THE INTERNATIONAL
C2 JOURNAL
VOLUME 4, NUMBER 2, 2010

Knowledge Sharing as a Contingency in the Design of Counterterrorism Organizations

Mark E. Nissen
Tara A. Leweling

CCRP
Focus
& Convergence
for Complex Endeavors

THE INTERNATIONAL C2 JOURNAL

About the Journal

The International C2 Journal was created in 2006 at the urging of an international group of command and control professionals including individuals from academia, industry, government, and the military. The Command and Control Research Program (CCRP, of the U.S. Office of the Assistant Secretary of Defense for Networks and Information Integration, or OASD-NII) responded to this need by bringing together interested professionals to shape the purpose and guide the execution of such a journal. Today, the Journal is overseen by an Editorial Board comprising representatives from many nations.

Opinions, conclusions, and recommendations expressed or implied within are solely those of the authors. They do not necessarily represent the views of the Department of Defense, or any other U.S. Government agency.

For more information

Visit us online at: www.dodccrp.org
Contact our staff at: publications@dodccrp.org

Knowledge Sharing as a Contingency in the Design of Counterterrorism Organizations

Mark E. Nissen and Tara A. Leweling
(US Naval Postgraduate School, USA)

Abstract

One of the key institutional responses to the terrorism threat is the counterterrorism intelligence organization. Traditionally very bureaucratic, such organizations have been criticized broadly, but their organizational structures remain largely unchanged. Given the dynamic, experience-based, knowledge-intensive nature of the counterterrorism task, Contingency Theory would suggest flatter, more flexible organization with *knowledge sharing* as a key contingency factor. Little is known, however, about interactions between organizational design and knowledge sharing. The research described in this article reports systematic laboratory experimentation to assess the structure of counterterrorism intelligence organizations in the context of alternate knowledge processes and to identify promising alternate approaches to organizing. Insights into how knowledge sharing affects alternate organizational designs highlight a theoretical contribution, and empirical results have immediate practical implications.

Keywords

Contingency Theory; counterterrorism; experimentation; knowledge.

Introduction

Although the date 11 September 2001 moves progressively into the past, the significance of how the terrorism events on this date transformed the world remains, and life under the persistent terrorist threat emerging from this disruptive change has never been the same (National Commission on Terrorist Attacks Upon the United States 2004). One needs only to read the newspaper about enduring conflict in the Middle East, stand in long security lines at the airport, or see large barricades and fences in front of government buildings to see apparent, sweeping, institutional changes stemming largely from these events.

Alternatively, many apparently sweeping institutional changes involve comparatively little impact. For instance, one of the key institutional responses to this threat is the counterterrorism intelligence organization, which is organized and staffed to detect and disrupt terrorism plots before they develop into attacks. Distributed previously among myriad different military, government and private organizations with little incentive to collaborate, in the US the Department of Homeland Security (DHS) was established in an attempt to coordinate counterterrorism and other institutional responses among dozens of previously independent organizations (US Government 2009).

Traditionally very hierarchical and bureaucratic, counterterrorism intelligence organizations were criticized broadly for their failure to disrupt the September 11 attacks, but even after DHS formation, their organizational structures remain largely unchanged; indeed, there appears to be an even larger, hierarchical and bureaucratic organization now than before. Given the dynamic, experience-based, knowledge-intensive nature of the counterterrorism task, organization and management theory and practice alike would suggest flatter, more flexible organization with *knowledge sharing* (cf., *information* sharing) as a key contingency factor (Birkinshaw, Nobel, and Ridderstrale 2002; Nissen 2005).

Knowledge is noted widely for the powerful and appropriate, individual and organizational actions that it enables and guides, and it is distinct from organizational information: knowledge enables action, whereas information provides meaning and context for action (Nissen 2006). Further, knowledge needs to *flow* (e.g., across individuals, organizations, places, and times) through the organization from where and when it is to where and when it is needed. This suggests that knowledge sharing—in addition to information sharing—is important.

Indeed, many scholars (Alberts and Hayes 2003; Leweling and Nissen 2007) argue now that hierarchical, bureaucratic organization itself represents a fundamental inhibitor to effective counterterrorism intelligence. Little is known, however, about interactions between organizational design and knowledge sharing. Moreover, adverse to risk and change—and comfortable with the hierarchy—government leaders and policy makers in this area hesitate understandably to make organizational structure changes without convincing evidence to support them (Alberts and Hayes 2006).

The research described in this article reports systematic laboratory experimentation to assess the structure of counterterrorism intelligence organizations in the context of alternate knowledge processes and to identify promising alternate approaches to organizing. As is known well, laboratory research enables investigators to assess alternate organizational approaches—systematically—without changing or disrupting operational organizations in the field, and through careful design of experiments, one can achieve considerable external validity and generalizability of laboratory results (Nissen and Buettner 2004).

Building upon Contingency Theory (Donaldson 2001), we identify flexible organizational structures with potential to transform counterterrorism radically. Then examining knowledge through a dynamic lens, we consider how knowledge sharing should affect counterterrorism organizational performance and learning. Using

an instrumented, distributed problem-solving environment for laboratory experimentation, we assess how well people collaborate and perform counterterrorism intelligence tasks through alternate organizational approaches and knowledge processes.

The remainder of this article is organized into four sections beginning with a focused summary of background literature to inform our research hypotheses. The research design is summarized next and followed by results of experimentation. Conclusions follow to highlight both theoretical and practical contributions through this empirical research, and they include a generative agenda for future research that offers promise to stimulate continued work in this important area.

Background

Contingency Theory has retained a central place in organization studies research for decades (Donaldson 2001), and organization scholars and managers understand well that no single approach to organizing is best in all circumstances. In most of this research, the concept *organizational fit* has been treated in a relatively static manner, with a particular organizational form (e.g., *craft, engineering*, see Perrow 1970) prescribed to fit well in a particular contingency context (e.g., comprehensible and predictable, complex and stable).

However, organizational scholars (Chaharbaghi and Nugent 1994; Donaldson 1987; Tung 1979) have noted widely that the environmental contexts of many modern organizations are not static. Rather, organizational environments can change rapidly and unpredictably, due to multiple factors such as globalization (Raynor and Bower 2001), technology (Rahrami 1992; Adner and Levinthal 2002), hypercompetition (Hanssen-Bauer and Snow 1996), knowledge-based innovation (Jelinek and Schoonhoven 1990), mounting competition from co-evolutionary firms (Barnett and Sorenson 2002), and others. Hence an organization that achieves good fit with

its environment at one point in time may not be able to retain such fit longitudinally, unless it changes structure in order to maintain fit—dynamically—across changing environmental conditions.

Indeed, an organization facing a constantly changing environment could fall into a condition of continuous (disruptive) change (Overholt 1997), or it might take the opposite approach, striving instead toward a single form that is flexible and robust to environmental change (Volberda 1997). Writing specifically about countering terrorism through military and government endeavors, Alberts and Hayes (2003; 2006) refer to such latter organizational form in terms of *agility*. In either case—and in most cases in between—leaders' and policy makers' focus on static organizational fit is incommensurate with the dynamics of contingent organization demanded by disruptive environmental change (Donaldson 2001). Drawing from our discussion of terrorism and counterterrorism above, the domain of counterterrorism intelligence appears to fit well this latter description of continuous (disruptive) change. This leads to our first research hypothesis.

Hypothesis 1. Agile and flexible organizational forms outperform their hierarchical and bureaucratic counterparts in the domain of counterterrorism intelligence.

Additionally, counterterrorism intelligence is a very knowledge-intensive task (National Commission on Terrorist Attacks Upon the United States 2004). This leads us to consider *knowledge* as an important contingency factor also (Becerra-Fernandez and Sabherwal 2001; Birkinshaw et al. 2002; Ibrahim and Nissen 2007). Indeed, the idea of *knowledge* as a critical organizational resource is well-established (Drucker 1995; Grant 1996; Nonaka and Takeuchi 1995), with more knowledgeable organizations described broadly as outperforming their less knowledgeable counterparts. Further, counterterrorism intelligence places a particular premium on the sharing of *information,* but the literature suggests that *knowledge* sharing may be critical in this context as well. This leads to our second research hypothesis.

Hypothesis 2. Organizations manifesting greater knowledge sharing outperform their counterparts with less sharing in the domain of counterterrorism intelligence.

Further, we understand well that organizations learn through time and experience (Inkpen and Dinur 1998; Levitt and March 1988). Noting the balance required between organizational exploration and exploitation (March 1991) and the persistent challenge to ambidextrous organizations working to excel simultaneously at both (Tushman and O'Reilly 1999), some organizations should be able to learn inherently faster than others. Hence *organizational learning*—knowledge flows that increase knowledge-based performance over time—emerges as another key factor to consider in terms of designing counterterrorism intelligence organizations. Drawing further from Alberts and Hayes (2003; 2006) to place this discussion in the context of countering terrorism through military and government endeavors, we find the assertion that agile organizations learn more quickly than their rigid counterparts do. This leads to our third research hypothesis.

Hypothesis 3. Agile and flexible organizational forms learn more quickly than their hierarchical and bureaucratic counterparts do in the domain of counterterrorism intelligence.

Research Design

In this section, we summarize the research design used to guide this laboratory experiment. We employ the ELICIT[1] multiplayer intelligence game to examine how people working together on a counterterrorism, information-sharing and -processing task perform across different organizational configurations. We describe the task environment, participants, measurement instruments, procedures, and experiment design.

1. ELICIT is an acronym for Experimental Laboratory for Investigating Collaboration, Information-sharing, and Trust.

Task Environment

The task environment involves a fictitious terrorist plot, about which a set of 68 informational clues called *factoids* have been developed. Each factoid describes some aspect of the plot, but none is sufficient to answer all of the pertinent questions (i.e., *who*, *what*, *where*, *when*). The factoids are distributed among a team of 17 players in a series of steps: each player receives two clues initially, followed by one after five minutes of play and another after ten minutes have elapsed. The factoid distribution is designed so that no single player can solve the problem individually and so that the team of players cannot solve the problem until after the final distribution. In other words, the players must collaborate to solve the problem.

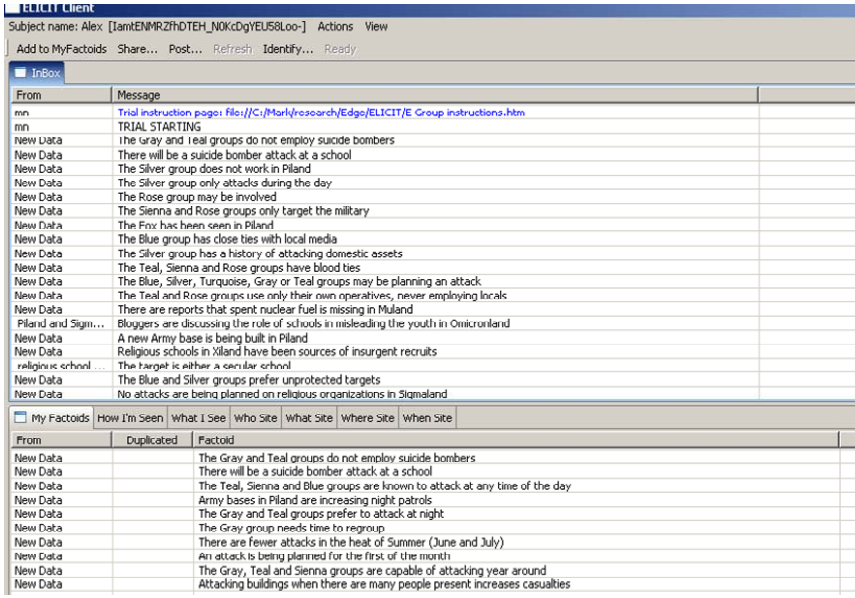

Figure 1. ELICIT Screenshot

Participants share and analyze factoids via ELICIT client applications on separate, networked computer workstations. Figure 1 shows a screenshot of a player's ELICIT view. Each participant has access

to a set of five functions supported by the client: (1) List, (2) Post, (3) Pull, (4) Share, and (5) Identify. The List screen displays all factoids that a particular player has received. Post enables a player to have one or more factoids displayed on a common screen that can be viewed by other players. Pull represents the complement to Post, as a player can display on his or her List screen common information that has been posted. Share enables players to send factoids directly to one another. Finally, Identify represents the manner in which participants communicate their "solutions" to the problem (i.e., the *who*, *what*, *where*, and *when* regarding a fictitious terrorist plot). Multiple versions of the factoids have been created, each of which is structurally similar but distinct; that is, each version includes the same number and kinds of factoids and provides a comparable task environment, but the specifics of each version differ and are unique.

Participants

Participants are recruited principally from a major west coast university offering graduate courses with bearing on organization and management of counterterrorism intelligence. A total of 68 participants (mostly students but supplemented by a few faculty members) range in age from 22 to 62 years ($\mu = 35.8$, $\sigma = 8.52$) and possess between 1 and 38 years of work experience ($\mu = 11.82$, $\sigma = 8.41$). All participants have undergraduate college degrees, and 42% have graduate degrees. Hence the participants are representative in part of the kinds of relatively experienced and well-educated people who serve as professional intelligence analysts, particularly in national intelligence organizations. Further, all of the participants have direct military or government service, and several have worked professionally in military or government intelligence organizations. Hence the participants are also representative of military and government employees who serve as professional intelligence analysts. However, there is some convenience to this sample, as we draw participants from graduate courses within the university.

Measurement Instruments

A two-component instrument is used to measure *performance* as a dependent variable comprised of: (1) time to complete the experiment task (i.e., time to identify the fictitious terrorist plot), and (2) accuracy of the task (i.e., details of the fictitious terrorist plot). This instrument is informed by technology-mediated laboratory experiments (Nissen and Sengupta 2006), in which *time* and *accuracy* reveal insightful tradeoffs and results.

For ease of comparison, the scales for both time and accuracy measurements are normalized to a 0-1 scale, with 1 being more desirable (i.e., faster, more accurate, respectively). All distributional and statistical analyses pertain to the scaled measurements. Performance data are captured automatically by the ELICIT software, which serves as an instrumented environment for conducting experiments along these lines.

Procedures

Participants are grouped into four teams of 17 and pre-assigned to play specific roles (e.g., as identified via pseudonyms to ensure anonymity and protect identity) in the experiment. When all ELICIT clients have connected with the server, participants sit down at the appropriate workstations, are informed verbally about the nature of the experiment, and are asked to read a set of instructions pertaining to both the experiment and the ELICIT environment. Participants are instructed not to reveal their pseudonyms to one another. Indeed, they are instructed not to talk or communicate with one another during the game via any mechanism outside of the two summarized above (i.e., post-pull, share).

Participants are given incentives to play the game well, as participation and performance are factored into the evaluation of students' coursework. Each participant is instructed to use the Identify

function only once during an experiment session. Participants are encouraged to ask questions throughout this process. When participants have read the instructions and have had their questions answered satisfactorily, they indicate via the ELICIT client that they are ready to begin. The experiment session begins at this point and ends when all players make their identification.

Experiment Design

The experiment design reflects a 2 x 2 full factorial: two different organizational forms (Hierarchy, Edge) and two different knowledge sharing models (information only, knowledge and information) are examined through 16 experiment sessions with each of the four teams participating in four sessions (each time with a different factoid set). This reflects a standard, balanced, textbook, two-factor design comparing individual performance across four sessions. Such design is conceived to assess main effects of the two manipulations and interaction effects between them. Hence the two main contrasts involve Edge vs. Hierarchy and knowledge sharing vs. information sharing.

Table 1 presents the assignment of teams to the different experiment manipulations. Participants in Group A perform only in the Edge mode and with information sharing only (labeled "E – I sharing" in the table); there is no within-subjects manipulation. Participants in Group D balance this manipulation, as they perform only in the Hierarchy mode also with information sharing only (labeled "H – I sharing" in the table); there is no within-subjects manipulation. Participants in Groups B and C balance those in A and D. Participants in Group B perform twice in Hierarchy mode (labeled "H – K sharing" in the table) and twice in Edge mode (labeled "E – K sharing" in the table), with both knowledge and information sharing in each case; there is a within-subjects manipulation involving organizational form but not knowledge sharing. Participants in Group C balance this manipulation, as they perform twice in the Edge mode

(labeled "E – K sharing" in the table) then twice in Hierarchy mode (labeled "H – K sharing" in the table), with both knowledge and information sharing in each case; there is a within-subjects manipulation involving organizational form but not knowledge sharing. We elaborate on these manipulations below.

Table 1. Experiment Groups and Manipulations

Group	Session 1	Session 2	Session 3	Session 4
A	E – I sharing	E – I sharing	E – I sharing	E – I sharing
B	H – K sharing	H – K sharing	E – K sharing	E – K sharing
C	E – K sharing	E – K sharing	H – K sharing	H – K sharing
D	H – I sharing	H – I sharing	H – I sharing	H – I sharing

Organizational form. The manipulation of organizational form addresses Hypothesis 1 and draws from Alberts and Hayes (2003), who detail a contrast between two forms: (1) the Hierarchy represents the kind of bureaucracy ubiquitous in military and government organizations, and (2) the Edge is noted specifically for its agility and appropriateness in the modern counterterrorism environment. In the Hierarchy organization manipulation, participants are assigned to play roles within a three-level, functional, hierarchical organization as depicted in Figure 2.

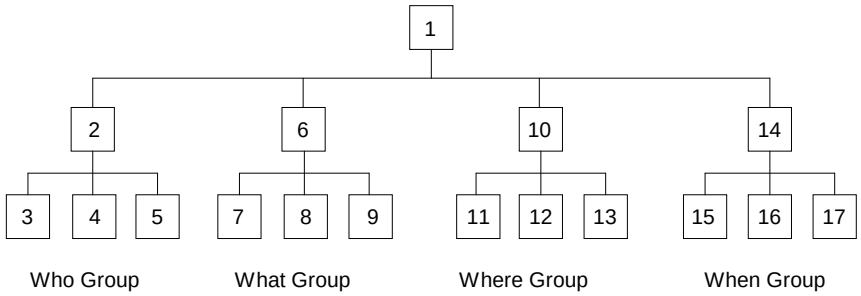

Figure 2. Hierarchy Organization

An overall leader (i.e., labeled "1") is responsible for the intelligence organization as a whole and has four functional subleaders (i.e., labeled "2," "6," "10," "14") reporting directly. Each subleader in turn has three analysts (e.g., labeled "3," "4," "5") reporting directly and is responsible for one set of details associated with the terrorist plot. For instance, Subleader 2 and team would be responsible for the *who* details (e.g., which terrorist organization is involved) of the plot, Subleader 6 and team would be responsible for the *what* details (e.g., what the likely target is), and so forth for the *where* and *when* teams. Participants are shown this organization chart, told of their responsibilities within the organization, and provided with a short description of the hierarchy.

In the Edge organization manipulation, there are no pre-assigned leaders or functional groups established in advance of the experiment. Rather, consistent with current Edge conceptualizations of flexible structure, the group begins without formal leaders, functional groups or restricted communications. Although the players are pre-assigned to specific roles (i.e., pseudonyms) within the game, such various roles reflect no hierarchical or functional differences from one another. As with the hierarchy manipulation above, participants are told about this organizational arrangement and are provided with a short description of the Edge as an organizational form. We characterize the nature of this Edge manipulation in Figure 3.

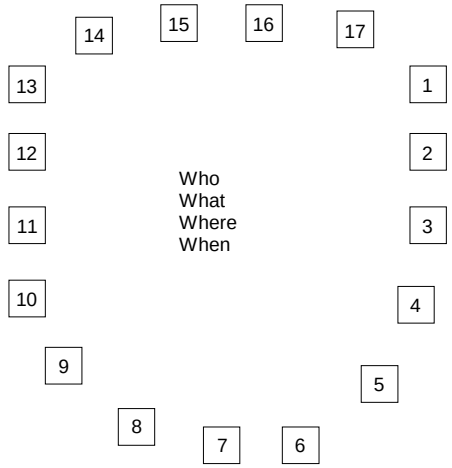

Figure 3. Edge Organization

Knowledge sharing. The manipulation of knowledge sharing models addresses Hypothesis 2 and draws from Nissen (2006), who details a contrast between two kinds of sharing: (1) shared information provides meaning and context, and (2) shared knowledge enables action. In terms of operationalization, information is represented by the factoids that are distributed, analyzed and shared through the ELICIT interface. Factoids provide meaning and context (e.g., which terrorist organization is likely to be involved, *what, where* and *when* it is likely to attack) for use in identifying the fictitious plot, but such factoids themselves are insufficient for timely or correct identification; they must be integrated with a participant's knowledge model of the plot.

Alternatively, knowledge is represented by *postcards*, on which participants articulate and share their best guesses at plot details (i.e., the *who, what, where* and *when*). Postcards enable action, in that a person receiving a postcard can take action by identifying the plot. This group has the ability to share factoids as well, hence the manipulation contrasts information sharing only with sharing both information and knowledge.

Organizing sequences. The manipulation of organizing sequences addresses Hypothesis 3 and assigns each group to organize through a different series of forms. Each experiment session employs a unique factoid set. Specifically, Group A participates in all four sessions in the Edge organization, and Group D participates in the Hierarchy organization all four times. In contrast, Group B participates in two sessions organized as a Hierarchy followed by two organized as an Edge, and Group C reverses this order with two sessions organized as an Edge followed by two organized as a Hierarchy. All four groups participate using the same, four, distinct factoid sets in the same order, but the sequence of organizational form—and hence organizational learning opportunities—varies.

RESULTS

We discuss the results of our laboratory experiments in this section. We begin with several general observations and then turn to address each of the hypotheses. The section closes with a summary of key implications.

General Observations

As summarized above, we conduct experimentation through 16 sessions. A total of 68 unique participants play the game and provide 210 useful observations at the individual level of analysis. Results are omitted for participants who fail to identify the terrorist plot. Although instructed not to, some participants submit multiple identifications. For consistency in the analysis and with the instruction set to the players, results reflect only the participant's *first* identification, regardless whether subsequent identifications are more or less accurate. The distribution of these 210 observations is summarized in Table 2 below (i.e., Edge vs. Hierarchy, knowledge and information sharing ("K+I") vs. information sharing ("I only").

Table 2. Cross-tabulation of Observations

	Organization Form		Total
	Edge	**Hierarchy**	
K+I	66	62	128
I only	46	36	82
Total	112	98	210

The two components of the dependent variable *performance* (i.e., time and accuracy) are checked for normality using probability plots, with acceptable results, and interestingly they are not correlated ($r = -0.058$, $p>0.40$). Normal distribution of and lack of covariance between the dependent variables supports the appropriateness of utilizing ANOVA to assess the results. Coupled with the low correlation between the primary manipulations (i.e., organizational form and knowledge sharing; 0.044, $p>0.52$), the normality of distribution supports the use of MANOVA also (Kerlinger and Lee 2000).

As summarized in Table 3, when knowledge is shared, players in the Edge configurations have an average time score of 0.47 (recall that 0 would represent the slowest time for any player to identify the details of the terrorist attack in any experimental round, while 1 would represent the fastest time for any player to identify details about the terrorist attack in any experimental round) and an average accuracy score of 0.75 (on a similar 0-1 scale). When knowledge is not shared, Edge time scores drop a bit (4%) to 0.45, but accuracy scores fall 19% to 0.61. Hence knowledge sharing improves Edge performance in terms of both time and accuracy, but the greater effect is in terms of accurate identification.

Table 3. Descriptive Statistics for Two Dimensional Performance

			Organizational Form		
			Edge	**Hierarchy**	**All**
Knowledge Sharing	**K + I**	*Time*	μ: 0.47 σ: 0.19	μ: 0.25 σ: 0.19	μ: 0.37 σ: 0.22
		Accuracy	μ: 0.75 σ: 0.27	μ: 0.69 σ: 0.26	μ: 0.72 σ: 0.26
		No Response	1	6	
	I only	*Time*	μ: 0.45 σ: 0.17	μ: 0.47 σ: 0.10	μ: 0.45 σ: 0.14
		Accuracy	μ: 0.61 σ: 0.35	μ: 0.60 σ: 0.25	μ: 0.61 σ: 0.31
		No Response	11	6	
	All	*Time*	μ: 0.47 σ: 0.18	μ: 0.33 σ: 0.20	
		Accuracy	μ: 0.69 σ: 0.31	μ: 0.66 σ: 0.26	

For the Hierarchy, the knowledge sharing results in a time score of 0.25 and an accuracy score of 0.69. This compares with respective time and accuracy scores of 0.47 and 0.60 when knowledge is not shared. Interestingly, knowledge sharing causes the Hierarchy to perform nearly 50% *more slowly* than when not shared. This is opposite of the effect observed for the Edge. Alternatively, consistent with Edge results, knowledge sharing improves accuracy by roughly 15%.

It appears that knowledge sharing among the players slows the hierarchy but yields greater accuracy over the case of simply exchanging information. The Edge, however, demonstrates negligible degradation in time when knowledge is shared and shows a comparable improvement in accuracy. The Edge also outperforms the Hierarchy

in most cases. This is intriguing since, as noted above, nearly all counterterrorism intelligence organizations in the field are organized hierarchically.

Organizational Form Hypothesis

Recall how Hypothesis 1 suggests that people working together in an Edge organization will outperform those who perform the same work in a Hierarchy. Our general observations above provide some support for this suggestion. As summarized in the table, the mean time score for all players working within Edge configurations (i.e., regardless of knowledge sharing) is 0.47 versus 0.33 (30% higher) for players working with Hierarchy configurations. This difference is statistically significant ($p<0.001$). Similarly, the mean accuracy score for players working within Edge configurations is 0.69 versus 0.66 (4% higher) for players working within Hierarchy configurations, but this difference is statistically insignificant ($p>0.38$). Given these results, Hypothesis 1 is partially supported. Persons working in an Edge organization, on average, perform their work *faster.* However, persons working in Edge and Hierarchy configurations produce *comparably accurate* results. These results are independent of knowledge sharing and reflect main effects.

Knowledge Sharing Hypothesis

Recall how Hypothesis 2 suggests that greater knowledge sharing will lead to superior performance. Our general observations above provide some support for this suggestion as well. As summarized in the table, the mean time score for participants in groups that shared knowledge is 0.37 versus 0.45 (22% lower). This difference is statistically significant ($p<0.01$). Alternatively, the mean accuracy score for participants in groups that shared knowledge is 0.72 versus 0.61 (15% higher). This difference is statistically significant ($p<0.01$) also. Given these results, Hypothesis 2 is partially supported. Persons

sharing knowledge, on average, perform their work *more slowly*. However, persons sharing knowledge produce *more accurate* results. These results imply an interesting trade space for organizational designers: the sharing of knowledge results in more accurate but slower performance. These results are independent of organizational form and reflect main effects.

Organizational Form and Knowledge models

Integrating data associated with both the organizational form and knowledge sharing hypotheses suggests that interaction effects are present. Recall that knowledge sharing in Edge organizations corresponds to slightly higher time score (0.47 vs. 0.45). This difference is not statistically significant ($p>0.55$). Alternatively, such sharing corresponds to significantly ($p<0.02$) higher accuracy score (0.75 vs. 0.61). Hence active knowledge sharing in the Edge improves accuracy without slowing the counterterrorism intelligence organization significantly.

Results are different for the Hierarchy. Recall that knowledge sharing in Hierarchy organizations corresponds to considerably lower time score (0.25 vs. 0.47). This difference is statistically significant ($p<0.01$). Alternatively, such sharing corresponds to significantly ($p<0.08$) higher accuracy score (0.69 vs. 0.60). Hence active knowledge sharing in the Hierarchy suggests the same kind of trade space noted above for organizational designers: sharing knowledge results in a more accurate but slower performance.

When considering these interaction effects, knowledge sharing within Edge organizations signals benefit without cost: accuracy improves with no speed degradation. With the Hierarchy, however, costs and benefits in terms of speed and accuracy must be traded off against one another. This suggests that the Edge organization may have a performance edge over the Hierarchy. Moreover, when knowledge is shared, the Edge is considerably faster (0.47 vs. 0.25) and more

accurate (0.75 vs. 0.69) than the Hierarchy is. Designers of counter-terrorism intelligence organizations may find it productive to consider active knowledge sharing within Edge organizational forms.

Organizational Learning Hypothesis

Recall how Hypothesis 3 suggests that organizational performance will improve through time. This implies that time and accuracy for the four groups will improve across each round of experimentation. Figures 4 and 5 provide contrary evidence. Looking first at Figure 4, for instance, time scores for Groups A and D appear to hover at about the same level throughout the experiment, with slight degradation or improvement from one round to the next. Group C improves, degrades, and then improves, while Group B degrades, improves, and improves. This does not reflect the kind of steady performance improvement expected through organizational learning.

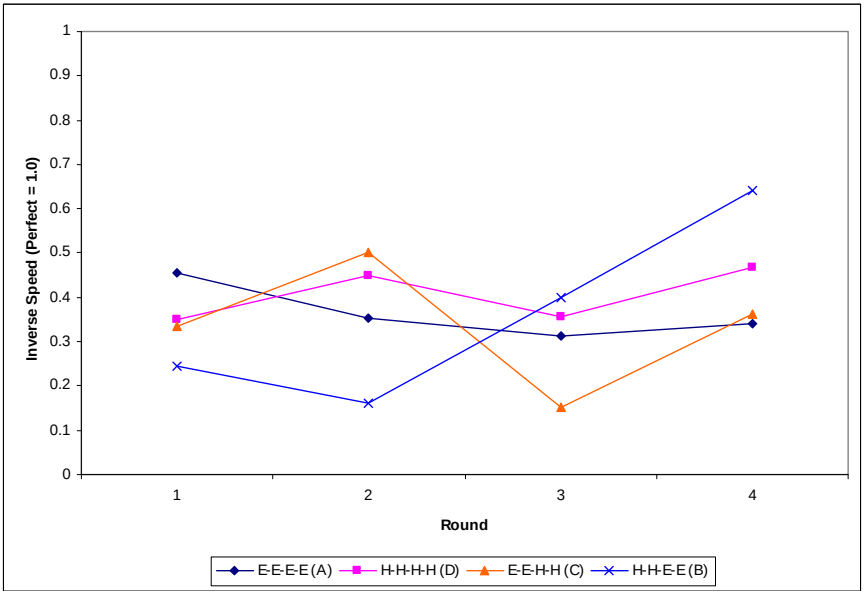

Figure 4. Observed Time, Groups A-D

Accuracy scores delineated in Figure 5 suggest mixed results also. Scores for Groups A, B, and C improve between Rounds 1 and 2 and Rounds 3 and 4 but also degrade somewhat between Rounds 2 and 3. Only Group D shows steady improvement in terms of accuracy scores across the four rounds. Neither reflects the kind of steady performance improvement expected through organizational learning.

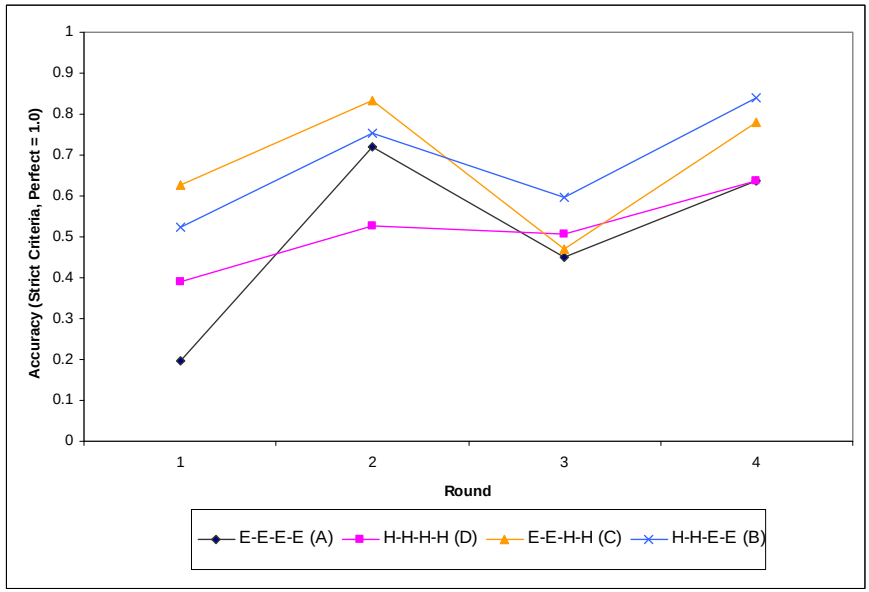

Figure 5. Observed Accuracy, Groups A-D

Key Implications

We identify several key implications of these results. First, we find mixed support for the hypotheses. As summarized in Table 4, the results do not provide strong support for any of the hypotheses. Indeed, only Hypotheses 1 and 2 are supported even partially, with negligible support for Hypothesis 3. These results are surprising on the surface, for the three hypotheses are grounded in the associated literatures. However, closer examination elucidates the situation.

In terms of organizational form, the two dimensions of our performance measure (i.e., speed and accuracy) reflect different results. Hypothesis 1 is supported in terms of speed, as the Edge groups outperform the Hierarchy groups significantly. Alternatively, the performance differential in terms of accuracy is detected but insignificant. For the organizational designer or manager interested in speed, the Edge appears to represent a superior design for the counterterrorism intelligence task, and it maintains a speed advantage without compromise in accuracy. Quick detection of terrorist plots is important, and the Edge form offers potential to improve organizational performance. This is particularly the case since nearly all counterterrorism intelligence organizations conform to the Hierarchy form.

Table 4. Summary of Support for Research Hypotheses

Hypothesis	Focus	Support	Comment
1	Organizational Form	Partially Supported	Edge outperforms Hierarchy significantly with regards to speed but not accuracy
2	Knowledge Sharing	Partially Supported	Knowledge sharing slows performance but increases accuracy significantly
3	Organizational Learning	Not Supported	Erratic longitudinal performance over time

In terms of knowledge sharing, exchanging knowledge via postcards improves accuracy significantly, as expected, but surprisingly it degrades speed significantly. This highlights an important trade space for organizational designers and managers to consider: both speed and accuracy are important in the counterterrorism domain, but it is unclear how one should trade one performance dimension against the other. Is it better, for instance, to identify correctly some details associated with a terrorist plot quickly, even though other details are incorrect, or would it be better to wait for all of the correct

details? The answer would depend upon individual decision makers' preferences, task environments, and risk tolerance. Highlighting this trade space represents a contribution of this study and indicates that additional research is needed to understand its implications better.

In terms of organizational learning, the results do not support our hypothesis, and this is surprising. One would expect for organizational learning to occur and manifest itself through performance improvement over time. The artificiality of the experiment task and task environment may contribute to this result, as may the relatively short length of time that participants in the four groups had to work and learn together. A follow-on study to address these limitations may elucidate the issue.

CONCLUSION

Although the date 11 September 2001 moves progressively into the past, the significance of how the terrorism events on this date transformed the world remains, and life under the persistent terrorist threat has never been the same. One of the key institutional responses to this threat is the counterterrorism intelligence organization, which is organized and staffed to detect and disrupt terrorism activities before they develop into attacks. Traditionally very hierarchical and bureaucratic, such organizations have been criticized broadly, but their organizational structures remain largely unchanged. Given the dynamic, experience-based, knowledge-intensive nature of the counterterrorism task, Contingency Theory would suggest flatter, more flexible organization with *knowledge sharing* as a key contingency factor. Little is known, however, about interactions between organizational design and knowledge sharing.

The research described in this article reports on systematic laboratory experimentation to assess the structure of counterterrorism intelligence organizations in the context of alternate knowledge processes and to identify promising alternate approaches to organizing.

Building upon Contingency Theory, we identify flexible organizational structures with potential to transform counterterrorism radically. In particular, the Edge organizational form, noted for flexibility and agility, is identified specifically for its potential in the counterterrorism domain, and a review of the literature leads to three research hypotheses for testing.

The ELICIT multiplayer intelligence game provides an instrumented, computer-networked environment for laboratory testing. Developed specifically for experimentation in the counterterrorism domain, ELICIT requires group information sharing and problem solving to uncover and identify the details of a fictitious terrorist plot. We construct a full-factorial research design that manipulates organizational form and knowledge sharing within a controlled and instrumented laboratory task environment.

Consistent with contingency theoretic understanding, results show that the flexible Edge structures have limitations as well as strengths and are not appropriate in all circumstances. In particular, the Edge organization outperforms the Hierarchy significantly in this experiment with respect to speed but not accuracy. Moreover, when we consider both speed and accuracy together, the Edge organization outperforms the Hierarchy when knowledge is shared. When knowledge is not shared, however, the Edge loses its edge over the Hierarchy. This elucidates a complex interaction between knowledge sharing and organizational design, one that suggests the contingency factor *knowledge sharing* is particularly important in a dynamic context, a contingency factor that has received negligible attention to date in the literature.

Results have several practical implications for organizational designers and managers as well. When considering counterterrorism intelligence organizations—which are predominantly hierarchical in nature—noteworthy performance improvements may be achievable through change toward more flexible and agile edge-like forms, particularly where active knowledge sharing is encouraged. Further,

results highlight an important trade space between performance in terms of speed and accuracy, as sharing knowledge improves accuracy but reduces speed. Organizational designers and managers may have to give up performance along one dimension in order to increase performance along one or more others.

Other topics for future research emerge naturally from this investigation. In particular, the promising Edge organizational form is not understood well either in theory or practice. More theoretical elaboration of this form and its relationships with other forms would likely inform our discussion well, and empirical research to identify Edge organizations in practice and assess their comparative performance strengths and weaknesses would amplify the kind of suggestive evidence found through the present study.

Finally, drawing from the literature, we examine two, contrasting organizational forms through this investigation: the Hierarchy and Edge. However, there are clearly myriad other organizational forms that have been described in both theory and practice, and one or more of them may be suited even better for counterterrorism intelligence work than the Edge appears to be. Research to identify and assess the comparative potential of such other organizational forms would appear to be highly relevant in light of this investigation.

Likewise, we understand well from Contingency Theory that no single organizational form is best in all circumstances. There are clearly many contingency factors beyond those associated with this investigation that may influence the relative efficacy of Edge, Hierarchy, and other organizational forms in the counterterrorism intelligence domain. Other approaches to knowledge sharing can be explored, and different combinations of tacit versus explicit knowledge sharing approaches warrant investigation as important factors in organizational design.

Given the importance of counterterrorism intelligence work, and how life under the persistent terrorist threat has never been the same since the terrorist attacks on 11 September 2001, future research along the lines of this investigation offers potential to impact the lives of many people. This places such scholarly work in a rarefied class of research and suggests considerable urgency.

REFERENCES

Adner, R., and Levinthal, D. A. 2002. The Emergence of Emerging Technologies. *California Management Review* 45(1):50.

Alberts, D. S., and Hayes, R. E. 2003. *Power to the Edge: Command and Control in the Information Age.* Washington, DC: Command and Control Research Program (CCRP) Publications.

Alberts, D. S., and Hayes, R. E. 2006. *Understanding Command and Control.* Washington, DC: CCRP Publications.

Barnett, W. P., and Sorenson, O. 2002. The Red Queen in Organizational Creation and Development. *Industrial and Corporate Change* 11(2):289-325.

Becerra-Fernandez, I., and Sabherwal, R. 2001. Organizational Knowledge Management: A Contingency Perspective. *Journal of Management Information Systems* 18(1):23.

Birkinshaw, J., Nobel, R., and Ridderstrale, J. 2002. Knowledge as a Contingency Variable: Do The Characteristics of Knowledge Predict Organizational Structure? *Organization Science* 13(3):274-289.

Chaharbaghi, K., and Nugent, E. 1994. Towards the Dynamic Organization. *Management Decision* 32(6):45.

Donaldson, L. 1987. Strategy and Structural Adjustment to Regain Fit and Performance: In Defence of Contingency Theory. *The Journal of Management Studies* 24(1):1.

Donaldson, L. 2001. *The Contingency Theory of Organizations*. Thousand Oaks, California: Sage Publications.

Drucker, P. F. 1995. *Managing In A Time of Great Change*. New York: Truman Talley Books/Dutton.

Grant, R. M. 1996. Toward a Knowledge-Based theory of the firm. *Strategic Management Journal* 17:109.

Hanssen-Bauer, J., and Snow, C. C. 1996. Responding to Hypercompetition: The Structure and Processes of a Regional Learning Network Organization. *Organization Science* 7(4):413.

Ibrahim, R., and Nissen, M. 2007. Discontinuity in Organizations: Developing a Knowledge-Based Organizational Performance Model for Discontinuous Membership. *International Journal of Knowledge Management* 3(1):10.

Inkpen, A. C., and Dinur, A. 1998. Knowledge Management Processes and International Joint Ventures. *Organization Science* 9(4):454.

Jelinek, M., and Schoonhoven, C. B. 1990. *The Innovation Marathon: Lessons From High Technology Firms*. Oxford, UK; Cambridge, MA, USA: B. Blackwell.

Kerlinger, F. N., and Lee, H. B. 2000. *Foundations of Behavioral Research* (4th Ed.). New York: Wadsworth Publishing.

Levitt, B., and March, J. G. 1988. Organizational Learning. *Annual Review of Sociology* 14(1):319.

Leweling, T. A., and Nissen, M. E. 2007. Defining and Exploring the Terrorism Field: Toward an Intertheoretic, Agent-Based Approach. *Technology Futures and Social Change* 74:165-192.

March, J. G. 1991. Exploration and Exploitation in Organizational Learning. *Organization Science* 2(1):71-87.

National Commission on Terrorist Attacks Upon the United States. 2004. (Philip Zelikow, Executive Director; Bonnie D. Jenkins, Counsel; Ernest R. May, Senior Advisor). *The 9/11 Commission Report. Final Report of the National Commission on Terrorist Attacks upon the United States, Official Government Edition.* US Government Printing Office. http://govinfo.library.unt.edu/911/report/911Report.pdf

Nissen, M. E. 2005. Dynamic Knowledge Patterns To Inform Design: A Field Study of Knowledge Stocks And Flows In An Extreme Organization. *Journal of Management Information Systems* 22(3):225.

Nissen, M. E. 2006. *Harnessing Knowledge Dynamics: Principled Organizational Knowing and Learning*. Hershey, PA: IRM Press.

Nissen, M. E., and Buettner, R. R. 2004. Computational Experimentation with the Virtual Design Team: Bridging the Chasm Between Laboratory and Field Research in C2. *Proceedings of the Command and Control Research and Technology Symposium*, San Diego, CA.

Nissen, M. E., and Sengupta, K. 2006. Incorporating software agents into supply chains: Experimental investigation with a procurement task. *MIS Quarterly* 30(1):145.

Nonaka, I., and Takeuchi, H. 1995. *The Knowledge-Creating Company: How Japanese Companies Create the Dynamics of Innovation.* New York: Oxford University Press.

Overholt, M. H. 1997. Flexible Organizations: Using Organizational Design as a Competitive Advantage. *Human Resource Planning* 20.

Perrow, Charles B. 1970. *Organizational Analysis: A Sociological View*. Belmont, CA: Wadsworth Publishing Company.

Rahrami, H. 1992. The Emerging Flexible Organization: Perspectives From Silicon Valley. *California Management Review* 34(4):33.

Raynor, M. E., and Bower, J. L. 2001. Lead From the Center: How to Manage Divisions Dynamically. *Harvard Business Review* 79(5):92.

Tung, R. L. 1979. Dimensions of Organizational Environments: An Exploratory Study of Their Impact On Organization Structure. *Academy of Management Journal* (Pre-1986), 22(000004), 672.

Tushman, M. L., and O'Reilly, C. A.,III. 1999. Building Ambidextrous Organizations: Forming Your Own "Skunk Works." *Health Forum Journal* 42(2):20.

US Government. 2009. US Department of Homeland Security. Retrieved March 2, 2009, from http://www.dhs.gov/index.shtm.

Volberda, Henk W. 1997. Building flexible organizations for fast-moving markets. *Long Range Planning* 30.