

Homeland Defense Journal

"He is best secure from dangers who is on his guard even when he seems safe."—Syrus Pabliius

Homeland Defense Journal, Inc. | Suite 1003 | 4301 Wilson Boulevard | Arlington, Virginia 22203
www.homelanddefensejournal.com | Phone: 703-807-2758 | Fax: 703-807-2758

Osama vs. Usama

The war on terror hamstrung by information management issues

By George Kondrach

October 15, 2003 - Post-9/11 information sharing among US intelligence and law enforcement agencies has not improved dramatically even though many of the problems hampering the war on terror are basic "content supply chain" issues – glitches that private-sector companies confront and overcome every day.

The FBI, CIA, Department of Homeland Security (DHS) and others continue to hunt for terrorists, but incompatible databases and communication networks rife with secrecy barriers and territorial walls often frustrate their best efforts.

Viewed as a whole, the information management challenge seems massive and hopelessly complicated, but many of these problems result from fundamental breakdowns in these agencies content supply chains. For example, one intelligence agency spells bin Laden's first name "Osama" and another spells it "Usama." Consequently, a collective search of their databases turns up incomplete results unless they set up translation registries, which they have not.

There are dozens of semantic traps to avoid and overcome. For example, there are different words that connote different items with the same meaning or identical words that represent different meanings. All of the pitfalls require a deliberate decision to map and manage meaning in the content supply chain. It's not just about information technology but about information science & their integration into a single effective approach.

This kind of problem has been tackled successfully in the private sector. Recently, an international shipping company called a truck a "truck" in the United States, but a "lorrie" in the United Kingdom. For that company's workers to communicate

effectively on one database, they built a translation registry that tied equivalent terms together, allowing for an unimpeded flow of information back and forth across the Atlantic.

A content supply chain is the information-age version of a manufacturer's supply chain: Car parts, for example, move along a chain from designer to maker to seller to reseller to dealership in the most efficient way possible. Though many organizations, including US intelligence and law enforcement agencies, do not work in a world of material "product," all organizations manufacture content of some kind. Whether that content is a parts manual or a classified dossier on bin Laden, it must be optimized for the demands made on content today, not least of which is reliable search and retrieval, information sharing and collaboration.

Since "information management" in the intelligence industry has national security implications, agencies have all kinds of firewalls and special blocking mechanisms to prevent classified content from slipping into the wrong hands. But some of those walls were created because of cultural differences between agencies, and they simply choke the flow of content from point to point, leaving holes for breakdowns.

Today, there are technologies and processes available – many of them put through their paces by information-intensive enterprises in industries like publishing, defense, aeronautics, pharmaceuticals and insurance, but the greatest obstacle to overcoming content supply chain issues is a fragmented awareness of their nature and import.

Step one is understanding a content supply chain. After acknowledging it and seeing it as a whole, it is possible to go beyond stabbing in the dark to problem solving.

About the author: George Kondrach is executive vice president with Innodata Isogen, a New York-based provider of content supply chain services and solutions.