ORGANIZATIONS, TECHNOLOGY, AND NETWORK RISKS:

How and Why Organizations Use Technology to Counter or Cloak their Human Network Vulnerabilities

By

Ekaterina (Katya) Drozdova

Dissertation submitted in partial fulfillment
of the requirements for the degree of
Doctor of Philosophy

Department of Information, Operations, and Management Sciences
Leonard N. Stern School of Business
New York University

May 2008

Professor Roy Radner, Co-Chair

Professor Roger Dunbar, Co-Chair

Professor Foster Provost

ABSTRACT

This dissertation is about *organizational fault-tolerance* and its implications for *national security* and *business continuity*. It investigates how technology effects organizational survival and performance in hostile and competitive environments. The study identifies how an organization's structure and processes involving technology-use relate to its mission and operating environment. By investigating how these relationships develop over time, the study identifies fault-tolerant and fault-intolerant humanly-managed network structures within organizations. It explains how these structures perform shaped by organizational mission, environment, and technology choices.

First, the study uses information theory and probabilistic information-entropy methods to identify missions and environments that implicitly predict contrasting organizational technology choices. Results generate dimensions for selecting two polar-opposite organization cases. Second, it uses organization theory and case-study methods to analyze technology choices made by the two organizations to implement their different missions in contrasting environments. A comparison of the two cases identifies alternative organizational approaches for structuring their networks and using technology to mitigate risks. These approaches also explain ways in which organizations may design their networks and use technology to reduce vulnerabilities or conceal them from adversaries.

The results uncover characteristics of organizational environments, missions, and structures that generate technology strategy options. Specifically, in environments dominated by a hostile opponent, organizations prioritize survival

above performance. Network designs include adopting sparsely connected structures, restricting information, and relying on “lower-tech” physical interaction based solutions that support node independence and self-sufficiency and limit network traceability. In subversive networks and non-monetary missions, these strategies curb the initiating power of potential failure points concealing network structure from the opponent. Alternatively, in the absence of hostility, organizations focus on performance. Network strategies include adopting highly connected structures, distributing information, and integrating redundant components to support network traceability and facilitate broad reach and economies of scale. These strategies identify two contrasting network organization classes based on their structural fault-tolerance.

The thesis contributes to our understanding of how and why technology choices affect organizations. Results contribute to organization theory and analysis methods, with applications for counterterrorism and energy security, among other business and policy issues.

CONTENTS

Chapter 1

PROBLEM DESCRIPTION AND RESEARCH QUESTION

Organizational failures can be catastrophic, and mitigating or eliminating them presents a formidable challenge. Hostile environments that threaten organizational survival compound the risk. This dissertation examines the role of technology in organization survival and risk mitigation strategies.

Research Question:

How does technology effect organizational survival?

Organization theory posits that technologies affect organizational abilities through networks that facilitate communications, actions and production. Organizations need networks not only to perform tasks but also to direct, coordinate, monitor and control actions. The technologies used in networks affect organization performance and survivability by enabling or restricting information flows, resource allocation, network connectivity, and action traceability.

The technologies and network designs that organizations choose both enable and constrain them. Specific technology choices diverge along a “hi-tech” vs. “lower-tech” dimension. Generally, low(er)-tech choices rely on interactions between people, whereas high-tech choices use the latest modern technologies to extend organization reach independent of people.

Lower-tech solutions tend to be technologically simple, robust and rely on people and physical objects for limited transactions. Typically, they are not scalable to large networks, nor are their uses easily traceable. Hi-tech solutions extend organizational networks and knowledge bases, efficiently support multiple transactions, and their actions are traceable across networks. They are technologically complex and rely on costly infrastructures. As hi-tech frontiers advance, lower-tech options remain available to individuals and organizations.

High- versus lower-tech choices may counteract each other. For example, in combating terrorism, despite the overwhelming technological and resource superiority of the United States (US), terrorists and insurgents continue to rely upon relatively rudimentary equipment. Yet, the difficulty in tracing their actions effectively threaten US national security. Their activities challenge government detection and counteraction strategies built around hi-tech cyber-warfare components, such as electronic surveillance. This low-tech challenge to a hi-tech solution combines civilian disguise with face-to-face messenger communications, cash or barter transactions, and basic-to-crude weaponry for attacks (using box cutters, homemade explosive devices, etc.). These tactics reflect an asymmetric use of technology and make ongoing terrorist activities difficult to detect, trace and counteract by hi-tech means.

Hi-tech vs. lower-tech interplay can reinforce rather than counteract. The 2003 electricity blackout in Northeast USA was partly due to simple human errors coupled with computer failures. Specifically, having completed manual (low-tech) repairs to a hi-tech energy information system, an operator failed to restart the system's automated mode. The repair appeared sufficient because it reflected energy outages at the time of the manual work. However, when new outages occurred and updating technologies failed, the lack of real-time status traceability

across the grid contributed to faulty decisions and actions by other organizations in the grid. Accumulated faults reinforced each other, cascading into massive disruptions of energy supply.

To advance our understanding of technology's effects on organizations, this study analyzes the ***relationships*** between: (1) *mission* and characteristics of an organization's ***outside environment***, (2) *network structures* and operational *processes* ***inside the organization***, and (3) organizational ***technology use***.

The analysis employs information and organization theories, as well as statistical and case study methods. Statistical methods explain how technology preferences may reflect contrasting organizational and environmental traits. These traits identify dimensions for selecting and comparing specific cases. Case-study methods explain why organizational participants use particular technologies to deal with the risks. By including a terrorist organization, al Qaeda, and an energy company, Cinergy, the cases contrast the effects of network structures and technology.

Chapter 2

SUMMARY OF PRINCIPAL FINDINGS AND CONTRIBUTIONS

The study found that the effectiveness of a technology to support an organizational network differs based on the *structure* of that network in the context of its *mission* and *environment*. The study classifies organizations as fault-tolerant or fault-intolerant based on their network structures. The contrast stems from the *differential impact of single node failure* within a network. *Fault-Intolerant Network Organizations (FINO)* are organizational structures with single nodes which, if one fails, can potentially cause catastrophic network-wide effects. *Fault-Tolerant Network Organizations (FTNO)* are all other organizations.

FTNOs *increase their structural tolerance to faults* through strategies and technologies that *increase their systemic reliability.* Specifically, FTNOs pursue reliability through redundancies in network nodes, links, and critical functions. Examples of FTNO include typical modern energy infrastructures, business corporations, and US military forces. FTNOs use technology to integrate the network and disperse information to quickly detect and remedy unit failures using substitute units. Sophisticated modern technologies support organization connectivity, traceability and scale-efficiency. Technologies enabling FTNOs include the Internet, electronic information processing, and computerized global positioning, financial and information systems—and this study characterizes these technologies as hi-tech.

In contrast, **FINOs** are vulnerable to disruption from network nodes. FINOs *reduce their structural intolerance to faults* through strategies and technologies that *increase individual-node reliability*. Because any link in the network may lead to a catastrophe, FINOs minimize the number of operational nodes and links. FINOs survive crises by disguising or destroying network units. FINO examples include terrorist, insurgent, and espionage networks, political campaigns, and some craft industries. They rely on simple, fail-safe technologies, which are largely independent of infrastructures. They support node self-sufficiency while impeding network connectivity and traceability. Technologies enabling FINOs include physical transactions, face-to-face communications, improvised techniques, and manually-oriented equipment. This study characterizes such technologies as low- or lower-tech. Although an individual node failure in a FINO can produce a catastrophic effect, low-tech strategies build reliability into individual nodes, limit damage and allow the organization to recover.

Why would an organization adopt FINO structures and then use low-tech technologies when higher-tech and more fault-tolerant ways are available? Their mission and environment determine this choice. In environments dominated by hostile opponents—defined as entities which seek to destroy their target organization—and where there is incomplete information, FINO networks and vulnerabilities are difficult to discover because they have fewer elements to trace. Use of technology by FINOs, however, can change opponent's information and knowledge of the FINO organization, and so technology choices become vital to FINO survival.

Improved knowledge enables one to better target interventions against the FINO, and FINO's choices of technology affect its vulnerability to such targeting. Modern hi-tech devices create electronic traces of organizational

activity. Monitoring traces improves the opponent's knowledge of the FINO, increasing its risk of detection and damage from counteraction. Alternatively, lower-tech effectively conceals FINO network vulnerabilities. Incomplete information obtained from monitoring a FINO is important because if a hostile opponent knows a FINO's network structure, survival strategies based on network concealment would not suffice. Rather, it would benefit from adopting FTNO strategies. The findings about FINO vulnerabilities and concealment strategies provide insights into detecting and affecting FINO networks, examples of which include terrorist networks.

The study finds that environmental hostility and network structures determine organizational technology preferences, with the organizational mission mitigating these preferences. Organizations with missions that are not monetary (e.g., ideological, political, scientific) have less incentive than profit-oriented organizations to pursue scale-efficiencies afforded by hi-tech. Organizations motivated by profit tend to operate in competitive markets where efficient use of resources often determines survival. In contrast, the survival of organizations with other missions often depends on issues (such as secrecy, security, adherence to ideological beliefs, etc.) that do not necessitate operational efficiency. Challenging or changing environments, such as combat zones or technologically-intensive markets, can expose organizational vulnerabilities.

Organizations design their networks and use network technologies differently, according to their missions and environments. The FINO vs. FTNO structures represent alternative extreme approaches. The two organization cases exemplify these extremes and their survival strategies.

The al Qaeda case shows that, although the organization has survived counterterrorist operations, its core organizing system is vulnerable. Strategies designed to cloak the organization's *fault-intolerant network structure* explain its *fault-tolerant behavior*. Al Qaeda consistently employed FINO networks, restricted information, and relied on low-tech solutions to suppress network traceability and evade US detection when planning and executing attacks. An effective way to address its low-tech tactics may be by infiltrating the organization and directly obtaining actionable intelligence. Operational dangers and constraints, however, necessitate alternative approaches that take advantage of the US edge in hi-tech, yet address low-tech threats which are at the forefront of combating such terrorist networks.

The findings provide insights and methods for developing such approaches, e.g., for computationally modeling intelligence data to generate indicators of impending terrorist attacks—based on the organization's detectable activity traces coupled with understanding of its structures, properties and motivations. Specifically, uncovered terrorist technology strategies suggest ways to prevent a major attack by focusing on certain low-tech activity patterns that both indicate and conceal the likely attack preparations.

The findings also suggest how to project and manage future developments. As it becomes more difficult for al Qaeda to function, train, and develop new operational methods, they may need to adapt the organizing system to survive and conceal activity. The analysis uncovered al Qaeda's strategies to evade detection and minimize network traces. By identifying the survival strategies, structures and potential failure modes of the al Qaeda organizing system, the analysis also found core properties of this system that are likely to persist. As long as al Qaeda pursues its hostile mission, and counterterrorist authorities pursue al

Qaeda, these core properties will persist because they derive from the organization's mission and hostile environment. Their knowledge can help destroy terrorist systems.

The case of Cinergy compares and explains a polar-opposite organizing system in terms of network structure, mission, environment, and technology's effects. Although Cinergy has experienced network breakdowns such as communications and energy disruptions during a blackout, its core organizing system's design sustained even multiple failures. Strategies designed to support organization's *fault-tolerant network structure* explain its *fault-tolerant behavior.* Cinergy consistently employed FTNO networks and dispersed information, in order to maintain network traceability and connectivity preventing network-wide effects of single failures. When hi-tech information technology (IT) systems broke down, Cinergy operators used lower-tech methods but in traceable ways to approximate hi-tech solutions. This helped manage the crisis locally but became unsustainable on a larger grid scale due to human as well as technological factors.

The findings provide insights and methods towards developing potentially more resilient energy systems—based on a better understanding of the interplay between their technological and human networks. Results identified and explained core properties of Cinergy's generally resilient organizing system, as well as its potential failure modes. These core properties will likely persist because they derive from the organization's mission and competitive yet regulated environment. Their knowledge can help strengthen energy systems.

The study's analytical framework integrates and extends insights from social and information sciences on network organizations and technology.

Chapter 5

ORGANIZATIONS FROM THE INSIDE: EXPLORING ALTERNATIVE NETWORK DESIGNS

5.1 Theoretical Framing using Discourse Theory

The case studies describe how technology links people to create alternative network organization designs. The cases illustrate how these designs interact with different environments to generate fault-tolerant or fault-intolerant organizational outcomes. To identify a design, one must trace how the technology allows an organization to function and respond to risks, threats and new situations. Crises are especially informative (see e.g., McClelland, 1961; May & Davis, 2006). The use of technology during a crisis often reveals obscure or inactive organizational properties, turning points and adaptive abilities (Fairclough, 1992). Choices and outcomes about technology use depend not only on relations among network nodes, but also on network processes. Participant skills, learning and motivations also affect outcomes (Dunbar & Starbuck, 2006).

The case studies identified how people used technology by analyzing narratives about participants' knowledge and use of available technologies and action options. In the narratives, members of these networks explain how they work. The data sources include documents issued by the organizations themselves, as well as industry, government, media, and court records.

Organizational narratives document how these networks link individuals, technologies, events and their subsequent interactions over time. The case studies use these documents to trace technology use, how and why uses occurred, and how they resulted in contrasting network designs.

5.2 Analytical Methods

Each case study used the same analytic process adapted from Greimas' (1987) approach to discourse analysis. According to Greimas (1987), organizational narratives span three levels of analysis: "deep structure", "surface structure", and "manifestation structure", also called "operational". Technology structure is ultimately an element of "manifestation structure" and is consistent with the content of the other two levels.

5.2.1 Deep Structure: Identifying Organizational Goals, Mission, and Environment

According to Greimas (1987), deep structure identifies and makes explicit rules and constraints that govern organizations through texts that convey their forces and values (Fiol, 1991). Rooted in structural linguistics (Fiol, 1991), deep structure summarizes the evidence for recurrent opposing forces governing organizational actions. This study focuses on how organizations use technology, hence, the deep structure originates in an organization's primary documents that describe what it does and what technology supports. These may be contained in sections of official leader accounts, bylaws, annual reports, operational and

training manuals, documents that describe organization goals, environments, purposes, procedures, actions, and documents about an organization's mission.

Deep structure analysis identifies the forces that an organization must deal with regularly in order to carry out its mission, survive and thrive. An organization's dominant positive force (value) emerges from emphasizing particular purposes in its mission statements and performance evaluation criteria. The opposing force emerges from the organization's depictions of its challenges and constraints. Evidence of these forces exists in statements about the organization and how they depict competitors or adversaries. It might also be evident in the restrictions inherent in providing services. A systematic analysis of narratives documenting organizational activity allows one to verify these forces and trace their manifestations in participant actions.

Research inquiries into deep structure focus on how participants define the purpose of the organization and what it does. The approach uses semiotics — a formal mode of analysis to identify the rules about how signs convey meanings in a particular social system (Eco, 1979; Fiol, 1991). Semiotic inquiries are context-specific, defining the meaning of the phenomenon based on its underlying value oppositions. Context-specific meanings demonstrated through recurrent actions reveal a value framework that is systematic enough to generate expectations that an analysis of events can confirm (Fiol, 1991). A "semiotic square" framework in Figure 1 (Greimas, 1987; Felluga, 2008; Fiol, 1991; Taylor & Van Every, 2000) represents deep structure:

> "The dominant positive value of the (organization) being analyzed is, by convention, positioned in the upper left corner of the square. Logical relations of implication, contrariety, and contradiction govern the positions of the other three values (such that) assertion of the dominant value presumes the negation of its contrary…, while negation of the contrary only allows the possibility of the dominant value… The emphasis… is on two value terms in a… tension of opposites" (Fiol, 1991, p. 553-557, emphasis added).

The "contrary", "contradiction" and "implication" terms in semiotic analysis refer to logical relations that play out in narratives. They can be traced back to Aristotelian "Contrary and Contradictory" definitions (350 B.C.E) and formal logic (Truss, 1998; Nilsson, 1980) but often manifest less precisely in particular narratives. The strength of the approach is that it allows one to systematically analyze narrative data generated by actual organization participants, map out different forces, constraints and their logical interpretations, and understand events, actions, and their implications.

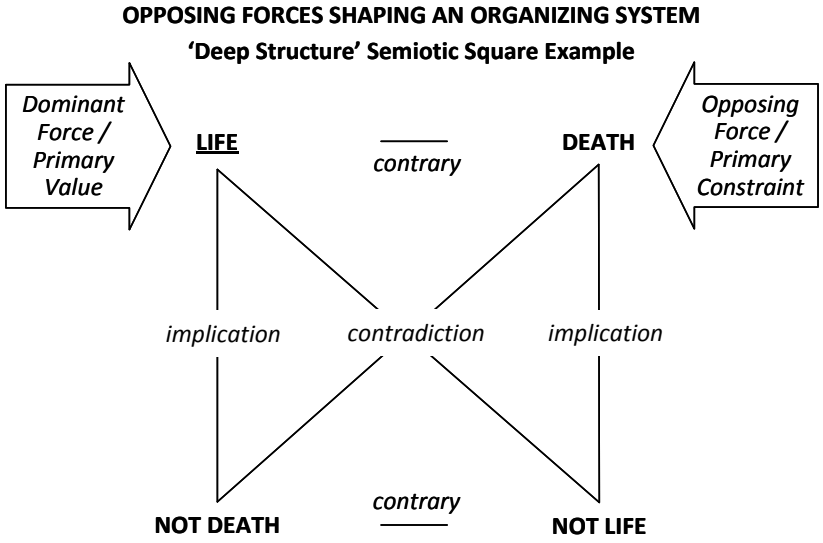

Figure 1: Illustrative example of deep-structure organizing system. A mapping of dominant positive and opposing forces shaping an organization, as represented by a "semiotic square" (following Greimas' (1987) et al. approach).

Fiol (1989, 1991) argued that the deep structure's countervailing forces lead to emergent events as an organization faces different situations. The semiotic-square representation of deep structure enables analyzing organizational narratives by systematically identifying alternative explanations for participant choices and outcomes. On the surface, the states of the forces can change over

time and so the situation faced by an organization can also change (Czarniawska, 2004). Tracing the manifestation of underlying relationships between contrary forces shows that they remain the same and reveals the principles underlying these relationships.

Thus, the approach avoids predictions based on the semiotic square but forces one to examine alternative implicit possibilities. These enable one to identify alternative states of the underlying forces that determine the situations and action options the organization may face. For instance, in Figure 1, "not life" in some situations may imply having died, whereas in others—not having been conceived or borne. An organization like the Catholic Church upholds the former position, whereas the 1973 US Supreme Court allowed the latter legal interpretation. The outcomes highlight alternative socio-cultural implications and action options. A semiotic square clearly focuses on various possibilities that are always implicit in the underlying forces facing an organization.

To identify the positive force in each case, this study examined official public statements to determine how each organization described its mission, goals, values and environment, and what it actually does. These documents included leaders' public statements, rules, manuals, and annual reports, which also provided evidence for the organization's challenges, threats and constraints. Additional evidence for opposing forces came from statements from organizations that pose some of these threats or impose these constraints (e.g., adversaries, competitors, regulators). The logical implications of two opposing forces constituted the deep structure in narratives about how an organization develops.

Consequently, the deep structure should be implicit and traceable in narratives that describe an organization's specific actions and development. These

narratives provide “surface structures”. The research question guides the choice of surface structure narratives and the unit of analysis (Fiol, 1991). In this study, the research aim was to identify patterns in how organization participants used technologies to do organizational tasks, how their uses of technology then formed networks, and how these networks performed, overcame crises, evolved, and survived over time.

5.2.2 Surface Structure: Examining Narrative Evidence

The surface structure is a narrative that documents organization activity over time. In each case, evidence came from transcripts of actual activities, recorded by organization participants, and made available by the US government via communications and transaction transcripts, court records, sworn witness testimony, and official congressional inquiry materials. We verified the facts using independent background sources, such as research investigations, publicly-available intelligence reports, media reports, and primary documents. (Each case study describes specific narratives and sources.) The standard legal format of these transcripts facilitated uniform data sources from surface structures.

5.2.3 Data Generation: Converting Surface Structure to Technology Use Data

Potentially, the narratives provide chronologies of events including participant accounts and activity records of what technologies were used, by whom, when, how, and to what effect. Narratives had to be coded to generate

analyzable chronologies. The unit of analysis was any documented use of technology to support information handling, with a focus on communications and financial transactions. Data were coded by extracting specific technology-use events and their characteristics from the surface structure narratives. Table VI presents the categories used to identify and code a particular technology-use event. The database reflected objective characteristics of the technologies as well as of the user and situation.

Agents (Organization Nodes)	…
Operational Roles	…
Mission Detail	…
Node Location	…
Technology Used	…
Technology Use Location	…
Task Type	…
Contact Direction	…
Event Description (narrative source quote)	…
Timeframe (Time, Day, Month, Year as appropriate)	…
Reference	…

Table VI: Data coding of technology-use events from surface structure narratives

The study used these data to convert narrative surface structures into codes which quantified technology use.

5.2.4 Manifestation Structure:
Identifying and Analyzing Operational Networks Manifest in Technology Use

Network designs manifested through technology use reveal an organization's operational structures and processes. As they use technologies, individuals create network links and become nodes in networks of people, which

result in structured social networks. In this analysis, networks emerged from the nodes using technology, and evolved as the nodes interacted or stopped interacting via different technologies as events unfolded.

The analysis investigated network structures that defined the technology use options, and factors that influenced participants' use of those options. The frequencies of particular technologies used and records of who used them, how and when, revealed patterns of choices and preferences. The analysis then identified how recurrent patterns emerged in response to new events.

Thus, the study investigated how these systems functioned, what risks they faced, where and why they were vulnerable, and how participants dealt with these risks and vulnerabilities. We examined how technology use choices mitigated or exacerbated these risks and vulnerabilities. Possible explanations for these developments formed propositions (Miles & Huberman, 1984). These propositions identified systematic differences between the network organization designs represented by the two cases. By comparison, the case findings clarify more generally the implications of technology use choices for fault-tolerant and fault-intolerant network designs.

5.2.5 Analytic Process Summary

Each case study uses the same analytical process: (i) identify the "deep structure" of countervailing forces that shape the issues each organization deals with, (ii) find narratives that document these forces in action over time, using transcripts of activities that constitute the "surface structure," (iii) code transcripts and convert them into chronologies of discrete events involving technology use , (iv) use these coded data to identify the relevant manifest structure and trace and

analyze the networks people created through technology use ("manifestation structure"). Further analysis of this manifestation structure identifies the vulnerabilities and survival strategies associated with these different networks.

5.3 Case Studies

Case 1: Al Qaeda

Al Qaeda Deep Structure: Goals, Mission, and Environment

Al Qaeda's leaders have explained that Al Qaeda attacks those it considers enemies of Islam (Bin-Laden, al-Zawahiri, Taha, Hamzah, & Rahman, 1998). The US Congressional investigation into the 9/11 attack on the United States, one of al Qaeda's most deadly and defining operations, depicts al Qaeda as a "new breed" of terrorist organization that favors militant Islamic agenda, lacks a state sponsor, and is loosely organized as a transnational network (9/11 Commission, 2002, p. 194). Its founding leader and financier, Osama bin Laden (OBL), with its chief ideologue, Ayman al-Zawahiri, established al Qaeda. It emerged after the war between the Soviet Union and anti-government mujahideen in Afghanistan, and has since carried numerous attacks. At the same time, it has trained, organized, funded, and inspired Islamic militants worldwide.

Al Qaeda traces its ideology to Salafist teachings of the Sunni branch of Islam: "our ideology is to fight a holy war" (jihad) with "full adherence to the Sharia (Islamic law) and… according to the Koran and the Sunna" (al Qaeda Bylaws). Al Qaeda's Constitutional Charter, Rules and Regulations describe the

organization as: “An Islamic Group, its only mission is Jihad, because Jihad is one of the basic purposes for which Al Qaeda personnel come together…” with the goals of “the establishment of an Islamic Regime and the restoration of the Islamic Caliphate”. Membership requires “compliance with Al Qaeda beliefs and goals”, “subordination and obedience”, and “taking the pledge of allegiance” (US Department of Defense “Harmony” Database of al Qaeda documents captured in Afghanistan and translated by the US Defense Intelligence Agency).

Al Qaeda’s Training Manual (discovered at its safe house in England and used as evidence for the prosecution in USA vs. OBL et al., 2001) elaborates: “Islamic governments have never and will never be established through peaceful solutions and cooperative councils. They are established as they (always) have been by pen and gun by word and bullet by tongue and teeth.” “The confrontation that we are calling for with the apostate regimes… knows the dialogue of bullets, the ideals of assassination, bombing, and destruction, and the diplomacy of the cannon and machine-gun”.

Among “apostate regimes”, in al Qaeda’s view, “American enemy is the principle and the main cause of the situation. Therefore, efforts should be concentrated on killing the enemy” (OBL, 1996) and causing “America to suffer human, economic, and political losses" (OBL, 2004). In a declaration of Jihad against the West and Israel (1998), Bin Laden and other al Qaeda leaders proclaimed that “to kill the Americans and their allies—civilians and military—is an individual duty for every Muslim who can do it in any country in which it is possible to do it”.

A comparison of al Qaeda and American leaders’ statements underscores the opposition of values and goals. For example, in the al Qaeda value system,

"freedom and democracy" constitute "destruction", whereas "terrorism and intolerance" constitute righteous "resistance" (OBL, 2004). On the contrary, President George W. Bush emphasized the need to fight al Qaeda and other terrorists until "the cause of freedom will once again prevail" (Bush, 2005). The US has devoted substantial resources to detecting, counterattacking, and destroying al Qaeda.

Al Qaeda's mission and survival also depend on its ability to evade detection. Al Qaeda documents consistently emphasize secrecy and concealment. For instance, even before US retaliation for 9/11, OBL proclaimed that "due to the imbalance of power between our armed forces and the enemy forces, a suitable means of fighting must be adopted i.e. using fast moving light forces that work under complete secrecy" (OBL, 1996). Operational and training manuals teach communications secrecy, use of disguises, organization concealment, undercover operations, detection evasion, how to withstand interrogations, and other intelligence and counterintelligence techniques (Al Qaeda Training Manual circa. 2001; "Harmony" Database).

US field reports corroborate al Qaeda's focus on concealing its operations to offset the US military superiority. For example, former (acting) CIA Director John McLaughlin testified that al Qaeda "compartments secrets down to a handful of people" and "use(s) secrecy as a strategic weapon." He explained that secrecy is "a strategic weapon for them because it asymmetrically works against us because we don't keep secrets very well" (Gertz, 2004).

These countervailing forces—attacking versus remaining concealed—shape the al Qaeda organizing system. Al Qaeda's militant Islamic ideology and funding, recruitment and other resources that sustain operations drive the forces

that contribute to its goals and represent the primary pole in this organizing system. Its need to conceal operations from external threats in order to survive counterattacks represent the opposing pole. They create contrary pressures, as neither can be fully achieved at the same time in the same situation: an attack reveals information. It exposes the organization to potential counteraction. Al Qaeda uses concealment strategies to limit exposure, but can only fully avoid it by ceasing attacks and ultimately ceasing operations, as al Qaeda's enemies may still attack even when it does not. The logical implications of these opposing forces generate additional outcome alternatives completing this mapping of al Qaeda's organizing system (Figure 2).

The poles in Figure 2 enable a systematic understanding of the pressures that shape al Qaeda's operational constraints and actions. For instance, al Qaeda may manage the risk in different situations by attacking physically, through cyberspace or political subversion; varying communications; and claiming or not claiming responsibility for actions that are difficult to attribute. Concealment effects of such choices will vary. Its stated mission, however, drives it to continue violent attacks in order to attract resources needed to survive. Yet, every such action provides Al Qaeda's enemies with information that can be used to destroy it, constantly forcing it to manage these countervailing pressures.

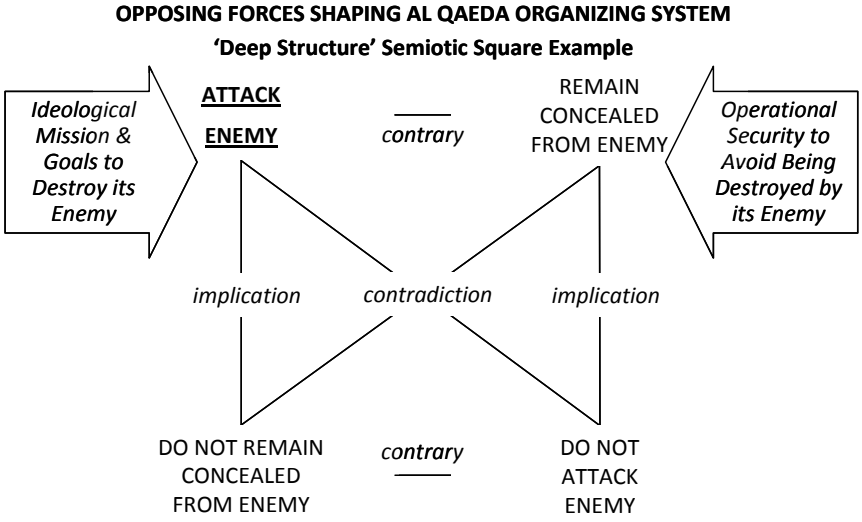

Figure 2: Al Qaeda organizing system's semiotic square

Proposition 1: The contrary forces defining al Qaeda organizing system are its mission to attack its enemies versus the need to stay concealed from its enemies to insure survival.

Technology use should reflect these underlying and confronting forces. The study examined the available evidence concerning two al Qaeda operations: the 1998 attack on US embassies in East Africa and the 9/11 attack on the US homeland. The 1998 events revealed al Qaeda system's vulnerability, whereas 9/11 did not. The contrast sharpens our understanding of this system and technology's role. The analysis below summarizes the core narratives and then examines the technology use over time based on released FBI documents.

Al Qaeda Operations Context A:
1998 Africa Attack on US Embassies

Al Qaeda Africa Surface Structure: Narrative Evidence –
"A Suicide Bomber Survives"

The surface structure documents the actions of al Qaeda members before, during, and after their August 8, 1998, bombing of US Embassies in Nairobi, Kenya, and Dar es-Salaam, Tanzania. The narrative centers on the Kenya suicide bomber, 'Al-Owhali', who unexpectedly survived. Kenyan authorities captured and delivered him to US custody.

The source of the narrative evidence is the two-thousand-five-hundred-page official transcript of the trial, United States of America v. Osama Bin Laden, et al. (2001) and, specifically, the seventy-page transcript of FBI agent, Stephen Gaudin's, sworn testimony as a witness for the prosecution. The narrative is based on Al-Owhali's signed statement as well as background intelligence, investigations, material evidence, and 'overt acts' enumerated in the Indictment. The US Government made the transcripts publicly available as part of the trial. Recorded in real-time during sworn testimony in the US court of law, these transcripts maintain high standards of fact. Evidence obtained under duress is generally inadmissible in the US court of law, but this evidence was not overturned during the trial, nor deemed biased by possible interrogation duress. The narrative documents how al Qaeda participants prepared and executed the bombing, and their subsequent attempts to evade detection. The analysis below describes the networks that emerged among these participants as events unfolded.

Al-Owhali grew up in Saudi Arabia and attended an Islamic university. In 1996, he went to Afghanistan to join jihad after failing to find a local al Qaeda cell in Saudi Arabia. In Afghanistan, he received basic military training at an al Qaeda camp and fought alongside the Taliban. Then he became ill and an al Qaeda associate, 'Azzam', helped him obtain medical treatment. This associate recruited him for the mission.

Al-Owhali prepared to become a martyr. He rode a truck filled with explosives to bomb the US embassy in Nairobi. His task was to disrupt the embassy guard so that the truck could enter the embassy compound. There, Azzam, the truck's driver, would detonate the explosives. Al-Owhali's job was to insure manual detonation should the electrical wiring to the cabin detonator malfunction. However, a traffic mix-up occurred as the bomb-truck approached the embassy. As instructed, Al-Owhali exited the truck, but he forgot the gun intended to force the guard to open the embassy's gates. He threw a grenade towards the gate and ran away. The truck entered and detonated inside the embassy compound, but al-Owhali was not in the truck and so he did not die. He fled and sought al Qaeda help, and was arrested on August 12, 1998.

To trace al Qaeda's human networks that formed and performed, the study generated technology use data from the Africa attack narrative transcripts and converted them into chronologies of discrete events involving technology use for handling mission information.

Al Qaeda Africa Data Generation

Table VII shows an example of coded technology use events. The coding generated 54 events total, summarized in Table VIII by technology used.

Agents (Nodes)	Al-Owhali
Operational Roles	Nairobi suicide bomber
Mission Detail	Directly involved
Node Location	Nairobi, Kenya
Technology Used	Street telephone
Technology Use Location	Outside of Ramada hotel, Nairobi, Kenya
Task Type	Communication
Contact Direction	Initiates contact
Event Description (narrative source quote)	"Al-'Owhali arrived in Nairobi on the Sunday, the 2nd of August. What did he do once he arrived in Nairobi? Upon arriving in Nairobi, he followed Khalid's instructions and he took a taxi to the Ramada Hotel. Upon arrival at the hotel, he used a phone service, not at the Ramada but nearby the Ramada, as he explained it to me, and telephones Khalid and advised Khalid that he, Al-'Owhali, had checked into room 24."
Event Timeframe	August 2, 1998
Reference	USA vs. OBL trial, FBI agent Gaudin direct examination, pp. 42-43

Table VII: Example al Qaeda's Africa attack technology use datum

Technology Used	***Use Frequency***	***Technology Type***
Physical interaction (face-to-face/courier)	63%	***Lower-Tech 92%***
Telephone (landline and street phone-booth)	27%	
Vehicle audio cassette player (used in the bomb-truck)	2%	
Electronic money transfer (international wire)	2%	***Hi-Tech 8%***
Mobile phone/satellite phone connection (calls)	4%	
Video recording (martyr video for propaganda distribution)	2%	

Table VIII: Al Qaeda Africa attack data by technology type used

Al Qaeda participants used these technologies to communicate, monitor and manage operations and transactions. Table IX summarizes a chronology of key technology use events.

Timeframe	*Chronological Summary*
Before attack	• The bomber-to-be traveled to Afghanistan to pursue jihad • An al Qaeda associate personally recruited him for a mission • The bomber-to-be committed to a mission without knowing specifics • He received advanced mission training in person cell organization, operational secrecy, handling explosives, and intelligence methods • Following instructions, he traveled to meet with al Qaeda members to record a martyr video and deploy to attack location in Kenya • In Kenya, the attack's operational commander arrived and personally communicated the attack location and method, and showed the bombers where to place the bomb. The bomb technician also arrived, finalized the bomb and instructed the bombers on its use
During attack	• The attack method used humans as guided bombs and relies on human capacity to conceal hostile intent • The bomber-to-be, however, escaped the scene after detonation, underscoring how human bombs can be difficult to control
After attack	• The bomber attempted to re-connected with surviving cell members, but had no contact information and could not locate the safe-house per al Qaeda's operational secrecy procedures • He contacted a friend and received an electronic money transfer • The contact initiated communications across al Qaeda network involving traceable cellular and satellite phone connections • This exposed the network to US surveillance and lead to the bomber's capture, as well as US retaliation against al Qaeda

Table IX: Al Qaeda summary chronology of Africa attack technology-use events

These interactions manifested al Qaeda's network organization in action.

Al Qaeda Africa Manifestation Structure:
A Fault-Intolerant Network Organization (FINO) Revealed

Al-Owhali, the surviving suicide-bomber, explained (USA vs. OBL transcript, p. 2019) that his organization was "loosely structured" such that "depending on the mission, you report to different people at different times". He "reported to the person who recruited him" who eventually drove and detonated the Kenya truck-bomb. This recruiter "in turn reported to somebody higher up, and that

person higher up and so on all the way up to the top". Osama Bin Laden was "at the very top" and had "several senior military leaders directly under him". Designated networks of individuals, or local cells, conducted specific missions. A cell contained four separate sections: intelligence, administration, planning and preparation, and attack execution. The intelligence section leader was in charge of the overall cell, and he assigned deputies to conduct various tasks. This narrative covers the activity of the attack execution cell.

This network also involved a cell leader ('Saleh') who served as operational commander; cell administrator ('Harun') who managed a safe house in Nairobi where the attackers assembled the bomb and finished their preparations; a Tanzania suicide-bomber ('Ahmed'); and a technician for both Kenyan and Tanzanian truck-bombs ('Abdel'). Two additional al Qaeda members provided logistical reliability support without directly participating in the mission. 'Bilal' arranged counterfeit documents, and ('Khalid') relayed communications. In the course of events, the surviving suicide-bomber also communicated with his father and another al Qaeda member ('Hazza') whom he befriended in Afghanistan. The friend and father did not participate in attack execution.

Figure **3** shows participant roles gleaned from the narrative. Solid lines indicate direct authority relationship. Dotted lines indicate implied authority relationship. This mission execution cell is consistent with al Qaeda's primary goal of attacking to destroy its enemy, the US. But its connections to al Qaeda leadership created vulnerability that interactions with the leadership may be detected and used against al Qaeda. Although not all al Qaeda's agents in Figure 4 executed this mission, even tenuous links among nodes exposed the network. Thus, each node and each traceable connection put the network at risk of being attacked and destroyed, should a node be detected. Resulting network is a FINO.

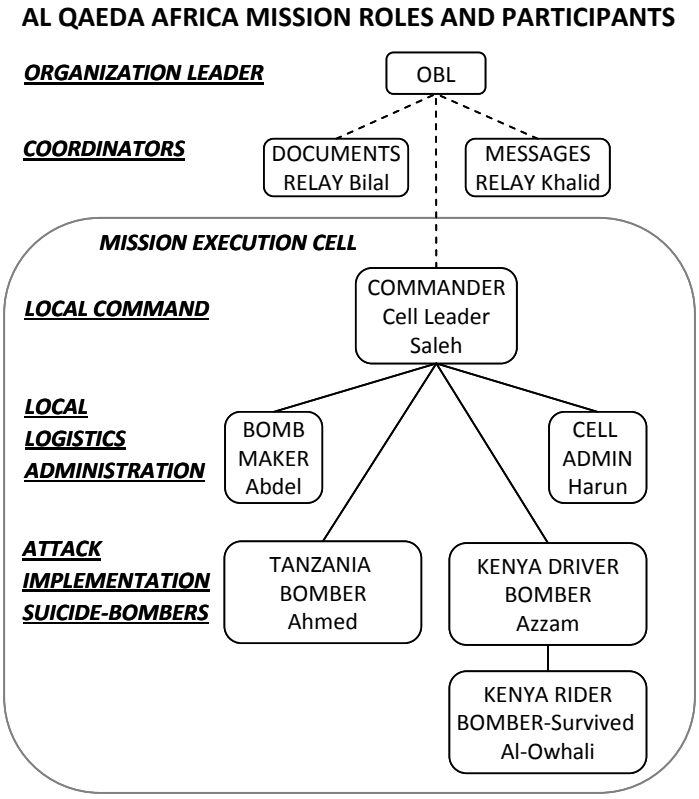

Figure 3: Al Qaeda Africa attack participants and roles

Proposition 2: Al Qaeda is a Fault-Intolerant Network Organization (FINO)

Al Qaeda mitigated this risk by limiting nodes and links, and avoiding redundancies in the network. For example, having substitute bombers and bomb-technicians for each attack would have enhanced mission performance by limiting node interdependence and critical reliance on each node. However, each additional node would increase the risk of detection. To reduce this risk, the network involved only one person in each mission-critical role (e.g., one bomb-technician for both locations, no substitute bombers, etc.).

The participants worked independently, and did not interact or learn about their task interdependencies until days before the attack. Mission success

depended on each participant doing his task correctly. Because each participant also constituted a network node, the organization's survival depended on each of these mission-critical nodes concealing their identities and network links.

For network concealment, al Qaeda compartmentalized mission knowledge and restricted the distribution of information. The surviving suicide-bomber explained (USA vs. OBL, p. 2019) that mission-critical information, such as attack plans, participant identities and their links to the mission, was disseminated top-down in terms of organization roles. Without participating in the attacks, Osama bin Laden provided "the political objectives" to leaders directly under him. Within this context, these individuals "would then provide the instructions down… to the lower chains of command". OBL typically did not provide detailed instructions directly to implementers at the lower level of the organization hierarchy, nor did implementers directly contact their superiors during missions.

The data analysis confirmed this pattern (Table X). The surviving suicide-bomber was at the bottom of the mission hierarchy and did not initiate direct contact with his mission superiors. They contacted him. The evidence suggests that he did not know how to reach his immediate superior, the bomb-truck driver. He also did not know who the other cell members were until days before the attack. (He had initially met the Tanzania bomber during training in Afghanistan, but learned of his participation in the mission within hours of the actual attack).

Most mission interactions in Table X were unidirectional, and the bi-directional links evolved as the mission progressed. The bomber interacted with OBL in Afghanistan, and he initiated contact to ask OBL for a mission. Once he received and committed to a suicide-mission, he no longer initiated contact with OBL. Similarly, he initiated contact with the documents-coordinator by traveling and meeting with him in Yemen to obtained counterfeit documents, but then

contact ceased. The message-relay coordinator initiated contact with the bomber to meet him in Pakistan, record his martyr video for al Qaeda propaganda, and provide instructions on travel to Kenya. However, once the bomber met the attack execution cell, this coordinator ceased initiating contact. The bomber's interactions with these two agents occurred before he learned the mission target, timing, weapon and executing network (narrative evidence suggests that neither coordinator knew these details). Thus, bi-directional contacts either ceased, or became unidirectional, as the time of attack approached.

	Surviving Suicide Bomber's Mission Communications						
Roles:	**TOP COMMAND (OBL) & RELIABILITY COORDINATORS** (not involved directly)			**OPERATIONAL AGENTS LOCAL COMMAND & CONTROL** (directly involved in executing attack)			
Surviving-Bomber's Directed Contacts by Direction:	Organization Leader (OBL)	Counterfeit Documents Coordinator	Message-Relay Communications Coordinator	Recruiter & Bomb-Truck Driver	Cell Leader & Operational Commander	Cell Administrator	Bomb technician
Initiates	50%	100%	60%	Ø	Ø	Ø	Ø
Receives	50%	Ø	40%	**100%**	**100%**	**100%**	**100%**

Table X: Al Qaeda directed contacts[3]

The coordinators worked in geographically separate locations. They facilitated tasks and secured communications, without directly participating in the mission. The documents' coordinator worked in Afghanistan and Yemen, and the communications' coordinator in Pakistan. Both locations were different from the bombing location. They improved reliability of some network functions, while helping to suppress node identities and information, and avoid operational network links. This indirect organizing was not as efficient as direct interactions.

[3] Percentages in Table X show relative distribution of Al-Owhali's directed contacts by role.

This network structure helped conceal the organization and reduce the risk of network traceability and, hence, destruction by the enemy. Detection of a node risked revealing downstream contacts, but not the command. Limiting knowledge about network structure and activity internally reduced potential damage in case of node detection or capture and, thus, enhanced the organization's ability to conduct future missions. As long as a captured agent did not know critical mission details, the mission remained secret. Thus, al Qaeda retained the option of executing the mission later using different personnel. However, this necessitated minimizing the number of people knowledgeable about network activities. These restrictions impeded operational logistics.

These countervailing tensions in the 1998 attack network structure reflect al Qaeda's organizing system. Concealment improved their survivability by limiting effects of potential node failures, but some information had to be transmitted in order to prepare and execute the attack, thereby endangering the organization. Al Qaeda contained the vulnerabilities by limiting the number of nodes, links, mission knowledge and interactions. This strategy mitigated network failure by reducing the probability of node detection as well as limiting network propagation of damage from detection or task execution failure.

Proposition 3: Non-redundant nodes and links in al Qaeda's sparsely connected mission network and compartmentalized information reduce its detection & destruction risk.

The mission network remained unconnected until immediately prior to the attack, which secured the network, but impeded operations. Technology use within the network manifested and shaped this dynamic. Alternative technology

use patterns before and after the attack (Figure 4) explain the effects of traceable hi-tech versus physical and other lower-tech interactions.

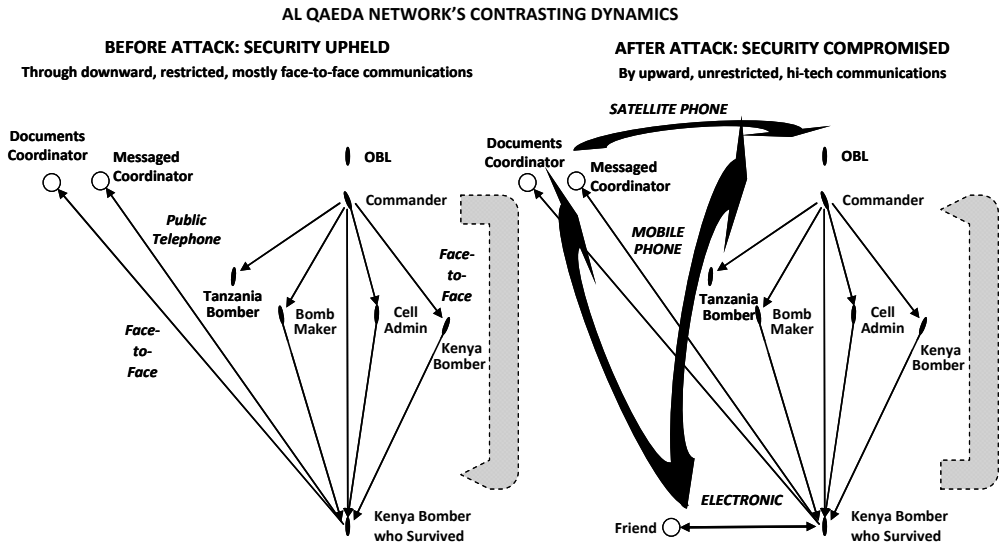

Figure 4: Al Qaeda Africa attack organizational network dynamics*. (Left)* Network structure and technology use pattern prior to the attack**.** Network security is upheld through the use of low-tech methods; *(Right)* Network organization and dynamics after the attack. Use of hi-tech including mobile and cell phones and electronic money transfers resulted in network being exposed and organization being compromised, which let to US retaliation against al Qaeda leadership and network.

The narrative provides evidence in context.

Before the attack, mission network interactions were almost non-existent. Initially, during basic military training in Afghanistan, the surviving bomber-to-be, Al-Owhali, personally approached an al Qaeda training camp official to request an audience with OBL. OBL did not immediately grant the request. Al-Owhali completed basic training and distinguished himself as a capable and loyal soldier. When he contracted tuberculosis, a fellow al Qaeda trainee helped him obtain

medical treatment and used the opportunity to recruit him for a mission. The bomber-to-be expressed interest without knowing the nature of the mission.

Over time, the recruiter probed his commitment and eventually suggested that it was time "to start getting ready", and they both completed advanced "operation and management of the cell training". The bomber-to-be also received "training in intelligence, in security and how to do site surveys of a particular target using cameras with both still and video photography" (USA vs. OBL, pp. 2003-2004). Though he did not know it, his mission was five months away.

The recruiter contacted him again saying (USA vs. OBL, pp. 2003-2006): "the mission is getting… ready. You need to travel from (Afghanistan) to Yemen." He prepared to travel by shaving his beard and obtaining a counterfeit passport. Al Qaeda's logistics coordinator, Bilal, assisted him using "connections in Yemen" to "make that happen". After the bomber-to-be obtained a Yemeni passport, the recruiter contacted him and instructed him to travel to Pakistan, meet with a person named Khalid, receive "instructions on what the mission was", and then "listen to Khalid".

In Pakistan, the bomber-to-be met Khalid but received only general information that "the mission was going to be a martyrdom operation that would… result in Al-'Owhali's own death; that there was… a US target somewhere in East Africa, but didn't specify the exact location of the target at that time", which was about three months before the attack (USA vs. OBL, pp. 2007-2008). Khalid then instructed him to his travel arrangements to Nairobi where he would be "met by others in the group" and receive "final instructions on the mission" (USA vs. OBL, p. 2010).

Al-Owhali's trip to Nairobi included four different flight segments. When he missed a connecting flight, he did not know whom to contact to re-schedule his Nairobi meeting. He telephoned the Khalid in Pakistan, who told him to call again upon arrival in Nairobi. Then Khalid instructed him to stay at a hotel outside of Nairobi and wait. Then Khalid relayed the message to the African attack commander in Mombasa who contacted the cell administrator at a safe house in Nairobi. Eventually, the cell administrator personally picked up the bomber-to-be, which was the first time that the two met. This contact sequence illustrates the unidirectional information flow down the chain of command implemented via mostly face-to-face communications (i.e. low-tech).

Finally, the commander arrived in Nairobi within days of the attack and met the bomber-to-be and the bomb-truck-driver who, the bomber then learned, was the same person who initially recruited him. The commander gave them, face-to-face, the final details of their mission. Then the bomb technician arrived and showed both of them how to activate the bomb. Once final preparations were completed, the commander ordered other al Qaeda personnel to leave the area. This order disseminated face-to-face down the chain of command.

The sequence of events reveals how al Qaeda consistently protected the organization by restricting mission-critical information. It safeguarded the information not only from outside observers but also from inside participants. Strategies restricted information flows and compartmentalized specific knowledge across participants and over time. The need for such restrictions mandated using technology that restricted network connectivity. Face-to-face meetings, with occasional one-way public telephone calls when necessary, met this need and manifested as preferred.

The pattern of low-tech use represents choices of technology because al Qaeda had access to hi-tech alternatives. The transcripts (USA vs. OBL) document that al Qaeda agents, who did not participate in this attack, had satellite and mobile phones, computers and access to the Internet in Kenya, Tanzania, Pakistan, Afghanistan, Yemen, and Saudi Arabia in the same timeframe. For the attack participants, however, two-thirds of all communications were face-to-face meetings and relaying messages through a coordinator. Within the network, hi-tech devices were available, but not used to plan the mission. For example, the Tanzania bomber had a mobile phone to keep in touch with cell commander "in case anything needed to be changed with the mission" (USA vs. OBL, p. 2019), but the transcript provides no record of its use.

Face-to-face communications down the chain of command dominated operational planning (shown in Figure 4, left-hand side). The bomber-to-be was recruited through personal interactions and then traveled to Yemen and Pakistan where he received partial instructions. When the executing team assembled in Nairobi, the operational commander traveled there to communicate mission details face-to-face. He also physically "took Al-'Owhali to the American Embassy in Nairobi and showed him where he wanted the bomb truck to be placed by the drop bar in the rear of the U.S. embassy" (USA vs. OBL, pp. 2019-2020).

Though often operationally inefficient, these physical communications kept the network structure hidden and untraceable by US electronic means. For instance, when the commander was in Tanzania he could have conveyed instructions to the Kenya team via the Tanzanian bomber's cell phone. This would have been more efficient (faster and less expensive) than traveling to Kenya to do it in person. However, such a call would have generated electronically traceable records, which were especially risky vis-à-vis US electronic surveillance. Records of

the call would have also connected the Tanzania and the Kenya cell members prior to the attack, risking attack detection and disruption. Alternatively, the low-tech strategies helped al Qaeda conceal its network. The physical meetings required no traceable infrastructures offering node independence and self-sufficiency.

Face-to-face interactions also provided flexibility and context to explain complex information, and assess how the recipients received and understood the information, as well as to assess their intent to act upon it. Alternatively, a hi-tech communication carries a greater risk of miscommunication or loss of information, due to poor signal quality, loss of connectivity, or insufficient shared context. Finally, physical communications allow management to exert personal oversight and transfer tacit knowledge. In the FINO structure, personal oversight was important for motivating and directing the suicide bombers who, by definition, lacked experienced at their job. Their death would then eliminate all traces of their organizational knowledge thus concealing al Qaeda's from US detection.

After the attack, however, interactions following the bomber's unexpected survival revealed al Qaeda's network vulnerabilities. Because he was supposed to die in the attack, there was no extraction plan for him. When he survived, he had neither travel documents nor money to escape. He first attempted to meet his associates in person following established network interaction procedures. But, he did not know the location of the safe house, nor how to contact his superiors. He then contacted his friend from a street-telephone and asked the friend to contact the logistics-coordinator in Pakistan for support.

These actions and subsequent contacts breached organizational controls and introduced redundant network links (shown in Figure 4, right-hand side). It initiated network-wide interactions, including OBL's satellite phone to contact the

surviving bomber's friend, plus a cell phone number in Yemen. The failure to rely on the preferred low-tech technologies exposed the network to US detection and counteraction, including identifying al Qaeda as the attack perpetrator, arresting organization participants and bombing its facilities. This outcome underscores the effects of countervailing forces that define the organization mission. The short-term attack mission was successful, but it revealed al Qaeda's presence and hostile intent that precipitated counteraction. The single node's failure to suppress mission-critical information led to detection and threatened the long-term survivability of the network.

Proposition 4: Low-tech use impedes network connectivity and traceability providing node independence, self-sufficiency, and network concealment needed for al Qaeda's mission and risk-mitigation. Hi-tech use undermines them.

The 1998 attack structure showed how Qaeda's alternative technology use choices served first to conceal, and then expose, the FINO network. The 9/11 operation, briefly discussed next, used the same network structure and technology strategy. This time, however, there were no mistakes and the network survived longer.

Al Qaeda Operations Context B:
9/11 Attack

Al Qaeda 9/11 Surface Structure: Narrative Evidence –
"There Were No Slipups"

The surface structure documents the actions of al Qaeda members before, during, and after 9/11. The narrative centers on the attack execution funding.

The source of the narrative evidence is the official fifteen-page transcript of the FBI Director Robert Mueller's sworn testimony to the US House Committee on the Judiciary (Mueller, 2002). It narrates how the 9/11 operation was funded from overseas and what the terrorists did once they arrived in the US. This evidence is part of the Joint Inquiry into The Terrorist Attacks of September 11, 2001, by The House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence, whose eight-hundred-page Report (Joint Inquiry, 2002) supplemented the narrative evidence source. The US intelligence community and other investigators obtained the underlying facts. The data sources, such as sworn US congressional testimony based on background intelligence, generally follow the same high factual standards as trial proceedings used as data source in the Africa operation analysis. The analysis below describes the networks that emerged among the 9/11 participants as events unfolded.

On September 11, 2001, nineteen al Qaeda terrorists hijacked four US commercial airline flights. They gained control over three aircraft and crashed them into the New York City's World Trade Center towers and the Pentagon respectively. The fourth aircraft crashed into a field in Pennsylvania. Mueller (2002, p. 14) explains:

> "Clearly, these 19 terrorists were not supermen using extraordinarily sophisticated techniques. They came armed with simple box cutters (and also) with sophisticated knowledge about how to plan these attacks abroad without discovery, how to finance their activities from overseas without alarm, how to communicate both here and abroad without detection, and how to exploit the vulnerabilities inherent in our free society… There were no slip ups. Discipline never broke down. They gave no hint to those around them what they were about. They came lawfully. They lived lawfully. They trained lawfully. They boarded the aircraft lawfully. They simply relied upon everything from the vastness of the Internet to the openness of our society to do what they wanted to do without detection".

The 9/11 funding mechanism centered around one of the suicide-pilots, supported by several individuals in United Arab Emirates (UAE). Support hijackers (i.e., non-pilots, referred to as "muscle") brought additional funds when they arrived in the US. Hours before the attack, the hijackers returned some of the money back to al Qaeda leadership through intermediaries in the UAE.

To trace al Qaeda's human networks that formed and performed, the study generated technology use data from the 9/11 funding narrative transcripts by converting them into chronologies of discrete events involving technology use for handling mission information.

Al Qaeda 9/11 Data Generation

Table XI shows an example of coded technology use events. The coding generated 116 events total, summarized in Table XII by technology type used.

Agents (Nodes)	Ali Abdul Aziz Ali
Operational Roles	Money relay coordinator
Mission Detail	Not involved in mission execution
Node Location	UAE
Technology Used	Electronic wire transfer
Technology Use Location	Western Union, UAE (Dubai)
Task Type	Financial transfer
Contact Direction	Initiates contact
Event Description (narrative source quote)	"On June 29, 2000, Ali Abdul Aziz Ali (using the alias Isam Mansur) wired $5,000.00 to Marwan al-Shehhi. The funds were sent via Western Union from the UAE to al-Shehhi in New York"
Event Timeframe	June 29, 2000
Reference	Statement for the Record FBI Director Robert S. Mueller III, Joint Intelligence Committee Inquiry (JICI) 09/25/2002 FBI24003

Table XI: Example al Qaeda 9/11 attack technology use datum

Technology Used	***Use Frequency***	***Technology Type***
Cash (delivered/received in person)	9%	***Lower-Tech 73%***
Courier (used to deliver bank cards)	1%	
Mail (used to deliver bank cards)	2%	
Traditional in-person banking (ATM/checking)	39%	
Third-party banking (anonymously or via power of attorney)	6%	
Travelers checks (issued in foreign country)	5%	
FTF in-store purchase (e.g., airline ticket purchase in person)	11%	
Electronic wire transfer (Western Union)	9%	***Hi-Tech 27%***
Credit card (own or third-party)	9%	
Financial exchange institution (money exchange)	3%	
Internet (online purchase)	6%	

Table XII: Al Qaeda 9/11 attack data by technology type used

Al Qaeda participants used these technologies to fund and manage the 9/11 attack. Table XIII summarizes a chronology of key technology use events.

Timeframe	***Chronological Summary***
Before attack	• The hijackers secured operational funding using cash and travelers checks • They disguised wire transfers through compartmentalized and one-way links through foreign banks and coordinators, ceasing contact once in the US • They lived together in group safe-houses sharing funds in person • Prior to the attack, local operational commanders traveled to meet with groups of hijackers in separate hotels to complete final attack preparations • Immediately prior to the attack they returned some of the remaining funds by physically mailing bank cards that can be used to withdraw funds and consolidating other funds in a UAE bank account (which UAE agents emptied)
During attack	• Attackers used simple implements and their knowledge of the aircraft and air travel system schedules to execute the attack
After attack	• The hijackers' disguised return-funds went undetected long enough for al Qaeda upper management to obtain them and vanish

Table XIII: Al Qaeda summary chronology of 9/11 attack technology-use events

These interactions manifested al Qaeda's network organization in action.

Al Qaeda 9/11 Manifestation Structure:

A FINO Concealed

Participants (Figure 5) included the nineteen hijackers and three financial logistics-coordinators, 'Alhawsawi', 'Ali' and 'Alqusaidi', who facilitated 9/11 funding from abroad, without direct involvement in the attacks. Alhawsawi coordinated the muscle-hijackers' transit through the UAE, where they received funds for use in the United States. Evidence suggests that one of the pilots, 'Shehhi', administered operational finds in the United States. One of the muscle hijackers, assisted other muscles' transfer through the UAE, and with their US arrangements. Upon completion of attack preparations, the hijackers returned some money to Alhawsawi, who consolidated these funds and made them available to an 'Abdulrahman A. A. Al-Ghamdi'. The US intelligence community subsequently identified Ghamdi as Khalid Sheikh Mohammed (KSM)—the 9/11 mastermind and associate of Osama Bin Laden (Mueller, 2002).

Figure 5 shows that this operation involved the same roles as the Africa attack (Figure 3). The top-down hierarchy, included top leadership, logistics and logistics reliability coordinators who did not directly participate in the attack. The attack execution cell involved operational command, cell administration, and implementer suicide-bombers. In this case, local command and administrators were also suicide bombers. This provided added security since, once deceased, these nodes no longer threatened the already vulnerable al Qaeda network by possibly revealing knowledge about its structure and procedures.

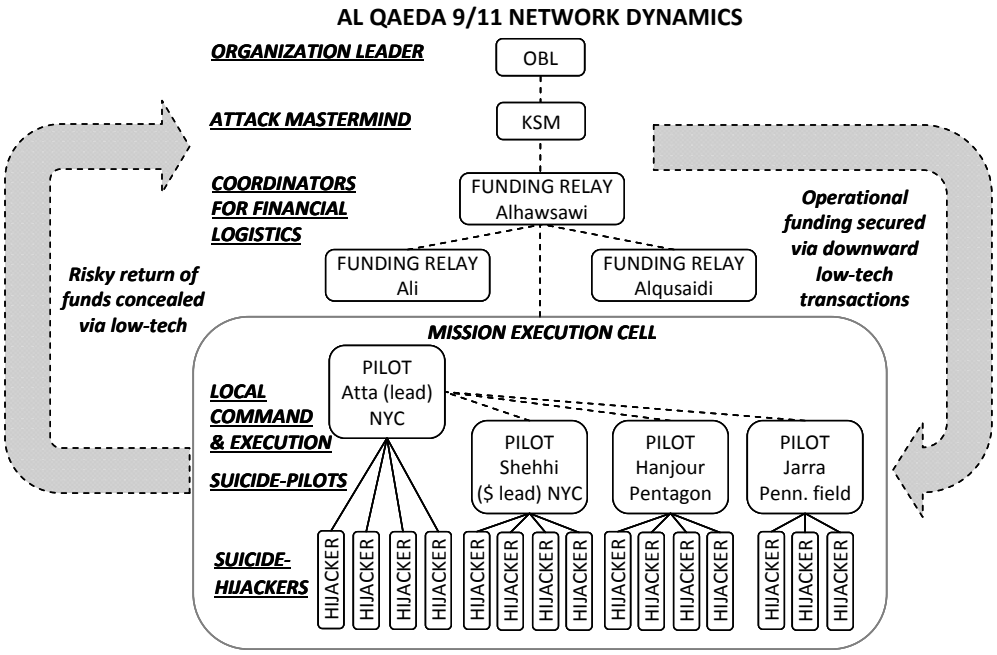

Figure 5: Al Qaeda 9/11 participants, roles, and organizational network dynamics. Al Qaeda used low-tech strategies to secure the network and risky transactions against detection.

Though all participants (nodes) in Figure 5 may not have directly interacted with one another, the operational funding network linked them all. As in the African operation, this linkage made al Qaeda vulnerable if any node failed to evade US detection. How did al Qaeda mitigate this risk? During 9/11 planning, "each of the hijackers, apparently purposefully selected to avoid notice, came easily and lawfully from abroad... effectively operated without suspicion, triggering nothing that alerted law enforcement and doing nothing that exposed them to domestic coverage... " (Mueller, 2002, p.1). Their operational network had limited connectivity thereby concealing the organizational network from detection, but also complicating local tasks.

This network design was structurally similar to the Africa operation—both shared the al Qaeda organizing system's FINO vulnerability to network-wide effects of single node failure (Proposition 2). In this network, Ali was the only person sending funds to the United States, suggesting that his failure to conclude these transfers risked disrupting the mission. Similarly, Shehhi was the only central money person among the hijackers, and his transactions with the UAE coordinators connected him to top-level commanders. Thus, his capture, or detection of his activities, risked not only hindering the mission but also exposing the broader al Qaeda network.

Tracing financial technology use events reveals a financial network that lacked node and link redundancies, and had sparse connections through compartmentalized interactions. Narrative evidence indicates that each of the three financial coordinator's role was unique in this mission. They sent funds to different geographical locations during three distinct timeframes. First, in the 1998-1999 timeframe, Alqusaidi sent money to Shehhi, while Shehhi was in Germany and until he opened a UAE account in July of 1999. Second, in late 2000, Alqusaidi sent money to Shehhi's UAE account. At this time, Ali also sent money to individuals in the United States. Third, in 2001, Alhawsawi provided funds to the muscle hijackers when they transited the UAE. Alhawsawi also managed the funds returned by the hijackers prior to 9/11.

Within the mission network, financial transactions were also limited and controlled. For instance, while still abroad, the hijackers Shehhi and Banihammad initiated network contacts by granting power of attorney over their separate bank accounts to Alhawsawi and Alquasaidi, respectively. Upon arrival in the US, however, the hijackers stopped initiating contacts with these UAE-based agents.

This network structure is consistent with the strategy of mitigating FINO risk by minimizing network elements and distribution of information that can initiate or propagate local failure (Proposition 3).

Participants' technology use patterns reflect the strategy of minimizing organizational links and activities traceable through technologies. Lower-tech use impeded network connectivity and traceability in favor of concealment and control (Proposition 4). For example, as in Africa, 9/11 activities centered around face-to-face contacts ranging from receiving cash or travelers checks in the UAE, to sharing lodging. According to Mueller (2002), the muscle hijackers arriving at Miami and Orlando airports settled in the Fort Lauderdale, Florida, area along with pilots Atta, Shehhi, and 'Jarrah'. Those arriving in New York and Virginia, settled in the area near Paterson, New Jersey, along with the fourth pilot, Hanjour, and another hijacker who had prior involvement with the pilots.

The pilots arranged for the "muscles" to share lodging. Living in the same place, exemplified an organizational tactic to share funds without necessarily sharing knowledge about the origin and transfer of funds. This facilitated network secrecy. Days prior to the attack, the four teams separately stayed at various hotels. Atta and Shehhi traveled to meet each team and finalize the mission, which provides another example of personal oversight and information management down the chain of command (Figure 5, downward arrow). As in the African attack, limited top-down contacts protected the network by limiting exposure to compartmentalized downstream contacts.

Leading up to September 11, however, several hijackers returned funds to the UAE, up the chain of command (Figure 5, upward arrow), which risked exposing the network. Specifically, Atta, Shehhi, and a muscle hijacker sent

approximately $18,000 via Western Union to an individual in Sharjah, UAE. A different hijacker also sent an Express Mail package addressed to a post office box in Sharjah, UAE, which contained the debit card for the account of another hijacker. Then, hours before the attack, Alhawsawi used a check and an ATM card to withdraw most of the money from yet a third hijacker's account. Alhawsawi deposited these funds, plus those received from the other hijackers, into his UAE bank account. He then transferred approximately $42,000 from this bank account to his bank's Visa card. Once this had been completed, he left the UAE for Karachi, Pakistan. In the meantime, a supplemental VISA card on Alhawsawi's bank account was issued to KSM under a pseudonym and later used to withdraw the money (Mueller, 2002).

These actions raised the possibility of compromising al Qaeda's network in a way similar to the African case (Figure 4, right-hand side). In Africa, the breach occurred after the attack following an operational security failure due to unexpected survival of the suicide-bomber. In 9/11, the network pattern breach was intentional and prior to attack. Why did al Qaeda take this risk endangering the mission as well as the network?

This choice highlights the tensions in al Qaeda's organizing system and suggests two possible reasons for the risk-taking behavior. One explanation is ideological, and based on al Qaeda's drive to attack and destroy its enemy. The other is practical, and based on al Qaeda's need to obtain and conserve resources for future operations. In either case, its ability to conduct future operations hinged upon remaining as concealed from the enemy as possible. Consistent reliance on lower-tech means to impede traceability again allowed this effect.

The majority of network interactions relied on physical and old-fashioned financial technologies (73% of technology use data in Table XII). According to the FBI (Mueller, 2002), none of the hijackers owned computers, laptops, or any kind of hi-tech equipment. They used hi-tech sparingly (27% of data in Table XII) and with security precautions. These included using code words and pseudonyms, anonymous transactions from public places, frequent changes of transaction locations, and avoidance of directly traceable links between superiors and subordinates. For instance, there were no direct wire transfers to the muscle-hijackers. One documented wire transfer intended for a muscle arrived through a third party who did not participate in the attack. He withdrew and delivered cash to the intended al Qaeda recipient. These strategies protected the network.

Al Qaeda Findings Summary:

FINO Security Strategy – Use Low-Tech to Cloak the Network

In both the Kenyan Bombing and 9/11 cases, al Qaeda's reliance on physical and other lower-tech means mitigated the FINO risk of catastrophic network-wide effects of single node failure.

Proposition 5: Low-tech secures FINO survival

The al Qaeda case study showed that its network structure was fault-intolerant (FINO) due to its reliance on limited number of connections between limited nodes. Such networks avoid operational node redundancy, limit information exchanges, and use technologies to disguise and conceal the network. In the hostile environment of al Qaeda's mission, this allows it to evade detection and destruction by its enemy.