5-8-2014

Information Sharing Tears of Irony: An Exploratory Study of the Information Sharing Paradox in the Intelligence Community

Kevin Odom Sr.

PERMISSION TO BORROW

In presenting this dissertation as a partial fulfillment of the requirements for an advanced degree from Georgia State University, I agree that the Library of the University shall make it available for inspection and circulation in accordance with its regulations governing materials of this type. I agree that permission to quote from, to copy from, or publish this dissertation may be granted by the author or, in his/her absence, the professor under whose direction it was written or, in his absence, by the Dean of the Robinson College of Business. Such quoting, copying, or publishing must be solely for the scholarly purposes and does not involve potential financial gain. It is understood that any copying from or publication of this dissertation which involves potential gain will not be allowed without written permission of the author.

Kevin Odom, Sr.

NOTICE TO BORROWERS

All dissertations deposited in the Georgia State University Library must be used only in accordance with the stipulations prescribed by the author in the preceding statement.

The author of this dissertation is:

Kevin Odom, Sr.
9406 Del Mar Circle
San Antonio, TX 78251

The director of this dissertation is:

Dr. Richard L. Baskerville
Department of Computer Information Systems
J. Mack Robinson College of Business
Georgia State University
Post Office Box 4015
Atlanta, Georgia 30302-4015

Information Sharing Tears of Irony: An Exploratory Study of the Information Sharing Paradox in the Intelligence Community

BY

Kevin Odom, Sr.

A Dissertation Submitted in Partial Fulfillment of the Requirements for the Degree

Of

Doctor of Philosophy

In the Robinson College of Business

Of

Georgia State University

GEORGIA STATE UNIVERSITY
ROBINSON COLLEGE OF BUSINESS
2014

ACCEPTANCE

This dissertation was prepared under the direction of the Kevin Odom Dissertation Committee. It has been approved and accepted by all members of that committee, and it has been accepted in partial fulfillment of the requirements for the degree of Doctoral of Philosophy in Business Administration in the J. Mack Robinson College of Business of Georgia State University.

H. Fenwick Huss, Dean

DISSERTATION COMMITTEE

Dr. Richard Baskerville
Dr. Nathan Bennett
Dr. Balasubramaniam Ramesh

ABSTRACT

Information Sharing Tears of Irony: An Exploratory Study of the Information Sharing Paradox in the Intelligence Community

BY

Kevin Odom, Sr.

May 8, 2014

Committee Chair: Dr. Richard L Baskerville

Major Academic Unit: Business

The sharing of information across government intra- and inter-agencies provides enormous benefits to Intelligence operations, but it also poses risks to Intelligence organizations' operational capability. These benefits and risks of sharing information within Intelligence Communities introduce a paradox that disturbs decision-making abilities and affect existing and future relationships with local and national Intelligence partners. With this paradox, there exist particular forces that affect the paradox, such as organizational factors and the behavior of an information sharer, the responsible actor that decides on how, when and with whom to share the information. Combining the two can produce a positive (desired) outcome that leads to successful mission accomplishment or negative (inadvertent) outcome that leads to loss of information disclosed or intentional loss of valuable information. An inadvertent outcome could result in an impact to the national defense of the United States. Do Intelligence Analysts share information when the risks outweigh the benefits? This research examines how understanding the paradox of information sharing is a critical element in understanding the behavior of Intelligence Analysts' decision-making in Intelligence operations.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

ABBREVIATIONS

List of Abbreviations (in Alphabetical Order)

CIA……..…..Central Intelligence Agency
DIA……Defense Intelligence Agency
DNI……Director of National Intelligence
DoD……Department of Defense
FBI……..Federal Bureau of Investigations
IC……Intelligence Community
ICD……Intelligence Community Directive
IED……Improvised Explosive Device
Info Share…...Information Sharing or Info Sharing
IA……...Intelligence Analysts
IS……....Information Security
IS(s)……Information Systems
IT……Information Technology
JDAM…….Joint Direct Attack Munitions
PEOU…….Perceived Ease of Use
PU……..... Perceived Usefulness
PWM……..Prototype-Willingness Model
NGA…….. National Geospatial Agency
NRO…….. National Reconnaissance Office
NSA……... National Security Agency
ODNI……. Office of Director of National Intelligence
TPB…… Theory of Planned Behavior
TRA……... Theory of Reasoned Action
UCMJ……. Uniform Code of Military Justice

ABSTRACT

The sharing of information across government intra- and inter-agencies provides enormous benefits to Intelligence operations, but it also poses risks to Intelligence organizations' operational capability. These benefits and risks of sharing information within Intelligence Communities introduce a paradox that disturbs decision-making abilities and affect existing and future relationships with local and national Intelligence partners. With this paradox, there exist particular forces that affect the paradox, such as organizational factors and the behavior of an information sharer, the responsible actor that decides on how, when and with whom to share the information. Combining the two can produce a positive (desired) outcome that leads to successful mission accomplishment or negative (inadvertent) outcome that leads to loss of information disclosed or intentional loss of valuable information. An inadvertent outcome could result in an impact to the national defense of the United States. Do Intelligence Analysts share information when the risks outweigh the benefits? This research examines how understanding the paradox of information sharing is a critical element in understanding the behavior of Intelligence Analysts' decision-making in Intelligence operations.

INTRODUCTION

1.1 Research Domain

This research study investigates the paradox of information (info) sharing. First, there are two important definitions regarding info sharing: non-electronic and electronic info sharing. Javernpaa and Staples (2000) define non-electronic info sharing as the volitional conveyance of information generated or obtained by one entity to another entity, whereas electronic info sharing occurs via computing and communication technologies. In addition, there are competing definitions and different ways to understand government info sharing and integration. Ramon Gil-Garcia, Soon Ae, and Janssen (2009) define information integration as "the forming of a large unit of organization entities, temporary or permanent, for the purpose of merging processes or sharing information" (p. 2). Within the literature, there are definitions that highlight the social and political nature, while other definitions focus more attention on info sharing and integration from technical aspects. Davenport and Prusak (1997), Pardo, Cresswell, Thompson, and Zhang (2006), Richardson and Asthana (2006), and Benjamin, Rockart, Morton, and Wyman (1984) suggest that research that highlights the social aspects of government integration focuses on info sharing, inter-agency collaboration, and coordination mechanisms. In contrast, research that deals with the technical aspects focuses on topics such as interoperability and the integration of data by means of various technologies, including standards-based document sharing, middleware applications, data warehouses, and consolidated information systems (Dawes, 1996; Larence, 2008; Lips, O'Neill, & Eppel, 2011; Luo, Zhang, & Leung, 2001; Miranda, 2003). The focus of this research study is towards the social aspects of government integration focusing on info sharing, inter-agency and intra-agency collaboration, coordination mechanisms, and the behavior of information technology users. An example of Gil-Garcia et al.'s (2009) definition of

integration and info sharing is the 2004 U.S. Intelligence Reform and Terrorism Prevention Act (IRTPA). The IRTPA authorized the president to create an *Info Sharing Environment* (ISE) for the sharing of terrorism information in a manner consistent with national security and with applicable legal standards relating to privacy and civil liberties. The plan of the ISE highlights sharing of terrorism prevention-related information among all ISE participants, in the forms of federal-to-state, state-to-state, state-to-locality, government-to-industry, and even federal government-to-foreign ally.

Next, since this research investigates the paradox of info sharing, it is important to understand and explain the meaning of *paradox*. Leaders in inter- and intra-agency organizations, including the military, are given responsibilities to increase efficiency, reduce budgets, foster innovation, and build teams for creativity, and are expected to think globally and, at the same time, to think locally. It has become common to suggest these types of everyday responsibilities are paradoxical in nature and it has become a cliché to managers and leaders. Handy (1994) argues that *paradox* is both overused and underspecified; thus, simply labeling something as a paradox does not necessarily advance the understanding of it. On the other hand, other researchers often avoid defining paradox altogether (e.g., Westenholz (1993), which does not advance the comprehension of paradox either. Although the term *paradox* provokes numerous and various meanings, Hampden-Turner (1981) and Schneider (1990) suggest that it begins with philosophers from the ancient Greeks to Existentialists who have viewed human existence as paradoxical with the understanding of its position in tensions between life and death, good and evil, self and other. Equally, psychologists have long stressed the cognitive nature of paradox, examining its impacts of tensions on creativity and mental health or using paradoxical therapy to help actors face their inner conflicts (Bateson, 1972; Harris, 1996; Rothenberg, 1979;

Wartzawick, Weakland, & Fisch, 1974). In organizational studies, researchers have defined paradox as contradictions embedded within a statement, human emotions, or organizational practices (Eisenhardt & Westcott, 1988; Murnighan & Conlon, 1991; Vince & Broussine, 1996). Conversely, others describe paradox as an observation that counters common beliefs or as an unintended consequence (Davis, Maranville, & Oblog, 1997; Sitkin & Bies, 1993). The approach of this research study is from the perspective of Koot, Sabelis, and Ybema (1996), which argues for using the notion of one of the great philosophers, Ludwig Wittgenstein, which suggests *paradox* as something surprising. In addition, the most useful definition is from Quinn and Cameron (1988), authors of one of the leading books in the field of paradoxes; to wit, "embracing clashing ideas, paradox . . . involves contradictory, mutually exclusive elements that are present and operate equally at the same time." They argued the importance of understanding the complexity, diversity, and ambiguity of organizational life and highlighted the insightfulness paradox offers the potentially powerful framework for examining the impacts of plurality and change, adding understanding of divergent perspectives and disruptive experiences. Therefore, the paradoxical view of this research is from Quinn and Cameron (1988) definition combined with Ford and Backoff (1988) perspective, which defines paradox as some *thing* that denotes a wide variety of contradictory, yet interwoven elements; i.e., perspectives, feelings, messages, demands, identities, interests, or practices. The paradox construct is between the benefits and risks in sharing information which is influence by two organizational factors: security policies and info sharing policies and Intelligence Analysts' (IA) behaviors: attitude and intuition, as actors attempting to make sense of an increasingly intricate, ambiguous, and ever-changing IT world. The paradox becomes apparent through the self or social reflection or interaction that

reveals the seemingly absurd and irrational coexistence of the actual benefits and inherent risks to info sharing.

In adopting the social aspect of info sharing, this research focuses on Information Technology (IT) users of electronic info sharing that occurs via computing and communication technologies. These particular IT users are both IA who have access to electronic information and decision-makers when using communication technologies and deciding to share information. Every day this unique group of IT users confronts the paradox: a mystery or consummate blend of opposites on the systems they use to communicate with one another. This paradox becomes apparent in the info sharing decision based on the IA knowledge of the organization's security and info sharing policies and the conflict that exists within them because of their personal behavior, attitude and intuition, and their subjective normative beliefs. They must internally analyze the benefit versus risk tradeoff propositions, which are impacted by the organization's security and info sharing policies and the individual's beliefs, typically influenced by an actor's background factors that influence his/her behavior intention. One key factor to understand within the paradox of info sharing in the organization is the inherent risk taker, not the individual. The organization position would always assume the optimum cost-benefit analysis, but the decision-maker, the IA, does not necessarily have all the information and can't possible consider all the variables in a cost-benefit analysis, which may very well conflict with the organization's security and info sharing policies. Would the government consciously hire risky IA to share Intelligence data? We know that technology systems drive policy every bit as much as policy drives technology systems. Policy and technology face paradoxes specifically where policymakers appear to be comfortable with paradoxical situations, and even reap value from its existence, because paradox can provide decision-makers critical wiggle room (John, Boardman,

& Sauser, 2008). On the other hand, technology developers prefer less ambiguity and more clear-cut specifications. John et al. (2008), suggest that the IT users' preference for unambiguous languages, like mathematics, desire for encyclopedic knowledge of prioritized requirements, and occasional reluctance to buck the engineering community's "conventional wisdom" limits the IT users' problem-solving approaches. Thus, there is conflict in the IT users' decision-making when sharing information from an organizational versus an individual behavior perspective.

Finally, in the info sharing domain, it is clear that, for an info sharing entity to survive, it must develop and maintain long-term relationships with the entities it decides to share with in the relationship. To this end, for the Intelligence Community (IC) to survive, it also depends on vast quantities of information to build rapport with each other that attracts the attention of national partners. Info sharing among government agencies gained considerable attention in the aftermath of the September 11 terrorist attacks, Hurricane Katrina, and mass shooting rampages, such as the one involving Fort Hood gunman Nidal Hassan who killed 13 people on a U.S. military post. Feldman-Stewart et al. (2007) argued that there was "near universal agreement" that fighting terror would require deeper data exchanges than ever existed before between inter- and intra-agencies, including our military forces. The improvement of info sharing among government agencies has become one of the highest priorities of decision-makers, and the lack of info sharing has been identified as a major point of failure leading to and responding to these horrific events (Akbulut-Bailey, 2011).

Today, many international and U.S. political leaders place great emphasis on the purpose of national and foreign policies that should establish a systematic bias in favor of much more info sharing. The ability to collect, analyze, and respond to user information is of growing

importance (Awad & Krishnan, 2006). One of the objectives of the IC is to be an integrated network of agencies that work together to protect our nation's defense. To this end, the Intelligence Community Directive (ICD) Number 501, addresses the mandates in the IRTPA of 2004 to strengthen the sharing, integration, and management of information within the IC, and establishes policies for discovery, dissemination or retrieval of intelligence, and intelligence-related information collected or analysis produced by the IC. The objective of ICD 501 is threefold: 1) to foster an enduring culture of responsible sharing and collaboration with an integrated IC; 2) to provide an improved capacity to warn of and disrupt risks to the U.S. homeland, and U.S. persons and interests; and 3) to provide more accurate, timely, and insightful analysis to inform decision-making by the president, senior military commanders, national security advisers, and other executive branch officials. Sharing information across inter-agencies, like foreign national partners, or intra-agencies, like the IC, is usually presented by the potential gains that government agencies could obtain from their participation in the inter- or intra-agency information exchange initiative. Some examples are to detect national security threats around the world, increasing government transparency and accountability; reducing costs and duplication; a more efficient agency or governmental organization; and improved decision-making for government officials and public servants. According to (Dawes, 1996), government info sharing offers a real opportunity to share databases and make sharper decisions based on more information that is complete.

Although there are number of potential benefits to sharing information, there are perhaps an equal number of challenges, barriers, and risks not to share information; thus, a paradox exists. The reasons not to share information, as highlighted within the literature, begin with the complex integration and flow along a contour of difficult tasks facing a myriad of political,

organizational, legal, and technical challenges (Gil-Garcia et al. (2009); Gil-Garcia, Chengalur-Smith, and Duchessi (2007); (Luna-Reyes & Gil-Garcia, 2003; Luna-Reyes, Gil-Garcia, & Cruz, 2007). This may include lack of political support, lack of financial resources, individual privacy, confidentiality, and secrecy concerns; WikiLeaks' and Live Leaks' release of damaging information inadvertently or intentionally; and poor technical skills. Given the benefits and challenges, this research suggests a gap exists which ends with a challenge not addressed by using the technologies and other processes that creates the current paradox. This research conjectures that the info sharing decisions of highly skilled or *smart* info sharers would reflect superior decisions on the information to share, while the decisions of relatively less skilled or *risky* info sharers are more likely to be induced by behavioral biases. This inference is motivated by recent research in behavioral economics (Frederick (2005); Benjamin, Brown, and Shapiro (2013); and Dohmen, Falk, Huffman, and Sunde (2010)), which finds that lower levels of smartness are associated with more *anomalous* preferences and stronger emotional behavioral biases. The studies show that smart individuals exhibit lower levels of risk aversion and greater patience (Korniotis & Kumar, 2011).

Within the literature, the fact that information has value in terms of monetary importance is well known, and there are several information models to measure it; however, one of the non-financial values of information where the preconception is not necessarily straightforward for information is the value of power (Ahituv & Carmi, 2007). According to Ahituv and Carmi (2007), the relationship between information and power in inter- or intra-agencies can pertain to many issues that senior officials are challenged with, such as knowledge management and info sharing. Specifically, the implication of these issues that senior officials face today, Ahituv and Carmi (2007) argue, on one hand, is a driver of change in the distribution

of power within the agency due to a change in the information distribution. However, on the other hand, the introduction of these issues is a process that involves interested parties intentionally using their power, deriving partly from the information they have, to affect the nature of the agency and to obtain more power by obtaining more information. To this end, Ahituv and Carmi (2007) postulate that this effect exists because there is a positive connection between information and power.

Moreover, there are strong political pressures on inter- and intra-agencies to engage in info sharing; however, in practical application, how consistently this is done really depends on our foreign partners' discretion as well as our inter-agencies' application of the Office of the Director of National Intelligence (ODNI) policies. There is plenty of guidance within the IC on info sharing; in fact, each agency has its own policies and supplements to national policies on whether information should be shared, and, if so, what information, to whom, and to some extent, the information shared is decided on a case-by-case basis. Our national partners also have their own info sharing policies on what information should be shared, most importantly, with whom, and may also decide to share, based on their nation's interest, on a case-by-case basis. Another concern for the IC's mission in national defense is sharing of information that may lead to classified information being mistakenly shared, resulting in information leakage, intentionally or unintentionally. Intentional information leakage may be the result of espionage. On the other hand, unintentional informational leakage can occur from inferences. Inferences occur when extrapolated classified information is from different sources of unclassified shared information. Inferences exist because of the inherent engineering relationships between different pieces of information and have a major impact on national defense. One inference that is occurring more frequently today is espionage. Espionage occurs because of the power of information.

1.2 Research Perspective

This study will use the adaptation of the Theory of Planned Behavior (TPB) which is an extension of Theory of Reasoned Action (TRA) (Ajzen, 2011, 2012; Fishbein & Ajzen, 2005) to inform this research in capturing the paradox in the info sharing decision of an IA analysis of the risks and benefits influenced by the organization's security and info sharing policies as well as his/her attitude and intuition. Although IA navigate the paradox of the benefits and risks in sharing information, the influences as mentioned, impacts the decision to share on not share information. These influences result in factors that drive behavior intentions of IA. An intriguing factor is that an IA's attitude and intuition may conflict with the organization's security and info sharing policies. Adaptation of the TPB to inform this research allows examination and further understanding of the process of IA behavior that deals with the relations among beliefs (attitudes and intuitions) and the intentions of sharing decisions. Perceived Behavioral Control (PBC) is added as a construct to TPB to solve the problem of explaining behaviors in which the actor does not have full volitional control (Fen & Sabaruddin, 2008). TPB, when applied to a wide range of behaviors in order to understand why individuals behave in a certain way, is one of the best-supported social psychological theories with respect to predicting human behavior (Sommer, 2011). According to (Smith, Manstead, Terry, & Louis, 2007), the central premise is that behavioral decisions are the result of a reasoned process in which the behavior is influenced by attitudes, norms, and perceived behavior control. With roots in a social psychological approach to behavior, TPB and TRA postulate that changing behavior is a matter of changing the cognitive structure underlying the behavior in question. The theories are a series of four hypotheses. The first hypothesis relates to behavior assumed primarily to be a function of an individual's intention to perform that behavior. The second hypothesis relates to

the intention to perform the behavior as a function of the weighted combination of two factors; a personal factor that is the attitude toward the behavior and a social factor that is the subjective norm. Thus, in this hypothesis, the attitude toward the behavior is the feeling of favorableness toward the behavior and the subjective norm suggests the perception that people of importance think that the individual should or should not perform the behavior. The third hypothesis suggests that underlying the attitude toward the behavior is an underlying cognitive structure of behavioral beliefs that performing the behavior will lead to certain outcomes and the evaluation of these outcomes. Finally, the last hypothesis suggests the subjective norm is an underlying cognitive structure of normative beliefs that particular individuals or groups think that one should or should not perform the behavior and the individual's motivation to comply with each of these significant others.

In using information for decision-making, the information processing perspective argues that individuals make decision based on the amount of information available to them and the effort they expend to arrive at their decisions. It is impossible to imagine that every IA will have all information available on a topic or complete understanding of the organization's behavior when deciding to share information with a given entity. Some researchers (Bettman, 1979; Bettman & Park, 1980) argue that individual decision-making strategies vary on a continuum from being completely rational normative to purely heuristic. This suggests that, where all the necessary information and resources are available, an individual makes a rational-normative decision for arriving at an accurate optimal decision. Conversely, in the situations where the context is novel and the information available is limited, individuals resort to heuristic decision-making style, through which they draw generalizations and projections to arrive at an appropriate decision, which minimizes perceived cognitive burden and risk (Bettman & Park, 1980).

Therefore, to understand an individual's behavior in info sharing decision-making, and perhaps to help the practitioners more successfully manage ways to identify, seek, assess, use and share information, the research will endeavor to answer the question: How do IA navigate the paradox between the benefits and risks affected by individual behaviors and organization factors that inhibit info sharing decisions?

The adaptation of the TPB is used to inform this research study in analyzing an individual's behavior intention in making the decision to share information with others, either within the government inter- or intra-agency organizations or publicly with other individuals. However, the research study will also use an exploratory approach from a grounded theory perspective. Charmaz (2010) argues this approach and method bring surprises, spark ideas, and foster seeing data in fresh ways and exploring ideas about the data through early analytic writing. It also offers flexible guidelines for collecting and analyzing qualitative data to construct theories *grounded* in the data themselves (Charmaz, 2010, p. 2). Thus, the data form the foundation of the theory and the analysis of the data generates the concepts that are constructed. In this approach, one attends to what he/she hears, sees, and senses during the interview. Using this approach, this research will take a constructivist approach to the exploratory study. Charmaz (2010) also argues a constructivist approach places priority on the phenomena of study and sees both data and analysis as created from shared experiences and relationships with participants and other sources of data. A critical element in the constructivist approach is that it studies the *how* and sometimes the *why* participants may construct meaning and actions in specific situations. Moreover, Charmaz (2010) argues constructivist grounded theorists take a reflexive stance toward the research process and products and consider how their theories evolve, from which she postulates that both researchers and research participants interpret meanings and actions. The

justification for building a theory as opposed to only using existing theory, Bartunek, Rynes, and Ireland (2006) argue for research that builds theory from cases are often regarded as the "most interesting" research and are among the most highly cited pieces in the *Academy of Management Journal*, with impact disproportionate to their numbers (Eisenhardt & Graebner, 2007). With the understanding that sound empirical research begins with strong grounding in related literature, which identifies a research gap and proposes research questions that address the gap, theory building from cases requires researchers to take an added step of justifying why theory building rather than theory-testing better addresses the research question. The critical point to the justification in building theory in this study is to convince readers that the research question is crucial for organizations and/or theory, and demonstrate that the existing research either does not address the research question at all, or does so in a way that is inadequate or likely to be untrue (Eisenhardt & Graebner, 2007).

1.3 Research Approach

Using an exploratory approach from a grounded theory perspective and employing the constructivist grounded theorist perspective allows for a set of principles and practices, not as prescriptions or packages, but emphasizes flexible guidelines, according to Charmaz (2010). Therefore, it is also important to understand additional approaches, methodological rules, recipes, and requirements to dealing with the how and *how* questions in research studies. (Van de Ven, 2007a) suggests there are two basic epistemologies that underlie the different approaches that are necessary to study research questions dealing with *what* and *how*. Bruner (1986), p. 147), distinguished them as representing two basic types of human intelligence: the paradigmatic, logical-scientific (variance) mode of thought and the narrative (process) mode of thought. He describes them as follows:

> There are two modes of cognitive functioning, two modes of thought, each providing distinctive ways of ordering experience, of constructing reality. The two (though complimentary) are irreducible to one another…. Each of the ways of knowing, moreover, has operating principles of its own and its own criteria of well-formedness. They differ radically in their procedures for verification. (Bruner, 1986: 11)

Bruner highlights that we have relatively little knowledge about how narrative understanding works compared to the vast literature on paradigmatic thinking and its methods. Although recent research in many fields is filling this void, much remains to be done. Aldrich (2001) distinguishes the *what* and *how* questions in terms of outcome-driven and event-driven research, as follows:

> Outcome-driven explanations are built backward, from an awareness of observed outcomes to prior casually significant events. Two related problems are introduced with this strategy. First, it often leads to investigators' selecting on the dependent variable, a well-known research bias. Second, even though we might include all organizations—those that have experienced the event and those that have not—we still observed them at only one point in time (Aldrich 2001: 118). Conversely, event driven explanations are built forward, from observed or recorded events to outcomes. (Aldrich 2001: 118).

Aldrich (2001) notes that researchers often run into trouble by not making explicit distinctions between event-driven and outcome-driven studies of organizational and other social processes. His argument is based on two different definitions of process used within the literature: 1) a category of concepts or variables that pertain to actions and 2) activities and a narrative describing how things develop and change (Van de Ven, 1992). The research question of this study is: How do IA navigate the paradox between the benefits and risks affected by individual behaviors and organizations factors that inhibit info sharing decisions? While the research question could fall in the category of the second definition, which typically takes an event-driven approach that is often associated with a process study of the temporal sequence of

events (Abbott, 1988; Pentland, 1999; Poole, 1983; Tsoukas, 2005), this study will use the first definition, which is associated with a variance model with an outcome driven explanation. According to Mohr (1982), when the first definition is used, process is typically associated with a variance model where an outcome-driven explanation examines the degree to which a set of independent variables statistically explain variations in some outcome criteria (dependent variables).

Mohr (1982) and Poole (1983) distinguished variance and process approaches to social scientific research. A variance model explains change in terms of relationships among independent variables and dependent variables, while a process model explains how a sequence of events leads to some outcome. The common thread running through both works is the difference between scientific explanations cast in terms of independent variables causing changes in a dependent variable, and explanations that tell a narrative or story about how a sequence of events unfolds to produce a given outcome. In this particular study, the variance method will seek to explain continuous change driven by deterministic causation, with independent variables acting upon and causing changes in dependent variables.

The research will closely examine the paradox confronting the IA when sharing, more specifically, the reasons the IA may be willing to share information with others, even when the risks may outweigh the benefits. The researcher will also closely examine the behaviors of the IA in their decision analysis of intelligence operational mission-based info sharing events. Although the intelligence mission scenarios are theoretic, they are possible mission events that will serve as the basis for examining a user's behavior in deciding to share information. The security and info sharing policies are independent variables as well as attitude and intuition. In any military battle, the formidable force is often the entity that has the most complete and

accurate information that is collected and shared among other reliable forces, but not the enemy. However, although each entity may share information with trusted partners, each side faces variations of information leakage, espionage, and political strife that affect the decision to share information, and that makes the information valuable in terms of power or less valuable over time in terms of diminishing return on investment. The researcher has selected to use intelligence mission scenarios because they examine the actor's decision and behavior intention. How will he/she evaluate risk (consequences) versus benefits, consider the security and info sharing policies, and will his/her personal or subjective norm be the controlling factors to the sharing decision? These similarities and differences will allow the researcher to combine literal and theoretical replication logic (Yin, 2009). While this will not ensure generalizability of the study, it will hopefully add to the robustness and confidence in the findings (Yin, 2009). To deepen the understanding and to help achieve satisfactory validity, the researcher will collect data from several sources using different data collection methods, including formal interviews with Intelligence community users, analysis of email correspondence, observations of recent events, and review of archival documents.

To improve its relevance to practice, this study will utilize the pluralistic methodology of engaged scholarship (Van de Ven, 2007b; Van de Ven & Poole, 1995) as a participative approach involving the perspectives of various stakeholders in order to understand complex problems (Van de Ven, 2007, p. 9). Although the researcher will remain in control and direct all research activities, advice and feedback will be solicited from various key stakeholders and informants, such as public users, information security managers, military IA and other researchers, in each step of the research process, including research design, theory building, problem solving, and problem formulation (Van de Ven, 2007 p. 26-29). The research will

follow data analysis procedures and display methods suggested by Miles and Huberman (1994b) for qualitative case studies using three concurrent flows of activity: data reduction, data display, and conclusion drawing and verification.

As a result, this research will make five valuable contributions: 1) describe the paradox of the info sharing decision of an IA analysis of the benefits and risks influenced by the organization's security and info sharing policies and an individual's behavior intention; 2) explain the decision-making behavior of people's willingness to share information with others, even when the risks may outweigh the benefits (to better understand how we might go about modifying behavior in a desirable direction); 3) demonstrate how TPB may be used as an analytical framework that describes how past behavior of users decisions to share information with others in the IC; 4) develop a conceptual framework to evaluate adherence to info sharing decision-making in the IC; and 5) provide practical guidance for improving IA decision-making in the presence of the paradox.

1.4 Summary

The subsequent chapters of this dissertation proposal detail the arguments underpinning the-research as follows:

- **Chapter 2 Literature Review:** This chapter presents a comprehensive review of the literature in the area of info sharing by examining what previous research reveals about first, the benefits of info sharing and the widespread need for more to conduct military intelligence operations; second, the power of information in the organizational environment both as positive and negative forces; and last, information sharing policy and political ramifications, as well as how info sharing results in information leakage and espionage, each of which pose serious threats to our nation's defense. In part, this chapter focuses on existing knowledge concerning the benefits of info sharing and the effects of info sharing because of the value in information or the power associated with

owning the information. The review reveals that few qualitative variance studies exist that explore the paradox in info sharing; specifically, the inconsistencies between the IA's behavioral intentions to share information and the organization's security and info sharing policies to actually release information that results in a positive or negative outcome based on the value of the data alone or the value of information when aggregated with other information. Why would the IA decide to share certain information with little regard for the risk in doing so and for little return (cost-benefit), while the disclosure of that same data puts the organization at risk and, doing so, affects national interest, meaning greater risk and a higher return?

- **Chapter 3 Theory of Planned Behavior:** This chapter provides a description of the Theory of Planned Behavior (TPB), its applications in prior case studies, and its constructs of a person's behavioral, normative and control beliefs. This review helps to illustrate how TPB, with its central focus on the background factors that may influence the beliefs people hold and how these factors are expected to influence intentions and behavior indirectly by their effects on the IA's decisions to share information. Therefore, the researcher's approach is to use the adaptation of the TPB to inform this research study in analyzing the decisions of the IA's info sharing decision-making risks outcomes using intelligence operational mission-based events that are interesting because of what they reveal about the common sense, everyday layman's view of the world.
- **Chapter 4 Research Design:** This chapter discusses the reasons for this study utilizing a qualitative, exploratory approach to discover answers to questions through the application of scientific procedures. The main aim is to answer a *how* or *why* question with the researcher having little control over the contemporary events to be examined. Further, this section explains the use of the engaged scholarship approach in an effort to increase the research's relevance and include the insightful perspectives of key stakeholders to gain familiarity with a phenomenon and to achieve new insights into it. In addition, it has to portray accurately the characteristics of a particular individual and situations. This segment also discusses the critical realist philosophy that underlies the engaged scholarship approach; a philosophy that adopts an objective ontology but a subjective epistemology.

- **Chapter 5 Data Analysis**: This chapter outlines the data collection strategy that will follow the three recommended principles of data collection for case studies in order to deepen understanding and improve validity through data triangulation: (1) using multiple sources of evidence; (2) creating a case study database; and (3) maintaining a chain of evidence. It also details the methods used in analyzing this qualitative data consisting of three concurrent flows of activity: data reduction, data display, and conclusion drawing and verification.
- **Chapter 6 Discussion:** This chapter discusses why people share information with others; primarily, what influences the individual's decision that drives him/her to violate security and info sharing policies. The understanding of IA behaviors allows a better understanding of how one might go about modifying behavior in a desirable direction. The results provide support that background factors do influence the beliefs people hold.
- **Chapter 7 Contributions and Limitations**: This chapter discusses the major contributions revealing the paradox in info sharing: 1) describing the paradox of the info sharing decision of an IA's analysis of the benefits and risks influenced by the organization's security and info sharing policies and an individual's behavior intention; 2) explaining the decision-making behavior of people's willingness to share information with others, even when the risks may outweigh the benefits, (to better understand how we might go about modifying behavior in a desirable direction.); 3) demonstrating how TPB may be used as an analytical framework that describes how past behavior of users decisions to share information with others in the IC; 4) developing a conceptual framework to evaluate adherence to info sharing decision-making in the IC; and 5) providing practical guidance for improving IA decision-making in the presence of the paradox.

LITERATURE REVIEW

2.1 Information

Information is a ubiquitous label whose meaning is almost never specified. According to McKinney Jr and Yoos Ii (2010), virtually all the extant IS literature fails to explicitly specify meaning for the very label that identifies information and, more important, that this is a vital omission, because without defining what we are talking about, we can hardly know it. Since IS has nominated a plethora of attributes, such as relevant, accessible, timely, accurate, variable, flexible, and complete to describe information, Newman (2001), argues that it is important to produce what *information* means, its scope or the implication of the various definitions. Since the pursuit of a more coherent understanding of information has become the subject of a new domain, the philosophy of information, McKinney and Yoos Ii (2010) present a taxonomy of information that secures the term.

From a *token view*, McKinney and Yoos Ii (2010)posit that information and data are both tokens manipulated by processes. There is a widespread view in IS on this understanding, particularly from Majchrzak, Rice, Malhotra, King, and B. (2000), who studied a virtual team's use of collaborative software. The software allowed team members to create, store, retrieve, distribute, and analyze data, a process that manipulates tokens. In the *syntax view*, information is the measureable relationship among tokens that reduces entropy. The tokens in this view are mental states; the effectiveness measure of information quantifies the change in mental states. In the *representation view*, information is meaning. Meaning emerges from a sign that stands for an object to a particular observer. An example from IS research is the personal information construct in privacy research. Personal information (sign) about an individual (object) gives meaning to an unknown their parity (observer). Finally, in the *adaptation view*, subjectivity

assumptions are introduced to explain how information is created by a system (e.g., person, organization). Information is created when a system perceives differences in its environment, which alters that system. Understanding the taxonomy of information is important to this research study because, as posited by McKinney Jr and Yoos Ii (2010, p. 339), "it purports to represent what information really is." To understand this leads to the value of information and its power in military operations and to Intelligence Operators who decide to share information.

2.2 Paradoxes

Quinn and Cameron (1988) define *paradox*, also referred to as *antinomy*, as a real or apparent contradiction between equally well-based assumptions or conclusions. They argue that, when considered separately, the arguments supporting paradoxical propositions appear sound; however, considered together, the arguments appear contrary or even contradictory. Within the literature, much effort has been devoted to resolving or understanding paradoxes, because they reveal inconsistencies in our logic or assumptions (Quinn & Cameron, 1988). Paradoxes can arise either from theoretical inconsistencies or from limited frames of reference. They often require us to alter our assumptions, to shift perspectives, to pose problems in fundamentally different ways, and to focus on different research questions. According to Quinn and Cameron (1988), when studying paradoxes, we are forced to ask very different questions and to come up with answers that stretch the boundaries of current theories. They postulate that the resulting formulations are likely to be of interest not only to organizational scholars, but also to all scholars of social process; therefore, addressing organizational paradoxes is both exciting and challenging and inspires new ideas and creative theory.

Within the literature, contingency theory is an alternative approach that is used as a response to tensions or conflict within organizational systems. Early contingency theory from

the late 1960s inspired decades of research exploring how contexts influence the effectiveness of opposing alternatives (Smith & Lewis, 2011). However, according to Smith and Lewis (2011), the paradoxical studies approach to tensions and conflict involves exploring how organizations can attend to competing demands simultaneously as opposed to contingency theory, which explores conditions by selecting among competing demands. They argue that, although choosing among competing tensions or conflict might aid short-term performance, a paradox perspective argues that long-term sustainability requires continuous efforts to meet multiple, divergent demands (Cameron, 1986; Lewis, 2000). Within the literature, Wendy K. Smith and Marianne W. Lewis (2011) found, after surveying over the past 20 years across several different management journals, not only have scholars increasingly adopted a paradox perspective, but there also has been an increase in the research in studies of organizational phenomena and levels of analysis. Their framework, built on four categories of paradox, represents core activities and elements of organizations: learning, belonging, organizing, and performing. The most interesting of the four are organizing and performance paradoxes. Smith and Lewis (2011) suggest that organizing paradoxes surface as complex systems, which create competing designs and process to achieve a desired outcome. These include tensions between collaborating and competing (Murnighan and Conlon (1991), empowerment and direction (Denison, Hooijberg, & Quinn, 1995), or routine and change (Flynn & Chatman, 2001; Gittell, 2004). Performing paradoxes stem from the plurality of stakeholders and result in competing strategies and goals. Tensions surface between the differing, and often conflicting, demands of varied internal and external stakeholders (Donaldson & Preston, 1995).

In summary, the literature highlights the richness and scope of a paradox perspective. The key finding is that there are conflicting yet inter-related elements identified across a range of

organizational phenomena as well across differing levels of analysis. The literature suggests tensions and conflict at the level of the individual (Markus & Kitayama, 1991), dyad (Argyris, 1988), group (Smith & Berg, 1987), project (Van Marrewijk, Clegg, Pitsis, & Veenswijk, 2008), and, most important, the organization (Cameron & Quinn, 1988). According to Cameron and Quinn (1988), there are four strategic approaches that can be used to resolve paradoxes and that each represent a different way of transforming research theories and ways of thinking. First, even with accepting the paradox and learning to live with it, we learn that it has a cost to bear. To accept a paradox is to acknowledge that things need not be consistent and that the seemingly opposed viewpoints can inform one another and our models are just models, incapable of fully capturing the conflict, no matter how strongly our logical arrogance tries to convince us otherwise. All the other strategies suggest resolving the tension or conflict between the contrary positions. Bertrand Russell's (1970) approach, which is the most interesting, attempts to resolve this by clarifying levels of reference and the connections among them. According to Cameron and Quinn (1988), level distinctions, such as part-whole, micro-macro, or individual-society, have proven extremely useful for social research, and to carry out this analysis, it is necessary to specify as precisely as possible how the levels interrelate. Supporting this approach is Reese and Overton's (1978) formulation where one side of the paradox may influence the conditions under which the other will operate.

2.3 Info Sharing Paradox

As a starting point, the *info sharing paradox* in this research study refers to the conflict between the benefits and risks confronted by the IA. This conflict is also influenced by the organization's security and info sharing polices as well as the attitude and intuition of the IA. Often times the influences that drive an IA's decision are also in conflict. The decision results in

a positive or negative outcome based on benefits and risks. Why would the IA decide to share certain information with little regard for the risk in doing so and for little return (cost-benefit), while that same data disclosed puts the organization at risk and doing so affects national interest; meaning greater risk and a higher return? Paradoxes are well-established concepts in many fields of the social sciences, even though the precise contours and cases of the paradox are quite controversial. There are opposing forces in the *info sharing paradox* between the benefits and risks influenced by the organization's security and info sharing policies as well as the IA's behavior all compete with one another and affect the outcome of the info sharing decision exchange. Another conjecture of this research is the IA's knowledge, *smart info sharer*, of the organization's info and sharing policies that facilitate sharing information appropriately with others. However, while navigating the conflict of the benefits and risks, the IA's knowledge, *risky info sharer*, may be biased when influenced by an IA's attitude and intuition. Some decisions to share information may put the organization at higher risks because of IA behaviors, which could result in little regard for benefits, whether the intentions are inadvertently or intentionally.

The *info sharing paradox*, weighting the benefits versus the risks, is based on the superior information advantage that exists from the organization's analysis that the IA has complete understanding of all the variables and associated risks (cost-benefit analysis) to sharing the information as well as his/her behavior. The organization's approach of optimal sharing trends is based on the principle that every IA completely *believes in* and understands the derived policy on the different classifications of the information; inter- and intra-agency relationships; and continuous internal meetings and agreements with national partners and the sharing of information. The organization's principle is based on the belief that information advantage will

alleviate the information asymmetry between the IA and the organization's assessment (cost-benefit analysis) of the risk and other organizational characteristics that will result in a more accurate risk decision to the sharing of information.

In the IS literature, there is a considerable body of academic research on the *privacy paradox*, similar to the *info sharing paradox*, which is premised on the assumption of rational choice (John, Acquisti, & Loewenstein, 2011). The work has been characterized by the following assumptions: 1) people make sensible and consistent trade-offs between privacy and other concerns (Derlega, Metts, Petronio, & Margulis, 1993; Petronio, 2000; Posner, 1981; Rosenfeld, 2000) and 2) there are reliable differences between individuals in concern for privacy (Laudon, 1996). This holds true for the info sharing paradox as well. An IA's decision to share information is based on the assumption of a rational choice with sensible trade-offs between the benefits and risks associated with sharing information. The argument is based on the consistency and the reliable difference between the IA's behavior (attitude and intuition) and the organization's security and info sharing policies when considering the benefits and risks trade-offs. It has been argued that disclosure decisions are made by balancing "the usefulness of privacy with the utility of openness" (Petronio, 2000, p. 37) and that people engage in "disclosure management," such that they disclose information only when they expect a "net benefit" (White, 2004, p. 48).

The similarities in the privacy and info sharing paradox are based on the trade-offs of the benefits and risks in disclosure of information. In the *privacy paradox,* active and willing participants are seen as individuals in the market for personal information and viewed as consumers or rational economic agents who are either fully informed or who based their decisions on probabilities coming from known random distributions. In the *info sharing*

paradox, these active and willing participants are the IA who are the individuals in the market for privilege information (secrecy or aggregated) and are certainly viewed as the rational economic agents in the IC. As in the *privacy paradox*, an important factor in the info sharing paradox is that the IA are agents who are either fully informed or who based their decisions on probabilities also coming from known random distributions. In the *privacy paradox*, consumers not only have the right to manage the privacy trade-offs without regulative intervention, they also can use that right in their own best interest. Unlike the *privacy paradox*, in the *info sharing paradox*, the IA must manage the benefits and risks of sharing info with regulative intervention; however, like the *privacy paradox*, they often may use their right in their own best interest. According to Canada (2012), the reason this exists in the privacy paradox is individuals concern about privacy is not absolute. The argument is the same for the info sharing paradox; info sharing is not absolute. He further explains that consumers are willing to knowingly trade off privacy concerns for economic benefits. He argues that, in some cases, private information is consciously exchanged for convenience, personalization, or merely the ability to use a website. How does this relate to the *info sharing paradox*? The argument in the privacy paradox is the very same in the info sharing paradox. Is there appropriate value or return on investment in the trade-off, for the disclosure or share of information? Therefore, theorists argue that what must be considered is the deviation between *attitudes* about sharing info and the *actual behavior* in the handling of sharing the info.

Weighing the risks and benefits in the privacy paradox are the same in the info sharing paradox. Often the IA does not have all the information for complete assessment of the risks and benefits when sharing info and consumers are faced with the same challenge. For example, in an online transaction, a consumer may possess incomplete information when considering the risks

and benefits in sharing info. The consumer is not fully aware of the nature and existence of privacy invasion. In other words, data collection by third parties may be taking place without the knowledge of the consumer. In considering the risks and benefits to sharing the privacy information, the consumer lacks complete information regarding the alternative or the ease of not only protective technologies, but also understanding how the disclosed information will be used by the collecting agent or the third party. Canada (2012) argues that most people do find it difficult enough just to find and understand a company's privacy policy, much less to monitor the company's use of personal information and detect when violations have occurred. In info sharing, the IA constantly navigates the paradox of the benefits and risks that are influenced by the organization's security and info sharing policies. This is relevant to the IA's decision of sharing info based on the concept of bounded rationality. The concept *bounded rationality* refers to our inability to acquire, memorize, and process information that is relevant to the decision-making process and applies to both the info sharing and privacy paradoxes. Specifically in the privacy context, John, Acquisti, and Loewenstien (2011) define *bounded rationality* as the inability to calculate and compare the magnitudes of the payoffs associated with various strategies the individuals may choose in privacy situations. He also suggest that it refers to the inability to process all the stochastic, meaning non-determinative, information related to risks and probabilities of events leading to privacy costs and benefits. Theorist arguments suggest even the most privacy-concerned individuals are not informed and cannot inform themselves about privacy risks, even when that information is available because they simple cannot process that amount of information. Therefore, individuals resort to simplified mental models, approximate strategies, and heuristics, such as intuition, an educated guess, or common sense.

2.4 Government Inter- and Intra-Agency Info Sharing

Akbulut-Bailey (2011) postulates that, "the improvement of information sharing among government agencies has become one of the highest priorities of decision makers as the lack of information sharing has been identified as a major point of failure leading to and responding to these horrific events" (p.53). From a historical perspective, Boudreau and Robey (2005) postulated that the need for info sharing was from the public administration reform in the 20th century based on the conviction that, "only through efficient government could progressive social welfare be achieved" (p. 3). Thus, government info sharing acquired its necessity from the goal of public service where the lens of efficiency was the pillar to democracy (mixed metaphor) (Wenjing, 2011).

From an inter- and intra-agency perspective, scholars from different theoretical traditions propose that, in order to realize the most important benefits from the use of information and the info sharing technologies, agencies should integrate their information across organizational boundaries (Caffrey, 1998; Dawes, 1996; Gil-Garcia et al., 2007; Ramon Gil-Garcia et al., 2009; Javernpaa & Staples, 2000; Pardo et al., 2006; Richardson & Asthana, 2006). Navarrete (2009) argues the national boundaries are changing and governments from different countries are collaborating and sharing information in order to face complex public problems, such as environmental degradation, terrorism, public health, national security, and economic crises. Within the literature, as suggested by Akbulut-Bailey (2011), there is very limited academic research on info sharing among government agencies. Chong, Lin, Ooi, and Raman (2009) conducted the first major study on inter-agency info sharing. Their study focused on the benefits and risks of info sharing among state agencies. Conversely, Dawes (1996) conducted research on inter-agency info sharing as it relates to the expected benefits and manageable risks. Each of

them categorized the benefits and risks into three areas as they related to state or inter-agency info sharing.

However, previous research has given minimal consideration to a fourth area of the behavior of users who share information while navigating in the risks and benefits as it relates to sharing information, specifically the reasons users are willing to share information with others, even when the risks may outweigh the benefits. Table 1 includes a fourth area that is considered in this research study and extends the areas considered by both Dawes (1996) and Chong et al. (2009).

Table 1: Categories of Benefits, Risks, and Barriers (Dawes, 1996)

Category	Benefits	Barriers/Risks
Technical	• Streamlines data management • Contributes to information infrastructure	• Incompatible technologies • Inconsistent data structures • Poor technical skills • WikiLeaks/Live Leak of damaging information, inadvertently or intentionally
Organizational	• Supports problem-solving • Expands professional networks	• Organizational self-interest • Domain professional frameworks
Political	• Supports domain-level action • Improves public accountability • Fosters program and service coordination	• External influences over decision-making • Power of agency discretion • Primacy of programs
Individual Behavior	• Tacit Knowledge • Superior Info Advantage • Absorptive Capability • Intelligence Analysis	• Media Exposure • Attitudes • Values, Emotions, and Intuition • Individual Interests • Age, Gender, Race, Ethnicity, and Religion

Is there a limit to the amount of information that a user has when considering to share? Are there certain types of information too damaging to share? Are there specific situations where the information shared is more detrimental to the agency that outweighs the benefit to share? Clearly, from this view, the answer to these questions is fundamentally "yes." However, a paradox exists with the benefits of info sharing. There are an equal number of challenges, barriers, and risks not to share information. Both have an impact on determining the power of the information and the sharer's decision to share the information during a time of war or crisis. This research does not suggest that information sharing should be avoided, nor does it imply that every scenario will lead to negative outcomes. This research offers another perspective: that information behavior that socially and culturally constitutes ways to identify, seek, assess, use, and share information changes and develops with the user's behavior and knowledge of the risks and benefits to sharing info. The main idea is that, if the user is someone knowledgeable about the risks versus the benefits, this may reflect a superior decision. While if someone who is less knowledgeable about the risks versus the benefits, his/her decision to share information may be induced by behavioral biases. Since this issue has been given minimal attention in the info sharing literature, the current research provides needed insight in this area.

With intra-agencies' info sharing, there is a trend to encourage groups to share information and knowledge (Zhang, Zeng, Wang, Li, & Geng, 2011; Zhang, Dawes, & Sarkis, 2005). Conversely, Wheatley (2006) highlights that, in the bureaucratic model, information flows within agencies are strictly controlled; the point being, with limited access to the sharing of information and knowledge, members lack the capability to develop integrated solutions to problems. In addition, members within the agencies often do not share information scattered among intra-agency communities (Ardichvill, Page, & Wentling, 2005; Cress & Kimmerle, 2006). Within

the literature, many factors can influence inter-/intra-agency info sharing. According to Yang and Maxwell (2011), the relationships between these factors are complex and each factor can influence the other.

In inter-agency info sharing, Landsbergen and Wolken (2001) state that interoperability across agencies represents cross-boundary info sharing. Within the literature, researchers have recognized the importance of cross-boundary info sharing, especially in the area of e-government research (Cresswell, Pardo, Canestrato, Dawes, & Juraga, 2005; Pardo et al., 2006; Pardo & Tayi, 2007; Schooley & Horan, 2007). Specifically, Pardo et al. (2006) state that leaders and IT executives in the public sector have increasingly recognized the importance of inter-agency info sharing to improve the efficiency of government agencies. However, info sharing and knowledge management can involve complex interactions between participating government agencies. Dawes' (1996) research in inter-agency info sharing and Zhang' et al. (2005) research in e-government knowledge sharing both define and view influential factors from the three primary perspectives of technology, management, and policy. The focus of this research study, however, is on the inter- and intra-agency info sharing from a user's change in behavior perspective and his/her decision to share based on the value or power of this information.

In summary, (Yang & Maxwell, 2011) postulate that, during the last 15 years, public and government organizations have shifted from a model that emphasized only information protection to one where cross-organization info sharing is the new goal. This is primarily due to events such as 9/11, policy changes that emphasized cross-government coordination to improve efficiency and reduce waste, and changes in technology that allowed organizations to exchange information based on standard transmission and information exchange protocols (Yang & Maxwell, 2011). Scholars from different theoretical traditions propose that, in order to realize

the benefits from the use of information and the info sharing technologies, agencies should integrate their information across organizational and national boundaries (Caffrey, 1998; Cresswell et al., 2005; Dawes, 1996; Gil-Garcia et al., 2007; Navarrete, 2009). In addition, there are a number of factors that influence info sharing across inter- and intra-agency boundaries, and the relationships among these factors influence info sharing. Finally, it is important to realize governments from different countries are collaborating and sharing information in order to face complex public problems in their environment.

Therefore, there are complex and paradoxical effects to the Intelligence and business leaders' decision-making with this shift to sharing of more information. Conversely, recent events, such as Edward J. Snowden, an American computer specialist who worked for the CIA and NSA and supposedly leaked details of several top-secret U.S. and British government mass surveillance programs to the press, suggest there should be greater emphasis on information protection. Today, the insider threat underscores the complex nature of sharing of information and the decision-maker's dilemma in determining the organizations' risks versus the greater good to info sharing. Within the literature an emphasis is placed on the need for more inter-/intra-agency info sharing and to interoperability between diverse information systems. (Gil-Garcia et al., 2009; JinKyu, Nitesh, Jing, Marijn, & Rao, 2010) suggested that, after the U.S. terrorist attacks and world natural disasters, our fragmented nature of policy-making and service provisioning revealed the need for more inter- and intra-agency information sharing.

2.5 Inter- and Intra-Agency Info Sharing Benefits, Risk and Barriers

Although the benefits realized from info sharing differ from organization to organization or agency to agency, Dawes (1996) classified them into three categories: technical, organizational, and political. He posits that technical benefits refer to potential positive results.

They relate to the processing and managing of information, such as reduced duplication of data collection, processing, and storage, as well as the creation of formal standards or shared technical infrastructure. The organizational benefit refers to positive results for the organization as a whole that includes better coordination, improved decision-making processes, and reduced costs; and the political benefit refers to the impact on the political image and policy goals of the organization leading the info sharing and integration effort.

Important benefits from government integration and info sharing will continue to be incentives for governments to design and implement initiatives to reduced duplication of data, more coordinated efforts, and efficiency. Although Dawes (1996) classified them into three categories, in terms of benefits as outcomes only, some other elements suggested by other researchers are active public participation, transparency, efficiency, cost savings, policy effectiveness, and service quality (Bertot, Jaeger, & Grimes, 2010; Fedorowicz, 2009; Garson, 2004; Luna-Reyes, 2010; Reddick, 2009). However, the literature suggests that organizational benefits are the more powerful incentives for government agencies in info sharing, particularly in terms of efficiency and cost savings. In contrast, public organizations place more emphasis on policy effectiveness, equity, openness, and accountability, from which enhancement can occur through information integration (Gil-Garcia, 2012). Political benefits from government info sharing are enhanced public image, value creation, increased government transparency and accountability; integrated planning and more comprehensive public information. Efficiency, being the goal of public administration, could be easily accepted as the justification of the necessity of government info sharing (Wenjing, 2011).

Sharing relevant, timely, and complete information for intelligence operations transforms the capability of intelligence systems to facilitate government info sharing and integration in a

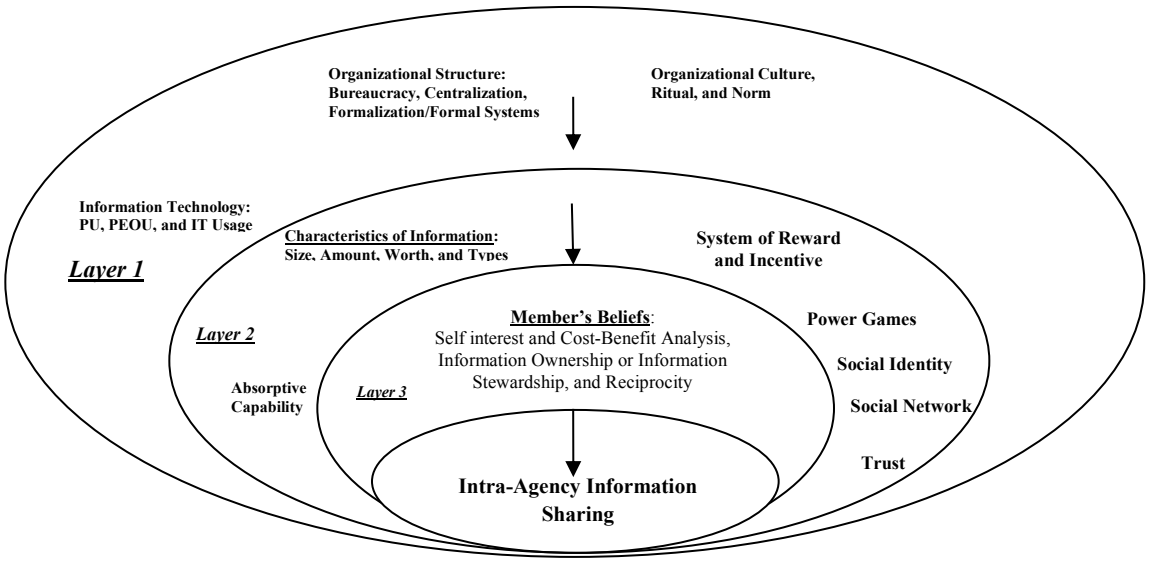
networked environment. From a military intelligence or even a business operations perspective, the more this information is complete, the more it offers the government, corporate entities, and their partners a real opportunity to share databases and make decisions based on the sharing of information. In addition, it offers important benefits, such as increased productivity, improved decision-making, and lower administrative burden, assuming that information already held somewhere in the inter- or intra-agency is not duplicated. Further, it offers better enforcement or greater information availability, higher information quality resulting in fewer mistakes, and integrated services (Gil-Garcia et al., 2009; Jhingram, Mattos, & Pirahesh, 2002; Landsbergen & Wolken, 2001; Otjacques, Hitzelberger, & Feltz, 2007).

In summary, Gil-Garcia (2012) argues that the important benefits of government info sharing in the current government environments leads to the need for solutions consistent with what he refers to as the "whole-of-government approach." In fact, Gil-Garcia (2012) suggests a need for more coordination and collaboration among government agencies, but also between government agencies and other social actors to realize the benefits from info sharing. Again, this specifically highlights the importance of the use of info sharing across organizational boundaries and the sharing of critical information in order to solve complex problems. To this end, the primary gain of the efficiency benefit as well as others mentioned throughout the literature, the trend is towards increased inter-organizational collaboration and information integration among government agencies, between government agencies (intra-agencies), other branches of government, national partners, and corporate organizations. Gil-Garcia (2012) postulates that, over the next 10 years, we could witness the emergence of a highly integrated virtual State in which all branches of government and multiple social actors seamlessly interact through the use

of sophisticated technologies that integrate business processes, physical infrastructure, organizational resources, and new institutional arrangements.

There are many influences on inter- and intra-agency info sharing. Yang and Maxwell (2011), suggest this type of sharing can viewed from a layered approach. In Figure 1, Factors Influencing Organization Info sharing, the influences to info sharing for the focus of this research are on the member's beliefs, and characteristics of information. IT focuses primarily on the technological issues, which dominate much of the early literature, and suggests that IT could play a central role in the management of an organization's info sharing. Hislop (2002) posits there are criticisms to the literature, which overemphasizes the technological issues and neglects social and cultural factors that can lead to a number of problems.

Figure 1: Factors Influencing Organization Info Sharing (Yang and Maxwell, 2011)



The key in the analysis of Yang and Maxwell's (2011) research study is that, while info sharing is influenced by the factors in layers one and two, members' beliefs at layer three that are focused towards intra-agency information sharing can be developed and mediated by self-interest

and cost-benefit analysis. Although Figure 1 depicts the influences in intra-agency info sharing, what is missing is the impact in the understanding of the attitude, intuition, and tacit knowledge of the actor and the organization's interest as it relates to the value of the information. The influences are missing a critical element. The IA behavior influences the decision to share information that may very well be in conflict with the organization's security and info sharing policies. The IA is, in fact, the entity that decides on the amount of risk that the organization inherits. Thus, the main idea of this research is, if the user, whose decision is to share, is someone knowledgeable about the risks versus the benefits, this may reflect a superior decision, while the decision of someone who is less knowledgeable about the risks versus the benefits, may be induced by behavioral biases. It has been argued that disclosure decisions are made by balancing "the usefulness of privacy with the utility of openness" (Petronio, 2000, p. 37) and that people engage in "disclosure management," such that they disclose information only when they expect a "net benefit" (White, 2004, p. 48).

In layer one, focus is on information technology, organizational structure, and organizational cultures. Yang and Maxwell (2011) argue that bureaucracy is an influential influence on info sharing. However, as a bureaucratic organization grows larger both vertically and horizontally, distributed duties in different hierarchies and sub-units become the drivers of decreased efficiency for info sharing. According to Creed, Douglas and Miles (1996) and Tsai, 2002, the formal hierarchical structure of bureaucracy can create barriers that impede info sharing activities within the organization. Horizontal structures of bureaucracy, such as departmentalization, inevitably bring obstacles to info sharing between different departments of an organization because of different functional mandates, processes, and expectations (Argote, Ingram, Levine, & Moreland, 2000; Willem & Buelens, 2007). In addition, bureaucracy is an

organizational structure where power and authority are centralized in higher management levels (Hall & Tolbert, 2004; Kim & Lee, 2006). Tsai (2002) argues that centralization has a significant negative impact on knowledge sharing in a multiunit organization. Kim and Lee (2006) point out that centralization can hinder initiatives of inter-group information exchange and collaboration. Interest in sharing information and knowledge can be reduced because an organizational member or group has limited action autonomy and needs approval from supervising levels regarding most decisions (Kim & Lee, 2006).

In layer two, primary focus is on the characteristics of information, absorptive capability, incentives, power, social aspects and trust. Yang and Maxwell (2011) argue that researchers assert the importance of incentive systems in motivating organizational members to share information with others in different groups or departments (Willem & Buelens, 2007). Through direct and indirect effects of incentives, sharing of information and knowledge can be greatly increased (Connolly, Thorn, & Heminger, 1992; Jian & Jeffres, 2006; Willem & Buelens, 2007). With performance-based reward systems, organizational members are more likely to share information and knowledge (Kim & Lee, 2006). Bonus systems are also able to increase the quality of shared information (Ardichvill et al., 2003). On the other hand, researchers discovered that when the system is not specifically designed for encouraging info sharing, a general reward or incentive system can actually deter the info-sharing activities of an organization (Zhang et al., 2005). Bock, Zmud, Kim and Lee (2005a) claim that anticipated extrinsic rewards can have negative influence on organizational members' attitudes toward sharing of information and knowledge. Barua, Ravindran and Whinston (2007) assert that general incentive systems can only increase info-sharing activities when a special type of information dependency exists between workgroups. Because of reward and incentive systems, workgroups and/or

organizational members may compete with each other for better performance; one potential consequence of this is that they might become reluctant to share information and knowledge (Barua, Ravindran & Whinston, 2007; Bock et al., 2005a; Zhang, Dawes & Sarkis, 2005).

Finally, in layer three, lie members' beliefs. According to Constant et al. (1994), member perceptions of self- interest can reduce support for info sharing in an organization. Cress and Kimmerle (2006) claim that info sharing presents a social dilemma. Social dilemmas are situations where personal interests are inconsistent with collective interests. According to Yang and Maxwell (2011), in social dilemmas, individuals are assumed to put more weight on their short-term personal interests than on long-term organizational interests (Dawes, 1980). Researchers point out many factors that organizational members may consider as costs to their sharing of information (Cress & Kimmerle, 2006; Goodman & Darr, 1998). For instance, before sharing tacit information and knowledge, a contributor may need to spend significant time and effort to articulate, prepare and arrange the information. In addition, a contributor may expect that sharing of information would evoke requests for further clarifications and assistances. The extra work may compete with the contributor's work time and resources. Furthermore, the fear of incurring criticism because of possible inaccurate and irrelevant information also affects the cost/benefit equation (Ardichvill et al., 2003). Without receiving clear recognition and benefit for a contribution, contributors may be reluctant to share information (Cress & Kimmerle, 2006; Goodman & Darr, 1998). By applying theories of collective action (Hardin, 1971, 1982) and social dilemma (Dawes, 1980; Jian & Jeffres 2006) extend the discussion by claiming that individuals are rational and self-interested, acting to maximize individual benefits and minimize individual costs. In their proposed utilitarian perspective, a contribution to the collective good

such as sharing of information and knowledge is a matter of calculation and compromise between cost and benefit (Jian & Jeffres, 2006; Marks et al., 2008)

THEORY OF PLANNED BEHAVIOR

3.1 Key Constructs of Theory of Planned Behavior

"Since its introduction 26 years ago, the Theory of Planned Behavior (TPB), has, by any objective measure, become one of the most frequently cited and influential models for the prediction of human social behavior" (Ajzen, 2011, p. 1113). In the TPB, the most detailed substantive information about the determinants of a behavior is contained in a person's behavioral, normative and control beliefs. The theory does not specify where these beliefs originated; it merely points to a host of possible background factors that may influence the beliefs people hold. These are factors of a personal nature, such as personality and broad life values; demographic variables, such as education, age, gender and income; and exposure to media and other sources of information. Factors of this kind influence intentions and behavior indirectly by their effects on the theory's more proximal determinants. Most empirical studies assess a few demographic characteristics if only considered as control variables. Some studies, however, focus on one or more background factors that, for intuitive or theoretical reasons, are relevant to the behavior under investigation. This research study will focus on IA attitudes and intuition beliefs. The adaptation of the TPB in the exploration of behavioral, normative, and control beliefs allows investigators the opportunity to identify important determinants of socially significant behaviors, thereby gaining a better understanding, according to Ajzen (2012), of how we might go about modifying behavior in a desirable direction.

3.2 Applications of Theory of Planned Behavior

A good application of TPB is reported by the study of Manning and Bettencourt (2011). The investigators used the TPB as their conceptual framework to examine adherence to a

medical regimen. Unlike Kor and Mullan (2011), who dealt with their behavioral category of sleep-related activities by assessing the TPB constructs in relation to each behavior, Manning and Bettencourt (2011) aggregated several regimen adherence behaviors and then assessed the TPB constructs with reference to the category as a whole. Within their case, the intentions to adhere were predicted very well, but the theory accounted for only a small proportion of variance in behavior. However, in addition to measuring the TPB constructs, the investigators also assessed depressive symptoms as a possibly relevant background factor. The results indicated the degree of depression correlated negatively with intentions and reported adherence to the medical regimen.

Other investigators in research studies (Courneya, Bobick, & Schinke, 1999; Courneya & McAuley, 1993; Rhodes & Courneya, 2003; Rivis, Sheeran, & Armitage, 2011) examined the role of specific personality traits in TPB (openness, conscientiousness, extroversion, agreeableness and neuroticism) in the context of the TPB. These research studies assessed the general tendency to compare oneself to important others. The results provide a different perspective from simply postulating a simple effect of the background factors on intentions and behavior, and their approach and method allowed them to examine the possibility that these variables influence the predictive validity of intentions relative to perceived prototype similarity. These investigations, like other studies (Sheeran, Orbell, & Norman, 1999; Trafimow & Finlay, 1996), show that there may be stable individual differences that influence the relative weights of the different predictors in the TPB.

Even though TPB has emerged as one of the most influential and popular conceptual frameworks for the study of human action (Ajzen, 2001; Ajzen, 2011, 2012), there are problems that remain (Armitage & Conner, 1999, 1999a; Sheeran et al., 1999; Sutton, 1998). One such

problem is the nature and measurement of perceived behavioral control. Since TPB is derived from TRA, it is assumed that most human social behavior is under volitional control and, therefore, can be predicted from intentions alone. The construct of perceived behavioral control was added in an attempt to deal with situations in which people may lack compete volitional control over the behavior of interest. The arguments suggest that behaviors can be subject to unforeseen obstacles, and volitional control over behavior is, therefore, best considered as a matter of degree rather than an actual type of behavior. Other arguments are on the specific facets that form perceived behavioral control that may include self-efficacy, perception of control and others. In addition, researchers argue whether future behavior should be observed or self-reported. The results within the literature suggest a gap exists between intention and behavior, and many researchers concluded that some elements are apparently missing in the model and have tried to enrich it by the inclusion of further constructs, such as moral norms and past behavior. In response to these criticisms, Ouellette and Wood (1998) argue and confirm that a relationship between past behavior and intention exist under special circumstances. "In domains that facilitated development and execution of habits, past behavior was a strong predictor and intention relatively weak, In domains that did not facilitate habits, past behavior was a relatively weak direct predictor and intention was quite strong" (Ouellette & Wood, 1998, p. 66). As such, though TPB may have shortcomings like all social theories, these shortcomings must be recognized, and the criticisms do not prevent it from being an effective tool in examining socio-technical process in organizations.

3.3 Theory of Planned Behavior and Decision-Making

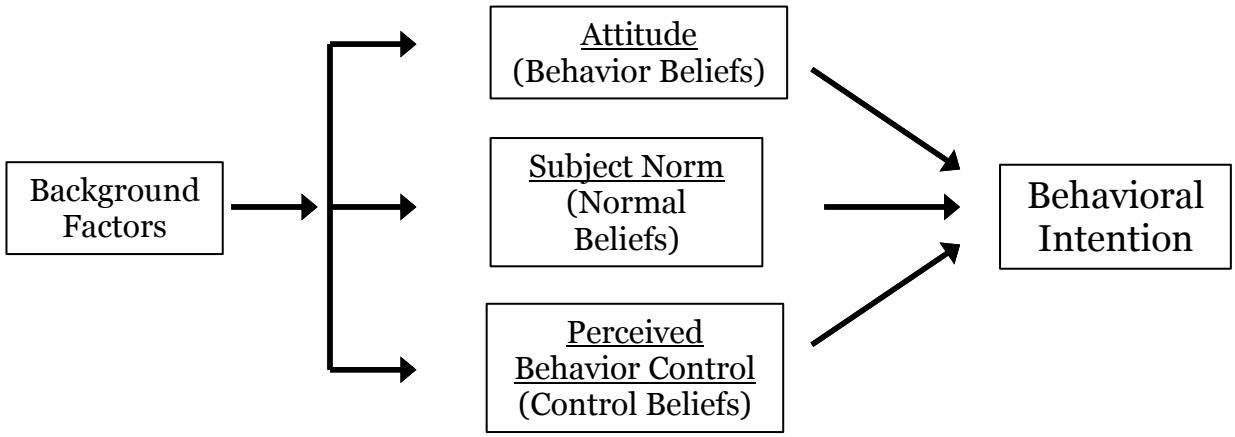
The Theory of Planned Behavior (TPB) uses background factors to analyze individuals' attitude, intuition, past behavior, and beliefs that affect their decision-making. Hodgkinson,

Sadler-Smith, Burke, Claxton, and Sparrow (2009a, p. 277) noted that, until recently, only the "bravest and most far-sighted" would recognize the utility of intuition in management decision-making. However, it is argued that increased time pressure, rising work pressure and ambiguity, high decisions costs, inadequate information, and fast-paced change have undermined the utility and effectiveness of relational decision-making models (Sinclair & Ashkanasy, 2005). It is also argued that the changing nature of work practices and structures creates environments where human information-processing capability is exceeded by the volume and complexity of the information that humans have to process (Hodgkinson et al., 2009a), thereby, according to Allen (2011), making intuition a more widespread strategy for decision-making. Allen (2011) further defines intuition as having the following information processing characteristics: reliance on long-term memory input processed automatically and sub-consciously or pre-consciously, input is holistic, and output from the process is feelings that can serve as a basis for judgments in decisions. Therefore, Allen (2011) postulates that intuition can be seen as a distinct and very different mechanism for information processing and decision-making.

Using the TPB framework, Ajzen (2011) describes that human behavior is guided by different subjective probabilities. As depicted in Figure 2, the framework is based on the assumptions of: 1) beliefs about the consequences of the behavior; 2) beliefs about the normative expectations of other people; and 3) beliefs about the presence of factors that may facilitate or impede performance of the behavior. In Figure 2, the background factors, or actor's personal beliefs, may include a wide range of factors. This research study will focus on the background factors of IAs' attitudes, intuition, and their experiences. Ajzen and Fishbein (1973) argue in the TPB framework that the aggregation of background factors the behavioral beliefs produce

attitude towards behavior, normative beliefs result in subjective norms and control beliefs generate perceived behavior control.

Figure 2: Theory of Planned Behavior, (Ajzen and Fishbein, 1973)



The combination of all the elements leads to the formation of a behavioral intention (Ajzen, 2011; Fishbein & Ajzen, 2005; Ajzen & Martin, 1970). An important postulation comes from the research done by Ouellette and Wood (1998), which confirmed a relationship between past behavior and intention under special circumstances (Ajzen, 2011). The combination of all the elements leads to the formation of a behavioral intention (Ajzen, 2011; Fishbein & Ajzen, 2005; Ajzen & Martin, 1970). "In domains that facilitated development and execution of habits, past behavior was a strong predictor and intention relatively weak. In domains that did not facilitate habits, past behavior was a relatively weak direct predictor and intention was quite strong" (Ouellette and Wood, 1998, p. 66). IA actions are typically triggered by environmental events and, because their activities are repetitive, their performance often requires minimal attention, because of experience over time, but certainly requires deliberate control. According to

Ouellette and Wood (1998), this is habitual behavior and past behavior may be a strong predicator, where intention may be relatively weak.

With its roots in social psychological approach to behavior, TPB postulates changing behavior is a matter of changing the cognitive structure underlying the behavior in question. The theories are best seen as a series of four hypotheses. The first hypothesis is made under the assumption that behavior is primarily a function of an individual's intention to perform that behavior. The second hypothesis is the intention to perform the behavior and is seen as a function of the weighted combination of two factors, a personal factor that is the attitude toward the behavior and a social factor that is referred to as subjective norm. Thus, in this hypothesis, the attitude toward the behavior is the feeling of favorableness toward the behavior and the subjective norm, which suggests the perception that people of importance think that the individual should or should not perform the behavior. The third hypothesis suggests the underlying attitude toward the behavior is an underlying cognitive structure of behavioral beliefs that performing the behavior will lead to certain outcomes and the evaluation of these outcomes. Finally, the last hypothesis suggests the subjective norm is an underlying cognitive structure of normative beliefs that particular individuals or groups think that one should or should not perform the behavior and the individual's motivation to comply with each of these significant others.

RESEARCH DESIGN

4.1 Subjects

As mentioned before, this study will endeavor to answer the question: How does the IA navigate the paradox between the between the benefits and risks affected by individual behaviors and organizational factors that inhibit information sharing decisions? A conjecture of this research study is that the info sharing of highly skilled or *smart sharers* would reflect superior decisions on the information to share, while the decisions of relatively less skilled or *risky sharers* are more likely to be induced by behavioral biases. However, the central gap where previous literature has given minimal consideration is the behavioral changes in users who share information in understanding the analysis of the risks and benefits as it relates to sharing information, as well as the reasons users are willing to share information with others, even when the risk may outweigh the benefits. As such, it is a study of the social, cultural, and behavioral aspects of the IA and inter-/intra-agency organizational security and info sharing policies. It seeks to understand why IA make the decision to share information and how they do it. It endeavors to understand the context within which they make decisions when analyzing the cost and benefit trade-off as it relates to putting the organization at risk inadvertently or intentionally.

The IA navigates the paradox between the benefits and risks affected by their behaviors and organizational factors that inhibit their info sharing decisions by performing and managing intelligence activities and functions including developing, evaluating, and providing intelligence information. To accomplish this, they instruct air crews on collecting and reporting requirements and procedures; matters such as evasion, recovery, and code of conduct; recognition techniques; and assessing offensive and defensive weapon system capabilities. They also prepare mission

reports, conduct intelligence debriefings of U.S. and allied military personnel involved in combat operations requiring careful analysis of the benefits and risks associated with successful execution of missions. Since this unique group within the IC often prepares, maintains, and presents intelligence displays, reports, and briefings and is responsible for producing all-source intelligence, situation estimates, order-of-battle studies, and other intelligence reports and studies, it represents important actors that navigate the paradox between the benefits and risks that are affected by their behaviors and the organization's factors that inhibit their info sharing decisions. In navigating the paradox, this actor group also performs geo-locational mensuration functions, maintains, and uses geospatial databases, targets materials, imagery, and other intelligence products shared within the IC. These actors extract coordinates and positional relationships from digital database systems and non-automated stereo-photographic models, and identify and establish unit requirements for intelligence reference materials typically stored in databases and for sharing. They also maintain intelligence reference files, automated intelligence databases, automated and non-automated systems applications, target materials data logs and prepare target materials for execution that includes performing targeting, weaponry, and damage assessment functions.

The IA group is important to this research study as opposed to typical IT users because of their specialty skill, mandatory knowledge, and system access. They are knowledgeable in intelligence organizations and systems; collection and reporting systems, procedures, and methods; intelligence information sources; techniques of identifying, collating, evaluating, and analyzing information as well as geographical and cultural aspects of foreign countries. They are required to be skilled at military capabilities of potential enemy offensive and defensive weapon systems; special operations; procedures for acquiring, updating, and maintaining intelligence

documents, maps, and charts; map and chart use techniques; graphic, oral, and written intelligence information presentations; target planning and materials; target folder construction techniques; and capabilities and application of automated data handling and management systems. They must also understand security classification marking and control; U.S. sensor systems, regional physical characteristics relative to radar significance; methods of verifying target intelligence information derived from imagery; basic electromagnetic theory; computerized systems supporting target intelligence and mission planning systems; digital terrain and feature databases; and principles of precise positioning systems and targeting and weaponeering.

IA use IT to help navigate the paradox between the benefits and risks of info sharing. The information held by IA alone is not as useful if it is not shared in the IC and the technology associated with information is generally oriented to the efficient transfer of that information to another individual or entity. IA capitalize on the speed of processing information, manipulation of large data sets, and dynamic adaptability to other IA needs. With the speed of processing, IA benefit from the correlation of data, its manipulation, with less redundancy resulting in gaining efficiency, and greater access across the community. IT also allows for the efficient storage and retrieval of information as well as enables the possibility of efficient info sharing by allowing electronic data to flow around the IC and around the world at the speed of light. An important aspect to navigating the paradox between the benefits and risks of info sharing is to increase the effectiveness and efficiency in sharing information. IA must consider access, which is part of the analysis in navigating the risks and benefits for effectiveness and efficiency. The access to shared information across a large and unique community allows efficiency as well as greater capability for accomplishing missions effectively. It also allows building of partnerships with

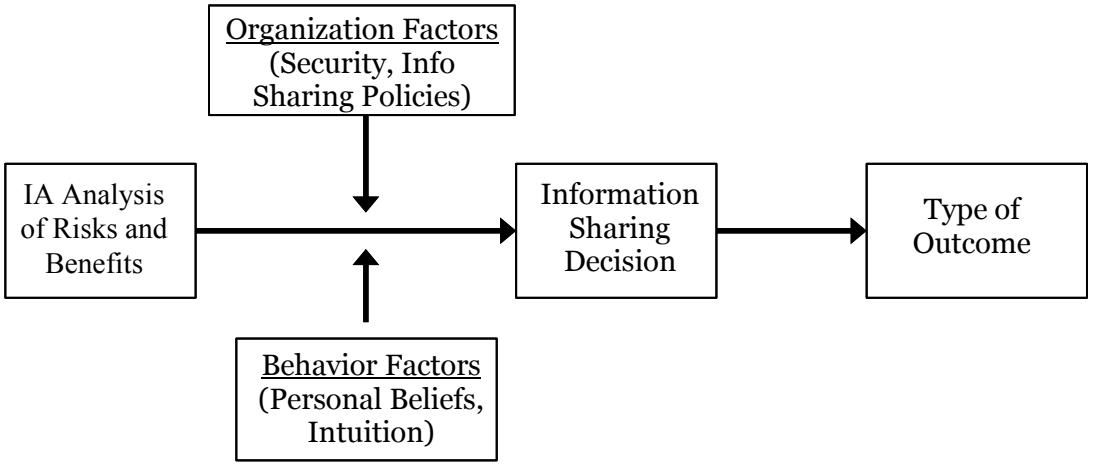
others to share information. IA must also navigate the paradox through military service organizations, national partners, and other government partners since these environments are unpredictable during operational missions. IA often cannot anticipate the nature of the demands of info sharing they will face. Analysis of the benefits and risks in the info sharing paradox in an ad hoc environment adds weighted pressure to IA decisions. These ad hoc environments are characterized by collaborative working, unlimited communication across all levels, and broad sharing of situation information. In situations of time pressure, IA do not fall back on well-establish routines, each doing what it is they are best doing. To the contrary, there is a behavioral change when sharing information in understanding the analysis of the benefits and risks as it relates to sharing information; specifically, reasons IA may be willing to share information with others, even when the risks may outweigh the benefits.

4.2 Information Theory Adaptation

The qualitative approach uses the adaptation of the TPB to inform this research to provide a deeper insight into the decision-making process by IA, highlighting the moderating impact of past behavior on the self-efficacy-intention linkage. In Figure 3, the conceptual framework, the IA benefits and risks analysis is moderated by organizational factors (security and info sharing policies) and behavioral intentions (attitude, values, and intuition), which influence info sharing decisions that result in desirable or undesirable outcomes. What would cause an IA to violate the rules and share information? How much does the behavioral intention influence his/her decision? Kidwell and Jewell's (2008) research study confirms that, on the one hand, past behavior does influence consumer decisions, and on the other “can influence the extent of deliberative processing when making decisions.” In other words, past behavior

obviously moderates the influence "… of attitude and internal and external control on intention" (Kidwell & Jewell, 2008, p. 1162). In TPB, the assumption is that a decision is the result of a deliberative, goal-oriented process; behavioral options considered, consequences of the option evaluated and the decision to do something made. Will an IA demonstrate risky behaviors? Gibbsons, Gerrad, and Lane (2003) developed the Prototype-Willingness Model (PWM) based on three assumptions about risky behaviors among adolescents and young adults. Gibbsons et al. (2003) posited risky behavior is neither reasoned nor intentional, which led to additional constructs of TPB with the predictors of behavioral expectations and behavioral willingness.

Figure 3: Conceptual Framework



IA access to information processing is approved based on security clearance level, need to know, and system access to the appropriate classification levels of the information. Generally, an IA has access to data at three classification levels: Unclassified, Secret, and Top Secret. Although there are other compartmented classifications within each of the general levels of access, the focus of this research study is on the access to information at these three general levels. It is important to understand how an IA attempts to process information since it is part of

his/her internal process to decision-making. According to Neisser (1967), most people operate in a perception-action cycle, suggesting that the senses take in information from the environment, the mid brain performs computations on that information and the outputs of those computations are used to guide subsequent goad-directed actions. However, Newell and Broder (2008) argue that, since most people's information capacity is limited, they must use cognitive models to propose heuristics or shortcuts.

The organization's security and info sharing policies have increased in complexity when sharing across an intra-/inter-agency. First, it changes rapidly with the increasing need for intra-/inter-agency sharing of information. There are partnerships that form and disband based on an organization's interest and mission execution. At any moment, a partnership must be formed under the conditions that info sharing is necessary based on a new agreement between the U.S. and a national partner because of the relationship in a particular environment that is later disbanded under the conditions that the partner now puts the organization at risk. The organization's need for sharing information often changes and is often unclear at different levels within the organization or across inter-/intra-agencies. At various levels, organizations have strict policies to sharing information, but they are created generically at very high levels and execution is done at much lower levels and could very well be left to different interpretations by individuals that could put the organization at risk. These types of conditions intensify when considering how IA seek information to share. Savolainen (2006) schematic model for information seeking highlights what IA face, in addition to understanding the organization's security and info sharing policies. Savolainen (2006) posits they are processing the following continuously: 1) concerns with the problem or task at hand to collect intelligence information for analyzing; 2) concerns with fulfilling the need of the IC for what has been just analyzed and

shared; 3) considering and identifying potentially relevant information sources and channels; 4) selecting and accessing information sources from intra- and inter-agency partners; 5) judging the relevance of the information to be shared; 6) interpreting the information to be shared to be appropriately classified; and 7) determining if new or modified information is necessary, based on classification and the intended source of the shared information. These are all important factors that affect IA decision-making, particularly given the limited amount of time that he/she has in certain environments.

The organization's security and info sharing policies are used to steer info sharing events and serve as the foundation for how to access information for operations, as well as how, when, and why an IA would share information with others. The organization's policies and goals are in the best interests of the organization to limit the risk of loss of information inadvertently or intentionally, and, most important, to protect the information shared with sources that will not be harmful to national defense. Also within the organization's security and info sharing setting, there is information processing during collection and distribution where the consumption triggers the desire for power by decision-makers. In the info sharing setting, having control over access to pieces of information and how and what is shared is power in the IC, particular in battle or conflict with the adversary. In the behavioral sciences, power is defined as the ability to influence others in a way that is desirable to the one exerting the influence (Ahituv & Carmi, 2007). This is important because, in the info sharing setting, exerting influence on another is not necessarily based on an individual's rank or authority, but more on the pieces of information known by the IA and the ability to influence him/her to the desired outcome. Often the desired outcome that strongly influences an IA to share information is successful execution of an operational mission. The relationship between power and info sharing may cause the IA to

engage in an inward-focused processing style characterized by attention to the self's internal attitudes and desires, with little consideration for the views and needs of others. This is important because the internal attitudes and desires influence the decision to share or not to share. Brinol, Petty, Valle, Rucker, and Becerra (2007) postulated that by priming power, which is providing control over the evaluation of a subordinate in a role-playing task, prior to processing a message about a topic, enhances the tendency to try to validate one's initial views on the topic that results in reduced information processing. Research on the organizational cultural values' view of power is that it is interpersonal and something that is used for advancing one's personal agenda obtaining praise and admiration from others, and, hence, maintaining and promoting one's powerful status in the eyes of others. However, it also can be organizational driven, specifically when the primary focus is to accomplish the organization's goals or objectives, such as successful execution of an operational mission.

The assumption is the value of the information with regards to national defense is already pre-determined, given the classification level of the information; however, in the info sharing paradox, an IA contribution is often able to influence the usefulness of a piece of information for others. For example, an IA may prepare the information very carefully to make it valuable for the specific purpose for a unique group, or he/she may just contribute to the analysis of a photograph needed for a specific mission. In many cases, higher value of pieces of information for the organization means higher risks to the organization, but does not correspond with higher risk for the IA. Costa-Gomes, Crawford, and Broseta (2001) demonstrated that individuals in social dilemmas consider their own benefits, but also the benefit to others in making decisions. In the study by Cress, Kimmerle, and Hesse (2006), participants were provided with two types of information: information with high value to others and information with low value to others.

The study demonstrated that people do, in fact, consider the benefit to others, and contribute more information of high value than information of low value.

Since IA perform and manage Intelligence activities and functions, including developing, evaluating, and providing Intelligence information in info sharing situations, they often influence the usefulness of this data for others. With the information being more valuable to others, which is continuously gaining value by contributions by all within the IC, the organization's investment is even higher with national Intelligence libraries where IA can seek and retrieve data individually. Individually, the information contributed is often labeled and can be traced to the IA responsible for the contribution, and tagged appropriately for the proper classification, such as unclassified, secret, or top secret. The labeling and tagging ensures the proper classification, but does not take into account the contribution to the entire community and is not higher in value from the perspective of the contributing IA, who is only focused on his/her single source of information and its classification. For example, an IA may develop and evaluate a map for a particular target and place it in a national Intelligence library classified at the lowest classification level for a high rate of sharing. A different person could retrieve the work completed by the previous individual and add important pieces of information keeping it at the lowest classification level as possible. However, the additional information added to the map involves multiple targets; therefore, the information returned to the library results in a higher value or higher classification. The info sharing process then generated information of much greater value to the IC, but not necessarily to the developer of the product focused on his/her piece of the information.

Some researchers (McClintock, 1978; Messick & McClintock, 1968) posited that human behavior is influenced by values that people assign to different action alternatives and their

consequences. What is the behavior that influences an IA to share classified material with others not authorized? Could this behavior have been influenced by values unconsciously inherited from being a member of the IC, practicing the mandated security and info sharing policies? Or could it have been influenced by another IA as social peer pressure that impacts the IA's decisions and actions resulting in success or failures? In TPB, the most detailed substantive information about the determinants of a behavior is contained in a person's behavioral, normative, and control beliefs. What are the most influential behavioral factors in the decision-making of IA when sharing information with others? Are there differences in the decision-making when an IA believes the recipient has authorization versus no authorization? (Allport, 1935, 1968) pointed out that the concept of attitude "is probably the most distinctive and indispensable concept in contemporary American social psychology" (1968, p. 59). With this understanding, often, consequences of action alternatives will not only affect the actors themselves but also others, most important, the IC. Using TPB, these values include an actor's background factors (social, personal, information) and beliefs (behavior, normal, control).

The background and beliefs of an individual represent a behavior intention, as well as a stable preference for distribution outcomes (inadvertent, desired, or intentional) between one's own self and the organization. The background factors and individual beliefs are extremely important influencing factors in the conflict between the behavior of IA and the organization's security and info sharing policies in the paradox of information sharing. Do IA consider their own benefits and risks in sharing information but also the benefit and risks to the organization? Will they contribute more information of high value than information of low value? The logical answer is that IA may very well, in their decision to share information, consider the benefit and risks to others. This could result in contributing more information of value or higher

classification that benefits an IA during a successful mission, but violates the organization's security and info sharing polices to do so. On the other hand, it may be consistent with the organization's security and info sharing policies, resulting in sharing information of low value or lower classification, but also in an unsuccessful mission.

As mentioned, this research focuses on the social, cultural, and behavioral aspects of IA and inter-/intra-agency organizational security and info sharing policies**.** Is the loss of information publicly and the decisions made to share this information inadvertent or intentional? Do IA consider the benefit to other Intelligence sources, and contribute more information of high value than information of low value that puts the organization at risk? The researcher selected an exploratory approach and the theoretic operational mission-based scenario events because they are similar in mission and impact to the gravity in actual loss of valuable information, yet different in terms of info sharing, decision-making, level of authority and responsibility, organizational structure, and consequences endured from the sharing of information. Given the similarities, this study will use literal replication logic to look for similarities within each scenario and likewise, given the differences, use theoretical replication logic to identify contrasts, if possible, between organizations within the IC (Yin 2009, p. 54). Though combining literal and theoretical replication does not ensure generalizability of the study, it may add to the robustness and confidence in the findings (Yin, 2009). The empirical part of the research will be informed by the interviews conducted and analyzed from responses to these particular mission scenarios. Interviews, that is, empirical data collection, may also be informed by recent events because we do not have a lot of knowledge in these areas. Therefore, in lieu, we will explore using the theoretic mission scenario-based empirical data to uncover the unknown, to answer

questions, to identify the relationship that the past has to the present, and to assist in understanding the culture in which we live.

As engaged scholarship, this research adopts a critical realist philosophy of science. As described by Van de Ven (2007a, pp. 37-38), this view adopts an objective ontology that there is a real world out there but that our individual understanding is limited. This view also espouses, however, a subjective epistemology where all facts, observations and data are capable of being adapted to acceptable theory; no form of inquiry can be value-free and impartial; understanding complex reality demands the use of multiple perspectives; evidence may converge but might also be inconsistent or contradictory; and, models are selected that better fit the problem they are intended to solve.

With this assumption of a subjective epistemology, the researcher conducted the study using the seven fundamental principles recommended by Klein and Myers (1999). Drawn from anthropology, phenomenology, and hermeneutics, these principles include the principles of hermeneutic circle (understanding is achieved by iterating between the interdependent meaning of parts and the whole they form); contextualization (critical reflection upon the social and historical background of the research setting); interaction between the researchers and the subjects (critical reflection on how the *data* were socially constructed through interaction between the researchers and participants); abstraction and generalization (relating the idiographic details to the application of theory); dialogical reasoning (sensitive to possible contradictions between theoretical preconceptions and actual findings); multiple interpretations (sensitivity to possible differences in interpretations by participants); and, suspicion (sensitivity to biases and distortions in narratives collected from participants). As Klein and Myers (1999) point out, these

principles are interdependent and the researcher did not apply these principles mechanically but rather used the researcher's own judgment.

Finally, in TPB, Ajzen (2012) argues the reasoned action approach explains human social behavior in terms of considerations that are readily accessible when people think about performing a behavior in question. He postulates that we gain an understanding of the factors that motivate people's behavior by examining their beliefs about the behavior's likely consequences and how these beliefs produce an attitude toward the behavior. He further explains that, by considering their beliefs about the expectations and behaviors of important others and how these beliefs lead to the formation of a subjective norm, and by studying their beliefs about control factors, we can learn how these beliefs produce a sense of behavioral control or self-efficacy. Ajzen (2012) suggests there is no real argument to suggest that people make decisions in a rational fashion, but one may assumed that intentions and behavior follow reasonably from these kinds of considerations, often spontaneously without a lot of cognitive effort. A large body of empirical research attests to the predictive validity of the TPB. Various techniques have been developed to increase behavioral control, although these techniques have not been used in a TPB context. Some methods focus on imbuing individuals with a sense of self-efficacy or perception of behavioral control. These methods can thus influence behavioral intentions; that is, the motivation to engage in the behavior, but they may also provide valuable information about actual behavioral performance.

4.3 Research Methodology

4.3.1 Data Collection. This study follows the three principles of data collection recommended by Yin (2009 p. 114-124): (a) using multiple sources of evidence; (b) creating a case study database; and (c) maintaining a chain of evidence. To deepen the understanding and help achieve satisfactory validity through data triangulation, the researcher collected data from several sources with different data collection methods. The primary source of data includes interviews and documents on the IC's security and info sharing policies. The concentrating of the research questions in the semi-structured interview guide seeks to understand why IA make the decisions to share information and how they do it. The Theory of Planned behavior (TPB) uses background factors to analyze individuals' attitudes, intuition, past behavior, and beliefs that affect their decision-making. TPB suggests that the changing nature of work practices and structures creates environments where human information-processing capability is exceeded by the value and complexity of the information that humans have to process, which suggests intuition is a strategy for decision-making. The interview questions address whether an individual uses intuition as an influencing factor to the decision. In addition, the questions are situated to examine if past behavior does influence the analyst's decisions and moderates the influence and control on intention. TPB is based on the assumption that a decision is the result of a deliberative, goal-oriented process; behavioral options are considered, consequences of the option are evaluated and the decision to do something is made.

4.3.2 Data Analysis Method. This study followed the data analysis procedures suggested by Miles and Huberman (1994a) for qualitative case data. Miles and Huberman (1994b, pp. 10-12) define data analysis as consisting of three concurrent flows of activity: data reduction, data display, and conclusion drawing and verification. These three types of analysis and the data collection process form an interactive, cyclical process. This research study moved among the four activities during data collection, data reduction, display and conclusion, and verification throughout the life of the research. Miles and Huberman (1994b) describe data reduction as data "condensation." In this form of analysis, the researcher sharpens, sorts, focuses, discards, and organizes collected data. During the interviews, an enormous amount of data was collected and the researcher used Miles and Humberman's (1994b) approach to focus and sharpen the collected data. As suggested by Miles and Huberman (1994b), when appropriate and in order to improve validity and help in analysis, the researcher used methods for summarizing (contact summary sheets, document summaries, case analysis meetings, and interim case summaries); different approaches to coding (at both descriptive and inferential levels); methods of thinking about data (annotations and memoing); and methods for producing extended reports (vignettes and pre-structured cases). In this research study, these methods were used continuously throughout the life of the research and before fieldwork commenced through initial research questions and the choice of a conceptual framework from which the researcher operated.

In applying these methods, there were three critical steps taken to establish an environment to examine the behavior in the IA who shares information when analyzing the risks and benefits as it relates to sharing information, as well as the reasons an IA is willing to share information with others, even when the risks may outweigh the benefits. The purpose is to examine the change in behaviors of IAs in their decision analysis of a typical intelligence

operational, mission-based info sharing event. To create the appropriate environment, it was important to develop actual operational mission-based scenario events that would serve as a basis to examining IA behavior in deciding to share information while analyzing the benefits and risks associated with sharing the information. Using actual Intel operational mission scenarios that were previously conducted or currently being executed could not be used for the semi-structure interviews since the scenarios could potentially classify the research study as well as put the IA at risk of violating security policies.

However, it was important to develop theoretic mission-based scenarios that simulated actual missions in complexity for critical thinking, effectiveness, and thoroughness, while keeping the research study at the appropriate unclassified level. Therefore, the first step was creating a working group of IAs from junior to senior levels to develop potential theoretic operational mission based scenarios that simulated actual missions and would effectively serve as the basis for examining IA behavior in deciding to share information while analyzing the associated benefits and risks. The group was tasked to generate operational mission-based scenarios that would cause IA to critically think what they would do in particular information sharing situations in the IC when deciding whether to share or not share information with others in the IC. They were also asked to take under consideration in generating the scenarios to also formulate them where an IA would consciously consider any potential benefits and risks associated with the decision when sharing the information with others. The group consisted of eight professional IA who generated 10 scenarios that could potentially serve as the basis for use in the research study. The theoretic operational mission-based scenarios collectively generated by the working group had to pass a second level of review for use and release. Thus, the next step in creating the appropriate environment consisted of submitting the scenarios to the

respective Special Security Offices (SSO) for review and determination of releaseability, to ensure they did not pose a threat to users or the IC, were not used in previous operational missions, or were perceived as a potential effect on a future operational mission. Finally, after review by SSO, three scenarios were determined as releasable and as simulating operational missions, and were adopted for use in the research study.

Although the intelligence mission-based scenarios are theoretic, a group of IA evaluated them as potential mission events that could serve as a basis to examining the behavior of an IA's decision when sharing information with others while analyzing the associated benefits and risks. In any military battle, the formidable force is often the entity that has the most complete and accurate information that is collected and shared among other reliable forces, but not the enemy. However, although each entity may share information with trusted partners, each side faces variations of information leakage, espionage, and political strife that affect the decision to share information and that makes the information valuable in terms of power or less valuable over time in terms of diminishing return on investment. The researcher proceeded with the group selected theoretic operational mission-based scenarios because they would allow examination of the actor's decision and behavior intention. Will the actor evaluate risk (consequences) versus benefits, consider the security and info sharing policies, or will the actor's personal or subjective norm be the controlling factors to the decision? These similarities and differences will allow the researcher to combine literal and theoretical replication logic (Yin, 2009). In addition, to deepen the understanding and to help achieve satisfactory validity, the researcher collected data from several sources using different data collection methods, including formal interviews with IC users, analysis of email correspondence, observations of recent events, and review of archival documents.

The interview data collected were analyzed interpretively using NVivo, a qualitative data analysis (QDA) computer software package, to uncover subtle connections, rigorously justifying findings, and to code. The overall decision-making of the subjects is based on the context of the theoretic operation mission-based scenario environments. The mission-based scenario environment provides the context for collective action as a network of interacting elements governed by certain motives. The subjects engaged in decision-making activities for a reason or reasons that form the motivation (such as to defend and protect the country or to simply support a fellow IA). The outcome is the transformation of the decision; success or failure or intentional or inadvertent release of information. The behavior of the subject is moderated by influences from the security and info sharing policies and the individual's beliefs (behavior intentions; attitude and intuition). They interact to influence the IA's analysis of the benefits and risks to the info sharing decision. For example, the security and info policies, peer pressure, and mission success influence a subject, but are also influenced by beliefs, experience, and tacit knowledge.

The researcher developed a semi-structured interview guide (See Appendix B) and conducted formal, semi-structured interviews with IA in the IC. The researcher designed theoretic mission-based scenarios that simulated an environment consistent with actual operational missions. It provided a context where multiple and interdependent decisions are made as a function of the decision-maker's actions and/or in response to environmental events. The questions were situated to understand the context in which the IA make these decisions, specifically when analyzing the trade-offs between the benefits and risks, while at the same time understanding the associated consequence as it relates to putting the organization at risk inadvertently or intentionally. IA were randomly selected from journeyman, junior and senior level grades within the military services and DoD civilians across the community based on their

unique job specialty code. Once selected, the IA received an email asking if they would like to participate in a research study, strictly voluntary.

There were 20 IA randomly selected and sent an email notification to participate voluntarily in the research study. There were 18 IA that responded as volunteers, which consisted of six journeymen, five junior, and seven senior IA. The subjects consisted of two females and 16 males, equaling seven civilians and 11 military members. The IC subjects consisted of a population of IA from the military service and IC agencies as follows: six in the Air Force, three in the Army, one from the Defense Intelligence Agency, three in the CIA, one from the NSA, two in the Navy, and one each from National Reconnaissance and National Geospatial Agencies.

The interviews were private and conducted in separate and secure environments. All subjects were interviewed in a location different from where they were currently employed. This was to ensure subjects felt relaxed, without any peer pressure, and comfortable in providing natural responses to the questions, and to help protect them from any scrutiny by an employee or employer identifying them as a participant in the research study. The information was collected using a digital recording device and later encrypted for security protection. The interviews lasted between 20 and 30 minutes. The sessions of the subjects that were digitally recorded were later transcribed and the digitally recorded data were destroyed. In addition, to maintain anonymity, the subjects were made aware of the destruction of the digitally recorded data and that names would not be used in the research study. This approach was to ensure the subject responses were natural and not hindered by the idea that the information provided would be incriminating or traceable to a single individual. Archival documents, such as website information, policy documents, standards and guidelines, operating procedures, published instructions, ICD, and

published strategies and visions were used for corroboration and clarification on the data collected through the interviews.

The subjects were given an option to randomly select from three different theoretic operational mission-based scenarios. The subjects were asked to choose a number between one and nine. If a subject's selection was between the numbers one and three, it resulted in scenario number two; if the selection was between four and six, it resulted in scenario number one, and; if the selection was between the numbers seven and nine, it resulted in scenario number three. After reading the scenario, the subject immediately answered the question that followed the scenario and then later answered a list of eight additional questions. The questions were the same for each scenario; however, since the interview was a formal semi-structured approach, subjects' responses did lead to additional inquires.

DATA ANALYSIS

5.1 Results

How do IA navigate the paradox between the benefits and risks affected by individual behaviors and organizational factors that inhibit info sharing decisions? In addition, is there a behavioral change, and why might IA share info with others, even when the risks may outweigh the benefits? In this exploratory study, respondents were asked what their first instinct was in their benefit and risk analysis in each of the operational scenarios. Displayed in Table 2 are the subjects' responses depicting their info sharing decisions from analyzing the theoretic operational mission scenarios. There were a total of 18 subjects that reviewed and analyzed the risks versus the benefits to sharing information and decided to share or not share information to successfully accomplish an operational mission. After reading the respective scenarios, overall responses to the questions immediately following the scenarios resulted in 10 out of 18 subjects who actually shared the necessary information that actually violated security and info sharing policies. Conversely, only two out of 18 subjects would not share information that was needed to successfully execute the mission because of religious belief; meaning they were in non-compliance with their oath of office or enlistment and the Uniform Code of Military Justice. However, when the question was rephrased to replace one's religious belief with an individual's sibling or a spouse, five out of 18 would not share the information needed.

Table 2: Info Sharing Decision

Decision to Share Information			
Mission	**Yes**	**No**	**Number of Subjects Responding (N=18)**
Scenario 1 (Violation of IC Info Sharing Policy)	6	2	8
Scenario 2 (Incident/Security Violation)	4	0	4
Scenario 3 (Compliance with oath of office/enlistment and UCMJ)	4	2	6*
Total	14	4	18
* Rephrased question to replace religion with sibling or spouse	1	5	

Scenario 1:

A communication between two foreign terrorists was acquired on 12 January 2008 using Executive Order (EO) 12333 collection. You discover the communication between the foreign terrorists includes vital raw Signals Intelligence (SIGINT) data (imagery) that a fellow Intel Analyst needs to successfully execute a mission on 28 January 2013; however, under EO 12333, the raw traffic is inaccessible to your fellow Analyst online because raw SIGINT data is only retained for up to five years. Since you were the originator of the raw SIGINT data, you have the raw data necessary to assist the Analyst in successful execution of the mission. Do you share the information with the Analyst to execute the mission successfully?

Eight subjects selected and responded to Scenario 1. Five out of the six subjects responded "*yes,*" they would share information with the other IA to execute the mission successfully. Only two subjects referenced that the violation of EO 12333 would not allow them to share information with the other IA. Typically, SIGNIT raw traffic is inaccessible after five years and could be destroyed or must have a destruction waiver to maintain it for longer than five years. In either case, since this scenario is intentionally situated beyond the five-year point, so it requires additional authority for access and to determine availability. The specific intent behind this question is to examine the actor's decision and behavior intention. Will the actor evaluate risk (consequences) versus benefit, consider the security and info sharing policies, or will the actor's personal or subjective norm be the controlling factors to the decision?

Scenario 2:

> *As an Intelligent Analyst, you served a tour in Afghanistan and had access to classified information. During your tour, you were privy to information that included imagery of raw SIGINT data tag, indicating that the legal authority category is the Foreign Intelligence Surveillance Act (FISA), F? Amendment Act (FAA). You have transferred to a new position as an IA. In your new position, you noticed you still have access to the SIGINT data without the appropriate re-justification. Simultaneously, during your discovery of your continued access, you also notice traffic of a special operations mission that requires use of the information under the legal authority of FAA. The target is to capture foreign terrorist and you have access to the imagery of raw SIGINT data that you can access and help with the capture of the terrorists. You know the IA are slightly less skilled at Intel analysis since your departure and have somehow missed the raw SIGINT data aggregation. Do you share the information with your previous IA to help capture the terrorist?*

Four subjects selected and responded to Scenario 2. All four subjects responded "*yes,*" they would share information with the previous IA to help capture the terrorist. This scenario illustrates a reportable incident since the IA still has access to the data without re-justification. The scenario suggests that, at the same time the IA discovers his/her access, discovery of a mission being executed to which he/she can provide assistance is also identified. The IA knows the appropriate skill set does not exist at the previous position and the unit will more likely lose an opportunity to capture the terrorist if there is no engagement to assist by sharing analysis of the information and the data from the intelligence library database. The rules are clear: if IA discover they still have access, the IA must contact a manager to have his/her access removed and inform leadership of the issue. In addition, since this involves Federal Foreign Intelligence Surveillance, it must be reported because of legal authority under the act. The specific intent behind this question is to examine the actor's decision and behavior intention. Will the actor evaluate risk (consequences) versus benefits and consider the security and info sharing policies, or will the actor's personal or subjective norm be the controlling factor to his/her decision?

Scenario 3:

> *As an IA assigned to the Defense Intelligence Agency, you're scheduled for your deployment rotation to Afghanistan. You and another IA are collaborating on the analysis of targeting information for the area to which you are being deployed. On your deployment, you are assigned to supporting the Central Intelligence Agency. You learned that the area you're being deployed to is in an area where you were originally born. In addition, on your deployment, during collaboration with another Analyst, you learn a mission will be executed that targets a particular asset that doesn't necessarily reside well with your religious faith or beliefs. The day of mission execution, the junior Analyst develops the package for targeting from the analysis of the data in storage. You review the analysis of the junior Analyst and realize there's*

> *additional information needed that you collaborated on prior to your departure for deployment. You are torn between your religious faith or belief and successful execution of the mission. The current Analyst is less skilled then you are and unaware of your prior analysis and your pertinent information. Do you share the information with the Analyst to ensure successful execution of the mission? Do you share the information if the target is where a sibling or spouse currently lives?*

Six subjects selected and responded to Scenario 3. Four out of the six subjects responded "*yes,*" that they would share information with the other IA to execute the mission successfully. The other two subjects responded that they would *"request separation of involvement and being accountable in execution of the mission."* However, when followed up with rephrasing the question to replace religious belief with a sibling or spouse, one subject stated *"yes,"* she would still share information with the other IA to execute the mission. Five subjects stated *"no,"* they would not share the information, and two of the responses were the same, stating they would *"request separation of involvement and being accountable in execution of the mission."* This scenario examines where subjects may intuitively place their values: on the information they intend to share or, in this particular scenario, on their religious faith or belief. In this particular scenario, there are no rules being violated in sharing the information or not sharing the information. However, if the Analyst chooses not to share because of religious faith or belief, the Analyst would be in non-compliance with his oath of office or enlistment and the Uniform Code of Military Justice. The important dilemma in this scenario is that only the Analyst knows that his/her decision to share or not to share the information is based on his religious faith or belief. The basis for this question is to examine the actor's decision and behavior intention. Will he/she evaluate risk (consequences) versus benefits, consider his/her own personal values over

those of the organization, and will his/her personal or subjective norm be the controlling factors to his/her decision?

5.1.1 Results Data Analysis. How do IA navigate the paradox between the between the benefits and risks affected by individual behaviors and organizational factors that inhibit info sharing decisions? In addition, is there a behavioral change and why might IA share information with others, even when the risks may outweigh the benefits? Table 3 displays the reasons given by respondents as explanations for sharing information. It turns out that the administrative pressure of security and information policies had only a small amount of influence on a subject's decision to share information; only two respondents mentioned administrative pressure. In scenario one, two different responses from IA regarding their first instinct in their decision to share or not share information was as follows:

> *Although the raw SIGINT data is inaccessible, I would be able to talk about my experience and my knowledge with my fellow analysts and tell them what I know, so I would share the information that way . . . common sense or whatever says, hey, we got lucky. Let's go ahead and share it since we're talking about terrorists, you know. We're not talking about, you know, like citizens or any of that kind of stuff.*

> *Yes I would . . . I felt like it was pretty easy . . . a necessity to the mission. There may have been some restrictions I may have violated, but the mission is more important.*

Conversely, 16 of the respondents felt their decision to share information was mostly influenced by the organization's goal of successful execution of operational missions; meaning an IA's first thought is the perceived successful execution of the mission (since success is determined afterwards). In addition, to ensure the perceived successful execution of the mission, IA sought mission first and fix policy later to adjust to meet the mission needs as their approach to sharing of information. They also viewed accuracy as a vital element to aid in the execution, potentially

overlooking the importance of the value of information shared in the IC. The subjects were asked in the theoretic operational based scenario execution of each mission, which was more important, the accuracy of the data or the value of the information being shared? It turns out that eight of the respondents thought providing accurate data during operational missions is more important than the value of the information. In scenario one, the subject's response is sought to, what is more important, sharing of accurate data for mission accomplishment or understanding the value of the information being shared? A subject responded with the following:

> *I would say ensuring accurate data is shared for mission accomplishment . . . a lot of times getting the accurate data to the right people who can determine the value is more important to mission accomplishment. I may not necessarily have the knowledge to know the value of the information, but if I can get that accurate data to the people who've got more experience and analyze that bigger data I would . . . you know, it's more important to share it than to understand it.*

This is substantial in providing explanation for the subject's response of feeling constrained by security and info sharing policies; in fact, 10 of respondents felt constrained by the organization's policies, but not enough to avoid violating them. Remember, as displayed in Table 2, 10 out 18 of the subjects actually violated the security and info sharing policies during analysis of the operational mission-based scenarios. It also alludes to the explanation of why subjects felt there was only a small amount of influence, and only two respondents felt administrative pressure from security and info sharing polices on their info sharing decision; subjects are not fully aware nor focused on the value of the information that requires protection through the enforced security and info sharing policies.

In line with the subjects' feeling of the perceived successful execution of the operational mission, the feeling magnifies when it involves ensuring that others do not impede the perceived

success. Thus, subjects felt compelled to assist others with sharing information that culminated in the perceived successful execution of the operational mission; 14 of the respondents felt compelled to share information with the other IA to ensure successful execution of the operational mission. In scenario three, subjects responded whether they would share or not share information with another junior analyst when it conflicted with religious belief. One IA's response was as follows:

> *My first instinct was to share the information because what he had was wrong or lacking and I had additional information that would provide clarity and ensure successful execution of the mission, but it hurts, very painful, very painful concept and I'm conflicted . . . for, you know, the rest of my life.*

In the data analysis, it was important from an IA's perspective that the organization characterized the actions or viewed the info sharing decisions as positive. Even when the subject's info sharing decisions conflicted with the subject's beliefs, when asked if they thought the decisions aligned with the organization's security and info sharing policies, respondents thought mission first above all else.

> *Wow! . . . That depends on the leadership, how they review that (positively or negatively), but how do you punish somebody who comes forward and says hey listen, I've been involved with this violation that resulted in successful execution of a mission. It'd be more of a cover up afterwards . . . deniable plausibility.*

Although subjects actually violated security and info sharing policies, most believed or felt their actions aligned with the organization's desired outcome of the perceived operational mission success. In most cases, subjects' beliefs were in conflict with the security and info sharing policies; six of respondents felt conflicted, although the desire to obtain the organization's desired goal of mission success impacted their behavioral intention, and thus influenced the decision to share information. However, if the stakes were too high, based on

personal beliefs (values and intuition), subjects' beliefs actually conflicted with the security and info sharing policies. Only six of the respondents actually shared information where others' beliefs (values and intuition) greatly influenced their decision not to share, which outweighed the organization's goal of operational mission success.

Table 3: Info Sharing Reasons

Reasons Given for Sharing Information				
Reasons/Motives	Number of Respondents Mentioning Items (N=18)	**Scenario 1**	**Scenario 2**	**Scenario 3**
Pressure from others if mission was unsuccessful	11	5		6
Felt compelled to help another IA	14	6	4	4
Execution of a successful mission is the most important objective	16	8	4	4
Administrative pressure from security & info security policies	2	2		
Felt constrained by security & info policies	10	6	4	
Mission first, fix policy later to adjust to meet mission needs	16	8	4	4
Accuracy of data is more important than the value of information	8	8		
Beliefs conflicted with security and info sharing policies	6			6
Experience/knowledge conflicted with security & info sharing policies	6	6		
Personal beliefs/values conflicted with mission success	6			6
Total	**95**	**49**	**16**	**30**

DISCUSSION

The aim of this exploratory study was to examine the behavior of IA, and to investigate the paradox of info sharing in the IC. Why do people share information with others; primarily, what influences the individual's decision that drives him/her to violate security and info sharing policies? The understanding of IA behaviors allows a better understanding of how one might go about modifying behavior in a desirable direction. The results provide support that background factors do influence the beliefs people hold. These factors, attitudes and intuition and broad life values, influence intentions; and, thus, an IA decision in info sharing. Hodgkisno, Salder-Smith, Burke, Claston, and Sparrow (2009a, p. 277) noted that, until recently, only the "bravest and most far-sighted" would recognized the utility of intuition in management decision-making. Why did IA actually violate security and info sharing policies so easily? There is a major external influence on IA in accomplishing the organization's goal of mission success. IA construct their own version of *reality* based on information provided by the senses, although this sensory vision is moderated by complex mental processes that determine which information is attended to, how it is organized, and the meaning attributed to it. According to Hodgkinson et al., (2009a), the changing nature of work practices and structures creates environments where human information-processing capability is exceeded by the volume and complexity of the information that humans have to process; thus, intuition is a more widespread strategy for decision-making (Allen, 2011). What people perceive, how readily they perceive it, and how they process this information after receiving it, are all strongly influenced by past experience, education, cultural values, role requirements, and organizational norms (the goal of successful operational missions), as well as by the specifics of the information received.

6.1 Intuition

IA intuition relies on long-term memory input processed automatically and sub-consciously or pre-consciously; input is holistic, and output from the process is feelings that serve as the basis for judgments in decisions, all of which, according to Allen (2011), are characteristics of information processing which is a distinct and different mechanism for information processing and decision-making. This intuition, based on the results of the study, conflicted with the organization's security and info sharing policies, partly because the attitude towards these security and info sharing policies hinders the perceived successful operational mission. The results also provide support to IA actions triggered by environmental events and because their activities are definitely not repetitive, and their performance requires greater attention, even with experience over time where intuition is a strong influence on behavioral intention. This is contrary to expectations as described by Outllette and Wood's (1988) postulation of habitual behavior, where past behavior may be a strong predicator and where intention may be relatively weak. However, perceived behavioral control, part of TPB, accommodates the non-volitional elements inherent in all behaviors. According to Ajzen (2002), even when not particularly realistic, perceived behavioral control is likely to affect intentions. A high level of perceived control strengthens a person's intention to perform the behavior, and increases effort and perseverance. Hence, attitude and intuition affect behavior indirectly, by its impact on the intention of the decision. Accordingly, when perceived behavioral control is veridical, it provides useful information about the actual control a person can exercise in the situation, and can, therefore, be used as an additional direct predictor of behavior (Ajzen, 2002).

6.1.1 Relationships and beliefs. Another interesting result is the strong relationship between one IA and another IA tangled together on the compelling need to support each other in

the perceived successful execution of an operational mission. Self-efficacy beliefs affect thought patterns that may be self-aiding or self-hindering. An IA behavioral intention in deciding to share information is influenced by the perceived success or failure of the mission; thus, another IA affects his attitude towards this effort as well as his mental model of the perceived outcome. The more strongly people believe that a certain response will lead to a certain outcome and the more positively they value that outcome, the stronger their intention to produce the response in question (Ajzen, 2012); in this case, to share information, and, in some cases, magnifying the violation, to execute a perceived successful operational mission. The self-efficacy beliefs function as an important set of proximal determinants of human motivation, affect, and action. Neither IA wants to fail in meeting the organization's goal of successful execution of an operational mission. Therefore, these self-efficacy beliefs are part of their motivational, cognitive, and affective intervening processes in the behavioral intention, which influences the decision to share information. Bandura (1989) postulates that people's perceptions of their efficacy influence the types of anticipatory scenarios they construct and reiterate. Those who have a high sense of efficacy visualize success scenarios that provide positive guides for performance. Those who judge themselves as inefficacious are more inclined to visualize failure scenarios that undermine performance by dwelling on how things will go wrong.

IA beliefs in achieving mission success over violations of security and info sharing policies are strongly influenced by the IA attitudes towards the policies as well as their intuition of success or failure. This aligns directly as described by Bandura (1989) who argues it is widely believed that misjudgment produces dysfunction and gross miscalculation can create problems. His argument is, although optimistic self-appraisals of capability are not disparate from what is possible can be advantageous (mostly advantageous for the organization), veridical judgments

can be self-limiting. IA assess the risks versus the benefits in their analysis before deciding to share or not to share information. The most impacted in the analysis is the perceived benefit based on the perceived mission success. Bandura (1989) postulates that often people err in their self-appraisals, and they tend to overestimate their capabilities. This is a benefit rather than a cognitive failing that needs to be eradicated. If self-efficacy beliefs always reflected only what people could do routinely, they would rarely fail; however, they would not mount the extra effort needed to surpass their ordinary performance. IA overestimates their capabilities and the benefits to the success of an operational mission. This benefit does not, and this process is so built into an AI belief that, for many it becomes routine; therefore, their beliefs are that they would rarely fail in an operational mission. Thus, many do not mount the extra effort needed to ensure security and info sharing policies are not violated. Conversely, according to Bandura (1989), evidence suggests that it is often the so-called *normals* who are distorters of reality. However, they exhibit self-enhancing biases that distort appraisals in the positive direction because they take an optimistic view of their personal efficacy to exercise influence over events that affect their lives (Bandura, 1986, Taylor & Brown, 1988). The results support the fact that subjects violated laws, violated their own principles, and violated the core of the military values. Their subjective normal beliefs were, essentially, that they were simply doing what they were supposed to do in order to uphold the values of their profession and their organization's larger purposes. Unfortunately, their actions would damage their careers, but in the long term, their behavioral beliefs are those that led them to stand up for personal and institutional integrity. Daily experience tells us that the deeper satisfactions we crave come from strong bonds of mutual attachment to other people and larger causes outside ourselves. Heclo (2008) argues that, with larger causes outside of oneself, the mirrors become windows and doors into a wider world

of loyalties. He postulates that, in that world, a sense of well-being and happiness finds us rather than our frantically chasing it down.

A surprising result is the weak relationship between the accuracy of data in info sharing and the value of the information contributed. In the exploratory study, IA placed an enormous amount of emphasis on the accuracy of the data shared, but very little attention to the value of the information shared. Despite the best available evidence presented to decisions-makers, there is always uncertainty inherent with the decisions made because it is impossible to have complete and perfect information that answers all questions. With IA decisions and analysis of the risks and benefits, uncertainty arises from the presence of conflicting influences: security and info sharing policies as well as the personal (attitude and intuition) and normative beliefs. Thus, making decisions in the presence of uncertainty is risky because wrong decisions could result in failure of the operational mission, resulting in high costs, possibly lives. In these situations, the IA has the added burden of knowing that, once these decisions are executed, they cannot be reversed. The rational approach would be to evaluate the accuracy of the data and its value (need) simultaneously for execution of the operational mission. However, during the period of uncertainty with the influences that affect the decision, the IA behavior places greater emphasis on experience and tacit knowledge, where accuracy of the data is vital to successful execution of the mission. However, recent research analysis studies show that information in its various types has a significant effect on increasing the power of an organization (Ahituv & Carmi, 2007). In other words, the IC being richer in information than its adversaries is more powerful. This defining of information as an influential factor is crucial to determining the power of the IC, thus strengthening the importance and real value of information. It also provides a possible explanation of the conflict in behavior of IA decisions. The argument is that IA are conflicted in

beliefs with their focus solely on the accuracy of data and not the value of information. Moreover, it can provide an additional possible explanation to the influence of their decisions (less value placed on the security and info sharing policies) in successful or unsuccessful execution of operational missions.

In info sharing, an IA contribution when sharing often influences the value of the information for others. In many cases, this higher value of the information for others is associated with higher risks to the IC. Each contribution possibly results in greater value, culminating in potentially greater risks. While accuracy was described as vital to successful execution of a specific operational mission, the value of the information being shared was only given second thoughts in comparison, resulting in violation of the security and info sharing policies. In info sharing, the IA would not necessarily have complete knowledge on the risk tolerance for a particular operational mission, thus relying heavily on accuracy for successful execution without consideration of the value of the information. This is significant because Messick and McClintock (1978) argued that human behavior is influenced by values that people assign to different action alternatives and their consequences. Often, consequences of action alternatives will not only affect the actors themselves but also other people; hence, the earlier reference of the strong relationship between two IA.

Table 3 shows the number of respondents mentioning components (reasons/motives) for sharing information. Another very interesting empirical finding of this research study is the lack of adherence to security and info sharing policies as it relates to the perceived usefulness of the policies in allowing successful execution of operational missions. The "e*xecution of a successful mission*" and "*mission first, fix policy later to adjust to meet mission needs*" reasons stood out significantly as large contributors (16 out of 18 on each) to the lack of adherence to security and

info sharing policies. IA work in environments where sharing of information must be protected at all levels to prevent loss of operational capabilities and to keep a competitive advantage over adversaries in mission execution. It also allows IA the ability to make better decisions when pieces of information are shared collectivity across the IC. The results found that most IA viewed the policies as constraining or inhibiting towards accomplishing the missions and in most of the scenarios actually violated the security and info sharing policies. In addition, when IA beliefs were strong influences, it affected their decision to share information forcing possible non-compliance with the oath of office or enlistment to include UCMJ authorities. This research study empirically found that the lack of adherence to the security and info sharing is contrary to what is understood in the IC and could shed light on this veil used by the IC that most IA described as inhibitors or roadblocks in their analysis when considering the risks and benefits to info sharing in deciding to share or not share information. As mentioned, the info sharing goals as explained in ICD 501 are to: 1) foster an enduring culture of responsible sharing and collaboration with an integrated IC; 2) provide an improved capacity to warn of and disrupt threats to the U.S. homeland, and U.S. persons and interests; and 3) provide more accurate, timely, and insightful analysis to inform decision-making by the president, senior military commanders, national security advisers, and other executive branch officials were the focus of most IA when deciding to share info, but contradicted other factors, specifically security policies, when focusing on successfully executing the operational mission.

Info sharing has become critical due to the U.S. Intelligence Reform and Terrorism Prevention Act creating an *Info-Sharing Environment* fused by the ICD to foster a culture of more sharing within inter-/intra-agency organization environments with pressures from organization factors, such as, security and info sharing policies. Controlling of info sharing by

solely focusing on the security and info sharing policies without the increasing demand for the need of info sharing coupled with ever-changing Intel operational mission environments forces IA to share info where the risks may outweigh the benefits. Due to these risks, amendments to existing policies should be evaluated continuously. IA in their decisions to share or not share information are faced with rapidly changing operational environments of available information being shared, coalition collaboration, and changes in the classes of information shared, all of which are evaluated by them in risk and benefit analysis influenced by their behavior. General or static policies are inhibitors and require continuous monitoring with additions and deletions to the rules to meet the changes in the environment that IA are faced with every day in the operational environments. In the IC today, it takes months to change a security policy with months of delays between the changes to be effective to the IA. What is needed is a capability that enables dynamic switching between policies within minutes, without introducing new risks or vulnerabilities, through a system that provides dynamic authoring, selection, and deployment of security and info sharing-related policies and also allows IA to fully execute the operational mission without risks and fully engage in the IC objective of inter-/intra-agency info sharing. When security and info sharing policies are perceived as useful to IA, they will be applied effectively in a risks-versus-benefits analysis and will influence their decision-making positively in executing Intel operational missions.

CONTRIBUTIONS AND LIMITATIONS

7.1 Contributions

This research makes five valuable contributions; to wit, it: 1) describes the paradox of the info sharing decision of an IA analysis of the benefits and risks influenced by the organization's security and info sharing policies and an individual's behavior intention; 2) explains the decision-making behavior of people's willingness to share information with others, even when the risks may outweigh the benefits (to better understand how we might go about modifying behavior in a desirable direction); 3) demonstrates how TPB may be used as an analytical framework that describes how past behavior of users' decisions to share information with others in the IC; 4) develops a conceptual framework to evaluate adherence to info sharing decision-making in the IC; and 5) provides practical guidance for improving IA decision-making in the presence of the paradox.

First, the findings of this research study empirically demonstrate the paradox of the info sharing decision of an IA analysis of the benefits and risks influenced by the organization's security and info sharing policies and an individual's behavior intention. In describing the paradox of the info sharing decision of IA analysis of the benefits and risks influenced by the organization's security and info sharing policies and an individual's behavior intention, it begins with understanding the behavior intention of IA. The decisions made within the paradox of info sharing are not necessarily made in a rational fashion. A large body of empirical research attests to the predictive validity of the TPB. Various techniques have been developed to increase behavioral control, although these techniques have not been used in a TPB context. Some methods focus on imbuing individuals with a sense of self-efficacy or perception of behavioral control. These methods can thus influence behavioral intentions; that is, the motivation to

engage in the behavior, but they may also provide valuable information about actual behavioral performance.

The behavior intentions of IA begin with the extent to which they possess an accurate understanding of their own mental processes as well as their understanding of the security and info sharing policies. The behavior intention is based on how good their insight into how they actually weigh evidence is in making judgments for each situation to be analyzed. In each situation, they have a mental model consisting of beliefs and assumptions as to which variables are most important and how the variables are related to each other. This research empirically found how the paradox in navigating the benefits and risks in info sharing is strongly influenced by IA beliefs, specifically their attitudes and intention, most important, their background beliefs, like the religious belief. This supports TPB, specifically the extended research on background factors conducted by Ouellette and Wood (1998). They postulated that, "in domains that facilitated development and execution of habits, past behavior was a strong predictor and intention relatively weak. In domains that did not facilitate habits, past behavior was a relatively weak direct predictor and intention was quite strong" (Ouellette and Wood, 1998, p. 66).

Since IA actions are typically triggered by environmental events, activities are not necessarily repetitive in nature and require great attention to detail. This research found that for subjects with more experience and more analytical skill, in most cases, past behavior was relatively weak and direct predictor and intention was strong; however, for the subjects that were less skilled, past behavior was a strong predictor and intention relatively weak. This research points out an exception in the research findings described by Ouellette and Wood (1998), although it validates the extended portion of TPB. This research found that, in either situation, certain factors can play a strong predicator whether habitual behavior or not, even where

intention may be quite strong. In this research study, the past behavior was a strong predictor and intention was strong despite the IA experience or skill level where the background factor was significantly influenced by a personal belief, such as a religious belief or the value the IA may place on the life of another.

Second, this research also explains the decision-making behavior of people's willingness to share information with others, even when the risks may outweigh the benefits. The empirical findings demonstrated subjects are willing to risk sharing information with others, even when the risks may outweigh the benefits, when the IA perceives that the sharing results in successful execution of an operational mission. To this end, subjects accepted the risks or misinterpreted the security and info sharing policies when they believed it was not to their advantage in accomplishing the perceived organization's primary goal, successful execution the operational mission. To affect the decision influenced by security and info sharing policies as well as behavior factors, such as attitude, intuition, and personal beliefs there must be behavior change interventions. Behavior change interventions must accomplish two major objectives: They must motivate individuals to perform the behavior, and once this has been accomplished, they must ensure that the behavior will be carried out.

There are two approaches to the behavioral change intervention. One approach involves intervention based on TPB, which focuses on targeting behavioral, normative, and control beliefs in an effort to produce positive intentions among the IA, who, prior to the intervention, either did not contemplate performing the behavior or were disinclined to do so. In other cases, inducing favorable intentions may not be enough to produce a change in the target behavior. First, the implementation stage for changing the behavioral change of IA is to focus on control issues, dealing with internal and external factors that can facilitate or inhibit performance of the

intended behavior. The empirical research study demonstrated focus should be on the information security and info sharing policies, which subjects felt inhibited their ability to accomplish the mission. IA cannot be exposed to all possible scenarios of operational mission events. This research study proves that introducing theoretic scenario-based operational mission events that are designed to challenge unfavorable beliefs (religious or personal) resulting in the consequences of violating the security and info sharing policies is a much greater risk to the IC than actual successful execution or even perceived accomplishment of the ongoing mission. IA believe that every piece of information that is shared contributes to successful execution of an operational mission. What happens when the mission is not successful? Unfortunately, the focus and control of the belief are weighted heavily on the perceived successful execution and not those that would result in an unsuccessful execution. The change in focus would move towards the needed behavioral change. IA should be exposed to scenario-based operational mission events with emphasis on perceived unsuccessful executions to force a behavioral change. This behavioral change would heighten the senses of IA focus on the benefits of using the security and info sharing policies as successful applications versus inhibitors to operational missions. Another approach is to use role models (senior officials) identified in stories of scenario-based operational mission events designed to influence behavioral, normative, and control beliefs. The interventions that balance the successful and unsuccessful will be quite effective, producing changes in beliefs that will be reflected in the intended and actual decisions of IA when sharing information. There should be less focus on the fact that shared information absolutely results in successful execution of an operational mission and more focus on the the fact that shared information only contributes to possible successful execution of an operational mission. A change in the behavior requires a change in the inherent belief of many IA that

shared information leads to successful execution of an operational mission; unsuccessful execution in operational missions is not part of the *attitude* of IA.

The third contribution of this research study is the adaptation of TPB as an analytical framework that describes how past behavior of users influences decisions to share information with others in the IC. Some researchers (McClintock, 1978; Messick & McClintock, 1968) posited that human behavior is influenced by values that people assign to different action alternatives and their consequences. What is the behavior that influences an IA to share classified material with others not authorized? In this research study, the behavior that influences an IA to share classified material with others not authorized was mostly influence by the organization's desired goal of absolute perceived execution of operational mission success. Could IA behavior have been influenced by values unconsciously inherited from being a member of the IC, practicing the mandated security and info sharing policies? In the research study, IA values were unconsciously inherited from the relationship of others within the IC, which felt inhibited by the security and info sharing policies when driving towards the unit's overall goal. In some instances, another IA as social peer, impacted the IA decisions and actions resulting in perceived success influenced the info sharing decision. In TPB, the most detailed substantive information about the determinants of a behavior is contained in a person's behavioral, normative, and control beliefs. What are the most influential behavioral factors in the decision-making of IA when sharing information with others? In this research study, the most influential behavioral factors were attitude, intuition and personal beliefs that changed IA behavioral intention. This supports TPB, which posits there are differences in the decision-making when an IA believes the recipient has authorization versus no authorization. (Allport, 1935, 1968) pointed out that the concept of attitude "is probably the most distinctive and indispensable concept in contemporary

American social psychology" (1968, p. 59). With this understanding, often, consequences of action alternatives will not only affect the actors themselves but also others; most important, the IC. In the adaptation of TPB, these values include an actor's background factors (social, personal, information) and beliefs (behavior, normal, control).

The background and beliefs of an individual represent a behavior intention, as well as a stable preference for distribution outcomes (inadvertent, desired, or intentional) between one's own self and the organization. The background factors (See Appendix A) and individual beliefs are extremely important influencing factors in the conflict between the behavior of IA and the organization's security and info sharing policies in the paradox of info sharing. Do IA consider their own benefits and risks in sharing information but also the benefits and risks to the organization? Will they contribute more information of high value than information of low value? The logical answer is, the IA may very well, in their decision to share information, consider the benefits and risks to others. This could result in contributing more information of value or higher classification that benefits an IA during a successful mission, but violates the organization's security and info sharing polices to do so. On the other hand, it may be consistent with the organization's security and info sharing policies, resulting in sharing information of less value or lower classification, but also in an unsuccessful mission.

In some cases, inducing favorable intentions may not be enough to produce a change in the target behavior. In these instances, two interventions may be required; one to produce the desired intention and another very different intervention to facilitate performance of the intended behavior. When asked to explain why they failed to act on their intentions, people often say that they forgot or it slipped their minds (Orbell, Hodgkinson, & Sheeran 1997; Sheeran & Orbell 1999). To close the gap, the focus must be on implementation intention. The approach is to ask

IA when, where, and how they will carry out their intentions, important for less and highly skilled analysts, increasing the likelihood that they will so. The focus should be on situations that violate security and info sharing policies and that inhibit operational missions. These will allow control of the behaviors and facilitate in practicing in environments where success is measured differently and total focus is not only on successful execution of the mission, but also on successful execution of compliance with security and info sharing policies.

Lack of adequate control over the behavior can make it difficult or impossible to perform an intended behavior. Internal factors, such as lack of sufficient willpower and perseverance or lack of requisite skills and resources or external factors, like cooperation from another person, can interfere with planned behavior. Additional methods can be developed to increase behavioral control that focus on instilling individuals with a sense of self-efficacy or perception of behavioral control. The methods would influence behavioral intention, which is the motivation to engage in the behavior, while also providing valuable information about actual behavioral performance. Observational learning, modeling techniques and mental simulation, all of which are the premises of the theoretic scenario-based operational missions in this research study, provide valuable information about actual behavioral performance. Successive approximation and simulation of the desired behavior are other methods that are designed to provide individuals with the tools and other resources needed to overcome potential hurdles and gain actual control over behavior performance.

The fourth contribution of this research study is the development of a conceptual framework to evaluate adherence to info sharing decision-making in the IC. Within the conceptual framework of this research study, the IA's benefits and risks analysis are moderated by organizational factors (security and info sharing policies) and behavioral intentions (attitude,

values, and intuition), which influence info sharing decisions that result in desirable or undesirable outcomes. As empirically found in this research study, past behavior influenced IA decisions during info sharing. This past behavior influencing factor was also empirically proven in Kidwell and Jewell's (2008) research study were the influencing factors where considered a critical part of the decision making process. Therefore, this research study further suggests that the past behavior, such as, intuitions and personal beliefs, are influencing factors on the intentions of the decision maker.

Gibbsons et al. (2003) developed the Prototype-Willingness Model (PWM) based on three assumptions about risky behaviors among adolescents and young adults. Gibbsons et al. (2003) posited risky behavior is neither reasoned nor intentional, which led to additional constructs of TPB with the predictors of behavioral expectations and behavioral willingness.

IA access to information processing is approved based on security clearance level, need to know, and system access to the appropriate classification levels of the information. Generally, an IA has access to data at three classification levels: Unclassified, Secret, and Top Secret. Although there are other compartmented classifications within each of the general levels of access, the focus of this research study is on the access to information at these three general levels. It is important to understand how an IA attempts to process information since it is part of his/her internal process to decision-making. According to Neisser (1967), most people operate in a perception-action cycle, suggesting that the senses take in information from the environment, the mid brain performs computations on that information and the outputs of those computations are used to guide subsequent goad-directed actions. However, Newell and Broder (2008) argue that, since most people's information capacity is limited, he/she must use cognitive models to propose heuristics or shortcuts.

The organization's security and info sharing policies have increased in complexity when sharing across an intra-/inter-agency. First, it changes rapidly with the increasing need for intra-/inter-agency sharing of information. There are partnerships that form and disband based on an organization's interest and mission execution. At any moment, a partnership must be formed under the conditions that info sharing is necessary based on a new agreement between the U.S. and a national partner because of the relationship in a particular environment that is later disbanded under the conditions that the partner now puts the organization at risk. The organization's need for sharing information often changes and is often unclear at different levels within the organization or across inter-/intra-agencies. At various levels, organizations have strict policies to sharing information, but they are created generically at very high levels and execution is done at much lower levels and could very well be left to different interpretations by individuals that could put the organization at risk. These types of conditions intensify when considering how IA seek information to share.

Given the need for the increase in info sharing across intra-/inter-agency organizations and the importance of the benefits and risks associated with sharing information, understanding the *how* and *why* provides insights into behaviors of IA decision-making. Moreover, previous studies reveal that computer supported info sharing plays an increasing role in a multitude of situations, such as organizational knowledge management, online collaboration, and decision-making. Since info sharing does not always flow as smoothly as expected and the decision to share is impacted by various factors, it is important for inter-/intra-agency organizations to understand the behavior of IA. Specifically, attitude and intuition, which influence the willingness or non-willingness of the IA decision to share information released inadvertently or intentionally that may violate security and info sharing policies and put the IC at greater risk;

and, thereby, possibly put the nation at risk. Developing more effective decision-making, however, requires organizations to fully understand not only how these intended decisions and past behaviors are developed in theory, but also how they are developed in practice. This study provides further insights into this process and the interactions that influence the decision while exploring the behavior of IA. This study also illuminates the mechanisms by which information behavior was propagated. These mechanisms include the use of mediators (attitude and intuition) which was perceived as one part of the paradox in the decision-making for IAs and was, therefore, propagated and legitimated in narratives. Hence, because intuition was perceived as an influenced mediator, it was perpetuated as a social norm in the perceived behavioral control of the TPB model. This occurred despite the conflict with the security and info sharing policies, the other part of the paradox, in the conceptual model.

By a close examination of the info sharing decision-making of IA using the theoretic operational mission based scenarios, this research provided revelations of the behaviors and behavior intentions through which IA info sharing decisions flow. Although one cannot generalize from these only, by exploring the analysis within each scenario and comparing across each of them, this provides approaches to understanding info sharing decision-making within organizations and the conflicts that exist. Background factors (past behavior) in general are understood as actions or reactions of a person in response to external or internal stimuli in the past. These factors include general attitudes, personality traits, values, emotions, intelligence, age, gender, race, ethnicity, education, religion, experience, knowledge, and media exposure. As such, specific interest in this research is in the relationship between past behavior and intention under special circumstances of IA experience or habits. Moreover, understanding behavioral intentions using past behaviors that lead to decision-making, specifically the role of past

behavior as predictor of intention, recently has had a considerable amount of attention in the literature, but is also criticized based on the relevance of past behavior being an extra predictor. Therefore, this study offers a further contribution in showing the value of applying past behavior and developing TPB as a framework for studying developing info sharing decision-making in inter-/intra-agency organizations.

Finally, the fifth contribution of this research study is to provide practical guidance for improving IA decision-making in the presence of the paradox. Most security policies address some form of vulnerability management. IT security professionals depend upon accurate assessments to determine whether intervention is necessary and implement proper steps for mitigation or remediation. There is no problem obtaining the data. Most security devices and scanners generate terabytes of data for analysis. The challenge is interpreting the data, specifically, identifying those specific vulnerabilities that truly represent a clear and present risk to intelligence information. IA need solutions that help them distinguish the danger signals from the noise that allows them to follow through with actions. For example, a mission-critical Web Server may have several known vulnerabilities, but which of those present a genuine risk and require analysis of the benefits and risks. For an IA Senior to be successful, vulnerability management solutions should identify and dismiss certain attacks as “noise” and flag the others as “signals” that require immediate attention that allows the IA to share information without background factor influences weighing heavily on their decisions

Compliance is another challenge with the perception that attaining compliance reduces risk to acceptable levels. For example, the Payment Card Industry Data Security Standards, (PCI-DSS), Health Insurance Portability and Accountability Act (HIPAA), North American Electric Reliability Corporation (NERC), Critical Infrastructure Protection (CIP) standards,

Federal Information Security Mandate Act (FISMA) and National Institute of Standards and Technology (NIST) standards all drive organizations to adopt security risk management approaches, but compliance guidelines and standards alone doesn't necessarily equate to successful info sharing. To achieve effective risk management in sharing information, IA must abandon the limitations and expenses of traditional, reactive approaches in favor of objective learning combined with the understanding of proactive security, data-driven investment models. In addition, they must overcome several challenges: analysis and interpreting massive amounts of data, monitoring dynamic assets, incorporating both compliance and security into best practices, moving beyond the traditional rational decision-making as well as the utilizing the standard "scan-and-patch" approaches to implement security best practice programs, and trusting conventional prioritization methods beyond their scope. Unfortunately, IA rely on rational decisions and the IC enterprise trust that "scan-and-patch" methods for security. However, training IA in methods based on rational choice coupled with security patching that inherently keeps cybercriminals or hackers ahead inhibits info sharing and greater allows for influence of background factors to affect the decision in info sharing. The focus cannot be solely on security patching, although an important step, IA need a variety of proactive solutions, like the objective learning, theoretical models and simulations combined with implementation of the security and info sharing practices in the IC.

7.2 Limitations

With any research, there are always anticipated limitations that may offer opportunities for future studies. First, since this research involves only three scenarios, there is a problem with the generalizability of the research from sample to population. Second, this study is limited to one intra-agency organization, the IC, including the military services, that varies greatly in their

operational missions, is decentralized in their decision-making, and is engaged in protecting the national defense of the United States. As such, changes in the findings may occur in studies involving public organizations or differ from these inter-/intra-agencies in size, location, degree of decentralization, mission, environment, and organizational structure. Third, interviews based upon past events may be biased, events may be filtered out that do not fit, or certain views could be censored, even though the researcher will make an effort to mitigate any biases through triangulation and verification using multiple data sources. Finally, past behavior must be examined to determine if further functions may be relevant and other factors may exist, the inclusion of which could improve explained variance of intention, which should be analyzed over time.

7.2.1 Generalizability. Firestone (1993) suggests three levels of generalization: sample to population; analytic, which is theory connected; and case-to-case research. With only three cases, this research will not be generalizable from sample to population, but will have analytic and case-to-case generalizability. The choice of the scenarios in this particular research study is based upon conceptual grounds not on representative ground. The research used multiple-case sampling and cross-case comparison in following replication strategy to identify repeating patterns (Miles & Huberman, 1994b; Yin, 2009). This cross-case comparison is made possible in that the selected scenarios are in similar settings, involve a coherent sampling frame, and focus on similar processes. According to Mason (2002), the limited sample to population generalizability of case study research should be balanced against advantages of its attention to context dynamics, and multiple participants perspective. In addition, Lincoln and Guba (1985) suggest audit procedures that will help other researchers to assess the findings in their transferability to other contexts. To ensure rigor, the study triangulated between different data

sources, checking against public data and internal communications, multiple interviewees, feedback from key participants, and field observations (Miles & Huberman, 1994b; Yin, 2009, p. 267).

7.2.2 Variance. An additional limitation in this research study is that a majority of the subjects actually shared information during their analysis of the theoretic operational based scenarios, resulting in actual violation of security and info sharing policies or in non-compliance with their oath of office or enlistment, potentially being in violation of the UCMJ. This is an issue with the research results producing insufficient variance in results to enable one to distinguish between the reasons for adherence to the security and info sharing policies when compared to reasons not to adhere to the security and info sharing policies. It would be interesting for future research to investigate the functionality of the security and info sharing policies in a way that better captures explanations that focus specifically in the area of adhering to the security and info sharing policies.

CONCLUSION

The aim of this exploratory study was to examine the behavior of IA and to investigate the paradox of info sharing in the IC. Why do people share information with others; primarily what influences the individual's decision that drives him/her to violate security and info sharing policies? The understanding of IA behaviors allows a better understanding of how one might go about modifying behavior in a desirable direction. The results provide support that background factors do influence the beliefs people hold. These factors (attitudes and intuition) and broad life values influence intentions, and, thus, an IA decision in info sharing. Hodgkinson, Salder-Smith, Burke, Claston, and Sparrow (2009a, p. 277) noted that until recently, only the "bravest and most far-sighted" would recognized the utility of intuition in management decision-making.

Why did IA actually violate security and info sharing policies so easily? There is a major external influence on IA in accomplishing the organization's goal of mission success. IA construct their own version of *reality* based on information provided by the senses. IA beliefs in their capabilities affect how much stress and depression they experience in threatening or taxing situations, as well as their level of motivation. Such emotional reactions can influence behaviors both directly and indirectly by altering their decision to share information and the course of actions they choose. IA who believe they can exercise control (perceived behavioral control) over beliefs do not conjure up apprehensive cognitions; in other words, they saw no conflict in their decisions when balancing them against the administrative security and info sharing policies; therefore, they are not perturbed by them. However, anxiety arose when their beliefs conflicted with organizational goals or personal values (attitudes and intuition) and they often

overestimated their decision when balanced against the core values of the military and the security and info sharing policies.

Part of ensuring the overall reliability of adherence to security and info sharing policies requires changes in the operation of how we develop and revise new policies, as well as, reviewing the processes on how these policies are understood and implemented. To implement the appropriate mechanisms for enforcing those policies, requires policy bundles that will contain a variety of components conducive to ever-changing environments in the execution of Intel operational mission. In addition, the policies must be adaptive to security enforcement of rapid deployment and within minutes without introducing new risk or vulnerabilities through a system that allows for dynamic authoring, selection, and deployment of security and info sharing related policies. Another approach to ensure adherence to the security and info sharing policies is to implement case-based training to facilitate IA understanding of importance of the policies that aid in their accomplishing Intel operational mission. In addition, behavior change intervention may be required. To do this, it must accomplish two objectives: motivate the IA to perform a different behavior, and, once this has been accomplished, it must ensure that the behavior be carried out. Focusing on the control issues, dealing with internal and external factors that can facilitate or inhibit performance of the intended behavior—in other words, mission first and always—are factors that will always drive an IA to think the mission is above the law. Intervention studies have shown that changing people's behavioral, normative, and control beliefs influences their intentions and actions.

APPENDICES

Appendix A: Theory of Planned Behavior and Information Sharing Paradox Constructs

Background Factors	Past behavior beliefs that are actions or reactions of a person in response to external or internal stimuli in the past; relational properties are general attitudes, personality traits, values, emotions, intelligence, age, gender, race, ethnicity, education, religion, experience, knowledge, and media exposure; specific interest in this research study is relationship between past behavior and intention under special circumstances of Intelligence Operators experience/habits (risky behavior)
Behavior Beliefs	Beliefs about the likely outcomes of the behavior and the evaluation of these outcomes; produces a favorable or unfavorable attitude toward the behavior
Normal Beliefs	Beliefs about the normative expectations and actions of important referents and motivation to comply with these referents; results in perceived social pressure or a subjective norm
Control Beliefs	Beliefs about the presence of factors that may facilitate or impede performance of the behavior and the perceived power of these factors; gives rise to perceived behavioral control
Behavior Intentions	With the combination of attitude toward the behavior (behavior beliefs), subjective norm (normal beliefs), and perception of behavioral control (control beliefs) leads to the formation of a behavioral intention
Intelligence Analyst Access	Independent variable and the unit of analysis identified as the who or what and is described and analyzed in this research study; relational proprieties are tacit knowledge, individual interests, values, emotions, intuition, attitudes, media exposure, age, gender, ethnicity, race, and religion
Risks To Be Taken	Dependent variable describing the level of risk to be taken under consideration by the (independent variable) Intelligence Operator moderated by the value of information and power behind information as well as moderated by the policies and directives of

	the organization; organizational portfolio conditions (independent variable) competes with the Intelligence Operator in determining the amount of risk under consideration for sharing information
Information Sharing Decision	The results of the risk to be taken decision by the Intelligence Operator is mediated by cost-benefit analysis and Intelligence Operators behavior biases; behavior biases are moderated by behavioral intentions
Type of Outcome	Dependent variable that reflects positive or negative information sharing decisions made by Intelligence Operators moderated by the cost-benefit analysis of Intelligence Operators and their behavior biases

Appendix B: Interview Guide

DESCRIPTION
1. What was your first instinct behind the analysis of your decisions?
2. How would you characterize your decision?
a) Positively **b) Negatively**
3. **How do you believe the organization would characterize your decision?**
a) Positively **b) Negatively**
4. Do you believe your decision in this scenario aligns with the organization's security and information sharing policy?
5. Does it make a difference what people you are interacting with when deciding to share information?
6. Which is more important to you? (Please explain your response.)
a) Ensuring accurate data is shared for mission accomplishment? **b) Understanding the value of the information being shared?**
7. If you identify negative actions (incidents) in sharing information that result in a desired outcome for the organization or Intelligence Community accomplishing the mission
a) What actions do you take? **b) How do you react?**
8. If you identify positive actions in sharing information that results in an undesirable outcome for the organization or Intelligence Community
a) What actions do you take? **b) How do you react?**

REFERENCES

Abbott, A. (1988). 'Transcending General Linear Reality'. *Sociological Theory*(6), 169-186.

Ahituv, N., & Carmi, N. (2007). Measuring the Power of Information in Organizations. *Human Systems Management, 26*(4), 231-246.

Ajzen, I. (2001). Attitudes. *Annual Review of Psychology, 52*, 27-58.

Ajzen, I. (2011). The Theory of Planned Behaviour: Reactions and Reflections. *Psychology & Health, 26*(9), 1113-1127. doi: 10.1080/08870446.2011.613995

Ajzen, I. (2012). Martin Fishbein's Legacy: The Reasoned Action Approach. *Annals of the American Academy of Political & Social Science, 640*(1), 11-27. doi: 10.1177/0002716211423363

Ajzen, I., & Fishbein, M. (1973). Attitudinal and Normative Variables as Predictors of Specific Behavior. *Journal of Personality and Social Psychology, 27*(1), 41-57. doi: 10.1037/h0034440

Ajzen, I., & Fishbein, M. (1970). The Prediction of Behavior from Attitudinal and Normative Variables. *Journal of Experimental Social Psychology, 6*, 466-487. doi: 10.1016/0022-1031(70)90057-0

Akbulut-Bailey, A. Y. (2011). Information Sharing Between Local and State Governments. *Journal of Computer Information Systems, 51*(4), 53-63.

Aldrich, H. E. (2001). 'Who Wants to be an Evolutionary Theorist: Remarks on the Occasion of the Year 2000 OMT Distinguished Scholarly Career Award Presentation'. *Journal of Management Inquiry, 10*(2), 115-127.

Allen, D. (2011). Information behavior and decision making in time-constrained practice: A dual-processing perspective. *Journal of the American Society for Information Science & Technology, 62*(11), 2165-2181. doi: 10.1002/asi.21601

Allport, G. W. (1935). *Attitudes*. Worcester, Mass: Clark University Press.

Allport, G. W. (1968). *The Historical Background of Modern Social Psychology* (Vol. 1). Reading, Mass: Addison-Wesley.

Ardichvill, A., Page, V., & Wentling, T. (2005). Motivation and Barriers to Participation in Virtual Knowledge Sharing Communities or Practice. *Journal of Knowledge Management, 7*(1), 64-77.

Argyris, C. (1988). *Crafting a Theory of Practice: The Case of Organizational Paradoxes*. Cambridge, MA: Ballinger.

Armitage, C. J., & Conner, M. (1999). The Theory of Planned Behaviour: Assessment of Predicitive Validity and "Perceived Control". *British Journal of Social Psychology, 38*, 35-54.

Armitage, C. J., & Conner, M. (1999a). Distinguishing Perceptions of Control From Self-Efficacy: Predicting Consumption of a Low-fat Diet Using the Theory of Planned Behavior. *Journal of Applied Social Pyschology, 29*, 72-90.

Awad, N. F., & Krishnan, M. S. (2006). The Personalization Privacy Paradox: An Empirical Evaluation of Information Transparency and the Willingness to be Profiled Online for Personalization. *MIS Quarterly, 30*(1), 13-28.

Bartunek, J. M., Rynes, S. L., & Ireland, R. D. (2006). What Makes Management Research Interesting, and Why Does It Matter? *Academy of Management Journal, 49*(1), 9-15. doi: 10.5465/AMJ.2006.20785494

Bateson, G. (1972). *Steps to An Ecology of Mind*. San Francisco: Chandler Publishing.

Benjamin, D. J., Brown, S. A., & Shapiro, J. M. (2013). "Who is Behavioral"? Cognitive Ability and Anomalous Preferences. *Journal of the European Economic Association*.

Benjamin, R. I., Rockart, J. F., Morton, M. S., & Wyman, J. (1984). Informaton Technology: A Strategic Opportunity. *Sloan Management Review, 25*(3), 3-10.

Bertot, J. C., Jaeger, P. T., & Grimes, J. M. (2010). Using ICTs to Create a Culture of Transparency: E-Government and Social Media as Openness and Anti-Corruption Tools for Societies. *Government Information Quarterly, 27*(3), 264-271.

Bettman, J. R. (1979). *An Information Processing Theory of Consumer Choice / James R. Bettman*: Reading, Mass. : Addison-Wesley Pub. Co., c1979.

Bettman, J. R., & Park, C. W. (1980). Effects of Prior Knowledge and Experience and Phase of the Choice Process on Consumer Decision Processes: A Protocol Analysis. *The Journal of Consumer Research*(3), 234. doi: 10.2307/2489009

Boudreau, M., & Robey, D. (2005). Enacting Integrated Information Technology: A Human Agency Perspective. *Organizational Science, 16*(1), 3-18.

Brinol, P., Petty, R. E., Valle, C., Rucker, D. D., & Becerra, A. (2007). The Effects of Message Recipients' Power Before and After Persuasion: A Self-Validation Analysis. *Journal of Personality and Social Psychology, 93*(6), 1040-1053.

Bruner, J. (1986). *Actual Minds, Possible Worlds*: Cambridge, MA: Harvard University Press.

Caffrey, L. (1998). *Information Sharing Between and Within Governments*. London: Commonwealth Secretariat.

Cameron, K. (1986). Effectiveness as Paradox: Consensus and Conflict in Conceptions of Organizational Effectiveness. *Management Science, 32*, 539-553.

Canada, N. (2012). The Privacy Paradox: How Personal Information has Become the Most Guarded, and Shared Currency *LoyaltyOnePrivacy-Svy*: Y.

Charmaz, K. (2010). *Constructing Grounded Theory: A Practical Guide Through Qualitiative Analysis*. Los Angeles, London, New Delhi, Singapore, Wasington DC: Sage.

Chong, A. Y., Lin, B., Ooi, K., & Raman, M. (2009). Factors Affecting the Apotion Level of C-commerce: An Empirical Study. *The Journal of Computer Information Systems, 50*(2), 13-23.

Costa-Gomes, M., Crawford, V. P., & Broseta, B. (2001). Cognition and Behavior in Normal-Form Games: An Experimental Study. *Econmetrica, 69*, 1193-1235.

Courneya, K. S., Bobick, T. M., & Schinke, R. J. (1999). Does the Theory of Planned Behavior Mediate the Relation Between Personality and Exercise Behavior? *Basic and Applied Social Psychology, 21*, 317-324.

Courneya, K. S., & McAuley, E. (1993). Predicting Physical Activity from Intention: Conceptual and Methodological Issues. *Journal of Sport and Exercise Psychology, 15*, 50-62.

Cress, U., & Kimmerle, J. (2006). Information Exchange With Shared Databse as a Social Dilemma: The Effect of Meta-Knowledge, Bonus Systems, and Costs. *Communication Research, 33*(5), 370-390.

Cresswell, A. M., Pardo, T. A., Canestrato, D. S., Dawes, S. S., & Juraga, D. (2005). *Sharing Justice Information: A Capability Assessment Toolkit*. Albany, NY: Center for Technology in Government.

Davenport, T. H., & Prusak, L. (1997). *Information Ecology: Mastering the Information and Knowledge Environment* New York: Oxford University Press.

Davis, A. S., Maranville, S. J., & Oblog, K. (1997). The Paradoxical Process of Organizational Transformation: Propositions and A Case Study. *Research in Organizational Change and Development, 10*, 275-314.

Dawes, S. S. (1996). Interagency Information Sharing: Expected Benefits, Manageable Risks. *Journal of Policy Analysis and Management*(3), 377. doi: 10.2307/3325215

Denison, D., Hooijberg, R., & Quinn, R. (1995). Paradox and Performance: Toward a Theory of Behavioral Complexity in Management Leadership. *Organization Science, 6*, 524-540.

Derlega, V. J., Metts, S., Petronio, S., & Margulis, S. T. (1993). *Self-Disclosure*. London: Sage.

Dohmen, T., Falk, A., Huffman, D., & Sunde, U. (2010). "Are Risk Aversion and Impatience Related to Cognitive Ability?". *American Economic Review*(100), 1238-1260.

Donaldson, T., & Preston, L. E. (1995). The Stakeholder Theory of the Corporation: Concepts, Evidence, and Implications. *Academy of Management Review, 20*, 65-91.

Eisenhardt, K. M., & Graebner, M. E. (2007). Theory Building From Cases: Opportunities and Challenges. *Academy of Management Journal, 50*(1), 25-32. doi: 10.5465/AMJ.2007.24160888

Eisenhardt, K. M., & Westcott, B. J. (1988). *Paradoxical Demands and the Creation of Excellence: The case of Just-In-Time Manufacturing*. Cambridge, MA: Ballinger.

Fedorowicz, J. (2009). Strategic Alignment of Participant Motivations in E-Government Collaborations: The Internet Payment Platform Pilot. *Government Information Quarterly, 26*(1), 51-59.

Feldman-Stewart, D., Brennenstuhl, S., McIssac, K., Austoker, J., Charvet, A., Hewitson, P., . . . Whelan, T. (2007). A Systematic Review of Information in Decision Aids. *Health Expectations, 10*(1), 46-61.

Fen, Y., & Sabaruddin, N. (2008). An Extended Model of Theory of Planned Behaviour in Predicting Excerise Intention. *International Business & Economics Research Journal, 1*(4), 108-122.

Firestone, W. A. (1993). Alternative Arguments for Generalizing from Data as Applied to Qualitiative Research. *Eductional Researcher, 22*(4), 16-23.

Fishbein, M., & Ajzen, I. (2005). Theory-based Behavior Change Interventions: Comments on Hobbis and Sutton. *Journal of Health Psychology, 10*(1), 27.

Flynn, F., & Chatman, J. (2001). *Strong Cultures and Innovation: Oxymoron and Opportunity?* Chichester, UK: Wiley.

Ford, J. D., & Backoff, R. W. (1988). *Organizational Change In and Out of Dualities and Paradox*. Cambridge, MA: Ballinger.

Frederick, S. (2005). Cognitive Reflection and Decision Making. *The Journal of Economic Perspectives*(4), 25. doi: 10.2307/4134953

Garson, G. D. (2004). *The Promise of Digital Government, in Digital Government: Principles and Best Practices*. Hershey, PA: Idea Group Publishing

Gibbsons, F., Gerrad, M., & Lane, D. J. (2003). A Social-Reaction Model of Adolescent Health Risk. *Social Pyschological Foundations of Health and Illness*, 165-180.

Gil-Garcia, J. R. (2012). Towards a Smart State? Inter-Agency Collaboration, Information Integration, and Beyond. *Information Polity: The International Journal of Government & Democracy in the Information Age, 17*(3/4), 269-280.

Gil-Garcia, J. R., Chengalur-Smith, I., & Duchessi, P. (2007). Collaborative E-Government: Impediments and Benefits of Information-Sharing Projects in the Public Sector. *European Journal of Information Systems, 16*(2), 121-133.

Gil-Garcia, J. R., Soon Ae, C., & Janssen, M. (2009). Government Information Sharing and Integration: Combining the Social and the Technical. *Information Polity: The International Journal of Government & Democracy in the Information Age, 14*(1/2), 1-10. doi: 10.3233/IP-2009-0176

Gittell, J. H. (2004). Paradox of Coordination and Control. *California Management Review, 42*(3), 101-117.

Hampden-Turner, C. (1981). *Maps of the Mind*. New York: Macmillian.

Handy, C. (1994). *The Age Of Paradox*. Cambridge, MA: Harvard Busiess School Press.

Harris, A. S. (1996). *Living With Paradox: An Introduction to Jungian Psychology*. Albany, NY: Brooks/Cole.

Hislop, D. (2002). Mission impossible? Communicating and Sharing Knowledge via Information Technology. *Journal of Information Technology (Routledge, Ltd.), 17*(3), 165-177. doi: 10.1080/02683960210161230

Hodgkinson, G. P., Sadler-Smith, E., Burke, L. A., Claxton, G., & Sparrow, P. R. (2009a). Intuition in Organizatons: Implications for Strategic Management. *Long Range Planning, 42*(3), 277-297.

Javernpaa, S. L., & Staples, D. S. (2000). The Use of Collaborative Electronic Media for Information Sharing: An Exploratory Study of Determinants. *Journal of Strategic Information Systems*(9), 129-154.

Jhingram, A. D., Mattos, N., & Pirahesh, H. (2002). Information Integration: A Research Agenda. *IBM Systems Journal, 41*(4), 555-562.

JinKyu, L., Nitesh, B., Jing, Y., Marijn, J., & Rao, H. R. (2010). Group Value and Intention to Use — A Study of Multi-Agency Disaster Management Information Systems for Public Safety. *Decision Support Systems, 50*, 404-414. doi: 10.1016/j.dss.2010.10.002

John, L., Boardman, J., & Sauser, B. (2008). Leveraging Paradox in Systems Engineering: Discovering Wisdom. *Information Knowledge Systems Management*(7), 357-376.

John, L. K., Acquisti, A., & Loewenstein, G. (2011). Strangers on a Plane: Context-Dependent Willingness to Divulge Sensitive Information. *Journal of Consumer Research, 37*(5), 858-873. doi: 10.1086/656423

Kidwell, B., & Jewell, R. (2008). The Influence of Past Behaviour on Behavioral Intent - An Information-Processing Explanation. *Psychology & Marketing, 25*(12), 1151-1166.

Klein, H. K., & Myers, M. D. (1999). A Set of Principles for Conducting and Evaluating Interpretive Field Studies in Information Systems. *MIS Quarterly*(1), 67. doi: 10.2307/249410

Koot, W., Sabelis, I., & Ybema, S. (1996). *Epilogue*. Amsterdam: VU University Press.

Kor, K., & Mullan, B. A. (2011). Sleep Hygiene Behaviours: An application of the Theory of Planned Behaviour and the Investigator of Perceived Autonomy Support, Past Behavior and Response Inhibition. *Psychology & Health, 26*, 1208-1224.

Korniotis, G. M., & Kumar, A. (2011). "Do Older Investors Make Better Investment Decisions?". *Review of Economics and Statisitics, 93*, 244-265.

Landsbergen, D. J., & Wolken, G. J. (2001). Realizing the Promise: Government Information Systems and the Fourth Generation of Information Technology. *Public Adminstration Review, 61*(2), 206-220.

Larence, E. R. (2008). *Information sharing [electronic resource] : Definition of the results to be achieved in terrorism-related information sharing is needed to guide implementation and assess progress : testimony before the Committee on Homeland Security and Governmental Affairs, U.S. Senate / statement of Eileen R. Larence*: [Washington, D.C.] : U.S. Govt. Accountability Office, [2008].

Laudon, K. C. (1996). Markets and Privacy. *Communications of the ACM, 39*(9), 92-104.

Lewis, M. W. (2000). Exploring Paradox: Toward a More Comprehesive Guide. *Academy of Management Review, 25*, 760-776.

Lincoln, Y. S., & Guba, E. G. (1985). *Naturalistic Inquiry*. Newbury Park, CA: Sage Publications, Inc.

Lips, A. M. B., O'Neill, R. R., & Eppel, E. A. (2011). Cross-Agency Collaboration in New Zealand: An Empirical Study of Information Sharing Practices, Enablers and Barriers in Managing for Shared Social Outcomes. *International Journal of Public Administration, 34*(4), 255.

Luna-Reyes, L. F. (2010). *Digital Government in North America: A Comparative Analysis of Policy and Program Priorities in Canada, Mexico, and the United States in Comparative E-Government*. New York: Springer.

Luna-Reyes, L. F. & Gil-Garcia, J. R. (2003). "E-Government Security, Privacy and Information Access: Some Policy and Organizational Trade-offs". In *international conference on public participation and information technologies* (pp. 10-12).

Luna-Reyes, L. F., Gil-Garcia, J. R., & Cruz, C. B. (2007). Collaborative Digital Government in Mexico: Some Lessons From Federal Web-Based Interorganizational Information Integration Initiatives. *Government Information Quarterly, 24*(4), 808-826. doi: 10.1016/j.giq.2007.04.003

Luo, X. D., Zhang, C. Q., & Leung, H. F. (2001). Information Sharing Between Heterogeneous Uncertain Reasoning Models in a Multi-Agent Environment: A Case Study. *International Journal of Appoximate Reasoning, 27*(1), 27-59.

Majchrzak, A., Rice, R., Malhotra, A., King, N., & B., S. (2000). "Technology Adaptation: The Case of a Computer-Supported Inter-Organizational Virutal Team". *MIS Quarterly, 24*(4), 569-600.

Manning, M., & Bettencourt, B. A. (2011). Depression and Medication Adherence Among Breast Cancer Survivors: Bridging the Gap With the Theory of Planned Behaviour *Psychology & Health, 26*, 1188-1207.

Markus, H., & Kitayama, S. (1991). Culture and the Self: Implications for Cognition, Emotion and Motivation. *Psychological Review, 48*, 268-305.

Mason, J. (2002). *Qualitative Researching* (Second ed.). Thousand Oaks, Califrornia: Sage Publications.

McClintock, C. G. (1978). Social Values: Their Definition, Measurement and Development. *Journal of Research and Development in Education, 12*, 121-137.

McKinney Jr, E. H., & Yoos Ii, C. J. (2010). Information About Information: A Taxonomy of Views. *MIS Quarterly, 34*(2), 329-A325.

Messick, D. M., & McClintock, C. G. (1968). Motivational Bases of Choice in Experimental Games. *Journal Of Experimental Social Psychology, 4*, 1-25.

Miles, M. B., & Huberman, A. M. (1994a). *Qualitative Data Analysis* (Second ed.). Thousand Oaks, CA: Sage Publications

Miles, M. B., & Huberman, A. M. (1994b). *Qualitative Data Analysis : An Expanded Sourcebook / Matthew B. Miles, A. Michael Huberman* (Vol. 2nd ed.). Thousand Oaks: Sage Publications.

Miranda, S. M. S. C. S. (2003). The Social Construction of Meaning: An Alternative Perspective on Information Sharing. *Information Systems Research, 14*(1), 87-106.

Mohr, L. (1982). *Explaining Organizational Behavior*. San Francisco: Jossey-Bass.

Murnighan, J. K., & Conlon, D. E. (1991). The Dynamics of Intense Work Groups: A Study of British String Quartets. *Administrative Science Quarterly, 36*, 165-186.

Navarrete, C. (2009). *Information Sharing at National Borders: Extending the Utility of Border Theory*. Paper presented at the 42nd Hawaii International Conference on System Sciences (HICSS), Waikoloa, Big Island, Hawaii.

Neisser, U. (1967). *Cognitive psychology*: New York, Appleton-Century-Crofts [1967].

Newell, B., & Broder, A. (2008). Cognitive Processes, Models, and Metaphors in Decision Research. *Judgement and Decision Making, 3*(3), 195-204.

Newman, J. (2001). "Some Observations on the Semantics of 'Information'". *Information Systems Frontiers, 3*(2), 155-167.

Otjacques, B., Hitzelberger, P., & Feltz, F. (2007). Interoperability of E-Government Information Systems: Issues of Identification and Data Sharing. *Journal of Management Information Systems, 23*(4), 29-51.

Ouellette, J., & Wood, W. (1998). Habit and Intention in Everyday Life: The Multiple Processes by Which Past Behaviour Predicts Future Behaviour. *Psychological Bulletin, 124*, 54-74.

Pardo, T. A., Cresswell, A. M., Thompson, F., & Zhang, J. (2006). Knowledge Sharing in Cross-boundary Information System Development in the Public Sector. *Information Technology and Management, 7*(4), 293-313.

Pardo, T. A., & Tayi, G. K. (2007). Interorganizational Information Integration: A Key Enabler for Digital Government. *Government Information Quarterly, 24*(4), 691-715.

Pentland, B. (1999). 'Building Process Theory with Narrative: From Description to Explanation'. *Academy of Management Review*(24), 711-724.

Petronio, S. (2000). *"The Boundaries of Privacy: Praxis of Everyday Life"* (Vol. 37). Mahwah, NJ: Elbaum.

Poole, M. S. (1983). 'Decision Development in Small Groups, III: A Multiple Sequence Model of Group Decision Development'. *Communications Monographs*(50), 321-341.

Posner, R. A. (1981). "The Economics of Privacy". *American Economic Review, 71*(2), 405-409.

Quinn, R. E., & Cameron, K. S. (1988). *Paradox and Transformation : Toward a Theory of Change in Organization and Management / edited by Robert E. Quinn, Kim S. Cameron*: Cambridge, Mass. : Ballinger Pub. Co., c1988.

Reddick, C. G. (2009). The Adoption of Centeralized Customer Service Systems: A Survey of Local Governments. *Government Information Quarterly, 26*(1), 219-226.

Reese, H., & Overton, W. F. (1978). *Models of Development and Theories of Development*. New York: Academic.

Rhodes, R. E., & Courneya, K. S. (2003). Relations Between Personality, an Extended Theory of Planned Behavior Model and Exercise Behavior. *British Journal of Health Psychology, 8*, 19-36.

Richardson, S., & Asthana, S. (2006). Inter-agency Information Sharing in Health and Social Care Services: The Role of Professional Culture. *British Journal of Social Work*, 657-669.

Rivis, A., Sheeran, P., & Armitage, C. J. (2011). Intention Versus Identification as Determinants of Adolescents' Health Behaviours: Evidence and Correlates. *Psychology & Health, 26*, 1128-1142.

Rosenfeld, L. B. (2000). *"Introduction to Secrets of Private Disclosures"* (Vol. 1). Mahwah, NJ: Erlbaum.

Rothenberg, A. (1979). *The Emerging Goddess*. Chicago: University of Chicago Press.

Russell, B. (1970). *The Problems of Philosophy*. London ; New York : Oxford University Press.

Savolainen, R. (2006). Time as a Context of Informaton Seeking. *Library & Information Science Research, 28*(1), 110-127.

Schneider, K. J. (1990). *The Paradoxical Self: Toward an Understanding of Our Contradictory Nature*. New York: Insight Books.

Schooley, B. L., & Horan, T. A. (2007). Towards End-to-End Government Performance Management: Case Study of Interorganizational Information Integration in Emergency Medical Services (EMS). *Government Information Quarterly, 24*(4), 755-784.

Sheeran, P., Orbell, S., & Norman, P. (1999). Evidence That Intentions Based on Attitudes Better Predict Behaviour than Intentions Based on Subjective Norms. *European Journal of Social Psychology, 29*, 403-406.

Sinclair, M., & Ashkanasy, N. M. (2005). Intuition: Myth or a Descision Making Tool. *Management Learning, 36*(3), 353-370.

Sitkin, S., & Bies, R. J. (1993). The Legalistic Organization: Definitions, Dimensions, and Dilemmas. *Organization Science, 4*, 345-351.

Smith, J. R., Manstead, A., Terry, D., & Louis, W. (2007). Interaction Effects in the Theory of Planned Behaviour: The Interplay of Self-Identity and Past Behaviour. *Journal of Applied Social Pyschology, 37*(11), 2726-2750.

Smith, K., & Berg, D. (1987). *Paradoxes of Group Life*. San Francisco: Josey-Bass.

Smith, W. K., & Lewis, M. W. (2011). Toward a Theory of Paradox: A Dynamic Equilibrium Model of Organizing. *Academy of Management Review, 36*(2), 381-403. doi: 10.5465/AMR.2011.59330958

Sommer, L. (2011). The Theory of Planned Behaviour and the Impact of Past Behaviour. *International Business & Economics Research Journal, 10*(1), 91-110.

Sutton, S. (1998). Predicting and Explaining Intentions and Behavior: How Well Are We Doing? *Journal of Applied Social Pyschology, 28*, 1317-1338.

Trafimow, D., & Finlay, K. A. (1996). The Importance of Subjective Norms for a Minority of People: Between-Subjects and Within-Subjects Analyses. *Personality and Social Psychology Bulletin, 22*, 820-828.

Tsoukas, H. (2005). *Complex Knowledge: Studies in Organizational Epistemology*. Oxford: Oxford University Press.

Van de Ven, A. H. (1992). 'Suggestions for Studying Strategy Process: A Research Note'. *Strategic Management Journal*(13), 169-188.

Van de Ven, A. H. (2007a). *Engaged Scholarship : A Guide for Organizational and Social Research / Andrew H. Van de Ven*: Oxford ; New York : Oxford University Press, 2007.

Van de Ven, A. H. (2007b). *Engaged Scholarship: A Guide for Organizational and Social Research*. Oxford: Oxford University Press.

Van de Ven, A. H., & Poole, M. S. (1995). Explaining Development and Change in Organizations. *Academy of Management. The Academy of Management Review, 20*(3), 510-540.

Van Marrewijk, A., Clegg, S. R., Pitsis, T. S., & Veenswijk, M. (2008). Managing Public-Private Megaprojects: Paradoxes, Complexity, and Project Design. *International Journal of Project Management, 26*, 591-600.

Vince, R., & Broussine, M. (1996). Paradox, Defense and Attachment: Accessing and Working with Emotions and Relations Underlying Organizational Change. *Organization Studies, 17*, 1-21.

Wartzawick, P., Weakland, J. H., & Fisch, R. (1974). *Change: Principles of Problem Formation and Problem Resolution*. New York: Norton.

Wenjing, L. (2011). Government Information Sharing: Principles, Practice, and Problems — An International Perspective. *Government Information Quarterly, 28*(3), 363-373. doi: 10.1016/j.giq.2010.10.003

Westenholz, A. (1993). Paradoxical Thinking and Change in Frames of Reference. *Organizational Studies, 14*, 37-58.

Wheatley, M. J. (2006). *Leadership and the New Science: Discovering Order in a Chaotic World*. San Francisco, CA: Berrett-Koehler Publishers.

White, T. B. (2004). Consumer Disclosure and Disclosure Avoidance: A Motivational Framework. *Journal of Consumer Psychology, 14*(1-2), 41-51.

Yang, T.-M., & Maxwell, T. A. (2011). Information-Sharing In Public Organizations: A Literature Review Of Interpersonal, Intra-Organizational and Inter-Organizational Success Factors. *Government Information Quarterly, 28*(2), 164-175. doi: 10.1016/j.giq.2010.06.008

Yin, R. K. (2009). *Case Study Research : Design and Methods / Robert K. Yin*: Los Angeles, Calif. : Sage Publications, c2009.

Zhang, D. Y., Zeng, Y., Wang, L., Li, H., & Geng, Y. (2011). Modeling and evaluating information leakage caused by inferences in supply chains. *Computers in Industry, 62*(3), 351-363. doi: 10.1016/j.compind.2010.10.002

Zhang, J., Dawes, S. S., & Sarkis, J. (2005). Exploring Stakeholders' Expectations of the Benefits and Barriers of E-Government Knowledge Sharing. *Journal of Enterprise Information Management, 18*(5), 548-567.

.