network where there are few structural holes.

Extended Family Relationships

For this network, actor A114 has the highest degree centrality (see Figure 6). The UCINET output below shows that A114 has the greatest out-degrees and in-degrees, followed closely by A214. Given that A114 is the chief of staff and A214 is Saddam Hussein, this measure supports the expected amount of influence that these two actors have in this network. Additionally, given that these actors also are related via extended family, this finding reflects the importance of family in the network structure.

	OutDegree	InDegree
	-----	-----
A114	5.000	5.000
A214	4.000	4.000
A161	3.000	3.000
A51	2.000	2.000
A159	1.000	1.000

Table 10: Extended Family Degree Centrality Measures

On the average, actors have a degree of 1.455. The range (minimum and maximum) of the out-degree (1 – 5) and that of the in-degree (1 – 5) are the same,

and the variability is also equal. This means that the network is relatively equivalent in terms of prominence and influence.

When examining the betweenness centrality of these relationships, actor A114 has the highest betweenness, followed by A214, A51, and A161. Actor A114 is in a favored position to the extent that the actor falls on the geodesic paths between other pairs of actors in the network. Therefore, the more people depend on this actor to make connections with other people, the more power he has. For the 22 nodes in this relationship, these are the only actors with a betweenness factor.

When analyzing the eigenvector for this relationship, I found that the percentage of the overall variation in distances that is accounted for by the first factor is 22.6 %. While larger than the variations of the previous relationships, this still indicates that this is a localized network where those on the periphery are “less connected.”

Given the smaller number of nodes for this network, another useful tool is to look at the eigenvector centralities for each actor. We do this by examining the scores of each of the cases on the first eigenvector. Higher scores indicate that actors are "more central" to the main pattern of distances among all of the actors, lower values indicate that actors are more peripheral. The result is very similar to those for our earlier analyses of centrality for this network with actor A114 being the most central. Interestingly, for the extended family relationship, A214 (Saddam Hussein) is among the most peripheral, likely because he is insulated by the people with whom he is directly connected.

		1	2
		Eigenvec	nEigenvec
		-----	-----
1	A114	0.707	100.000
2	A12	0.316	44.721
3	A14	0.316	44.721
4	A15	0.316	44.721
5	A159	-0.000	-0.000
6	A16	0.316	44.721
7	A160	-0.000	-0.000
8	A161	-0.000	-0.000
9	A162	-0.000	-0.000
10	A163	-0.000	-0.000
11	A164	-0.000	-0.000
12	A165	-0.000	-0.000
13	A167	-0.000	-0.000
14	A169	-0.000	-0.000
15	A190	-0.000	-0.000
16	A191	-0.000	-0.000
17	A214	-0.000	-0.000
18	A45	-0.000	-0.000
19	A51	-0.000	-0.000
20	A73	-0.000	-0.000
21	A8	0.316	44.721
22	A89	-0.000	-0.000

Table 11: Extended Family Eigenvector Centralities

Finally, when considering structural holes and the measure of dyadic redundancy, there were no actors who displayed a high dyadic redundancy. In fact, the dyadic redundancy of all actors was 0.

Close Friend Relationships

The extract of the UCINET output below (Table 12) lists those 5 actors with the highest degree centrality. This shows that A114 has the greatest out-degrees, and the largest in-degrees. On the average, actors have a degree of 1.724. The range (minimum and maximum) of the out-degree (0 – 16) and that of the in-degree (0 – 16) are the same, and the variability is also equal.

	OutDegree	InDegree
	-----	-----
A114	16.000	16.000
A214	6.000	6.000
A51	3.000	3.000
A116	1.000	0.000
A1	1.000	1.000

Table 12: Close Friend Degree Centrality Measures

When examining the betweenness centrality of these relationships, actor A114 has the highest betweenness, followed by A214 and A51. All other actors in this network have a betweenness factor of 0. Clearly, actor A114 is in a favored position to the extent that the actor falls on the geodesic paths between other pairs of actors in the network.

When analyzing the eigenvector for this relationship, I found that the percentage of the overall variation in distances that is accounted for by the first factor is 44.6 %. While larger than the variations of the previous relationships, this still indicates that this is a localized network where those on the periphery are “less connected.” The analysis of the scores of each of the cases on the 1st eigenvector – given that higher scores indicate that actors are “more central” to the main pattern of distances among all of the actors, and lower values indicate that actors are more peripheral – indicates that actor A114 is the most central (see Table 13).

Lastly, concerning structural holes and dyadic redundancy, there were no actors who displayed a high dyadic redundancy. Similar to the previous relationships, the dyadic redundancy of all actors was 0, indicating that there are no actors who are embedded in local networks where there are few structural holes.

		1	2
		Eigenvec	nEigenvec
		-----	-----
1	A116	0.065	9.218
2	A1	0.169	23.933
3	A10	0.169	23.933
4	A11	0.169	23.933
5	A114	0.689	97.417
6	A115	0.065	9.218
7	A116	0.065	9.218
8	A119	0.169	23.933
9	A120	0.169	23.933
10	A121	0.169	23.933
11	A122	0.169	23.933
12	A123	0.169	23.933
13	A13	0.169	23.933
14	A166	0.065	9.218
15	A168	0.065	9.218
16	A17	0.169	23.933
17	A170	0.065	9.218
18	A195	0.000	0.000
19	A2	0.169	23.933
20	A206	0.000	0.000
21	A214	0.265	37.522
22	A24	0.169	23.933
23	A47	-0.000	-0.000
24	A48	-0.000	-0.000
25	A49	-0.000	-0.000
26	A5	0.169	23.933
27	A51	-0.000	-0.000
28	A7	0.169	23.933
29	A9	0.169	23.933

Table 13: Close Friend Eigenvector Centralities

Bodyguard Relationships

The extract of the UCINET output shows that A114 has the greatest out-degrees. A22 is one of 10 actors with an in-degree of 1.

	OutDegree	InDegree
	-----	-----
A114	8.000	0.000
A116	1.000	0.000
A51	1.000	0.000
A22	0.000	1.000
A26	0.000	1.000

Table 14: Bodyguard Degree Centrality Measures

On the average, actors have a degree of 0.769. The range (minimum and maximum) of the out-degree (0 – 8) is larger than that of in-degree (0 – 1), and there is more variability (standard deviations and variance) across the actors in out-degree (2.118 and 4.485) than in-degree (0.421 and 0.178). In this case, the population is more homogeneous with regard to in-degree (prominence) than to out-degree (influence).

When examining the betweenness centrality of these relationships, all of the nodes have a betweenness factor of 0. There is no actor that others depend on to make connections with other people. With respect to the eigenvector for this relationship, I found that the percentage of the overall variation in distances that is accounted for by the first factor is 58.6 %. Again, while larger than the variations of the previous relationships, this still indicates that this is a localized network where those on the periphery are “less connected.” The analysis of the scores of each of the cases on the first eigenvector indicates that actor A114 is the most central.

	1	2
	Eigenvec	nEigenvec
	-----	-----
1 A114	0.707	100.000
2 A116	0.000	0.000
3 A118	0.000	0.000
4 A22	0.250	35.355
5 A26	0.250	35.355
6 A27	0.250	35.355
7 A28	0.250	35.355
8 A29	0.250	35.355
9 A30	0.250	35.355
10 A31	0.250	35.355
11 A32	0.250	35.355
12 A51	0.000	0.000
13 A52	0.000	0.000

Table 15: Bodyguard Eigenvector Centralities

Lastly, concerning structural holes and dyadic redundancy, there were no actors who displayed a high dyadic redundancy. Similar to the previous relationships, the dyadic redundancy of all actors was 0.

Strategy and Goals Mapping Networks

Money and Resources Relationships

On average, the actors in this network have a degree centrality of 0.821. The range (minimum and maximum) of the out-degree (0 – 8) is larger than that of in-degree (0 – 2), and there is more variability (standard deviations and variance) across the actors in out-degree (1.833 and 3.361) than in-degree (0.467 and 0.218). Thus, the population is more homogeneous with regard to in-degree (prominence) than to out-degree (influence). Finally, actor A114 has the greatest out-degree, and actor A59 has the largest in-degree.

	OutDegree	InDegree
	-----	-----
A114	8.000	0.000
A51	5.000	0.000
A214	4.000	0.000
A56	2.000	1.000
A59	0.000	2.000

Table 16: Money and Resources Degree Centrality Measures

For the betweenness centrality of these relationships, actor A56 has the highest betweenness factor, followed by A54. All other actors in this network have a betweenness factor of 0. Thus, actor A56 is in a favored position to the extent that the actor falls on the geodesic paths between other pairs of actors in the network.

When examining the eigenvector for this relationship, the percentage of the overall variation in distances that is accounted for by the first factor is 23.8 %. As

with previous relationships, this indicates a localized network where those on the periphery are “less connected.” The analysis of the scores of each of the cases on the first eigenvector indicates that actor A114 is again the most central.

	1	2
	Eigenvec	nEigenvec
	-----	-----
1 A114	0.707	100.000
2 A116	0.000	0.000
3 A131	0.000	0.000
4 A132	0.000	0.000
5 A149	0.000	0.000
6 A150	0.000	0.000
7 A151	0.000	0.000
8 A168	0.000	0.000
9 A18	0.250	35.355
10 A19	0.250	35.355
11 A20	0.250	35.355
12 A21	0.250	35.355
13 A214	0.000	0.000
14 A22	0.250	35.355
15 A24	0.250	35.355
16 A25	0.250	35.355
17 A48	0.000	0.000
18 A50	0.000	0.000
19 A51	0.000	0.000
20 A54	0.000	0.000
21 A55	0.000	0.000
22 A56	0.000	0.000
23 A57	0.000	0.000
24 A58	0.000	0.000
25 A59	0.000	0.000
26 A6	0.250	35.355
27 A62	0.000	0.000
28 A73	0.000	0.000

Table 17: Money and Resources Eigenvector Centralities

Finally, with respect to structural holes and dyadic redundancy, there were no actors who displayed a high dyadic redundancy. Similar to the previous relationships, the dyadic redundancy of all actors was 0, indicating that there are no actors who are embedded in local networks where there are few structural holes.

### Insurgent Operations Relationships

On average, the actors in this network have a degree centrality of 0.915. The range (minimum and maximum) of the out-degree (0 – 15) is larger than that of in-degree (0 – 2), and there is more variability (standard deviations and variance) across the actors in out-degree (2.577 and 6.641) than in-degree (0.366 and 0.134). Thus, the population is more homogeneous with regard to in-degree (prominence) than to out-degree (influence). Finally, actor A214 has the greatest out-degree, and actors A116 and A159 have the largest in-degrees. Taken independently, such a finding makes more plausible a conclusion that actor A214, Saddam Hussein, exerted a large amount of influence in insurgent operations. This is the third important finding in this chapter.

	OutDegree	InDegree
	-----	-----
A214	15.000	0.000
A116	11.000	2.000
A73	9.000	1.000
A114	6.000	1.000
A51	6.000	1.000
A159	0.000	2.000

Table 18: Insurgent Operations Degree Centrality Measures

When examining the betweenness centrality of these relationships, actor A116 has the highest betweenness, followed by A73, A89, and A77. Actor A116 is in a favored position to the extent that the actor falls on the geodesic paths between other pairs of actors in the network. Therefore, the more people depend on this actor to make connections with other people, the more power he has. Given that this actor's position in the Link Diagram is that of chief of operations, such a finding supports

this template when considering insurgent operations. Figure 7 highlights this finding, but also demonstrates that A116 is more isolated than even Saddam Hussein, and that A73 really may be the crucial node here. Figure 8 depicts the remainder of A116's network (this part of the network does not include A73).

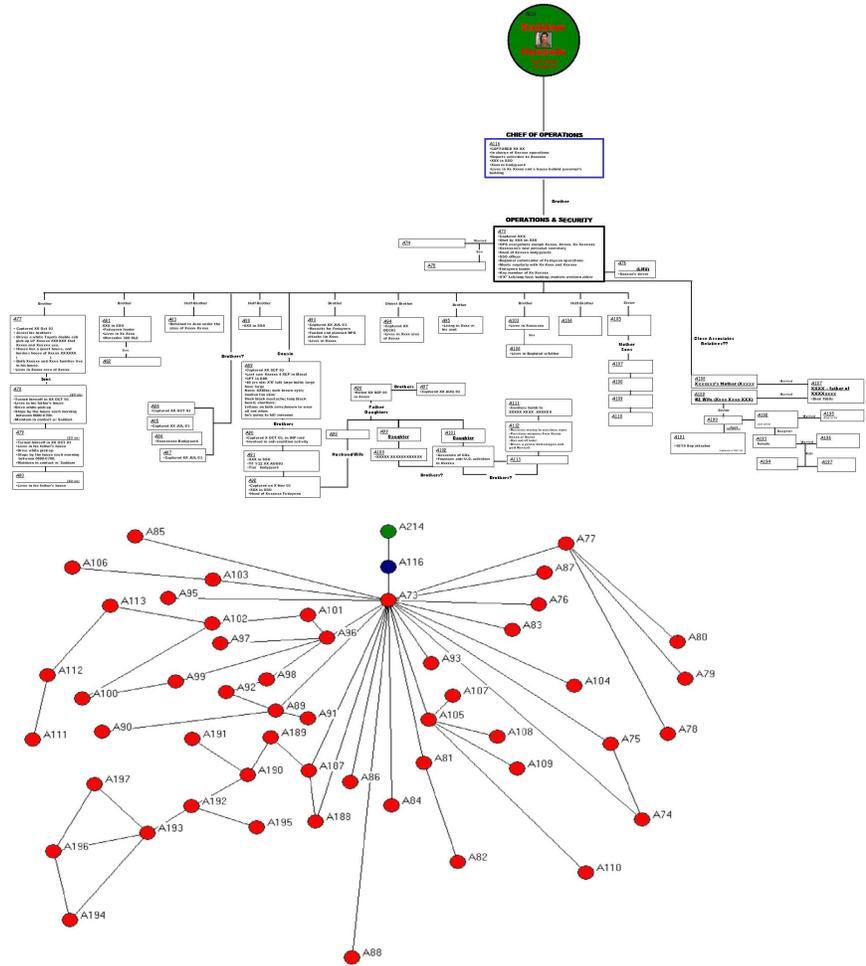


Figure 7: Chief of Operations (A116) Sub-Network

When examining the eigenvector for this relationship, the percentage of the overall variation in distances that is accounted for by the first factor is 15.6 %.



A115's only other connection is to A214 – Saddam Hussein – who is also connected to A116. Given that A214 is the Personal Security Officer for Hussein, it is not completely surprising that he has no other connections to anyone else in the network, other than the Operations Officer. Likewise, A159 (son), A161 (son), and A214 (Saddam Hussein) are embedded in a local network where there are no structural holes (Figure 9). This finding highlights the collaboration between Saddam and his sons in directing insurgent operations and further indicates how the insurgency network is superimposed on traditional family linkages.

### Discussion

Degree centrality, betweenness, and eigenvectors are all useful measures that give us insight into who are the key players and how connected is the network. From degree centrality I was able to confirm our projected positions of several significant actors. For example, based on what we knew about actor A114, we believed his role in the insurgency, and his link to Saddam, to be that of his chief of staff (Figure 6). My analysis of degree centrality confirmed that A114 was, in fact, an influential person as evidenced by his high out-degree. Similarly, when considering just the insurgent operations relationship, the high out-degree score of Saddam Hussein offers evidence of the amount of influence that he exerted. In other words, such a finding makes more plausible a conclusion that Hussein played a large role in directing insurgent operations.

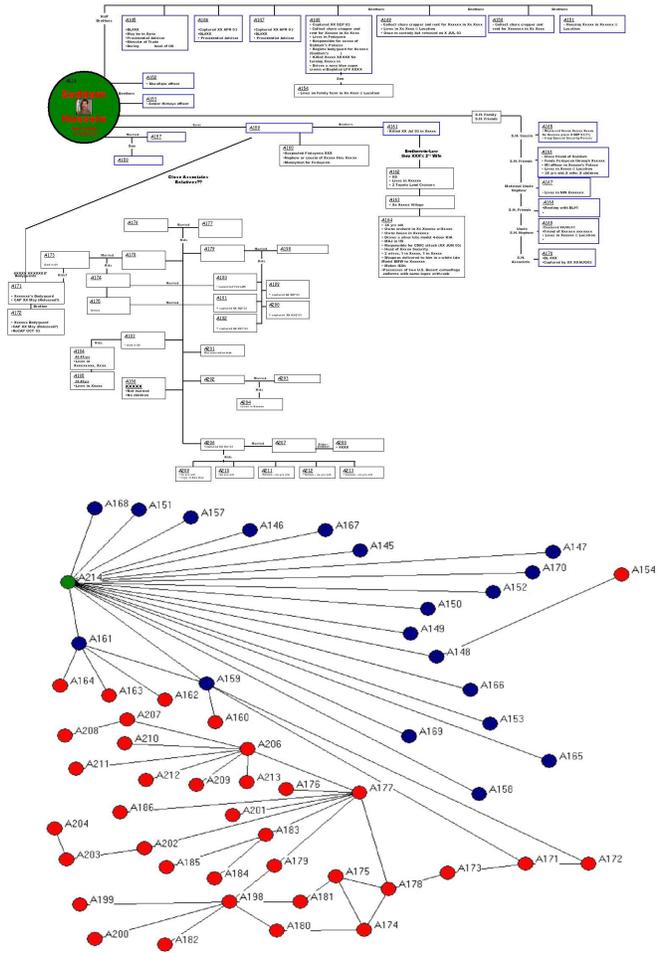


Figure 9: Other Sub-Networks

Betweenness allowed me to highlight those actors who potentially might have some control over the interactions between other, nonadjacent actors. One example was very revealing. Actor A187 had a high betweenness score. Interestingly, our unit's initial information on him was that he died in the 1980s (this is accurate). However, looking at his connections is valuable. Upon closer examination it is apparent that his immediate ties link two significant sub-networks, one of which has

direct ties to A73, the operations and security officer (Figure 7). In short, such an analysis allows me to re-evaluate how information may have been disseminated and orders issued in support of insurgent operations, and is revealing in identifying who may lead to the identification of an individual with direct ties to Saddam Hussein.

Finally, the actor analysis measure, the eigenvector score, was equally revealing. From this it is apparent that the Network of Saddam Hussein is a localized network where those on the periphery are “less connected” – that is, there are great inequalities in actor centrality. Those with power have it, and those without it do not! Therefore, while those on the exterior of the network have a specific role and function, the reality is that they may not be so instrumental in helping us either locate Saddam Hussein or in neutralizing the insurgency. They are not necessarily decision makers. Important to note, however, is that such an analysis should be done in conjunction with other specific actor or role measures. There may be, in fact, actors on the periphery who are critical to the insurgency.

With the exception of the immediate family relationships and the insurgent operations relationships, A114 clearly emerges as one of the more influential actors. Given that his position in the network is that of chief of staff, such a finding supports this projection. In general, there are great inequalities in actor centrality as indicated by the finding that those on the periphery are less connected to the main network. Likewise, there are almost no redundant ties. Taken together, these two findings allow us to conclude that this network is “not connected” and that the power is

consolidated amongst a few actors. Therefore, those actors on the periphery will, in general, not know much about the intricacies, actions, decisions, etc. of the network.

This analysis offers support for the working assumption that Saddam Hussein was active in the insurgent leadership. The degree centrality clearly demonstrates that he exerted a large amount of influence. Supporting this is the eigenvector analysis that shows he is the most central actor. Finally, an equally critical finding is the importance of A116's position (Figures 7 and 8). In the link diagram, he is identified as the chief of operations. The betweenness analysis shows that this is in fact the case, or that at least he is an important player in terms of information flow and decision-making. Others definitely depend on this individual to make connections with other people, thus resulting in him having a large amount of power. There is evidence that he is important enough that other actors have redundant ties – dyadic relationships – with him.

In summary, there are three substantive findings in this chapter. First, A114, the chief of staff, is the most prominent and influential actor in the network. This confirms what we know to be true within organizations – that is, the importance of the chief of staff. Second, those connected by immediate family relationships form a local network, and thus are an elite, tight, close-knit group. This confirms what we know from the previous chapter about the importance of family structure in this network. Finally, this analysis clearly demonstrates that Saddam Hussein exerted a large amount of influence in insurgent operations.

From this chapter, coupled with what we learned from the general network measures in the preceding chapter, a picture of the network structure begins to emerge. We know from the research on resistance networks that power is a function of one's position in the network of communication and social relations, where this position is assessed not only simply in terms of prestige and influence, but also in terms of the power of the people with whom one is connected. In this network there is a core group of individuals who, through their connections with one another, wield the most prestige and influence. Furthermore, these individuals are linked via pre-existing familial ties.

On the periphery, the analysis seems to indicate that those in this area of the network are less important, or that they are on the "short-end" of the power distribution curve. Of note is that these apparent inequalities in power may be due to data collection shortfalls since the information gathering for this network focused on those closest to Saddam Hussein. Considering, though, that this power inequality is a reflection of the true nature of the network, another insight into the structure emerges. Namely, in the periphery zone we see less dense patterns of interactions and looser relationships than the core. Consistent with the resistance networks' literature, this periphery allows the network to operate at a far greater distance – both geographically and socially – than would otherwise be the case. This facilitates more extensive operations, more diverse activities, and the capacity to carry out effective intelligence collection (Williams 2001). The next chapter will provide more specificity as to the roles and positions of the actors in the network, both in the core and the periphery.

## CHAPTER 9

### ROLE ANALYSIS

In contrast to most social network methods that focus on the properties of actors or the subsets of actors, network role analysis focuses on associations among relations. Where actor analysis considers the number and type of ties that an actor may have, role analysis describes the associations among actors based on how these associations combine to link actors or positions. In other words, we gain a sense of the “nature” of the ties and the positions actors hold.

#### The Network of Saddam Hussein

When analyzing the entire network using the role analysis measures – structural equivalence (actors have identical ties to and from all other actors in the network), automorphic equivalence (actors occupy indistinguishable structural locations in the network), and multiplexity (two actors are linked by more than one relationship) – I ran the UCINET procedure for all 197 actors and 388 relationships. The output for all three measures was much too tedious and cumbersome to be useful. Equally at issue was that I was going to analyze each relationship in accordance with my pre-established mapping networks later in the analysis. Therefore, I only ran the procedure for the designated relationships.<sup>39</sup>

---

<sup>39</sup> With a large data set, UCINET contains an optimization function for the equivalence measure. I decided not to use this function due in part to Borgatti et al.'s (2002) warning that care should be taken when using this routine. The function is an approximation that sorts nodes into a user-defined number of partitions in such a way as to maximize automorphic equivalence. There is no guarantee, however, that the number of partitions (equivalence classes) chosen is "correct," or that the automorphisms identified are "exact."

## Trust Mapping Networks

### Immediate Family Relationships

Two actors are structurally equivalent if we can exchange them one-for-one, and not affect any properties of the graph. By trying to find actors who can be swapped for each other, we are really paying attention to the positions of the actors in a particular network. We are trying to find actors who are clones or substitutes. A widely used measure of structural equivalence is the correlation coefficient. This is especially useful when the focus is on measuring similarity in pattern. Actor pairs with a coefficient of +1.0 are structurally equivalent.

<b>CLUSTER</b>	<b># OF ACTORS</b>	<b>ACTORS (A)</b>
1	10	146, 151, 145, 149, 150, 147, 152, 153, 157, 158
2	4	40, 46, 39, 41
3	2	197, 194
4	3	182, 199, 200
5	2	184, 185
6	3	186, 176, 201
7	5	213, 209, 210, 212, 211
8	10	136, 126, 129, 127, 128, 135, 133, 134, 124, 125
9	4	109, 110, 108, 107
10	3	79, 80, 78
11	3	118, 115, 117
12	2	91, 90
13	2	75, 74
14	9	104, 83, 84, 85, 86, 87, 88, 93, 95
15	2	161, 159
16	3	56, 58, 59
17	2	70, 69

Table 19: Immediate Family Structural Equivalence

There are 17 structurally equivalent clusters, with each cluster having a varying number of actors (Table 19). The actors are structurally equivalent within

each cluster, but not across clusters. Since these are immediate family relationships, the actors within each cluster are directly related to one another and have an immediate family “position” in the network. For example, the actors in cluster 3 are siblings; likewise for clusters 2 and 5. The actors in cluster 16 are father (A56) and sons. Thus, while their positions are statistically equivalent, realistically they do not have the same roles – the brothers, A58 and A59, could not be substituted for their father, A56

<b>CLUSTER</b>	<b># OF ACTORS</b>	<b>ACTORS (A)</b>
1	10	126, 136, 135, 128, 133, 124, 125, 127, 134, 129
2	2	159, 161
3	4	46, 39, 40, 41
4	3	56, 58, 59
5	2	77, 116
6	2	197, 194
7	2	184, 185
8	2	90, 91
9	9	86, 83, 85, 104, 88, 93, 87, 95, 84
10	2	174, 175
11	2	181, 180
12	10	147, 146, 153, 157, 149, 150, 145, 152, 158, 151
13	2	69, 70
14	2	75, 74
15	2	103, 81
16	3	201, 186, 176,
17	3	182, 200, 199
18	5	213, 212, 210, 209, 211
19	2	106, 82
20	4	107, 110, 109, 108
21	5	117, 115, 118, 78, 79

Table 20: Immediate Family Automorphic Equivalence

Automorphic equivalence asks if the whole network can be re-arranged, putting different actors at different positions, but leaving the relational structure or

skeleton of the network intact. Automorphic equivalence is not as demanding a definition of similarity as structural equivalence. Actors are automorphically equivalent if we can alter the graph in such a way that exchanging the two actors has no effect on the distances among all actors in the graph. In this relationship, there are 21 automorphically equivalent clusters (Table 20). Again, this refers to equivalence within a cluster, not within the whole network. Like the structural equivalence table earlier, these are immediate family relationships. The actors within each cluster are directly related to one another and have an immediate family “position” in the network.

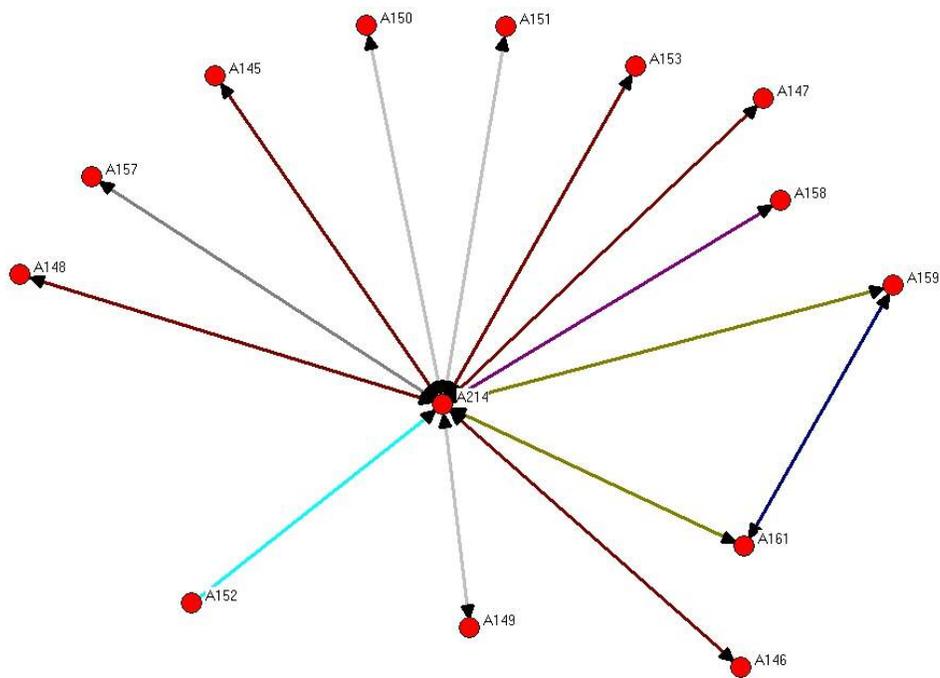


Figure 10: Immediate Family Multiplexity<sup>40</sup>

<sup>40</sup> Relationships and color codes (relationship/color): father/red, husband/black, wife/gray, son/purple, brother/green, half-brother/aqua, son & insurgent operations/olive, brother & insurgent operations/navy, half-brother & money and resources/silver, half-brother & insurgent operations/maroon.

Multiplex data are data that describe multiple relations among the same set of actors. For relatively small networks, drawing graphs is the best way of "seeing" structure. One approach to representing multiple relations among actors is to use multiple lines (with different colors or styles) and over-lay one relation on another (Hanneman and Riddle 2005). Given the relatively large number of actors (127) for this analysis, I isolated the ego network of Saddam Hussein (A214) and depicted the multiple relations for which he is connected (Figure 10).<sup>41</sup>

This figure nicely identifies the immediate family clique A159-A161-A214. The arrowheads demonstrate the direction of the relationship and the colored lines indicate the relationship. So, for example, the navy line and the double arrowhead show that A159 and A161 are brothers and both are active in the insurgency. The olive line and arrowheads from A214 to actors A159 and A161 indicate that A159 and A161 are Saddam Hussein's sons and all are active in the insurgency. Once again, this highlights the importance of pre-existing family ties in the structure of the insurgent network.

#### *Extended Family Relationships*

In this relationship, there are 6 structurally equivalent clusters, with each cluster having a varying number of actors. Table 21 shows each cluster and the associated actors. Thus, for example, cluster 2 has 5 actors who can be exchanged for one

---

<sup>41</sup> NETDRAW is a great feature that allows us to "see" multiple relationships in a network. However, the diagram produced is not easily copied to a written document, primarily due to the vast array of colors that do not translate well to paper. Another drawback is that colors are transposed upon other relationships, thereby obscuring a previous/existing relationship. You can "build" the network, relationship-by-relationship, in NETDRAW. This is extremely useful for analyzing all of the multiple relationships on the computer screen or with different NETDRAW "shots."

another. Since these are extended family relationships, the actors within each cluster have an extended family “position” in the network. For example, in cluster 1, A169 and A167 are uncles of Saddam Hussein, while A165 is a cousin of Saddam Hussein; in cluster 5, A190 is the aunt of A191 (a nephew); or in cluster 4, A159 and A160 are cousins. As in the immediate family relationships, while some positions are statistically equivalent, realistically they do not have the same roles.

<b>CLUSTER</b>	<b># OF ACTORS</b>	<b>ACTORS (A)</b>
1	3	169, 165, 167
2	5	8, 14, 15, 12, 16
3	3	163, 164, 162
4	2	159, 160
5	2	190, 191
6	2	73, 89

Table 21: Extended Family Structural Equivalence

In this relationship, there are 4 automorphically equivalent clusters. Table 22 shows each cluster and the associated actors. Like the structural equivalence table above, these are extended family relationships. The actors within each cluster have an extended family “position” in the network. For the actors in these clusters, statistically we can put different actors at different positions, but leave the relational structure or skeleton of the extended family network intact.

<b>CLUSTER</b>	<b># OF ACTORS</b>	<b>ACTORS (A)</b>
1	3	162, 163, 164
2	3	169, 165, 167
3	5	15, 12, 8, 16, 14
4	6	159, 160, 190, 73, 191, 89

Table 22: Extended Family Automorphic Equivalence

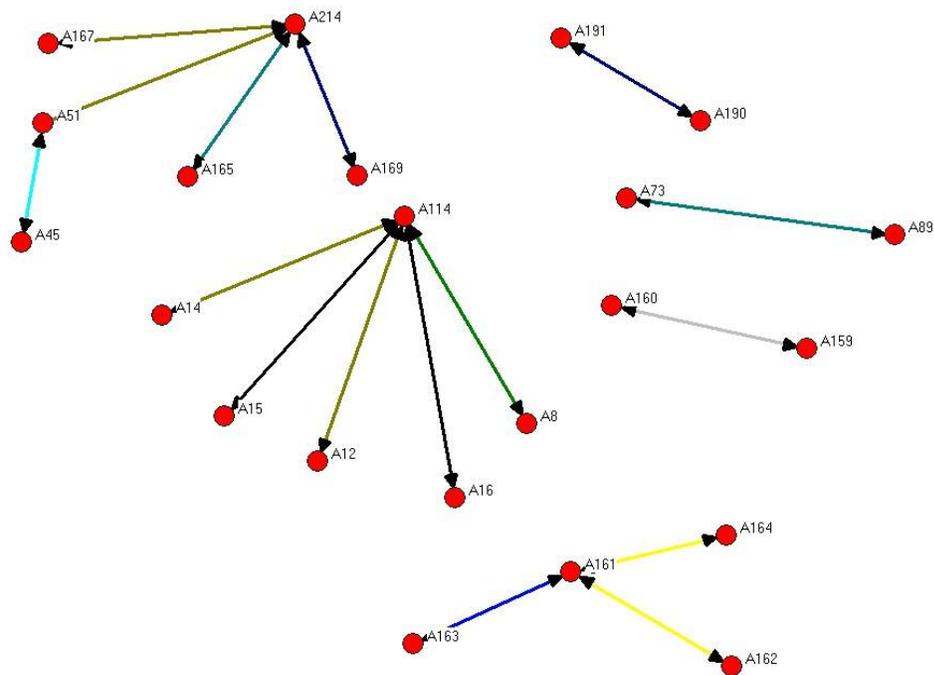


Figure 11: Extended Family Multiplexity<sup>42</sup>

Figure 11 shows the multiple relations for the actors contained within the extended family relationship. Saddam Hussein (A214) and his chief of staff (A114) appear to be the central players and have several relationships that are exclusively extended family and others that are extended family and “some other” relationship (bodyguard, money and resources, or insurgent operations). However, this graph highlights that Hussein and his chief of staff are not linked by an extended family relationship.

<sup>42</sup> Relationships and color codes (relationship/color): father-in-law/red, brother-in-law/blue, cousin/black, nephew/gray, aunt/purple, uncle/olive, son-in-law/green, brother-in-law & bodyguard/aqua, brother-in-law & insurgent operations/yellow, cousin & money and resources/silver, cousin & insurgent operations/teal, nephew & insurgent operations/navy.

Close Friend Relationships

For this relationship, with the exception of four nodes, all of the actors are structurally equivalent and automorphically equivalent (although not necessarily with each other). This is not a surprising finding when considering “close friends.” This is a very specific category without much variation. As a contrast, with any of the family relationships there is a certain “degree of family” – that is, father, mother, cousin, niece, etc. Interestingly, the four actors who are not equivalent are “major” actors in the network: A215 (Saddam Hussein), A114 (chief of staff), A51 (personal secretary), and A116 (chief of operations).

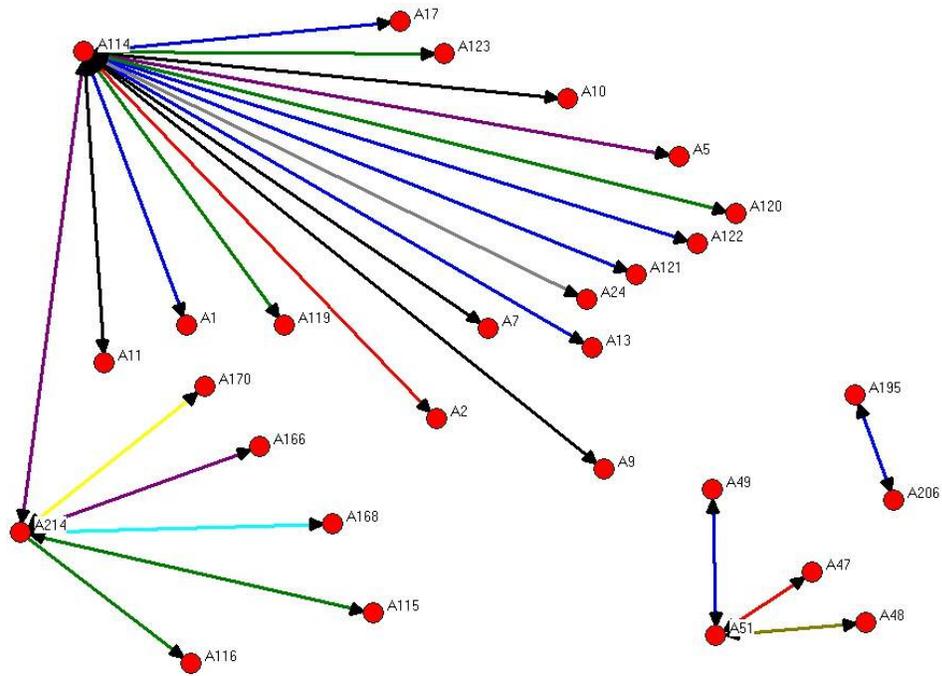


Figure 12: Close Friend Multiplexity<sup>43</sup>

<sup>43</sup> Relationships and color codes (relationship/color): former regime official/red, tribe or village association/blue, school, military, or political association/black, former regime official & money and resources/gray, former regime official & insurgent operations/purple, tribe or village association & money and resources/olive, tribe or village association & insurgent operations/green, school, military,

Figure 12 depicts the multiple relations for the actors contained within the close friend relationship. From this graph, it is clear that A114 (chief of staff) has several relationships to other actors that are at least due to the close friendship network. Likewise, A214 (Saddam Hussein) and A51 (personal secretary) have more multiple ties with other actors that at a minimum are because of the close friend relationship. For example, A51 and A47 are related due to their association in the former regime; A51 and A49 due to a tribe or village association; and A51 and A48 due to a tribe or village association and a money and resources link pertaining to support of the insurgency. This is a clear demonstration that friendship is part of the package of linkages in these cases. Friends, unlike relatives, can be picked, thereby making the basis for attributing causality to these voluntary relationships a weak one. However, this finding strongly shows that the functional insurgency network is superimposed on more traditional kinds of linkages.

#### *Bodyguard Relationships*

For this relationship, nine actors are structurally equivalent with one another: A29, A30, A22, A26, A27, A28, A32, and A31. All of the actors are automorphically equivalent (although not necessarily with each other) with the exception of A114, and are split into two clusters – cluster one: A116, A51; and cluster two: A22, A26, A118, A28, A29, A30, A31, A32, A27, A52.

---

or political association & money and resources/aqua, school, military, or political association & insurgent operations/yellow.

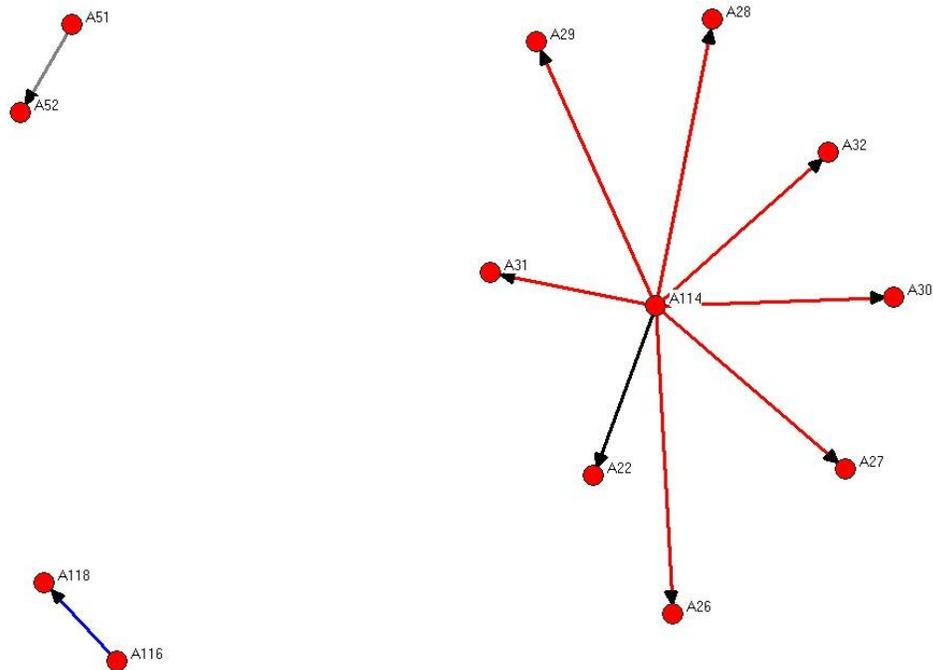


Figure 13: Bodyguard Multiplexity<sup>44</sup>

Figure 13 represents the multiple relations associated with the bodyguard network/relationships. Clearly, A114 has the majority of relationships associated with the bodyguard network. However, it is important to realize that this does not reflect a dearth of bodyguards for other actors, but only that we identified the bodyguards whom we knew about.

### Strategy and Goals Mapping Networks

#### Money and Resources Relationships

In this relationship, there are 3 structurally equivalent clusters, with each cluster having a varying number of actors. Table 23 shows each cluster and the associated actors. So, in the case of cluster two, actors, A48, A50, and A57, are

<sup>44</sup> Relationships and color codes (relationship/color): bodyguard/red, son & bodyguard/blue, bodyguard & money and resources/black, bodyguard & insurgent operations/gray.

structurally equivalent since they have identical ties to and from A214 (Saddam Hussein) and, theoretically, they can be exchanged for one another with no impact on the structure of the network. Realistically, however, each provides a different type of “money and resource” service. A50 and A57 are weapons’ distributors, while A48 provides transportation for insurgents.

<b>CLUSTER</b>	<b># OF ACTORS</b>	<b>ACTORS (A)</b>
1	4	168, 150, 151, 149
2	3	48, 50, 57
3	8	25, 18, 22, 20, 21, 19, 24, 6

Table 23: Money and Resources Structural Equivalence

For automorphic equivalence, there are 2 clusters, each with a varying number of actors. Table 24 shows each cluster and the associated actors. Again, while the actors in each cluster are statistically equivalent, their positions are not always interchangeable in reality. Considering cluster one, 8 actors provide housing for insurgents (A25, A18, A21, A22, A24, A149, A150, A151), 3 actors are weapons’ distributors (A50, A57, A6), 2 perform a bodyguard-type role (A20, A19), A131 provides medical care to insurgents, A48 provides transportation for insurgents, A168 facilitates meetings between insurgents, and A62 recruits insurgents.

<b>CLUSTER</b>	<b># OF ACTORS</b>	<b>ACTORS (A)</b>
1	17	25, 18, 50, 21, 131, 22, 24, 57, 48, 20, 149, 150, 151, 168, 6, 19, 62
2	2	132, 116

Table 24: Money and Resources Automorphic Equivalence

The equivalence measures for this relationship confirm existing literature on the division of labor among network members and some of the discernible roles in

resistance networks.<sup>45</sup> Clearly there is evidence of extenders, or recruiters, and guardians, or bodyguards. This analysis also demonstrates other roles that are critical for the daily operation and day-to-day existence of an insurgent network – for example, meeting facilitators, transporters, weapons’ distributors, housing coordinators, and medical personnel.

Figure 14 represents the multiple relations associated with the money and resources relationships. Interesting is how many money and resources relationships are aligned with “other” relationships. Looking at A214, none of the actors tied to Saddam Hussein for this network are due solely to money and resources, but instead each tie is a combination of this with another relationship. For example, A168 was in a school, military, or political association with Saddam as well as providing a meeting place for him. Likewise, A151 is a half-brother of Saddam while also providing housing for insurgent members. Relationships are not simply based on functional roles. This reflects the importance of pre-existing relationships and the structure of an insurgency.

Also of interest is that there are 5 separate sub-graphs that comprise the larger relationship. Further analysis ought to examine how these sub-networks are linked, or not. Given the preceding analyses we know that at least two of the sub-networks are linked, namely those including Saddam Hussein (A214) and his chief of staff (A114). Also, along the same considerations, we would expect the personal secretary (A51) and the chief of operations (A116) to be linked to Hussein (and/or his chief of

---

<sup>45</sup> Common roles are organizers, insulators, communicators, guardians, extenders, monitors, and crossovers (Williams 2001).

staff) as well. The graph in Figure 14 highlights gaps in the information gathering process and thus provides a clue as to the direction in which future data and information gathering efforts ought to proceed – namely, identifying those individuals (or individual) who connect the sub-networks containing the aforementioned members.

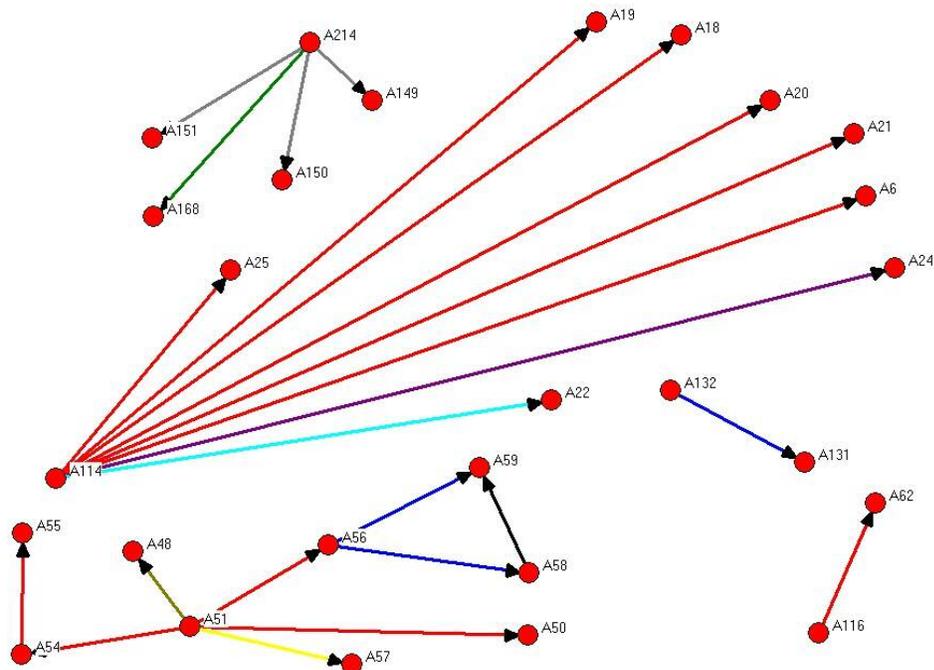


Figure 14: Money and Resources Multiplexity<sup>46</sup>

Insurgent Operations Relationships

In this relationship, there are 8 structurally equivalent clusters (Table 25).

Previous research on resistance networks provides insight into some of the discernible

<sup>46</sup> Relationships and color codes (relationship/color): money and resources/red, son & money and resources/blue, brother & money and resources/black, half-brother & money and resources/gray, former regime official & money and resources/purple, tribe or village association & money and resources/olive, school, military, or political association & money and resources/green, bodyguard & money and resources/yellow, money and resources & insurgent operations/aqua.

roles: for example, the actors in cluster 2 are insulators, while the actors in cluster 3 are communicators. What we also see in this analysis is the existence of another role – that is, operators. For example, the actors in cluster 1 are those who carry out orders and may be classified as the “foot soldiers” of the insurgency.

<b>CLUSTER</b>	<b># OF ACTORS</b>	<b>ACTORS (A)</b>
1	9	72, 71, 65, 66, 67, 64, 68, 61, 63
2	2	162, 164
3	9	148, 147, 170, 166, 169, 145, 146, 153, 165
4	5	40, 39, 52, 53, 46
5	6	119, 123, 4, 3, 120, 5
6	2	79, 78
7	3	91, 92, 90
8	6	87, 83, 84, 85, 81, 93

Table 25: Insurgent Operations Structural Equivalence

Also, there are 6 automorphically equivalent clusters (Table 26). These are the actors, within each cluster, for whom we can put at different positions, while leaving the relational structure or skeleton of the network intact. Again, these findings confirm existing research on the roles within a resistance network, as well as the identification of insurgent operators, those charged with the “dirty work” of the insurgency.

<b>CLUSTER</b>	<b># OF ACTORS</b>	<b>ACTORS (A)</b>
1	6	112, 171, 190, 207, 174, 130
2	15	145, 165, 132, 153, 170, 148, 111, 180, 146, 147, 206, 169, 172, 191, 166
3	13	3, 40, 46, 164, 4, 52, 53, 123, 162, 39, 120, 119, 5
4	9	64, 68, 63, 61, 67, 72, 71, 66, 65
5	7	84, 81, 85, 70, 83, 87, 93
6	6	78, 79, 92, 91, 90, 97

Table 26: Insurgent Operations Automorphic Equivalence

Figure 15 shows the multiple relations for this network. Because of the rather large number of actors in this network, I only have presented the analysis for the ego network of Saddam Hussein. Such an analysis gives us a good idea of whom he is connected to with respect to insurgent operations. Of note is that each of the connections is also related to Saddam via an immediate family, extended family, or close friend tie. Also of interest is that the arrows from Hussein to the other actors are consistent with the out-degree finding that he exerted much influence within the insurgency. Like the money and resources multiplexity, this finding demonstrates that relationships are not simply based on functional roles, and highlights the importance of pre-existing relationships and the structure of an insurgency.

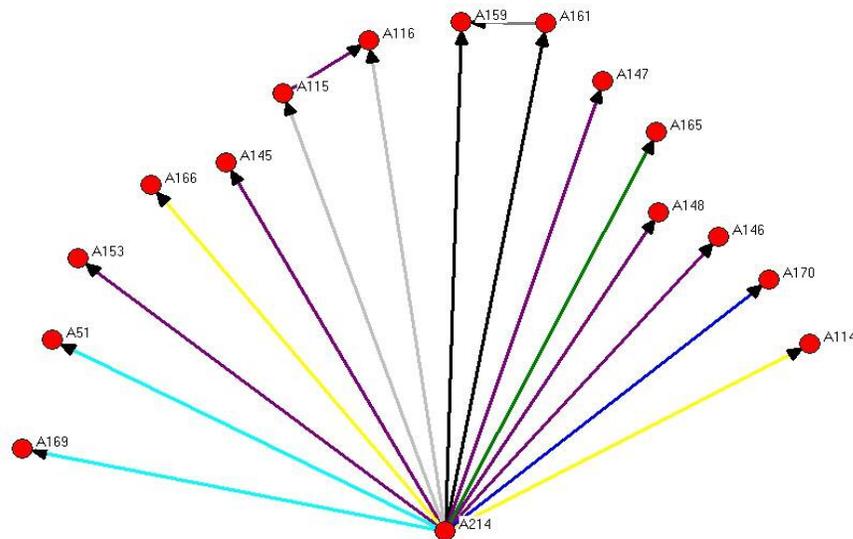


Figure 15: Insurgent Operations Multiplexity<sup>47</sup>

<sup>47</sup> Relationships and color codes (relationship/color): son & insurgent operations/black, brother & insurgent operations/gray, half-brother & insurgent operations/purple, cousin & insurgent

## Discussion

The preceding role analysis has demonstrated that within each of these sub-networks there is a generally strong tendency toward structural equivalence. Accordingly, there is also a strong tendency toward automorphic equivalence. Theoretically, then, we can exchange many of the actors with no effect on the distances among all actors in the graph. Since actors who are structurally equivalent are also automorphically equivalent, it follows that for most of these mapping networks/relationships, many of the actors can be exchanged with one other with no structural alterations from the original graph. However, as I indicated on several occasions, one needs to proceed with caution. Some of the services provided may be different between two equivalent actors.

Measures of equivalence and role identification are relevant to any analysis of an insurgent network. With respect to destabilizing the network, a measure of equivalence will give us a sense of who is replaceable, and who is not. The measure alone will tell us which actors are equivalent. However, a complete analysis requires an elaboration on the specific information about the actor. As noted above, through the equivalence measure I was able to discern which actors were interchangeable with respect to providing money and resources. This can be misleading, though, because some actors fulfill different requirements within the network. Therefore, care needs to be taken in either how the data is coded (for example, break out as separate

---

operations/green, nephew & insurgent operations/aqua, former regime official & insurgent operations/yellow, tribe or village association & insurgent operations/silver, school, military, or political association & insurgent operations/blue.

categories of analysis the following: money, transportation, weapons, etc.) or in the analysis of the actor characteristics before one draws a conclusion about exchangeable actors.

This analysis confirms existing literature that resistance networks feature a considerable division of labor among members, and that it is possible to identify a series of critical roles. Several of these roles were readily discernible in this network. Additionally, my analysis highlighted several other important roles. For example, there are those individuals in the network who sustain the insurgency on a daily basis and allow for its day-to-day operation. These are your transporters, housing coordinators, meeting facilitators, weapons' distributors, and medical personnel. Likewise, there are the operators, or "foot soldiers," of the insurgency. These are the individuals responsible for executing the orders of the insurgent organizers and decision makers.

Looking at the multiple relations within each of the mapping networks was valuable. From these analyses, it is clear who are the prominent and/or influential actors and how they are connected to others – that is, what relationships connect them. The multiplexity measure is a powerful one. Particularly insightful was the analysis of the ego network of Saddam Hussein as it applied to insurgent operations. Two actors were not just linked because of the insurgency. An important finding is that all those connected to him who were involved in the insurgency are also "related" through trust – that is, pre-existing ties formed by family, military associations, tribe, etc. Pre-existing ties are exactly the ones along which insurgent networks are built.

In summary, the role analysis confirms two important findings from preceding analyses. First is that Saddam Hussein was active in the insurgency, and second, pre-existing ties, but especially family ties, are critical in forming the structure of the network. In addition, this analysis shows how such ties were co-opted to facilitate insurgent operations. Finally, from a methodological standpoint, it is important how we define the relationship. In this case, this is especially true for the money and resources mapping network. Statistically two actors may be equivalent, yet realistically this may not be true. Their equivalence may be an artifact of how I defined the relationship.

At this point, a more complete understanding of the nature of the network structure emerges. There is a clear division of labor within the network – financiers, decision makers, operators, logisticians, weapons’ distributors, etc. Control over the resources, and the importance of the node in the network, is derived from the division of labor, which gives some positions more control over critical tasks than others. Often, these roles are defined according to pre-existing ties – primarily familial ties, but also those linked by previous political, tribal, or organizational association. In turn, the key individuals in control of these critical tasks are connected to one another, thus forming a domain for each that gives them a high status in terms of prestige and influence. Finally, those that are not part of this core group and who sit on the periphery of these critical task relationships extend the network and allow it to operate at a far greater distance.

Consistent with prior research, this network clearly shows that cells – centered mainly around the chief of staff, the operations officer, the personal secretary, the operations and security officer, and Hussein’s sons – operated with relative independence and little oversight in the intermediate term, with Saddam providing long term oversight. It is likely that within these cells there was some turnover, or would be some turnover, in personnel. Such dynamics, however, are aided by the considerable equivalence of roles in the network so that persons can be deployed in different locations with ease, or eliminated if need be. Moreover, the equivalence in roles and positions creates a degree of resiliency by allowing for the development of certain forms of redundancy that facilitate recovery if part of the network is degraded or damaged.

## CHAPTER 10

### CONCLUSION

***Interviewer:** Had you been trained to cultivate intel, do investigative work, when you're trying to track these guys down, or was this something that you had to just learn on the job?*

***LTC Reed:** I don't think we've been trained specifically in the sense that, "Hey, when you're dealing with an insurgency or a Mafia-type organization, this is how you piece things together." I don't want to pat ourselves on the back too hard, but we're all pretty smart...the short answer to your question is no, we didn't really have any specific training, but I think it became intuitive for us... We had a couple folks we were looking for that we knew were pretty critical to leading us to Saddam, and we sort of fingered these guys through some old fashioned methods of looking at pictures and things like that. You look at all these pictures of people that appear with Saddam and you start putting names to them: "Okay I know that guy, I know that guy. Wait a minute, I don't know this guy, but he's part of this family." And you start putting this network together, so that's sort of how we got to a couple folks who were close to him.<sup>48</sup>*

The United States is confronted with an enemy who has adopted asymmetric strategies and tactics that enable it to mitigate U.S. strengths. Despite our conventional military superiority and successes in the effort to stem asymmetric attacks, the ability of our current adversaries to innovate and rapidly adapt their techniques continues to highlight gaps in U.S. conventional force capabilities. The enemy that we face as a nation requires that our military continue to change and modify its approach in order to ensure that it can accomplish its assigned missions (Lovelace and Votel 2004).

This is not the first time that the United States has had to confront the reality of an approach that was not aligned necessarily with the threat. In the late 19<sup>th</sup>

---

<sup>48</sup> This is an excerpt from an interview with the Operational Leadership Experiences group, Fort Leavenworth, Kansas, on 26 October 2005.

Century, for example, the U.S. Army embraced the conventional Prussian military system as the paradigm of professionalism at the same time the American Army was engaged in the frontier wars against the Indians – the most unorthodox of the U.S. Army’s 19<sup>th</sup> Century enemies (Cassidy 2004). The organization of the frontier Army in companies and regiments seemed absolutely conventional within the context of the times, but not the enemy! The American Army’s system of border outposts resembled the conventional strategic approach of the British in the American War of Independence. Unfortunately, although most Army officers recognized the Indian as the master of guerrilla warfare, the Army never institutionalized a counter-guerrilla doctrine, nor were there training programs, military schools, or literature on how to fight the Indians (p. 93).

A central component of the U.S. Army’s 20<sup>th</sup> Century organization and practice can be traced to its frontier mission – that is, a vigorous strategic and tactical offensive making use of the full array of military assets that the United States can bring to bear (Cassidy 2004, p. 99). Unfortunately, such an approach is less useful against a “guerrilla-type” enemy. One only needs to consider the Vietnam War and America’s preference to fight the war in a conventional manner with minimal constraints and limitations. In fact, the most significant feature of the United States’ 12-year effort in Vietnam was what little impact it has had on strategic thinking in the U.S Army – until now.

United States Army Chief of Staff, General Eric K. Shinseki, recognized the need for the Army to transform from one focused on a Cold War scenario to a force

that could meet the range and diversity of missions that it would need to undertake in the 21<sup>st</sup> Century. With the events of 9/11 as an even greater, albeit unfortunate, catalyst, current Army leaders have continued with Shinseki's initiatives. What is immediately clear is that the Army leadership has recognized that we are at war with a foe who requires us to adapt the organization in such a way that will allow for quick, integrated responses to the threat of asymmetry. I maintain that social network analysis provides the investigative skills necessary to analyze, understand, and exploit enemy vulnerabilities. In turn, this assists with better-tailored intelligence processes for understanding and targeting a constantly changing, decentralized, and asymmetric adversary.

We were all shocked by the tragic events of September 11, 2001. In the non-stop stream of news and analyses one phrase was continuously repeated - "terrorist network." Everyone talked about this concept, and described it as amorphous, invisible, resilient, and dispersed, but no one could produce a visual (Krebs 2002). Nowadays, many writings about terrorists, criminals, and activists observe that one grouping or another is organized as a network. However, the analyst should be able to specify more than simply that. Among other things, assessment at this level should include showing exactly what type of network design is being used, whether and how members may act autonomously, where leadership resides and/or is distributed, and whether and how hierarchical dynamics may be mixed in with the network dynamics (Ronfeldt and Arquilla 2001).

This dissertation uses the intelligence data that coalition forces gathered in Iraq that led to the capture of Saddam Hussein. I have subjected this data to a more rigorous analysis using the formal conceptualizations and methods of social network theory. However, as indicated in several places throughout this project, such an approach lends itself to data gathering effects in the findings. Information gathering focused on a particular individual, or individuals, may result in findings skewed in favor of one's importance, and the lack of importance of others, when in reality this may not be completely true. Nonetheless, I believe a significant contribution of this project is a description of which of these concepts and methods might prove to be useful when applied to an insurgency, thereby resulting in a systematic, network approach for analyzing an insurgent network.

In general, I found all of the selected measures to be useful in better understanding the Network of Saddam Hussein. However, they were not all useful to the same degree. The general network measures gave me an overview of what the network looked like – that is, the size of the network, the cohesiveness of the network, and key or significant ties – but most useful were the transitivity and clique analyses. Transitivity showed which linked network members drew others with whom they are linked into a cluster of ties, and further highlighted that it was family ties that accounted for many of the linkages. The clique analysis showed which actors were closely tied to other actors, and I also was able to discern which actors were in multiple cliques. In all, there were six major substantive findings. First, of the 214 actors in the total network, there are only 23 actors with direct ties to Saddam

Hussein. Second is that the overall network is not very dense. Third is the low transitivity of the total network. Fourth, there are a small number of cliques, and fifth, no clique is larger than three actors. The last important finding is that family relationships account for much of the identified clique structure.

The actor analysis helped me identify those actors who exerted the most influence or were the most prominent, or both, and re-confirmed the previous findings that the insurgency was aligned along pre-existing familial ties. Most useful were the measures of degree centrality, betweenness, and eigenvectors because they provided insight into who were the key players and how connected was the network. From this analysis, there were three substantive findings. First, actor A114, the chief of staff, was the most prominent and influential actor in the network. This confirms what we know to be true within organizations – that is, the importance of the chief of staff. Second, those connected by immediate family relationships form a local network, and thus are a cohesive, close-knit group. Third, this analysis clearly demonstrates that Saddam Hussein exerted a large amount of influence in insurgent operations.

Finally, the role analysis clarified positions of individuals in the network and which relationships tied actors to one another. The most useful measure in this analysis was the multiplexity measure because it clarified the multiple relationships of the network members. The role analysis confirmed two important findings from the preceding analyses. First is that Saddam Hussein was active in the insurgency, and second, pre-existing ties, but especially family ties, are critical in the forming the structure of the network. In addition, this analysis shows how such ties were co-opted

to facilitate insurgent operations. The equivalence measure was revealing from a methodological standpoint. Namely, it is important how we define the relationship. In this network, this is especially true for the money and resources mapping network. Statistically two actors may be equivalent, yet realistically this may not be true. Their equivalence was possibly an artifact of how I defined the relationship.

One of the more important findings in this analysis is how the network members co-opted the family structure for other purposes – for example, waging insurgent warfare or hiding Saddam Hussein. A tribal society already has at its disposal affiliated social, economic, and military networks easily adapted to war-fighting. The ways in which insurgents exploit a tribal network does not represent an evolved form of insurgency but the expression of inherent cultural and social customs (McCallister 2005). It is the traditional tribal network that proffers rebels and insurgents a ready-made insurrectionary infrastructure to draw on. Saddam Hussein's state reflected a mixture of traditional and modernizing autocracy in which he and his extended family functioned as patrons dispensing favors to social, economic, and military networks in return for their support. It was these ties and relationships that formed the core of the network which waged insurgent warfare and supported the ousted dictator's evasion from coalition forces.

To draw an accurate picture of a covert network, we need to identify task and trust ties between the conspirators. In my case, I defined task ties as those incorporating insurgent strategy and goals. Trust ties are those characterized by strong bonds formed over time either by family, friendship, or organizational

association. This data is occasionally difficult to unearth with cooperating clients. With covert criminals, the task is enormous, and may be impossible to complete. For Hussein's network, we gathered this data by pouring over historical documents and records, interviewing individuals in the network (and those outside of it), and looking over photos and books. It was painstaking work, but there is really no alternative when one is trying to piece together a network that does not want to be identified.

I constrained my analysis to the general categories outlined in Table 1 – trust ties: immediate family, extended family, close friend, and bodyguard; and strategy and goals ties: money and resources and insurgent operations. However, there are several relationships that could/should be analyzed separately in conjunction with another relationship. Taking the issue of multiplexity and insurgent operations as an example – by analyzing the link between Hussein and other insurgent members through the lens of either previous political association, village association, or school association, we may find that the one tie that most links members of the insurgent network is prior political association. This is a valuable insight in terms of understanding how to destabilize the network and/or locate Saddam Hussein. However, the only way to identify such a phenomenon is by analyzing the sub-networks of each of the larger categories, or, in this case, the close friend relationship.

While the mapping networks that I chose were grounded in previous research, I altered the categories a bit in light of my previous experiences and my belief that trust is an important component of this particular network. In general, I believe that these are a good starting point for analyzing the relationships within an insurgent

network. Clearly there are those who plan and execute attacks and those who resource operations. In this case, family relationships (immediate and extended) as well as close friendships were important in terms of understanding why and how ties formed. One category that I did not include, however, was ideology. Future analysis ought to include it. My relationships go beyond ideology since ideology is subsumed within each. However, considering present insurgent networks, this may not always be the case. Where kin and family were important in the Hussein network, this may not be true in an insurgent network presently operating in Iraq, and instead it may be only ideology that ties together certain members.

When we began to piece together Saddam Hussein's network, it started with Saddam. His ego network developed into an elaborate diagram that not only identified those tied to him by family or friendship, but also those linked to the insurgency. This project offers a method to build on such a process. Once one has determined how to destabilize the insurgent network (for example, to disrupt the leadership, or to disrupt the money supply), we can take a more systematic approach to collecting data and information on the insurgent members. For example, if the objective is to disrupt the issuance of orders that initiate an insurgent attack, we can focus our intelligence collection and information gathering on those who are central to the information flow from planner to executer. In turn, the betweenness measure then offers insight into which actors are more critical in this role than others.

The strength of this analysis lies in the identification of social network methods and measures that are useful in understanding the intricacies of an insurgent

network, most specifically with respect to why and how ties are formed between members. There is a value-added to employing a social network analysis approach to analyzing these networks. The methods that we used to piece together the Network of Saddam Hussein were obviously successful. Would the application of specific network methods as described in this project have made the process smoother and quicker? I do not know. What I do know, however, and what I have learned from this project, is that there is a very relevant and applicable body of knowledge within the social sciences that makes a very real contribution to understanding the dynamics and relationships of a networked, asymmetric enemy in the 21<sup>st</sup> Century.

The lessons from this research go beyond solely insurgent networks, but apply equally to all resistance-type networks, such as al Qaeda, the Ku Klux Klan, or the Mafia. As opposed to a more Weberian-influenced, hierarchical analysis, the challenge is to look across linkages and at the relationships between people and groups, similar to Simmel's conceptualizations. One needs to identify the significant patterns of motivation, interest, and need around which common action is organized. Once we have identified the system, we can then begin to tell something about the way behavior is summoned and constrained using the network concepts outlined in this project. Objectives and motivations may be different, but the conceptual network concepts remain the same.

As previous research indicates, the traditional paradigm of resistance organizations as hierarchical or pyramidal structures is not completely accurate. Instead, these organizations are often fragmented and chaotic with webs of affiliations

linking people of various positions and power. These patterns of affiliation and influence are far more important than any formal structure and allow criminals and the like to maximize many opportunities. This is why my work is relevant to not just insurgent networks, but to all types of criminal-like organizations.

Since Weber (1968) used the Prussian Army as his prototypical modern rational/legal bureaucratic organization (in *Economy and Society*), it has been common for military and police forces to both organize themselves along these lines, and to think of their adversaries in the same way. We now see that another classical German sociological theorist, Georg Simmel, offers us an alternative way to think about adversaries, be they insurgencies or criminal networks, and that networked organization might even be a direction in which military and police forces might be transformed to better address such adversaries.

I began this project by essentially asking how one understands the properties of an informal<sup>49</sup> and often unobserved social association, and then the impact of the structure of this association on the functioning of the group and/or the influence of this structure on the individuals in the group. In the end, I believe that the sociological contribution of my work is the demonstration of social network concepts, rooted in Simmel's work on affiliations, dyads, and triads, in addressing each part of this larger question.

Network concepts allow one to highlight the structure of a previously unobserved association by focusing on the pre-existing relationships and ties that bind

---

<sup>49</sup> "Informal" implies that there is the lack of a visible, formal structure. It may in fact exist, but it is not noticeable to an outside party.

together such a group. Likewise, by focusing on roles, positions, and those actors who are prominent and/or influential, one can get a sense of how the association is structured and thus how the group functions and how members are influenced and power is exerted. Finally, an understanding and examination of triads within the association of networked members will provide a window into how and why relationships are formed between the triadic members and to consider further whether such relationships are stable or unstable. The triads in this project were formed along pre-existing ties and were not newly formed, and are thus more likely to be stable. Network disruption should focus on newly formed triads.

## REFERENCES

- Alexander, C.N. 1963. "A Method of Processing Sociometric Data." *Sociometry* 26: 268-269.
- Arlacchi, Pino. 1986. *Mafia Business: The Ethic and the Spirit of Capitalism*. London: Verso.
- Babcock, Robert O. 2005. *Operation Iraqi Freedom I: A Year in the Sunni Triangle. The 4<sup>th</sup> Infantry Division and Task Force Ironhorse in Iraq*. Tuscaloosa, AL: St. John's Press.
- Baker, Wayne E. and Robert R. Faulkner. 1993. "The Social Organization of Conspiracy: Illegal Networks in the Heavy Electrical Equipment Industry." *American Sociological Review* 58(6): 837-860.
- Beckett, Ian F.W. 2005. *Insurgency in Iraq: A Historical Perspective*. Carlisle, PA: Strategic Studies Institute, U.S. Army War College
- Block, Alan. 1979. *East Side-West Side: Organizing Crime in New York 1939-1959*. Swansea, United Kingdom: Christopher Davis.
- Bonacich P. and P. Lloyd. 2001. "Eigenvector-like Measures of Centrality for Asymmetric Relations." *Social Networks* 23: 191-201.
- Borgatti, S.P., M.G. Everett, and L. C. Freeman. 2002. *UCINET for Windows: Software for Social Network Analysis*. Harvard, MA: Analytic Technologies.
- Burk, James. 1998. "Introduction, 1998: Ten Years of New Times." In *The Adaptive Military: Armed Forces in a Turbulent World*, edited by James Burk. New Brunswick, NJ: Transaction Publishers.
- Burk, James. 1998a. "Thinking Through the End of the Cold War." In *The Adaptive Military: Armed Forces in a Turbulent World*, edited by James Burk. New Brunswick, NJ: Transaction Publishers.
- Burlas, Joe. 2004. "'TF Soldier Focuses on Warrior Readiness.'" *Army News Service* 13 January.
- Burt, Ronald S. 2001. "Structural Holes versus Network Closure as Human Capital." In *Social Capital: Theory and Research*, edited by Nan Lin, Karen S. Cook, and R.S. Burt. New York: Aldine De Gruyter.

- Carley, Kathleen M., Ju-Sung Lee, and David Krackhardt. 2002. "Destabilizing Networks." *Connections* 24(3): 79-92.
- Cassidy, Robert M. 2004. *Peacekeeping in the Abyss: British and American Peacekeeping Doctrine and Practice After the Cold War*. Westport, CT: Praeger.
- Cebrowski, Arthur K. and John J. Garstka. 1998. "Network Centric Warfare: Its Origin and Future." *Proceedings* 124(1).
- Charrad, Mounira M. 2001. *States and Women's Rights: The Making of Postcolonial Tunisia, Algeria, and Morocco*. Berkeley, CA: University of California Press.
- Czarniawska, Barbara. 2005. "Networks, Networking, and Nets: NCW from an Organization Theory Perspective." In *Directions in Military Organizing*, edited by Karl Ydén. Stockholm, Sweden: Elanders Gotab.
- Clausewitz, Carl von. 1832/1984. *On War*. Princeton, NJ: Princeton University Press.
- Dekker, Anthony. 2002. "Applying Social Network Analysis Concepts to Military C4ISR Architectures." *Connections* 24(3): 93-103.
- Department of Defense News Transcript. 2003. *Ambassador Bremer Briefing from Baghdad* 14 December.  
<http://www.globalsecurity.org/military/library/news/2003/12/mil-031214-dod01.htm>
- Department of the Army. 2006. *Field Manual 3-24: Counterinsurgency (DRAFT)*. Fort Leavenworth, KS: U.S. Army Combined Arms Center.
- Egnell, Robert. 2005. "Achieving Effect in Contemporary Operations: Network Enabled Capabilities in a Changing Strategic Context." In *Directions in Military Organizing*, edited by Karl Ydén. Stockholm, Sweden: Elanders Gotab.
- 1st Brigade Combat Team, 4th Infantry Division Media Briefing, *Operation Red Dawn*, 15 December 2003.
- Fontenot, Gregory, E.J. Degen, and David Tohn. 2004. *On Point: The United States Army in Operation Iraqi Freedom*. Fort Leavenworth, KS: Combat Studies Institute Press.
- Forsythe, George B., Scott Snook, Philip Lewis, and Paul T. Bartone. 2002. "Making Sense of Officership: Developing a Professional Identity for 21<sup>st</sup> Century Army Officers." In *The Future of the Army Profession*, edited by Lloyd J. Matthews. Boston: McGraw-Hill.

- Franks, Frederick M. 2002. "Forward." In *The Future of the Army Profession*, edited by Lloyd J. Matthews. Boston: McGraw-Hill.
- Freeman, Linton C. 1979. "Centrality in Social Networks: Conceptual Clarification." *Social Networks* 1: 215-239.
- Friedman, Norman. 2003. *Terrorism, Afghanistan, and America's New Way of War*. Annapolis, Maryland. Naval Institute Press.
- Garstka, John J. 2000. "Network Centric Warfare: An Overview of Emerging Theory." *Phalanx* 33(4).
- Goodwin, Jeffrey Roger. 1988. *States and Revolutions in the Third World: A Comparative Analysis*. Unpublished Ph.D. dissertation, Department of Sociology, Harvard University.
- Gould, Roger V. 1995. *Insurgent Identities: Class, Community, and Protest in Paris from 1848 to the Commune*. Chicago, IL: The University of Chicago Press.
- Hage, Jerald. 2004. *The Intersection of Philosophy and Theory Construction: The Problem of the Origin of Elements in a Theory*. Unpublished paper presented at a conference on philosophy and sociology and anthropology at Emory University, Atlanta, Georgia, August 12-14.
- Hammes, Thomas X. 2004. *The Sling and the Stone: On War in the 21st Century*. St. Paul, MN: Zenith Press.
- Hanneman, Robert A. and Mark Riddle. 2005. *Introduction to Social Network Methods*. Riverside, CA: University of California, Riverside
- Haythornthwaite, C. 1999. *A Social Network Theory of Tie Strength and Media Use: A Framework for Evaluating Multi-level Impacts of New Media* (Technical Report UIUCLIS--2002/1+DKRC). Champaign, IL: Graduate School of Library and Information Science, University of Illinois at Urbana-Champaign.
- Henderson, Simon. 1991. *Instant Empire: Saddam Hussein's Ambition for Iraq*. San Francisco: Mercury House.
- Janowitz, Morris. 1960. *The Professional Soldier: A Social and Political Portrait*. New York: The Free Press.
- Karsh, Efraim and Inari Rautsi. 1991. *Saddam Hussein: A Political Biography*. New York: The Free Press.

- Kestnbaum, Meyer. 2005. "Mars Revealed: The Entry of Ordinary People into War among States." In *Remaking Modernity: Politics, History, and Sociology*, edited by Julia Adams, Elisabeth Stephanie Clemens, Ann Shola Orloff. Durham, N.C.: Duke University Press.
- Krebs, Valdis E. 2002. "Mapping Networks of Terrorist Cells." *Connections* 24(3): 43-52.
- Lind, William S. 2004. "Strategic Defense Initiative: Distance from Disorder is the Key to Winning the Terror War." *The American Conservative*. 22 November.
- Lind, William S., Colonel Keith Nightengale (USA), Captain John F. Schmitt (USMC), Colonel Joseph W. Sutton (USA), and Lieutenant Colonel Gary I. Wilson (USMCR). 1989. "The Changing Face of War: Into the Fourth Generation." *Marine Corps Gazette* October, pp. 22-26.
- Loeb, Vernon. 2003. "Clan, Family Ties Called Key to Army's Capture of Hussein." *Washington Post* 16 December.
- Lovelace, James J., Jr. and Joseph L. Votel. 2004. "The Asymmetric Warfare Group: Closing the Capability Gaps." *Army March*, pp. 29-34.
- Manwaring, Max G. 2005. *Street Gangs: The New Urban Insurgency*. Carlisle, PA: U.S. Army War College.
- Marsden, Peter V. 1990. "Network Data and Measurement." *Annual Review of Sociology* 16: 435-463.
- Martin, Gregg F. and Jeffrey D. McCausland. 2002. "The Role of Strategic Leaders for the Future Army Profession." In *The Future of the Army Profession*, edited by Lloyd J. Matthews. Boston: McGraw-Hill.
- McCallister, William S. 2005. "The Iraqi Insurgency: Anatomy of a Tribal Rebellion." *First Monday* 10(3).
- McIlwain, Jeffrey Scott. 1999. "Organized Crime: A Social Network Approach." *Crime, Law, and Social Change* 32(4): 301-323.
- Mitchell, J.C. 1969. "The Concept and Use of Social Networks." In *Social Networks in Urban Situations*, edited by J.C. Mitchell. Manchester: Manchester University Press.
- Moreno, J.L. 1978. *Who Shall Survive?* Beacon, N.Y.: Beacon House Inc.

- Moskos, Charles C. and James Burk. 1998. "The Postmodern Military." In *The Adaptive Military: Armed Forces in a Turbulent World*, edited by James Burk. New Brunswick, NJ: Transaction Publishers.
- Musallam, Musallam Ali. 1996. *The Iraqi Invasion of Kuwait: Saddam Hussein, His State, and International Power Politics*. London: British Academic Press.
- Nagl, John A. 2002. *Counterinsurgency Lessons from Malaya and Vietnam: Learning to Eat Soup with a Knife*. Westport, CT: Praeger.
- Operational Leadership Experiences. 2005. *Interview with LTC Brian Reed (2005-10-26)*. Fort Leavenworth, KS: Combat Studies Institute.
- Pfeffer, Jeffrey. 1992. *Managing with Power: Politics and Influence in Organizations*. Boston, MA: Harvard Business School Press.
- Ritzer, George. 1996. *Classical Sociological Theory*. New York: McGraw-Hill.
- Ronfeldt, David and John Arquilla. 2001. "Networks, Netwars, and the Fight for the Future." *First Monday* 6(10).
- Rothenberg, Richard. 2002. "From Whole Cloth: Making up the Terrorist Network." *Connections* 24(3): 36-42.
- Sarkesian, Sam C., John Allen Williams, and Fred B. Bryant. 1995. *Soldiers, Society, and National Security*. Boulder, CO: Lynne Rienner Publishers, Inc.
- Segal, David R. 1993. *Organizational Designs for the Future Army*. Alexandria, VA: U.S. Army Research Institute for the Behavioral and Social Sciences.
- \_\_\_\_\_. 1989. *Recruiting for Uncle Sam: Citizenship and Military Manpower Policy*. Lawrence, KS: University Press of Kansas.
- Segal, David R. and Dana P. Eyre. 1996. *The U.S. Army in Peace Operations at the Dawning of the Twenty-First Century*. Alexandria, VA: U.S. Army Research Institute for the Behavioral and Social Sciences.
- Segal, David R. and Ronald B. Tiggler. 1997. "Attitudes of Citizen-Soldiers Toward Military Missions in the Post-Cold War World." *Armed Forces and Society* 23: 373-390.
- Selznick, Philip. 1960. *The Organizational Weapon: A Study of Bolshevik Strategy and Tactics*. Glencoe, IL: The Free Press.

- Simmel, Georg. 1950. *The Sociology of Georg Simmel*. Glencoe, IL: The Free Press.
- Simmel, Georg. 1908/1955. *The Web of Group-Affiliations*. Glencoe, IL: The Free Press.
- Skocpol, Theda. 1994. *Social Revolutions in the Modern World*. New York: Cambridge University Press.
- Sparrow, Malcom K. 1991. "The Application of Network Analysis to Criminal Intelligence: An Assessment of the Prospects." *Social Networks* 13: 251-274.
- Von Lampe, Klaus and Per Ole Johansen. 2003. *Criminal Networks and Trust*. Paper presented at the 3<sup>rd</sup> Annual Meeting of the European Society of Criminology, August 29.
- Wasserman, Stanley and Katherine Faust. 1994. *Social Network Analysis: Methods and Applications*. New York: Cambridge University Press.
- Watts, Duncan J. 1999. *Small Worlds: The Dynamics of Networks Between Order and Randomness*. Princeton: Princeton University Press.
- Weber, Max. 1968. *Economy and Society*. Totowa, N.J.: Bedminster Press.
- Wellman, Barry. 1983. "Network Analysis: Some Basic Principles." *Sociological Theory* 1: 155-200.
- Williams, Phil. 2001. "Transnational Criminal Networks." In *Networks and Netwars: The Future of Terror, Crime, and Militancy*, edited by John Arquilla and David Ronfeldt. Santa Monica, CA: The RAND Corporation.
- Zogby International. 2006. *U.S. Troops in Iraq: 72% Say End War in 2006*. <http://www.zogby.com/news/ReadNews.dbm?ID=1075>