Chapter XXXVI
Intelligence and Security Informatics

Jimmie L. Joseph
University of Texas at El Paso, USA

INTRODUCTION

Intelligence and security informatics (ISI) is the application of information systems (IS), databases, and data coding schemes to issues of intelligence gathering, security, and law enforcement. ISI differs from other disciplines of informatics because of the critical role played by the general public in data gathering and information dissemination.

Informatics provides a means of quantifying and organizing information in a manner that is meaningful to practitioners of a specific field (Sawyer & Rosenbaum, 2000; Yeh, Karp, et al., 2003). Often, informatics is of little value to the general public. Generally, understanding informatics systems requires a significant investment of time in extensive educational preparation or significant work experience in the subject being coded (von Solms, van de Haar, et al., 1994; Brancheau, Janz, et al., 1996; Sawyer & Rosenbaum). The fields of biology, sociology, medicine, and museums and archival employ informatics, but these fields filter the results through professionals who communicate mostly with other professionals in the respective fields (Kling 1999; Lorence & Ibrahim, 2003). When it is necessary to inform the public of key findings, a basic synopsis of the information is typically distributed via the general media, with a reference to professionals or organizations that can discuss, explain, or clarify the information.

While it is important to consider the user in any information system (Kling, 1999), the time-sensitive nature of intelligence gathering requires that information be collected from or delivered to the public, not just the professional informatics system user, as quickly as possible. From the perspective of IS, ISI poses unique concerns not pertinent to other disciplines that employ informatics (Atkins 1996; Kling; von Solms et al., 1994). The success of ISI is dependent upon informatics systems designed for the rapid dissemination of critical information to the general public to a degree not present in medical, biological, museum and archival, or other areas of informatics (Besser & Trant, 1994; Danchin, 2000).

IS can provide a conduit for disseminating the information in a manner that is useful to the general public. Protecting the public from security threats requires the dissemination, in a timely manner, of the threat analysis results in a format that is readily available to (and quickly digestible by) the general public. From an IS perspective, a significant factor differentiating ISI from other fields employing

informatics is the need to design a bidirectional communication with the general public.

Three major differences exist between ISI and other forms of informatics, and these differences make ISI unique in terms of data collection and dissemination. The differences are the following:

1. Data source reliability
2. The need to determine which datum is relevant
3. The need to disseminate the finding to the general public without knowing in advance the appropriate individuals or institutions needing to be informed

BACKGROUND

Disciplines using informatics traditionally acquire input from medical professionals (Database, 2003; Greiner & Knebel, 2003), scientists (Besser, Trant, et al., 1996), and professional researchers (Besser, 1995; Trant, 2000). The education and training of the contributors allows for a simplification in the coding systems because writers and coders may assume a minimal (albeit relatively high) level of audience sophistication. The results produced are for consideration by individuals and institutions steeped in the vocabulary, traditions, and skills of their specific discipline (Besser et al.; Kling, 1999; Trant). The research from disciplines such as social science informatics, bioinformatics, and archive and museum informatics impact our lives through the efforts of professionals and consultants who interpret and implement the advantages found through the research using coding systems unique to each field.

While IS contributes to medical informatics, bioinformatics, and museum and archival informatics, ISI has different characteristics. The differences, relevant to the information input and dissemination requirements for ISI, represent significant hurdles for the design of an ISI system, but also present unique opportunities to design ISI constructs that maximize the advantages offered by modern IS infrastructure. The need for the rapid dissemination of ISI results to the target audience produces public policy issues unique to the field of ISI.

Designing for Dissemination

Reliability of the Data

Reliable data are essential to both scientific and intelligence communities, and determining data reliability is a crucial factor in an intelligence system. Intelligence data may contain intentionally false information (disinformation), unintentionally false information (misinformation), correct data, and noise (information unassociated with the current problem, the correctness of which is immaterial to the current issue). Given the nature of security threats, it is possible that data that are of no value in a low-priority investigation may be lifesaving data of inestimable value in a higher priority threat investigation.

The need to gather data that are useful but uncorroborated and filter false data and noise makes ISI different in concept and implementation from other forms of informatics. In other disciplines, peer review's need for replicability of the experiment make the verification of results a core, standard part of the discipline, not a function of the informatics system (Lorence & Ibrahim, 2003).

In ISI, the data input is often raw intelligence or law enforcement data. The data represent phenomena that are not reproducible and are often unverifiable. For example, it is possible that the simple act of verifying the information may provide clues to an opponent that indicates a security leak exists within the organization, and signal that operations have been compromised. Indeed, a concern for intelligence agencies is the placement of information designed to isolate the source of a security concern by the targets of the investigation. Once false data are entered into an ISI system, analysts must decide which data are false and which are reliable.

Determination of Relevant Data

The nature of the problem dictates the types of data that are likely to be important to most re-