

The War on Terrorism – Technology Capability and Expertise

The United States of America's War on Terrorism is a challenge unlike anything that this country has faced before. Dispersed, loosely connected terror cells with little visible physical assets dictate an increased level of intelligence gathering and management focused on the identification, assessment, disruption and destruction of these terror cells. The technology tools of the civilized world are being hijacked to facilitate the coordination and communications of these cells, therefore, Internet technology is one of the key assets available to the civilized world in this ongoing war on terrorism. Surveillance of terror cell Internet-based assets and their wireless data access channels is essential to the early detection and identification of terror threats. The pervasiveness of the Internet is also a key asset to the anti-terrorism warfighters ability to easily acquire, distribute, manage and data mine information on terrorist plots, assets, organization and human resources.

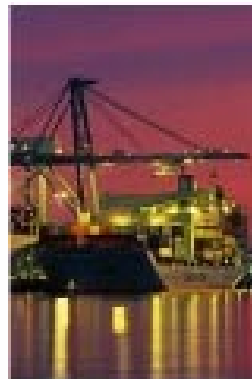
Argosy Omnimedia, Inc., a Maryland-based information technology professional services small business has been developing leading-edge Internet technology since the commercialization of the Internet in the mid-90s. This data sheet provides an overview of Argosy's capabilities, expertise and core competencies that can be marshaled in the war on terrorism.

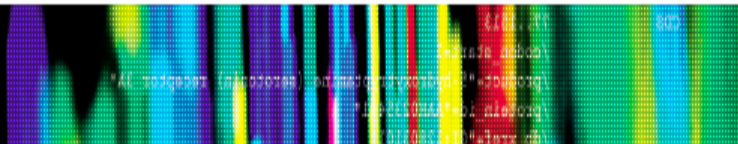
Argosy's staff has acquired or developed information technology expertise in several areas that can be applied to the tasks of secure information gathering, management, dissemination and analysis in the war on terrorism. Examples of this technology capability are:

•**DiscoveryLink** – is an IBM technology for the integration of data queries and mining across multiple, distributed, networked databases. DiscoveryLink provides an unified query interface to various disparate database technologies.

•**Web Site Content Surveillance Software Agent** – technology is embodied in Argosy's patent-pending, commercial AgentProxy product. This product gathers information using Argosy's "Go See" web site surveillance engine to acquire select information from websites and store this information in a data repository for information mining and data management of web site interaction proxies.

HubZone – Argosy is establishing a hubzone-based location in PA Congressional District 12 for an information technology development and support center.





Steganography – is the science of embedding hidden information in other content to prevent detection. The ability to detect this information relies on high-performance statistical analysis of the content and identification of patterns in seemingly random content.

Enterprise Portal – technology is used to securely acquire, manage, analyze and disseminate structured and unstructured information through a convenient browser based web site interface. The portal is the user front-end that manages secure, controlled access, auditing and user interface to a variety of information formats.

Knowledgebase – technology is designed to acquire, organize, centralize, and manage information in a number of data warehouse schemas/formats in support of rapid data mining, algorithmic analysis and human-based search. The knowledgebase is the core, back-end to the enterprise portal.

Copyrighted Intellectual Property – protection technology utilizes a number of encryption techniques that can be applied to the controlled dissemination of top secret content via the Internet. Active, interactive encryption controls can be applied to who can access information, where they can access it and for what purposes and duration (the Internet “walled garden”).

CyberSecurity – technology utilizing IP management, controlled device access, agent-based topology discovery and monitoring of IP devices (e.g. workstations, laptops, PDAs) and IAVA compliance can be applied to creating Internet “walled garden” subnetworks.

Chemi/Bioinformatics – data management and analysis tools are essential to the identification of terrorism WMDs and human resources. These tools used sophisticated data analysis tools and data mining analytics to provide DNA or RNA based identification and provenance information.

High-performance Computing – using GRID, Massively Paralleled Processing (MPP) and Symmetrically Paralleled Processing (SMP) have been utilized to manage large digital media data sets and content. These technologies enable the rapid, interactive, real-time data management and analysis of these large data sets.

Signals Acquisition and Identification – using digital demodulators enables the monitoring, acquisition and decoding of analog and digital signals across broadband frequencies. The software to automate the management of collection and analysis is essential to successful surveillance and real-time interpretation.

Linux & Open Source – have provided a vast resource of scientific analytics that can be applied to a variety of information technology challenges.

Wireless, PDA & Pocket PC – expand the ubiquity of the Internet, ease of use, and in some cases, vulnerability. These technologies can be used for both intelligence gathering and counter-intelligence initiatives.

