Competitive Intelligence and Information Quality: A Game-Theoretic Perspective

DOV BIRAN, Fitango, Inc.
MICHAEL H. ZACK, Northeastern University
RICHARD J. BRIOTTA, Bay Path College

To better understand a competitor's tactical and strategic plans, companies need to take a closer look at competitive intelligence or they risk missing lucrative opportunities. Because of this there is a growing interest in competitive intelligence and intelligence information gathering systems (IIS). This article uses game-theoretic concepts to develop an analytic framework to assess the value of deploying a competitive intelligence gathering information system. Modeling the competitive environment as a game provides a useful approach to study and evaluate competitive strategies given diverse assumptions about the quality of the information known by the players. When determining the value of deploying an IIS, decision makers need to examine three components of the competitive environment: the competitive rules of the game, the state of player knowledge, and the reliability of the information gathered. This framework focuses on competitive environments where the players' state of knowledge (i.e., common versus covert knowledge) and the reliability of the information generated are essential to the decision making process. The article concludes with implications for research and practice.

Categories and Subject Descriptors: H [**Information Systems**]: H1.2 [**User/Machine Systems**]: Human factors, Human information processing

General Terms: Management, Theory, Reliability, Measurement

Additional Key Words and Phrases: Game theory, competitive strategy, knowledge management, competitive intelligence, intelligence information gathering systems, strategic knowledge management

ACM Reference Format:
Biran, D., Zack, M. H., and Briotta, R. J. 2013. Competitive intelligence and information quality: A game-theoretic prespective. ACM J. Data Inf. Qual. 4, 3, Article 12 (May 2013), 20 pages.
DOI: http://dx.doi.org/10.1145/2458517.2458520

1. INTRODUCTION

Imagine that you are a senior executive with a company in the highly competitive consumer-packaged goods industry. Your organization and your primary competitor are trying to determine whether or not to launch a similar new product. Your product introduction process and timing may look very different depending on whether, when, where, and how your competitor launches its product. What you know about your opponent (including what you think your opponent knows about you) may change your decisions and actions regarding your own launch significantly. What would it be worth to have access to reliable information enabling you to learn about your competitor's decision?

Authors' addresses: D. Biran, Fitango, Inc.; M. H. Zack, Northeastern University, Boston, MA; R. J. Briotta (corresponding author), Bay Path College, Longmeadow, MA; email: rbriotta@baypath.edu.

DOI: http://dx.doi.org/10.1145/2458517.2458520

Interest in competitive intelligence has increased dramatically as a direct result of increasing competition, and improved technical capabilities for gathering this information [Shing and Spence 2002; Metayer 1999]. Directing business intelligence efforts towards gathering useful information about competitors is seen increasingly as a means of securing competitive advantage [Boatright 2000; Weinberg and Montgomery 1979]. For example, when Motorola, Inc., won a $146 million mobile telecom contract in China during year 2000, it was due, in no small part, to the efforts of the company's business intelligence group [Arensmann 2001].

In this article we develop an analytical framework for assessing the value of a competitive intelligence gathering information system (IIS) using game theory [Harsanyi 1994, 1967; Luce and Raiffa 1957; Mertens and Zamir 1971; Ponssard 1976]. We model our information system after McGuire and Radner's notion of an "information structure" and show how this formulation can be used within a game-theoretic setting to establish the value of a strategic intelligence gathering capability as a function of the quality of the information it generates [McGuire 1972]. An information system, in these terms, is synonymous with the information it generates, rather than with the technology itself. By integrating this formulation for information into a game-theoretic framework, we are able to model a key aspect of information quality, namely the reliability of the information. We subsequently use this model to propose how to evaluate the effect of reliability on the value of that information.

Our contribution is twofold. First we believe that game theory has been underutilized by the information management field, yet we believe it offers a useful framework for assessing the value of information. Second we propose a relaxation of the traditional assumption in game theory that decisions and actions are simultaneous. By separating decision making and action, we provide the ability to analyze the impact of using an intelligence gathering capability to learn about a competitor's decision while preserving the ability to make a countervailing strategic decision prior to the implementation of the decisions.

Harsanyi [1994] states that "[g]ame [t]heory is a theory of strategic interaction. That is to say it is a theory of rational behavior in social situations in which each player has to choose his moves on the basis of what he thinks the other player's countermoves are likely to be". Here "games" are an analytical formalism used to represent competitive situations, specified in terms of the overall payoff to the competitors resulting from the combinations of strategies they and their opponents may choose, and the nature of their respective knowledge regarding the game. As such, game theory provides a natural framework for linking information, knowledge, information systems, and competitive advantage [Brandenburger and Nalebuff 1995]. It further provides an analytical framework for defining the economic value of a strategic knowledge management system [Krieble and Moore 1982]. Our aim is to demonstrate the potential usefulness of this framework by illustrating the kinds of issues and questions that it addresses for both practitioners and researchers regarding strategic knowledge gathering systems [Postrel 1991].

Our framework posits that competitive games occur within some state of knowledge among competitors, and that an IIS may be used to predict, with some arbitrary level of reliability, the strategies chosen by competitors. Decisions about investing in an IIS require the simultaneous consideration of: (1) the competitive rules of the game, (2) the quality and reliability of the information provided by the IIS, and (3) the state of participant knowledge.

In the following section we describe the links among knowledge and strategy, and we establish the value of competitive intelligence as an important strategic aspect of KM. In subsequent sections, we discuss game theory and its relationship to knowledge, strategy, and information systems. We present a specific game-theoretical framework for defining and assessing an IIS, and frame the use of an IIS within the state of knowledge of a competitive game. We illustrate our framework with a numerical example and conclude with implications for future research and for managerial decision making regarding investing in this information gathering capability.

2. KNOWLEDGE AND STRATEGY

The term knowledge is often treated as being synonymous with information. We draw a distinction between them. Zack [1999] presents it as follows.

> Knowledge is commonly distinguished from data and information. Data represent observations or facts out of context, and therefore not directly meaningful. Information results from placing data within some meaningful context, often in the form of a message. Knowledge is that which we come to believe and value based on the meaningfully organized accumulation of information (messages) through experience, communication or inference. Knowledge can be viewed both as a *thing* to be stored and manipulated and as a *process* of simultaneously knowing and acting—that is, applying expertise. As a practical matter, organizations need to manage knowledge both as object *and* process.

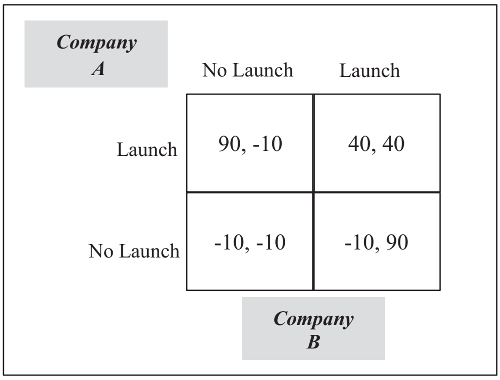
Although KM in general, and intelligence gathering systems in particular, are assumed "strategic" and to offer competitive advantage, little has been written to explain or show evidence of why this is so. In fact, practitioners of KM rarely specify strategy or competitive advantage as either a motivator or success metric regarding their own KM initiatives [Zack 1999]. KM can be linked to competitive advantage, however, by focusing on the strategic value of knowledge [Zack 1999]. The argument is that if knowledge is strategic, then managing it effectively should provide a competitive advantage, and keeping the knowledge fresh via organizational learning should sustain this advantage.

The study and practice of strategy over the past four decades has been grounded by the SWOT (Strengths/Weaknesses/Opportunities/Threats) framework [Andrews 1971]. This framework proposes that strategy is the process of choosing competitive positions that provide opportunities to leverage an organization's strengths while avoiding its weaknesses and minimizing competitive threats.

Strategy, then, comprises both internal and external dimensions that must be kept in balance over time, and which create particular knowledge requirements. Initially, one must focus on the external perspective, the organization's competitive environment, and decide on a distinctive value proposition within the industry and then shift perspective to the internal side and tailor one's organizational activities toward accomplishing this value proposition [Porter 2000]. The internal perspective focuses on the decisions and actions necessary to execute a competitive strategy. A change in competitive strategy, strategic positioning, requires not only a change in strategy but also a change in the knowledge necessary to implement the new position [Zack 2005, 1999].

An effective strategic KM capability aligns an organization's internal operating knowledge with external knowledge about its competitive environment[1]. Most KM efforts, however, have focused primarily on internal knowledge gaps (and often those that are not strategic). Little attention has been paid to the external side of the knowledge-strategy equation. While business intelligence has been functioning in many organizations for years, it suffers by rarely being integrated with the "mainstream" internal KM efforts of an organization, thus preventing the organization as a whole from closing the strategy loop. Our objective is to redress this imbalance by providing a framework for assessing the value of investing in the external side of strategic KM.

[1] Our use of the term competitive environment is equivalent to the game-theoretic notion of a competitive field.



Company A	No Launch	Launch
Launch	90, -10	40, 40
No Launch	-10, -10	-10, 90

Company B

Fig. 1. An example of a competitive game.

3. THE RULES OF THE GAME

Game theory, introduced by von Neumann and Morgenstern [1947], is the study of how strategic interactions among rational players (e.g., competitors) produce outcomes with respect to the preferences (or utilities) of these players. The theory is an analytical formalism for describing situations of mutual conflict or competition in terms of the value or payoff of a particular combination of strategies among players. Its key contribution is that it shifts the notion of the economic value of strategy from an inward focus to one that takes others' potential actions into account [Brandenburger and Nalebuff 1995]. If the outcome of a player's decision depends on an opponent's knowledge and the predictions that an opponent might make from it, then for a player to make future-oriented strategic decisions, the player needs to know what the opponent knows, part of which is what the opponent knows about what the player knows, and so on [Brandenburger and Binmore 1990]. Thus the strategy of an organization is inextricably entwined in the knowledge and strategies of its competitors.

While originally applied to military strategy [Smith 1996], game theory has been usefully applied to business strategy as well [Brandenburger and Nalebuff 1995]. We illustrate the formalism with a simple example of a *competitive* game, the focus of our discussion (Figure 1). Games can be formally represented as a matrix where each cell represents the payoff resulting from the intersection of the independent choices of the players. Competitive games comprise self-interested players seeking to understand their opponents' intentions so that they may choose a strategy that maximizes their own payoff. As player actions are based on assumptions about the knowledge held or not held in common among competitors regarding the nature of their competition [Brandenburger and Binmore 1990], the ability to affect this balance of knowledge directly affects the outcome of the game and therefore the value of a particular chosen strategy. Game theory is therefore directly tied to information systems, as the ability to access information regarding the state of the game, especially regarding competitors, is an integral part of playing the game [Biran 1991].

Consider again the two competing consumer goods manufacturers contemplating a new product launch. Assume that each company has two possible strategies it can execute: launch or no launch. Further assume that each invests $10 million to develop the product regardless of whether it launches or not, and that the total market for the products is $100 million to be realized in full by one company if only one launches its product, and to be split evenly if both launch. The payoff to each company therefore depends on the joint actions of both companies. If only one launches its new product, it enjoys the $100 million market less its 10 million investment for a net payoff of

$90 million, while its competitor merely absorbs the $10 million cost of the investment. If neither launches, both suffer the $10 million expense and no revenue. If both launch, they each realize $50 million less their $10 million expense for a net of $40 million.

As the payoff from any strategy depends on the actions of the competitors, making a decision depends on being able to predict their actions; and this predictive ability is subject to one's knowledge of the game. From this perspective knowledge can be of two types: (1) unique, possessed by only one competitor; and (2) common, shared by all competitors. When both competitors know the structure of the game (i.e., the payoff matrix) and both know that the other knows, and both know that the other knows that they know, and so on, ad infinitum, then we have common knowledge and the game can be easily "solved." (We address the implications of unique knowledge in later sections.)

In the example in Figure 1, both companies A and B have common knowledge of the game. Each knows the payoffs to each combination of strategies. From B's perspective, if A launches the new product, then the best action (i.e., the one with the greatest payoff) is for B to launch as well; if A does not launch, then the best action for B is still to launch. In the example case, A and B's perspectives are identical and as such the choice to launch dominates all other choices.

Knowing that both of A and B know that they should launch under any and all circumstances provides the "solution" to the game. This is an example of what is referred to as a pure strategy Nash equilibrium game. That is, there is no need for one player to guess the probability of the other player choosing between strategies, because in all cases there is a pure strategy that makes sense for a rational player to choose. In this case, investing in an information system to reveal a competitor's strategy would have no value, as everything each competitor needs to know about the other is already included in the game itself, that is, it is common knowledge. In most real-world situations, however, the mutual payoffs are not as symmetrical and straightforward. Typically, the best strategy is found by computing a weighted average of the payoffs based on the probability of an opponent choosing among its available strategies. This is referred to as a mixed strategy game and is similar to using a decision tree to compute the expected payoff of some set of actions, with each action being assigned a probability of generating this payoff.

Having or not having common knowledge can directly affect the outcome of the game. Knowledge provides an ability to predict the other player's actions, and an ability to determine the overall payoff to all players of the game (assuming some notion of rationality among the players). If a player were to have unique knowledge (i.e., noncommon knowledge) about the game and about her opponents, this player might have an ability to exploit the game for her own benefit, subject to the reliability of the predictions concerning the strategies chosen by the opponents. This begs the question, what would it be worth to be able to learn, with some arbitrary degree of reliability, what strategy your opponent has chosen?

We now add another level of complexity to the formalism by introducing two modifications, each of which reflects a more real-world context and provides a basis for attributing value to having an intelligence gathering capability. The first assumes a mixed strategy game, where equilibrium value (expected payoff) of a game is realized by weighting (mixing) the strategies available to each of the participants. There is no clear, dominant strategy, therefore players have strategic choices, and learning about a competitor's decision may have value. Second, if instead of assuming that each side chooses its strategy simultaneously, as implied before, we view the decision making process as a set of sequential stages, then a player has an opportunity, using an IIS, to discover its opponent's chosen strategy before executing its own and thus change the equilibrium value of the game. We adopt Simon's [1945] formulation that intelligence (i.e., information gathering) precedes design (i.e., creation of strategic alternatives),

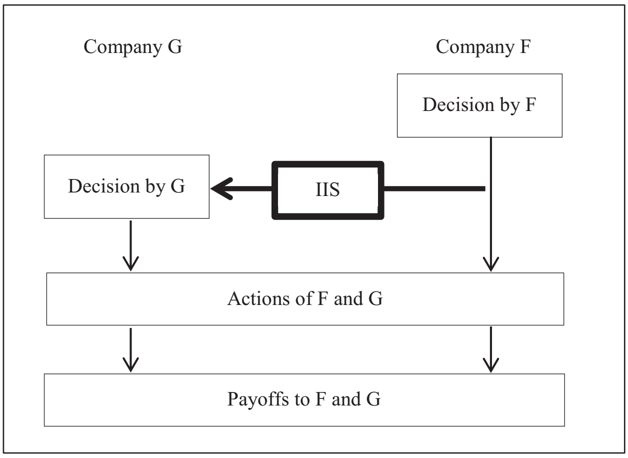


Fig. 2. Stages of the game when using an IIS, assuming the separation of decisions from actions.

which in turn precedes choice (i.e., implementation). To examine the implications of using an IIS to reveal the opponent's decision, we could calculate the equilibrium value of the game with and without this capability. The difference between the value of the competitive game with and without an IIS represents the value of the IIS (e.g., Neave and Wiginton [1976]).

4. THE COMPETITIVE INTELLIGENCE GAME: A FORMAL ROLE FOR AN IIS

IIS in competitive situations. In a competitive game without an IIS, the decisions and actions taken by the opponents are made a priori based on the payoff matrix and other characteristics of the competitive game. In competitive games with an IIS, there are two categories of knowledge components that have the potential to directly affect the value of the competitive game: (1) the existence and use of the IIS and (2) the reliability of the information generated by the lIS[2] [Biran 1991].

To explore the implications of using an IIS, we need to separate players' decisions from the simultaneous actions taken by the players. This separation enables a player to use the IIS-generated information concerning a competitor's decision prior to making her own strategic decision. Figure 2 illustrates a game where there is the potential for one competitor, G, using an IIS to delay her decision until after she has collected information about F's decision. It is interesting to note that F may have made a different decision if she had prior knowledge of G's ability to employ an IIS. In this example, G ("the offender") may or may not take the offensive by using its IIS against F ("the defender"). We denote this potential offensive use of an IIS by G on F as G → F.

Having separated player decisions from actions has changed the traditional simultaneous decision-action rules of the game and in order to present and discuss the different knowledge states possible in competitive situations we assume the following sequence of events.

(i) F selects its strategy.
(ii) G may activate an IIS to acquire information about F's decision.
(iii) G selects its strategy.

[2] Note that the opponent may have several IISs, however, for simplicity in building the conceptual framework, we limit ourselves to the case of a single IIS.

$$\begin{array}{cccc} & \begin{array}{cc} \multicolumn{2}{c}{\text{Actual}} \\ \text{Intro} & \text{No Intro} \end{array} & & \\ \phi_{G\to F} = & \left(\begin{array}{cc} .8 & .1 \\ .2 & .9 \end{array}\right) & \begin{array}{l} \text{Intro} \\ \text{No Intro} \end{array} & \text{Signal} \end{array}$$

Fig. 3. Matrix of probabilities.

(iv) F and G simultaneously execute their decisions made in phases (i) and (iii) respectively.
(v) Both receive their payoffs based on a payoff matrix (as in Figure 1).

An important competitive aspect of this game is whether or not the use and reliability of the IIS is common knowledge. Note that in this example the preceding sequence of events is considered to be common knowledge; however, this does not imply that all players possess the same knowledge of the use and/or reliability of the IIS. As we will explore later, different states of F's knowledge about G's IIS represent different game situations with different values. Hence our discussion will focus on how strategic decisions are impacted by the knowledge each competitor has about the IIS and the knowledge they have about each other's knowledge.

The reliability of an IIS refers to both the predictive accuracy of the information regarding a defender's strategic decision and the degree to which the defender knows how the offender interprets the information to predict the defender's propensity to choose a particular strategy. This is represented in our model as the ability of an offender to predict a defender's actions from the intelligence information garnered by the IIS[3].

Due to noise, uncertainty, and inadequate knowledge in interpreting signals, intelligence systems are not 100% reliable. For example, given two possible strategies {1 and 2} for F, the signal could suggest strategy 1, when F is actually taking strategy 1 or could suggest strategy 1 when F is actually taking strategy 2. Similarly, if F actually chose strategy 2, the signal might indicate strategy 1 or strategy 2. Therefore, the IIS potentially used by G on F's decision space will generate a particular signal (or informative message) for each strategy chosen by F, with some probability of this message being correct.

We can represent the reliability characteristics of the IIS as a matrix of probabilities (see Figure 3), with the signal received on one axis and the actual strategy chosen on the other. Each cell of the matrix contains the probability of receiving the signal indicating a particular strategy, given the strategy the competitor actually chose. In the example that follows, each cell would contain the contingent probability of receiving a particular

[3] Intelligence comprises two primary activities: (1) collection of information and (2) analysis of this information. While we have referred to one aspect of reliability, in actuality we can think of reliability as comprising two stages: the reliability of the IIS signal and the reliability of the interpretation of that signal. For simplicity, we have assumed that signals (correct or not) are faithfully interpreted. However, as signals become more complex or ambiguous, the ability to interpret them becomes less precise and reliable [Zack 2001], thus we could define another (α') that refers to the reliability of the interpretation of the signal. Modeling the impact of α' is beyond the scope of this article.

Table I. Probability of Occurrence

F's Decision	Signal Received by G's IIS indicates:	Probability of Occurrence
Introduce the new product	"F is introducing new product"	.8
	"F is not introducing new product"	.2
Not introduce the new product	"F is introducing new product"	.1
	"F is not introducing new product"	.9

signal (e.g., 1) given the actual strategy chosen, 1 or 2. The signal characteristics or "reliability" of the IIS $\phi_{G\rightarrow F}$ can be summarized as shown in Figure 3.

So, for example, the probability of G receiving an "introduction" signal when F is actually planning "not to introduce" is 0.1. We refer to the matrix of values $\phi^{G\rightarrow F}$ as the IIS structure, or the IIS for short, and we say that an opponent "knowing" the IIS is equivalent to knowing the reliability matrix of the IIS.

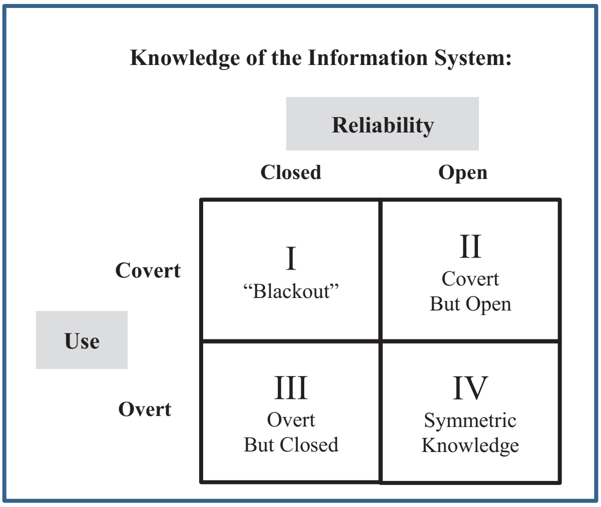
The reliability of an IIS falls on a continuum ranging from complete fidelity to complete inaccuracy. The best possible IIS is one that perfectly and completely maps the offender's decisions to the signal (i.e., the probabilities in the matching diagonal of matrix $\phi^{G\rightarrow F}$ are 1 and the probabilities of the other cells are 0). The notion of "worst" IIS is not as straightforward. As the reliability of an IIS decreases, the entropy of its signal set increases until the point at which the probability of a signal mapping to any strategy is equal across all strategies (e.g., in the previous case, all probabilities in the IIS are 0.5). That is, the signal tells the decision maker nothing, and the IIS has no value. Even an IIS that consistently maps signals to events incorrectly offers more information. From that point on, as the reliability decreases, assuming consistency, the value of the system actually increases. For example, if every time an opponent chooses strategy B the system signals strategy A, then this provides as much information as a perfectly accurate IIS. Achieving this state, however, requires a repeating situation that allows for learning over time.[4]

To illustrate a situation similar to that in Figure 3, let us assume that two cell phone companies, F and G, are competing on gaining market share and that F has a new product for elementary school pupils and has decided on one of two potential actions: {Introduce New Product, Do not Introduce New Product}. Assume that G is using a "noisy" IIS to gather intelligence about F's decision and that the IIS may transmit with some degree of probability for either decision, one of two possible signals, as shown in Table I.

We can generalize this situation by formally describing an IIS used in a competitive situation as a Markovian stochastic matrix of dimension $n_F \times n_F$, where n_F is the number of potential pure strategies available to F [Marschak and Radnor 1971; McGuire 1972]. In Figure 3, the matrix would be of dimension 2×2. Each cell of the matrix includes the contingent probabilities of receiving a particular signal y_j from a finite group of signals Y, where $Y = \{y_1, \ldots\ldots y_{nF}\}$ and j indicates the particular signal received out of n_F possible signals, for each chosen strategy (s^k) of company F. We designate each of the contingent probabilities of receiving signal y_j given strategy k as, $\phi_{G\rightarrow F_{J,K}}$ and the probabilities of all the possible signals for a given strategy must total 1 (meaning that we have accounted for all the possible signals, accurate or not, that could be received given a particular strategy). Formally stated,

$$\phi_{G\rightarrow F_{J,K}} = p\{y_j | s^k\}, \text{ where} \sum_{j=1}^{n_F} \phi_{j,k} = 1, \phi_{j,k} \geq 0, \text{ for each } s^k \in S^F,$$

[4] Note that the case of double, triple, etc., agents who strategically and intentionally employ the use of misinformation is beyond the scope of the article. Our assumption is that all secret agents are faithful.



		Closed	Open
Use	Covert	I "Blackout"	II Covert But Open
	Overt	III Overt But Closed	IV Symmetric Knowledge

Fig. 4. The knowledge states matrix.

where s^k is the k$^{\text{th}}$ strategy of player F. In the case where F has only two potential actions (i.e., j, $k = 2$) we use the short notation $\phi_{G \to F}$.

We have allowed before for the reliability of the information to differ for each potential state that is observed. To simplify our analysis, however, we will use the case where the reliability matrix is symmetric. Therefore we can formally designate the reliability of the IIS using a single metric α, with a value ranging from 0.5 to 1. Here $\alpha = 1$ means that the IIS is perfectly reliable; when it says that A is planning to choose a particular strategy it is always correct. An $\alpha = .5$ means that the IIS is essentially useless, as anytime it indicates that A is planning to choose a particular strategy, there is only a 50/50 chance of it being correct. Thus, while it is clear that an IIS with maximum entropy is the least useful, for the purpose of our discussion we suggest only that a "bad" IIS is one that yields a negative expected payoff (not including the cost of the IIS) in the context of a competitive game.

5. KNOWLEDGE STATES

The two components of IIS knowledge (i.e., use and reliability) can be assembled into a two-dimensional knowledge-state matrix (Figure 4) that shows all possible states of knowledge. Defenders can either know or be ignorant of an offender's use of an IIS and they can either know or be ignorant about the predictive accuracy (reliability) of an offender's IIS. It is important to note that in order to investigate mathematically the behavior of both competitors within game theory, the quadrant in which the game is taking place is assumed known to both competitors and can therefore be regarded as common knowledge. In Figure 4, the "overt" case refers to when the use of the IIS is common knowledge. In the covert case, the defendant does not know whether or not the offender is using an IIS, and the defendant's ignorance is common knowledge. Similarly, if the defendant knows about the reliability of the IIS (i.e., it is common knowledge), we call this the "open" case; if not, the "closed" case. This results in the following four knowledge zones.[5]

[5] It is important to note that in order to investigate mathematically the behavior of both competitors within game theory, the quadrant in which the game is taking place is assumed known to both competitors and can therefore be regarded as common knowledge.

(I) *Blackout*. The defendant has no information either about the use or the reliability of an IIS that the offending side may use.

(II) *Covert but Open*. While the defendant company does not know whether the offending company is using an IIS, the reliability of the IIS is common knowledge.

(III) *Overt but Closed*. The existence and use of the IIS is common knowledge, yet the defendant does not know its reliability.

(IV) *Symmetric Knowledge*. In this case the existence and use as well as the reliability of the IIS are common knowledge. Though it may seem that this situation is equivalent to the situation without an IIS, we may assume that existence of such an IIS, with sufficient reliability, may change the behavior of the defendant and the offender.

Moving between knowledge states. The payoffs from strategic decisions about investing in an IIS are directly related to the knowledge states represented in Figure 4. This representation makes it possible to compute a payoff for each of these four cases. The different situations also enable us to discuss a few interesting questions.

What is the value of the IIS for each of the four knowledge states? Although the calculation for each value is context specific, it is intuitive that the lowest value is realized in the “Symmetric Knowledge” situation while the “Blackout” situation is the worst for the defender, producing the highest value for the offender using an IIS. The other two cases (“Overt but Closed” and “Covert but Open”) provide values that are smaller than in the “Blackout” case but larger than in the “Symmetric Knowledge” case.

What is the maximal amount an organization should be willing to invest in order to keep the IIS hidden? This amount is a function of the IIS use and the difference between the equilibrium payoff in the overt case compared to the covert case.

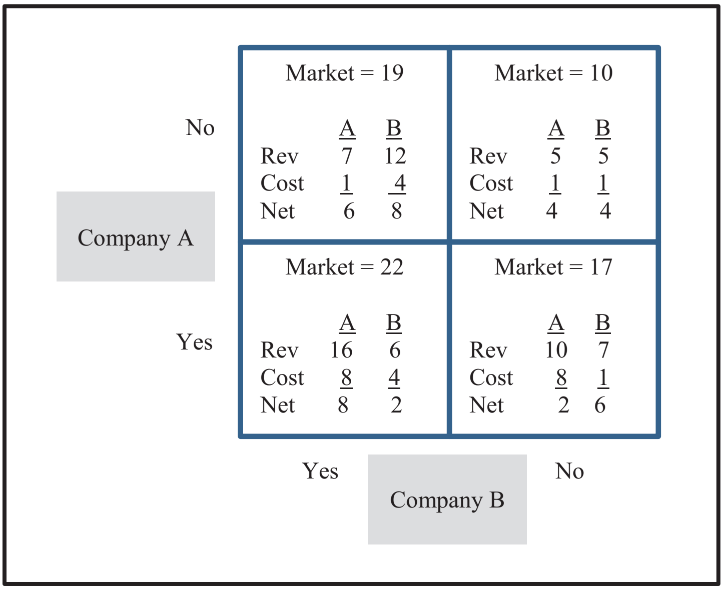
In a similar way, for a covert IIS, what is the maximal amount an organization should be willing to invest for keeping the reliability of its IIS covert? This case depends on the specific characteristics and quality of the IIS and the value of the conflict in the covert closed case compared to the open case.

Following the initial decision to invest in a specific IIS, an organization may need to consider further decisions with regard to investing more in the intelligence function, either by improving the state of knowledge or improving the reliability of the intelligence system. Again, the value and cost of each of these moves can be computed by comparing the equilibrium payoff for each quadrant.

6. EXAMPLES

In this section we provide numerical examples of our game-theoretic framework for evaluating an IIS. In the Introduction we presented an example of a symmetrical pure strategy Nash equilibria game and concluded that an IIS would provide no value in that situation. We now present an example of a nonsymmetric mixed strategy game, that is, one in which the payoffs are not zero-sum and in which no strategy dominates, and therefore the equilibrium strategy is a probabilistic weighting of all of the available strategies. This scenario is more reflective of real-world competitive games.

Again, assume we have two competing telecommunications companies as before (Figure 5). Both companies are considering an investment to update their cellular telephony infrastructure to support the launch of new revenue-generating services. Company A’s infrastructure will be based on 4G technology standards, while Company B will use 3G. Investment in 4G is more expensive than 3G; however, it could yield a better net income. Both have been investing $1 billion per year on an ongoing basis and have been splitting the market equally. Each company has two options: to invest in new infrastructure (“Yes”) or not (“No”). We further assume that any investment



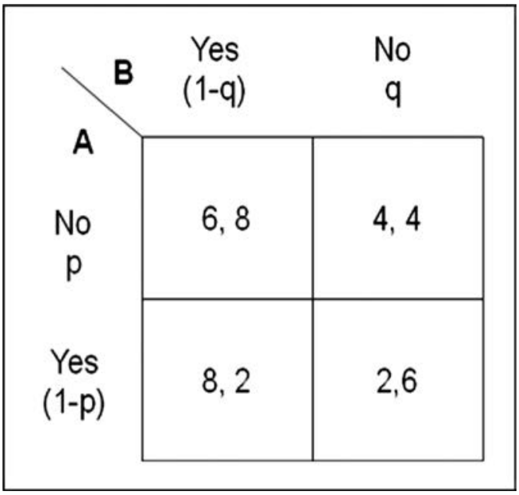
Company A		Company B: Yes		Company B: No	
No		Market = 19		Market = 10	
		A	B	A	B
	Rev	7	12	5	5
	Cost	1	4	1	1
	Net	6	8	4	4
Yes		Market = 22		Market = 17	
		A	B	A	B
	Rev	16	6	10	7
	Cost	8	4	8	1
	Net	8	2	2	6

Fig. 5. Example of a nonsymmetric-mix strategy game.

by either company will increase the total size of the market (although not necessarily monotonically). Specifically, if neither invests in new infrastructure, then the total market will remain at 10. If both invest in new infrastructure, then the total market will increase to 22. If either invests while the other does not, the total market will grow to an intermediate value (17 or 19). Revenue will be split asymmetrically.[6] Figure 5 shows the revenue split, infrastructure costs, and net payoff.

The no-IIS case. To create a benchmark value for this game, we first compute the value of the game to each player assuming no IIS is being used by either player (although, as usual, both companies know the payoff matrix). The value of the game to a player is the weighted average payoff at the point of equilibrium; that is, the weighted mix of strategies for which the expected payoff for your opponent would be equal regardless of which strategy was chosen by you, and the point at which an opponent therefore has no preference for either strategy. A simplified net payoff matrix for the game is shown in Figure 6. Each strategy is assigned a probability or weight (to be solved for), and the total weighting for all strategies for a company must equal 1. We designate the probabilities for Company A's choices in terms of p, and for Company B, q.

[6] This more closely reflects a real-world context. In this case, if only Company A adopts the new technology, then some of Company A's customers will chose to remain with the existing technology (defecting to the competition) rather than pay more, as will Company B's customers. However, if both companies adopt new technologies, then all customers will have to switch, and Company A will have an advantage (viz., better technology). If only Company B invests, then it will retain proportionally more customers, as the cost to upgrade will be less than for customers of Company A, and a greater portion will choose to pay the higher (but less than the Company A increase) cost. Also, more customers may defect from Company A. In other words, if only one company upgrades, than the customers of the other company can choose to remain with their existing technology at no additional cost. If companies decide to upgrade, then customers of B would have to adopt a new technology anyway and more would be inclined to upgrade to Company A's 3.0 rather than Company B's 2.5 for a slightly higher cost.



A \ B	Yes (1-q)	No q
No p	6, 8	4, 4
Yes (1-p)	8, 2	2,6

Fig. 6. Simplified payoff matrix.

To find the equilibrium point, A would like to know the weights at which B is indifferent between its strategies, that is, the expected payoff to B when B chooses "yes" equals the expected payoff to B when B chooses "no." Therefore, equilibrium will be realized when

$$4\mathrm{p} + 6\,(1 - \mathrm{p}) = 8\mathrm{p} + 2\,(1 - \mathrm{p}).$$

Solving for p, we get $\mathrm{p} = 0.5$, and $(1 - \mathrm{p}) = 0.5$. From Company B's perspective, we can state this similarly as

$$4\mathrm{q} + 6\,(1 - \mathrm{q}) = 2\mathrm{q} + 8\,(1 - \mathrm{q}).$$

In this case, solving for q, we again get $\mathrm{q} = 0.5$, and $(1 - \mathrm{q}) = 0.5$.

If we substitute the terminology for the game in Figure 6 so that both A and B are given the option to invest either small (no) or big (yes), then mathematically, we can state this as follows: given that B knows that A will invest "small" with probability p and "big" with probability $(1 - \mathrm{p})$, if B chooses small, then the expected payoff to B is 25, p of the time and 35, $(1 - \mathrm{p})$ of the time. When B chooses big, the payoff to B is 30, p of the time and 30, $(1 - \mathrm{p})$ of the time. Solving for p, we get $\mathrm{p} = 0.5$, and $(1 - \mathrm{p}) = 0.5$, therefore it follows that

$$25(.5) + 35(.5) = 30(.5) + 30(.5).$$

Thus, to maximize the value of the game, each player should randomly choose each strategy half of the time (i.e., with a probability of 0.5). The expected value of the game is found by multiplying Company A's and B's equilibrium weights for each quadrant and multiplying that times the payoff to that company (Table II), for example, the expected payoff to A is 5.

Similarly we could compute the total value to Company B as

$$0.25(4 + 6 + 8 + 2) = 5.$$

The value of 5 to both A and B establishes the benchmark value of the game with no IIS involved.

The IIS case under symmetric knowledge. We now assume that Company B has an IIS that it will use to reveal Company A's strategic choice before Company B has to

Table II. Expected Payoffs to A

Company A strategy	Company A weight	Company B strategy	Company B weight	Expected Payoff to A	
No	p = .5	No	q = .5	4 x p x q	$4 \times 0.25 = 1.00$
Yes	1 − p = .5	No	q = .5	2 x (1 − p) x q	$2 \times 0.25 = 0.50$
No	p = .5	Yes	1 − q = .5	6 x p x (1 − q)	$6 \times 0.25 = 1.50$
Yes	1 − p = .5	Yes	1 − q = .5	8 x (1 − p) x (1 − q)	$8 \times 0.25 = 2.00$
				Total Value to A:	**5.00**

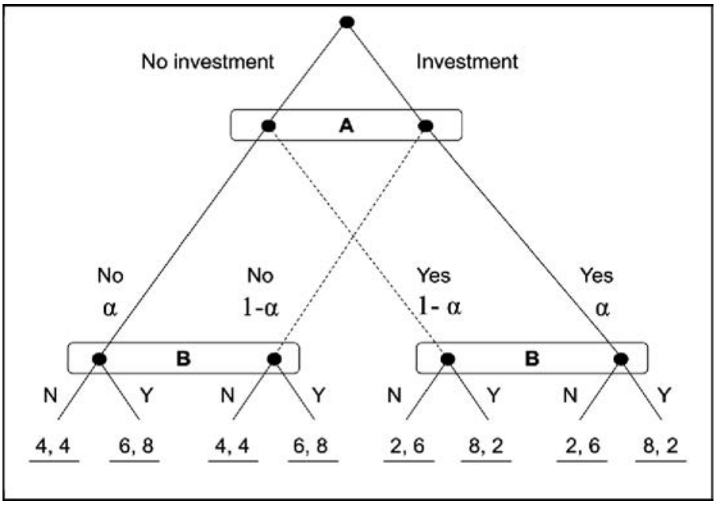


Fig. 7. IIS case under symmetric knowledge.

make its own choice. We also assume that the IIS is not perfectly reliable, but rather has a reliability of α. We further assume that the IIS is open and overt, that is, Company A knows about the use and reliability of the IIS. Adding an IIS to the scenario adds another layer of choice to the game. Not only must B chose a strategy given what it believes A might do, but B must also chose a strategy given what it believes the IIS is really indicating.

The range of possible combinations is shown in extended tree form in Figure 7. Company A can choose either not to invest or to invest. Company B receives a signal indicating either investment ("No") or investment ("Yes"), however for each signal there is a probability $(1 - \alpha)$ that the actual strategy indicated is not the one chosen by A. Therefore for each signal received and for each strategy chosen by Company A there is a different expected payoff in combination with each strategy chosen by Company B.

Whereas Company A still has two choices, Yes and No, Company B now has extended its choices to four because the IIS can give one of two signals, and for each signal there are two possible decisions or strategies: Always choose No regardless of what the IIS indicates, choose according to whatever the IIS indicates, choose according to the opposite of what the IIS indicates, or always choose Yes regardless of the IIS.[7]

[7] Note that while some of the new strategies appear to be the same as in the non-IIS case, they actually differ because the new strategies are now contingent upon a reading of α, whereas the prior strategies were not. Each new strategy is now chosen in light of how the IIS signal is interpreted. So, for example, choosing "Invest" in the previous example is not the same as the current choice of "IIS indicates competitor will invest, so invest," because when the system says invest one could also choose not to invest.

Table III. Expected Payoffs for All Combinations

			B's Decisions (strategy)			
		Expected	(No, No)	(No, Yes)	(Yes, No)	(Yes, Yes)
A's Decision	No	Payoff A	$4\alpha + 4(1-\alpha)$	$4\alpha + 6(1-\alpha)$	$6\alpha + 4(1-\alpha)$	$6\alpha + 6(1-\alpha)$
		Payoff B	$4\alpha + 4(1-\alpha)$	$4\alpha + 8(1-\alpha)$	$8\alpha + 4(1-\alpha)$	$8\alpha + 8(1-\alpha)$
	Yes	Payoff A	$2(1-\alpha) + 2\alpha$	$2(1-\alpha) + 8\alpha$	$8(1-\alpha) + 2\alpha$	$8(1-\alpha) + 8\alpha$
		Payoff B	$6(1-\alpha) + 6\alpha$	$6(1-\alpha) + 2\alpha$	$2(1-\alpha) + 6\alpha$	$2(1-\alpha) + 2\alpha$

Table IV. Reduced Expected Payoffs for All Combinations

			B's Decisions (strategy)			
		Expected	(No, No)	(No, Yes)	(Yes, No)	(Yes, Yes)
A's Decision	No	Payoff A	4	$6 - 2\alpha$	$4 + 2\alpha$	6
		Payoff B	4	$8 - 4\alpha$	$4 + 4\alpha$	8
	Yes	Payoff A	2	$2 + 6\alpha$	$8 - 6\alpha$	8
		Payoff B	6	$6 - 4\alpha$	$2 + 4\alpha$	2

Table V. Eliminating the (No, Yes) Option

			B's Decisions (strategy)		
		Expected	(No, No)	(Yes, No)	(Yes, Yes)
A's Decision	No	Payoff A	4	$4 + 2\alpha$	6
		Payoff B	4	$4 + 4\alpha$	8
	Yes	Payoff A	2	$8 - 6\alpha$	8
		Payoff B	6	$2 + 4\alpha$	2

The expected payoffs to both companies for each combination of choices are shown in Table III. For Company B, the first strategy in parentheses indicates B's action if the IIS indicates No, and the second if the IIS indicates Yes. So (No, No) represents the case where Company B chooses No regardless of the IIS signal, (No, Yes) represents compliance with the IIS, (Yes, No) represents choosing the opposite of the signal, and (Yes, Yes) represents always choosing Yes regardless of the signal.

This can be simplified to what is shown in Table IV.

Since $\alpha > {}^{1}\!/_{2}$, by inspection we can see that strategy (Yes, No) for Company B strictly dominates strategy (No, Yes), therefore we can eliminate strategy (No, Yes) from consideration without changing the value of the game. In Table V the reduced matrix becomes as shown.

Given this strategic matrix, Company B would appear to have four possible options for creating a mixed strategy: three options to mix any of the two strategies, plus the option to create a weighted mix of all three. Specifically, we have the following.

- *Case 1.* Company B is mixing only the two pure strategies (Yes, Yes) and (Yes, No) and assigns zero probability to the pure strategy (No, No).
- *Case 2.* Company B is mixing only the two pure strategies (Yes, No) and (No, No) and assigns zero probability to the pure strategy (Yes, Yes).
- *Case 3.* Company B is mixing only the two pure strategies (Yes, Yes) and (No, No) and assigns zero probability to the pure strategy (Yes, No).
- *Case 4.* Company B is mixing all three pure strategies (Yes, Yes), (Yes, No), and (No, No).

Biran and Tauman [2008] show that equilibrium points for Cases 2 and 4 cannot be calculated, and that Case 3 applies only if the IIS has a low α. As we wish to illustrate the case of an IIS with high α, we are left with Case 1. While it may appear that we are back to two strategies, it must be noted that by introducing an IIS of reliability α,

Table VI. Reduced Matrix

			B's Decisions	
		Expected	(Yes, Yes)	(Yes, No)
A's Decision	No	Payoff A	6	$4 + 2\alpha$
		Payoff B	8	$4 + 4\alpha$
	Yes	Payoff A	8	$8 - 6\alpha$
		Payoff B	2	$2 + 4\alpha$

Table VII. Payoff Matrix at $\alpha = .9$

			B's Decisions	
		Expected	(Yes, Yes)	(Yes, No)
A's Decision	No	Payoff A	6	5.8
		Payoff B	8	7.6
	Yes	Payoff A	8	2.6
		Payoff B	2	5.6

the two strategies in this case are different than the two strategies in the non-IIS case, and as will be shown, produce a game with a higher value as anticipated.

In Table VI we are then left with the shown reduced matrix.

If we take, for example, the case of $\alpha = .9$, we get the payoff matrix shown in Table VII.

To solve this game, assume that Company A chooses the mixed strategy (p, 1 − p) and Company B chooses the mixed strategy (q, 1 − q) where $0 < p, q < 1$. If Company B chooses (Yes, Yes) it obtains $8p + 2(1 - p)$. If B chooses (Yes, No), its expected payoff is $7.6p + 5.6(1 - p)$. Since company B is mixing these two pure strategies, namely (Yes, Yes) with (Yes, No), it must find the equilibrium point at which it obtains the same payoff whether it chooses (Yes, Yes) or (Yes, No), namely

$$8p + 2(1 - p) = 7.6p + 5.6(1 - p).$$

Solving for p, we get $p^* = 0.9$.

To compute the equilibrium value of q we similarly assume that if Company A chooses not to invest in new infrastructure (i.e., "No" strategy) it obtains $6q + 5.8(1 - q)$. If Company A chooses to invest in new infrastructure ("Yes") then it obtains $8q + 2.6 (1 - q)$. In equilibrium it exists that

$$6q + 5.8(1 - q) = 8q + 2.6(1 - q).$$

And solving for q we get $q^* = .62$.

Calculating the value of the conflict we obtain

$$\begin{aligned} V_a^* &= (6(.62) + 5.8(.38) + 8(.62) + 2.6(.38))/2 = 5.93 \\ V_b^* &= (8(0.9) + 2(.1) + 7.6(.9) + 5.6(.1)/2 = 7.40. \end{aligned}$$

This example illustrates several interesting points. First, the use of an IIS is shown to increase the value of the game to Company B as we would have expected. Second, it could be shown mathematically that the value of the game to both players increases (decreases) monotonically with an increase (decrease) in α. The more reliable the IIS, the higher the expected payoffs, therefore it might pay to invest in improving the reliability of an IIS, depending on the increase in costs required. Our framework provides a useful means to evaluate this investment.

Interestingly, the use of an IIS by Company B also slightly increases the value of the game for Company A. The game we have illustrated is an example of a nonzero-sum game. This means that one does not always win at the expense of one's competitor. Improving your own strategic position may improve that of your competitors as well. This is actually a very common but typically neglected aspect of investing in strategic initiatives such as intelligence information systems. One major contribution of game theory is that it reminds us of how intertwined our actions and outcomes are with those of our competitors.

By investing in an IIS, Company B adds more strategic choices to its arsenal, changing the game. Because the IIS is common knowledge, competitors enjoy more options as well, especially as illustrated here in the case of an open, overt IIS. Because our competitors know we have an IIS of a particular reliability, it influences their strategic choices as well as ours, even though we get to make our choice after theirs. This is where the notion of "gaming" the system comes from, and has direct real-world implications.

Exposing one's use of an IIS may actually be beneficial in certain cases. The signaling literature (e.g., Eliashberg and Robertson [1988] and Moore [1992]) provides examples of how revealing one's capabilities or intentions may actually benefit an organization, because these signals can be used to influence competitors' behaviors in ways beneficial to the revealing organization. If an organization announces it will be entering a market, then its competitors may decide not to enter, and both realize a better payoff than if both entered the same market. If an organization reveals that it is "spying" on another, then competitors may behave in a way dictated by their mutual knowledge of how the new game is structured, and both may benefit. While game theory does not offer a prescription for when to reveal, it does offer a means for analyzing the value of that strategy [Postrel 1991].

For rational players, the primary motivation is to improve one's lot regardless of the effect on other players. However, this does not preclude attempting to use secrecy to improve the value of the game for the offending player who is using the IIS. The previous example represents the open/overt IIS case. Next we briefly discuss the cases where use and reliability are not revealed, that is, the closed and/or covert IIS cases.

The IIS case under asymmetric knowledge. The case of asymmetric knowledge exists when either the use or reliability of the IIS is not common knowledge among the opponents. Both cases are more complex than those of symmetric knowledge; however, we can still use a game-theoretic framework to examine how decision makers might model this situation to evaluate implementing an IIS.

Game theory assumes that something is known among the players in common (for the purposes of rendering the theory mathematically tractable). In the case of asymmetric knowledge, while the offender knows the reliability or use of its IIS, a defender knows only a probability distribution over the reliability or use of the IIS. However, this probability distribution is assumed to be common knowledge among the players. This is similar to a common real-world scenario of organizations estimating the probability of a competitor having some capability or taking some action.

When the reliability of the IIS remains common knowledge, but the use of that system is not known by competitors (Quadrant II: covert, but open), the difference in the game becomes one of factoring the costs to use a system into the payoff matrix. The computations for any particular scenario are relatively straightforward, and as expected the value of the game would increase for both players [Biran 1991][8]. Essentially, the defender estimates the expected cost for the offender to use the system (based on its knowledge of the probability distribution of costs), adjusts the payoff matrix accordingly, and then determines the probability that the offender would use the system (assuming rational behavior). We can think of this as a metagame, as once the defender estimates the probability of use, the game can be broken into the two symmetric games we have already considered: known use of the IIS and known nonuse of the IIS

[8] We exclude all games where the cost exceeds the value and therefore would not represent a rational choice.

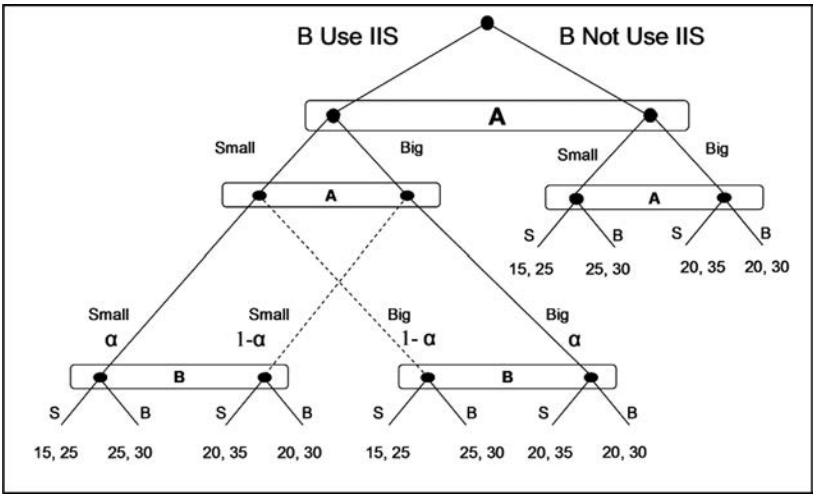


Fig. 8. IIS case under asymmetric knowledge.

(Figure 8). We could assign values and compute the value of the game as before. The important contribution is not the particular values but the decision framework.

The case of maintaining secrecy about the reliability of the IIS (Quadrant III: overt/closed) is similarly complex. In this case, we would assume that while defenders do not know the actual reliability of the offender's IIS, they are aware of a probability distribution of reliabilities from which this particular IIS is drawn. For example, they may not know with certainty that the IIS has an $\alpha = 0.8$, but we would assume that they know that there is a distribution of reliabilities over some range and with some probability of occurring. They might believe that there is a 10% chance that a competitor's IIS is either perfect ($\alpha = 1$) or useless ($\alpha = 0.5$), a 25% chance that it is either between, say, 0.6 and 0.7 or between 0.8 and 0.9, and a 30% chance that it is somewhere between 0.7 and 0.8. Again, it is not so much the mathematical values or the solution as it is the process and set of questions to be asked that represents the value of using a game-theoretic framework to evaluate the use and configuration of an IIS. Were we to mathematically compute the value of a game in which the α of the IIS is hidden, we would again see an increase in the value of the game [Biran and Tauman 2008].

7. CONCLUSION

We have presented a game-theoretic framework for assessing the impact and value of an intelligence gathering capability in terms of the use and quality (i.e., reliability) of the information it generates. Game theory offers a useful framework for evaluating information that may have a strategic impact. Specifically, game theory addresses the value of information and knowledge held by competitors about their strategic options and about each other, and how changing that state of knowledge among competitors can influence the value of the game and therefore the value of investing in the technologies to produce that information. Further it allows us to evaluate the economic impact of the quality of this information.

The value of game theory is that it provides a well-formed structure for analyzing the economic impact of information and information technology in competitive situations. While well-developed in the economics literature, it is a perspective that has been generally underutilized by the IS community, but offers useful and well-defined guidance for advancing research in this area. Beyond mathematical precision, it offers a disciplined means to analyze real-world investments in IS capabilities. Often the questions it raises and the perspectives it provides are as important as the methods and outcomes. Most notable is having to take competitors' knowledge and potential actions and reactions into account when attempting to determine the value of one's own IT initiatives and investments.

Specifically, we defined four possible states of knowledge an organization might operate under regarding its information intelligence gathering capabilities, based on information quality and IIS use. We showed that each has a particular value, and that knowing which quadrant one is operating in is important to making good investment decisions regarding this capability. We provided examples illustrating the value of an IIS. The game with an information intelligence system was shown more valuable than that without an IIS. We also provided a framework for addressing the following questions.

—*The value of the IIS.* What is the maximum price an organization is willing to pay in order to move from a situation in which it acts without an IIS to a situation in which it acts with an IIS?

—*The value of secrecy.* What is the (maximal) price an organization will be ready to pay in order to move from a situation in which it has an overt IIS to a situation in which it operates a covert IIS? Conversely we can derive the maximal price an organization should be willing to pay to expose its competitor's IIS. Likewise, what is the maximal price a company is willing to pay in order to prevent exposing the information about the existence and activation of a covert IIS?

—*Marginal return.* Where should an organization make its marginal investment? Should it be on improving the quality of the IIS (i.e., the reliability of its intelligence information) or investing in keeping it secret?

Our examples illustrate that there is value in secrecy; however, with game theory it is always possible to construct a game to provide any outcome [Postrel 1991]. The key is to create a set of assumptions that reflect the nature of the game and to follow the rules of the game to determine the value of that particular game. We have provided an introduction to the nature of these rules, and a foundation on which to build additional research. Some of the questions that remain to be addressed include the following.

—What is the impact of moving from a single interaction game to a repeated game, where the organization has an opportunity to use an IIS and evaluate the outcomes over and over? We can assume that in the "Symmetric Knowledge" case, the transition to the repeated case will have no impact since the existence and the reliability of the IIS are common knowledge. The situation becomes more complicated and more interesting in the three other cases but especially in the cases where the reliability of the IIS is not common knowledge. We may assume that based on the "Rules of the Game", the defender will continuously learn from the offender's decision making process about the existence and reliability of the IIS. A metagame emerges in which the offender may be taking actions to conceal the existence and/or reliability of its IIS capability while the defender is attempting to create organizational processes that enable it to learn about the defender's intelligence gathering capabilities. Repeated games also enable the introduction of misinformation campaigns, adding a layer of complexity to the game we have described here. That is, opponents not only have a choice of a particular action strategy, but in addition they have a choice regarding a communication strategy (viz., whether or not to distribute misinformation). For example, our consumer goods company may choose to announce the release of a new product into a market not inhabited by its competitor, when it actually intends to release a product into its competitor's existing market.

—What is the impact of using more than one IIS, thereby providing multiple signals about the same event? How should we select the best IIS among several alternatives or integrate multiple signals? Although also outside the scope of this article, our framework can be used to evaluate the implementation of additional IISs.

—Most models of game theory assume, explicitly or implicitly, common knowledge regarding certain facts [Monderer and Samet 1989]. How crucial are these assumptions for our situation? What is the meaning of diverting from the classic "rules of the game" and allowing an IIS that acts as double or triple agent? Can a common belief effectively substitute for the common knowledge assumption? What methods should be used to validate an IIS and prevent it, if possible, from acting as double agent?

Based on the preceding discussion, we can conclude that a decision maker in a competitive situation, when considering the usage of an intelligence gathering capability, must evaluate all three components: the "Rules of the Game", the state of knowledge, and the reliability of the information gathered. To better understand a competitor's strategic plans and what they are doing tactically, companies may need to take a closer look at competitive intelligence or they risk missing lucrative opportunities. The proposed framework enables decision makers to better understand the role and ingredients of this competitive situation where intelligence gathering systems may be used.

REFERENCES

ANDREWS, K. R. 1971. *The Concept of Corporate Strategy.* Dow-Jones Irwin, Homewood, IL.

ARENSMANN, R. 2001. Shedding the trench coat. *Electron. Bus.,* 70–76.

AXELROD, R. 1984. *The Evolution of Cooperation.* Basic Books, New York.

BIRAN, D. A. 1991. Distributed information systems under strategic conflict. Ph.D. thesis, Tel Aviv University.

BIRAN, D. A. AND TAUMAN, Y. 2008. The role of intelligence in a strategic conflict. Working paper, Center for Game Theory in Economics, SUNY at Stony Brook.

BOATRIGHT, J. 2000. *Ethics and the Conduct of Business* 3rd Ed. Prentice Hall.

BRANDENBURGER, A. M. AND BINMORE, K. 1990. Common knowledge and game theory. In *Essays on the Foundations of Game Theory*, Basil Blackwell, 105–150.

BRANDENBURGER, A. M. AND NALEBUFF, B. J. 1995. The right game: Use game theory to shape strategy. *Harvard Bus. Rev. 13*, 55–71.

ELIASHBERG, J. AND ROBERTSON, T. S. 1988. New product preannouncing behavior: A market signaling study. *J. Market. Res. 25*, 3, 282–292.

HARSANYI, J. C. 1994. Games with incomplete information. Nobel Prize in Economics documents 1994-1, Nobel Prize Committee.

HARSANYI, J. C. 1967. Games with incomplete information played by "Bayesian" players, I-III, Part I- The basic model. *Manag. Sci. INFORMS 14*, 3, 159–182.

KRIEBEL, C. H. AND MOORE, J. H. 1982. Economics and management information systems. *Data Base*, Fall, 30–40.

LUCE, R. D. AND RAIFFA, H. 1957. *Games and Decisions*. John Wiley, Hoboken, NJ.

MA, H. 2000. Of competitive advantage: Kinetic and positional. *Bus. Horizons 43*, 1, 53–64.

MARSCHAK, J. AND RADNOR, R. 1971. *The Economic Theory of Teams*. Yale University Press, New Haven, CT.

MCGUIRE, C. B. 1972. Comparisons of information structures. In *Decision and Organization*, C. B. McGuire and R. Radnor, Eds., North-Holland Publishing, Amsterdam, 101–130.

MERTENS, J. F. AND ZAMIR, S. 1971. The value of two-person zero-sum repeated games with lack of information on both sides. *Int. J. Game Theory 1*, 39–64.

METAYER, E. 1999. Demystifying competitive intelligence. *Ivey Bus. J.,* Nov./Dec., 70–74.

MONDERER, D. AND SAMET, D. 1989. Approximating common knowledge with common beliefs. *Games Econ. Behav. 1,* 170–190.

MOORE, M. C. 1992. Signals and choices in a competitive interaction: The role of moves and messages. *Manag. Sci. 38*, 4, 483–500.

NEAVE, E. H. AND WIGINTON, J. C. 1976. Evaluating security performance forecasts. *Manag. Sci. 23,* 4, 371–379.

PATEL, P. AND PAVITT, K. 2000. How technological competencies help define the core (not the boundaries) of the firm. In *The Nature and Dynamics of Organizational Capabilities*, G. Dosi, R. Nelson, and S. G. Winter, Eds., Oxford University Press, 312–333.

PONSSARD, J. P. 1976. On the concept of value of information in competitive situations. *Manag. Sci. 22*, 739–747.

PORTER, M. E. 2000. What is strategy? *Harvard Bus. Rev.*, Nov.-Dec., 1–19.

POSTREL, S. 1991. Burning your britches behind you: Can policy scholars bank on game theory? *Strat. Manag. J. 12*, 153–155.

SMITH, R. W. 1996. Business as a war game: A report from the battlefront. *Fortune 30*, 134, 6.

SHING, M. N. K. AND SPENCE, L. J. 2002. Investigating the limits of competitive intelligence gathering: Is mystery shopping ethical? In *Business Ethics: A European Review*, Blackwell Publishers, 343–353.

SHOR, M. 2001. Game theory and business strategy: Mixed strategies in american football. http://mba.vanderbilt.edu/Mike.Shor/courses/game-theory/docs/lectures0456/Football.html.

SIMON, H. A. 1945. *Administrative Behavior*. The Free Press, New York.

VON NEUMANN, J. AND MORGENSTERN, O. 1947. *Theory of Games and Economic Behavior*. Princeton University Press, Princeton, NJ.

WEINBERG, C. B. AND MONTGOMERY, D. B. 1979. Toward strategic intelligence systems. *J. Market. 43*, 4, 41–52.

ZACK, M. H. 2005. The strategic advantage of knowledge and learning. *Int. J. Intellect. Capital Learn. 2,* 1, 1–20.

ZACK, M. H. 2001. If managing knowledge is the solution, then what's the problem? In *Knowledge Management and Business Model Innovation*, Y. Malhotra, Ed., Idea Group Publishing, Hershey, PA, 16–36.

ZACK, M. H. 1999. Developing a knowledge strategy. *Calif. Manag. Rev. 41,* 3, 125–145.

Received December 2010; accepted December 2012