9-11 Information Failures: A Semiotic Approach

Kevin C. Desouza and Tobin Hensgen

The terrorist attacks of 11 September 2001 devastated the US in a manner that it had not experienced in 60 years. But before emergency crews cleared the debris at Ground Zero, the agencies charged with security were busy pointing fingers of censure at one another. Unfortunately, their intent was not to remedy the shortcomings that demanded immediate correction, but rather to distance their respective bureaus from fault.

Coupling information gathering systems with cohesive, associative applications might have left the US better prepared.

In truth, the events leading to 9-11 seem to indicate an interaction of oversights, which, in concert, compromised security. Here, we use a semiotic model to explain some of what went wrong prior to 9-11. *Semiotics* involves the study of signs and symbols to better understand their meaning and contextual relation, as the "What is Semiotics?" sidebar explains. Our model, shown in Figure 1, addresses the cohesions of data. In another study, we explore the concepts in detail (K.C. Desouza and T. Hensgen, "On 'Information' in Organizations: An Emergent Information Theory and Semiotic Framework," *Emergence: A Journal of Complexity Issues in Organizations and Management*, vol. 4, no. 3, Dec. 2002); here, we outline the main thesis.

UNIVERSALITY IN INFORMATION REPRESENTATION

We begin with so-called information. Today, academics and practitioners alike have a tendency to overuse, perhaps misuse, the term information. They have become accustomed to seeing such phrases as information economy, information systems, information society, and information management in a myriad of applications. In a world where people immediately regard everything as information, the word itself loses value, and to be without value severely restricts the motivation for purposeful research.

For information to be useful, it must be necessary; and to be necessary, it must be universal in the same way as a mathematical expression is understandable by mathematicians worldwide, regardless of their native language. In a mathematical equation, the mapping of symbols provides participants a common way to communicate. In such instances, participants organize the mathematical expression's syntax from data "in reality" rather than allowing any single definition "of reality" to imprint itself on the data. For example, by late June 2001, several governmental agencies were privy to information that had value in reality. This information indicated that the US might expect an act of terrorism by Islamic fundamentalists who might use domestic airlines against cities. Instead of sharing this information, these agencies imprinted their own reality on this context and kept this to themselves. They would not share this information until after 9-11.

Continued on page 61

What is Semiotics?

To assist in a standardization process, we reviewed the works of Sanders Pierce (1839-1914), a mathematician and logician who founded the field of *semiotics*, the study of information flow, examining it from data capture through to some actionable event (for example, decision making). Sanders' semiotic work dealt with distinctions involved with the communication of ideas through signs acting in dependent relationships with their meanings. For example, a stoplight conveys a different meaning when the color changes.

We suggest the use of a semiotic approach to events preceding 9-11 might have left the US better prepared to anticipate what did transpire.

Published by the IEEE Computer Society

1520-9202/03/$17.00 © 2003 IEEE

Continued from page 64

Current systems literature provides little that addresses what is necessary and why there is a requirement for universality in information representation and processing. Our semiotic model, adapted from the existing domain of semiotic models, provides such a universal model, defining it in five levels.

MORPHOLOGICAL LEVEL: GATHERING GENERATIVE DATA

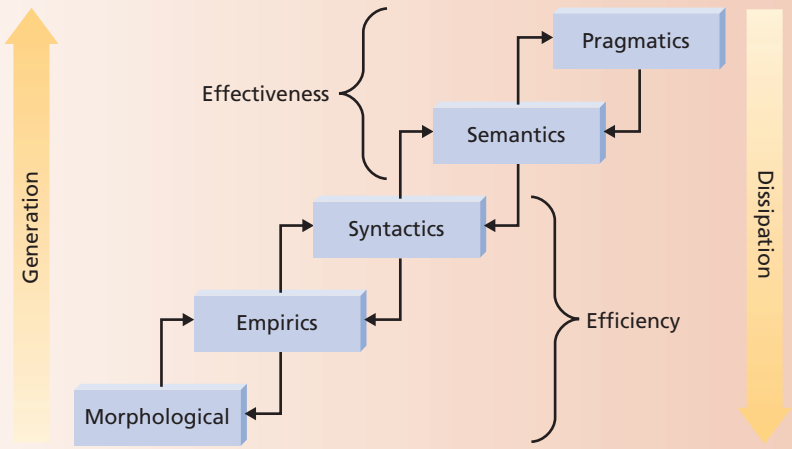
At the morphological level, generative data is general and potentially unnecessary; it represents a start in data collection that might be the seed of some information. Not all data will sprout useful information. Organizations identify the type of data to collect by flagging any source that fits rather broad, though established, parameters. This data can come from trade or international journals, newspapers, lectures, or rumors.

At this level, it's more critical to begin the process in step with the semiotic model than to become weighed down overanalyzing the types of data to collect. In our 9-11 example, media reports from several sources provide an outline of the types of data likely available before 9-11. But because of the lack of any coordinated scheme, this data was improperly channeled.

Starting in December 2000, surveillance activities had identified unusual spikes in communications traffic among known terrorist factions. This traffic was consistent through June 2001 and the Central Intelligence Agency (CIA), in particular, was concerned with the possibility of terrorist strikes intended for either the Fourth of July holiday or perhaps for President George W. Bush's late July appearance at the G8 economic summit in Genoa, Italy.

The US appeared to focus little on the probability of strikes aimed at domestic targets. John Parachini of the Monterey Institute of International Studies repeatedly had warned against the US government's inability to calculate threat assessments because, he said, it too often relied "on what people think terrorists could do ... (and not) on what they are able to do" (C. Dickey and A. Nagorski, "Who's the Mastermind," *Newsweek* Web exclusive; http://www.msnbc.com/news/627496.asp, 2001).

Figure 1. Semiotic model.



The following data would have been useful at the semiotic model's morphological level:

- From December 2000 to March 2001, intelligence sources, including the CIA, become aware of increased communications activity among Islamic extremist groups. Such activity often indicates impending terrorist action.
- In February 2001, Arizona flight schools report to the Federal Aviation Administration that an Arab student, Hani Hanjour, might have a fraudulent pilot's license and be seeking advanced certification to fly jets. The FAA allows Hanjour's credentials but informs him that it will not certify him. Hanjour was aboard, and might have piloted, the plane that struck the Pentagon on 9-11.

At the morphological level, focus is on the quantity, rather than the quality, of data. As the data filters upward in the semiotic model it quickly becomes more focused.

EMPIRICS LEVEL: FIRST-LEVEL DATA ANALYSIS

At the empirics level, investigators have broadly filtered data but not critically evaluated it. This appraisal should validate usefulness and give weight to the significance of the collected data, as well as determine whether synthesis is likely to provide information. This process assigns a value to data. Media reports indicate the likelihood that some data related to 9-11 might have reached a level similar to that of the semiotic model's empirics level:

- In a June 2001 memo to his superiors, an Arizona Federal Bureau of Investigation (FBI) agent theorizes that the Al Qaeda terrorist organization might be training pilots to use planes in terror plots; supervisors defer the memo.
- The Egyptian government tells the CIA that Muslim terrorists might use planes to crash into buildings.
- A member of the Senate Intelligence Committee (SIC) tells CNN that her staff has advised her of the "probability of a terrorist incident within the next three months."

These bits of data are at an empiric stage: Each represents a raw observation and one conclusion, based on other empirical data sources from a

single civilian intelligence group. No one evaluated or investigated this information further. Had this data been allowed to progress along the semiotic chain, other connections to planned attacks for 9-11 would have become apparent.

SYNTACTICS LEVEL: THE RELATIONAL INTERPRETATION OF DATA

Failures in intelligence occur not because data is not collected; rather, there are "failures to put (it) together properly" (K. Anderson, "US Intelligence Efforts Fractured," *BBC News Online,* 18 May 2002). The syntactics level is a crucial stage in which investigators have purposefully synthesized collected data to uncover the possible and meaningful relationships among data from divergent sources. At this level, deductive processes establish a virtual reality upon which to base preliminary decision-making. In our 9-11 case, we see several activities among agencies that are intransigent because they did not properly channel available intelligence along the semiotic model.

- In August 2001, responding to FBI information, the CIA asks the Immigration and Naturalization Service to place Khalid al Midhar, a suspect from the attack on the USS Cole (in October 1999), on a watch list. The INS knows al Midhar entered the US in July 2001 but his whereabouts are unknown. Al Midhar is one of the hijackers aboard the plane that crashes into the Pentagon on 9-11.
- In early September 2001, a Minnesota FBI agent writes an analytical memo, based on the case of Zacarias Mossaoui, the "20th hijacker," arrested before the 9-11 incident. The agent theorizes about a scenario in which Islamic extremists fly a plane into New York's World Trade Center. The SIC seeks a meeting with Vice President Dick Cheney to address terrorism but the chief of staff replies that it will take six months to prepare for such a meeting.

These activities demonstrate an inability to react or respond because required information is unavailable. To properly channel these bits of information, the agencies should have acted immediately or in concert with anyone who could provide answers instead of hiding behind excuses. In effect, these agencies prevented these bits of information from passing on to the syntactics level.

SEMANTICS LEVEL: MEASURE OF SYSTEM UNCERTAINTY

Semantics, the next-to-last level of the semiotic model, derives higher-level meaning from information. Think of it as preemptive, rather than reactive, information in that if the investigators act on information efficiently and effectively, decision-makers can act preemptively rather than wait for the information-based, calculated act to materialize and then react to it. We consider semantics similar to the concept of entropy (degree of uncertainty); the value of information here is in its surprise factor.

The intelligence community again failed to attain this level of information representation. By late June 2001, a specific message seemed to be building, which indicated the intelligence community might have cause for concern. The channel that carried that message experienced noise, like all channels, but it also contained elements of certainty associated with the message. We must first consider elements in the state of positive certainty that also occupy the channel.

For example, the World Trade Center had been a target of religious extremists in 1993. Subsequent terrorist activities against US interests, though overseas, gave no indication such activities would abate. Individual bombers who strapped themselves with explosives were always a concern of the intelligence community, until agents found larger bombs in parked cars. Agents checked cars near secured buildings until terrorists started driving trucks into their targets, at which point targeted organizations erected barricades. In 1999, a

Circulation: IT Professional (ISSN 1520-9202) is published bimonthly by the IEEE Computer Society. IEEE Headquarters, Three Park Avenue, 17th Floor, New York, NY 10016-5997; IEEE Computer Society Publications Office, 10662 Los Vaqueros Circle, PO Box 3014, Los Alamitos, CA 90720-1314; voice +714 821 8380; fax +714 821 4010; IEEE Computer Society Headquarters, 1730 Massachusetts Ave. NW, Washington, DC 20036-1903. Annual subscription: $39 in addition to any IEEE Computer Society dues. Nonmember rates are available on request. Back issues: $10 for members, $20 for nonmembers. This magazine is also available on microfiche.

Postmaster: Send address changes and undelivered copies to IT Professional, IEEE Service Center, 445 Hoes Lane, Piscataway, NJ 08855. Periodicals Postage Paid at New York, N.Y., and at additional mailing offices. Canadian GST #125634188. Canada Post Publications Mail (Canadian Distribution) Agreement Number 1445669. Printed in USA.

Editorial: Unless otherwise stated, bylined articles, as well as product and service descriptions, reflect the author's or firm's opinion. Inclusion in IT Professional does not necessarily constitute endorsement by the IEEE or the Computer Society. All submissions are subject to editing for style, clarity, and space.

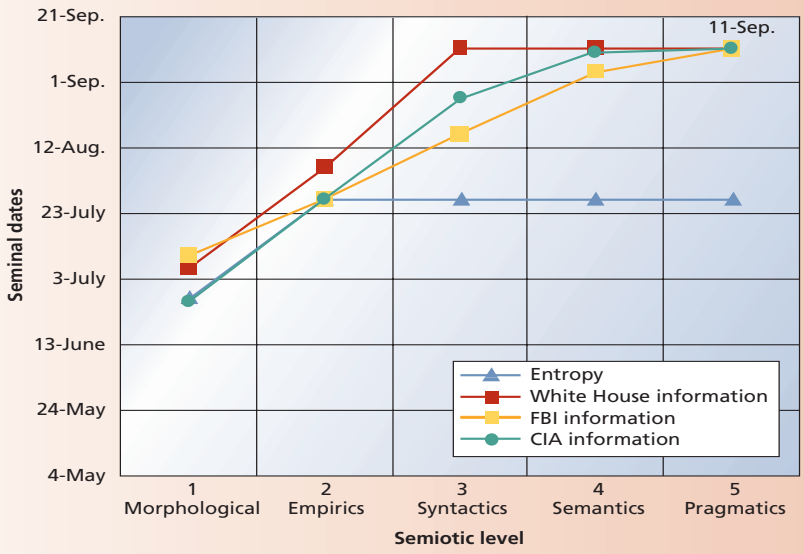
small, simple watercraft outfitted with explosives attacked a US warship and the US Navy ordered procedural changes. So it appeared the method of convenience used by terrorists was expanding. It should not have been too much of a stretch to consider that someday they might use planes. The possibility had been presented in US popular fiction (Tom Clancy, *Debt of Honor,* Berkley Press, 1994).

On 9-11, despite the erratic behaviors of four in-flight jets in the eastern US, no authority provided information indicating any threat. Following the crash at the first tower, no intelligence agency issued a threat alert. After the attack on the second tower, there was confusion. In a seemingly unrelated incident, a third jet crashed 40 miles southeast of Pittsburgh. A fourth flight made a wide pass over Washington, D.C., before banking and crashing into the Pentagon. It is only then that US military commanders took some action, activating the country's air defenses.

By mid-July 2001, this case's existing information structure lost any certainty that might have resulted in the discovery of an event that the US could identify and take action against. This does not imply that the US could have averted the events of 9-11, but the probability for a less reactionary response would certainly have been higher. In this scenario, scores of lives might have been saved.

The graph in Figure 2 represents information cited earlier and indicates approximate dates when White House, CIA, and FBI information streams crossed paths. By July, this system's entropy was at a maximum and likely irreversible. This graph represents levels of the semiotic model along the *x*-axis starting with the morphological level (data gathering) at the left and ending with the pragmatics level (beginning of actionable events) at the right. The *y*-axis indicates date ranges during which agencies collected data, evaluated information, or took independent action before attaining the pragmatics level.

Figure 2. Information timeline.



PRAGMATICS LEVEL: ACTIONABLE INFORMATION

Plausible actions are a function of the semiotic model at the pragmatics level. One objective of this level includes the action of debriefing members associated with each level as to the effect (success or failure) of their contribution to the ultimate decision(s) for action.

In Figure 1, the conclusion of the semiotic cycle is on the left side because after generation you have dissipation. As people take action, they uncover other information. Using this new information, the cycle begins again, moving through the five steps to formulate new actions.

Ultimately, the model should modify the behavior of personnel involved at various levels of the model's generation side. The change will arise from information use or nonuse.

Today's technology allows for greater data collection, but future concerns will center on how to use such data. The answer will come with the correct use of techniques in coupling systems with cohesive, associative applications. We contend that use of a semiotic approach is a viable template on which to build such techniques. ■

Kevin C. Desouza *is a research associate and doctoral candidate at the Center for Research in Information Management at the Department of Information and Decision Sciences, the University of Illinois at Chicago. Contact him at kdesou1@uic.edu.*

Tobin Hensgen *is a doctoral candidate at Loyola University of Chicago. Contact him at maxim@core.com.*