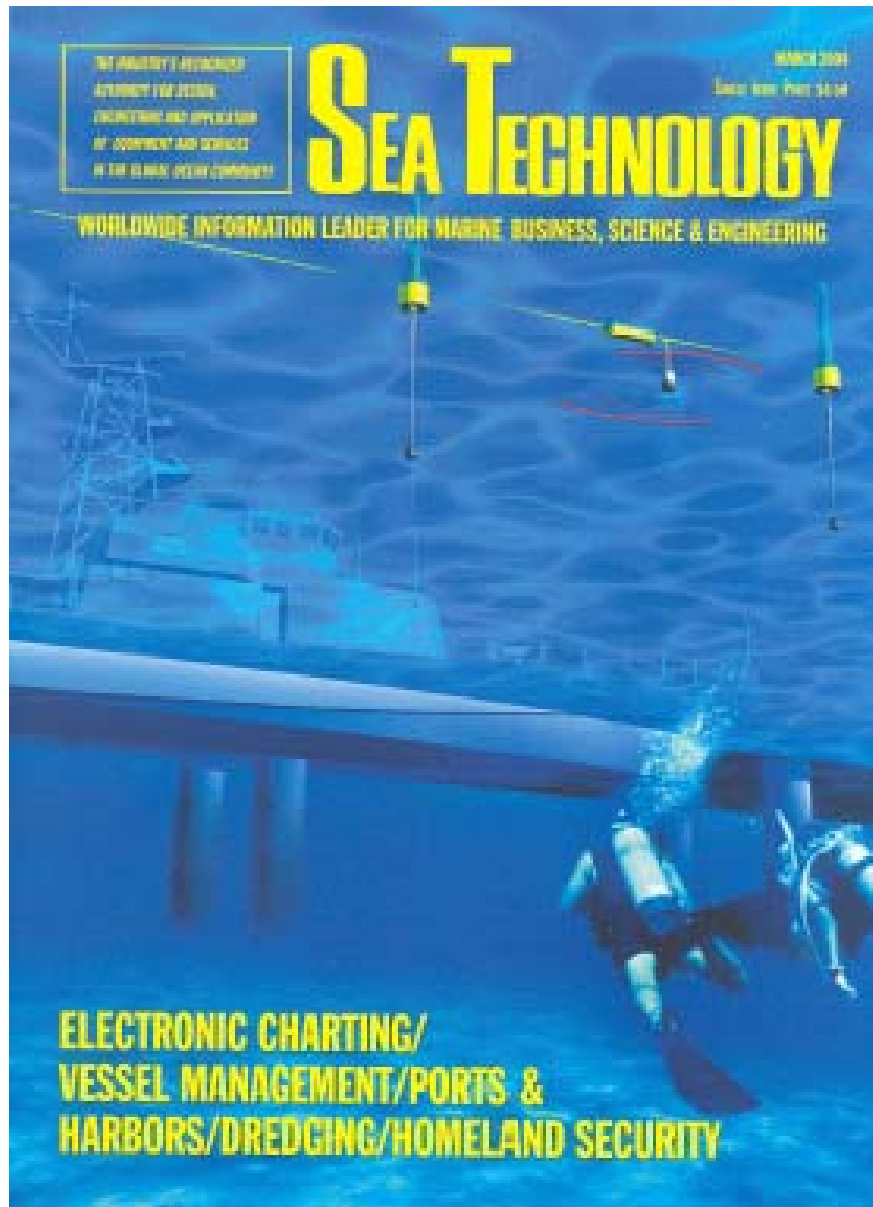


U.S. Port Security in the War on Terrorism



Published March 2004

Article Reprint

By Mr. Stephen T. Makrinos
Chief Scientist
CACI Technologies Incorporated
745 Hope Road
Eatontown, NJ 07724
Phone: (732) 578-5214
Fax: (732) 578-5201
<http://www.caci.com/>

WHITE PAPER
U.S. Port Security in the War on Terrorism

1.0 INTRODUCTION

The ever-increasing volume of globalized trade poses a particular new security threat to the United States in the post-9/11/01 period. Indeed, providing adequate security for 361 ports along 95,000 miles of open shore line is daunting to say the least. Each year more than 7,500 commercial vessels make over 51,000 port calls in the United States, unloading over seven million ISO–cargo containers. That number is expected to reach 30 million over the next 20 years, based on industry projections. And with less than three percent of shipping containers currently being inspected, the potential of terrorists exploiting these entry points into our country is frighteningly high. In order to mitigate new terrorist threats such as this, revolutionary solutions are required to minimize the physical, psychological and economic impact that such an event could have on a major U. S. port or high-density population center. CACI International Inc is working with our technology partners to identify a variety of commercial off-the-shelf and emerging technologies to be integrated into an open and flexible architecture to extend the security zone around the U.S. ports. A Concept of Operations (CONOPS) can be readily developed and adopted to a specific region that will enable the incorporation of existing sensors and capabilities, while embarking on a spiral development process that will enhance overall security, yet at an affordable price.

2.0 APPROACH

One potential solution is a Web-based information portal that can enable the various security and government agencies (Figure 1) to share and exchange information currently available in their respective databases, in near real time, and jointly create a user-based, common operational picture of the relevant security zone. This will enable users to track and engage numerous potential target vessels, over extended periods, prior to them posing a threat to any U.S. destination.

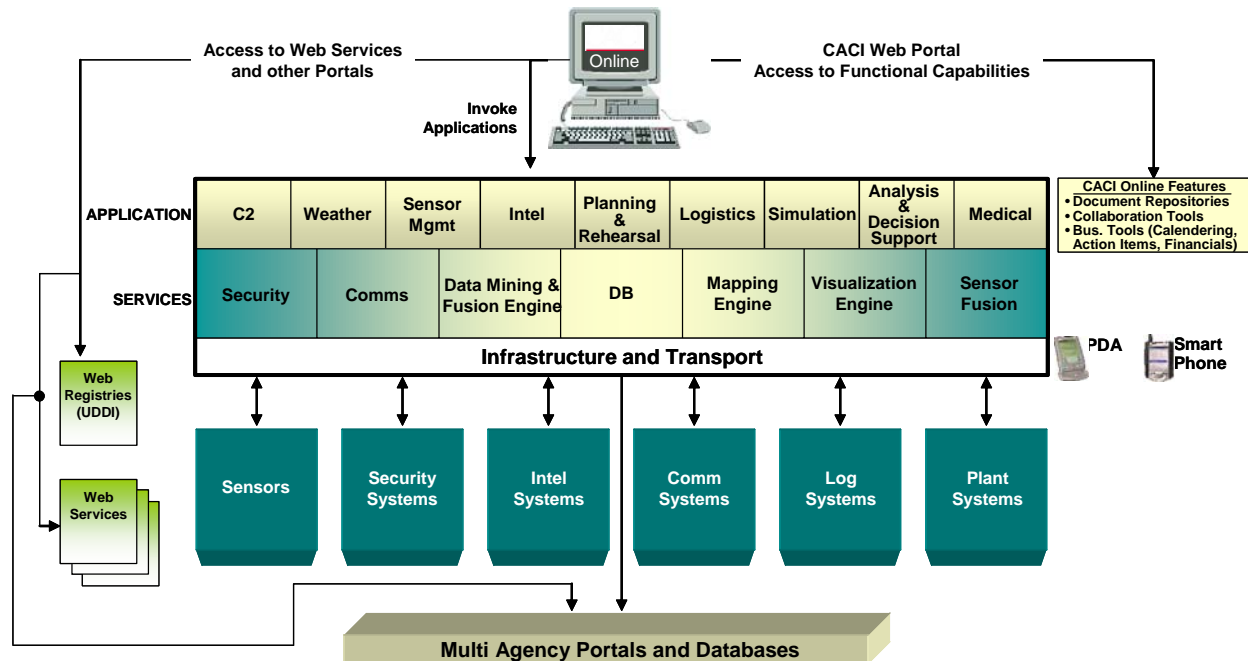


Figure 1—Architectural Concept to Coordinate Multiple Databases

The CACI Web-based information portal (Figure 2) is based on the Instaknow-ACE™ collaboration engine that enables data mining and information exchange among disparate databases without the need for new software code. The portal has the capability to gather information in the background based on pre-selected criteria set by the specific operator or initiate a process based on a trigger event. Business processes that have been identified can be stored and activated when specified conditions or pre-determined criteria are met, thus providing the required information to agency personnel and enabling them to rapidly collaborate and take action.

The CACI Web-based information portal is based on the Instaknow-ACE™ collaboration engine (Figure 3) that enables data mining and information exchange among disparate databases without the need for new software code. The portal has the capability to gather information in the background based on pre-selected criteria set by the specific operator or initiate a process based on a trigger event. Business processes that have been identified can be stored and activated when specified conditions or pre-determined criteria are met, thus providing the required information to agency personnel and enabling them to rapidly collaborate and take action.

In addition, incident management tools such as E-Team™, SPECS™, Critical Situation Management (CSM)™ and Digital Sandbox™ when integrated with the CACI portal can provide a comprehensive emergency response capability. This allows personnel from local, state or federal agencies to respond in near real time to a variety of emergency threat situations.

Space-based, airborne, sea-borne or terrestrial sensor systems currently used by the Department of Defense (DoD) or other state and federal agencies can also provide a wealth of near real time information that can be used to create and maintain a user-tailored common operational picture of the security zone. If a dedicated capability is required to meet this threat, many of these systems can be reconfigured and integrated as necessary to address the requirements of a particular region.

For example, the United States Coast Guard (USCG) may desire to attain surveillance of vessels for 36 or more hours prior to arrival in the U.S. Long endurance, high altitude Unmanned Aerial Vehicles (UAV), or other fixed wing Multi-INT platforms such as the Army's Air Reconnaissance Low (ARL), equipped with long range surveillance radars (Figure 4) can cover vast areas of ocean and coastline, providing detection, location and near real time tracking information of approaching vessels. Today, certain UAVs have the ability to remain aloft for several weeks and are being used by federal agencies to detect and track low flying aircraft as well as surface vehicles. When equipped with a variety of long range electro-optical and infrared sensors, these platforms can provide visual or thermal information and tracking of suspect vessels.

Unmanned surface and sub-surface vehicles can be directed towards a target for a closer examination of its hull and possible hazardous materials that may appear below the waterline. Underwater vehicles equipped with digital X-ray sensors can be used to penetrate the hull and provide high resolution images of the cargo holds and other compartments. Nuclear, biological and radiological sensors can also be deployed to gather additional information about the vessel's cargo in a non-intrusive manner.

Advanced intercept systems can now monitor communications and provide a vessel's location through triangulation techniques, augmenting the tracking capabilities of other systems. These and other types of multi-sensor platforms can be strategically placed and integrated along our borders to further increase security.

Newly enacted or pending international maritime security agreements will require that ship owners install devices on their vessels that would enable them to be tracked and interrogated much like the FAA tracks and identifies aircraft

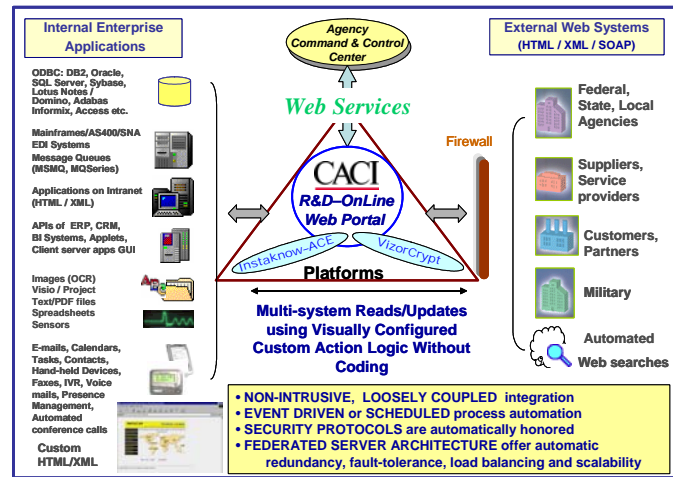


Figure 2—CACI's Web Portal Architecture Facilitates Broad, Concise, Protected Collaboration

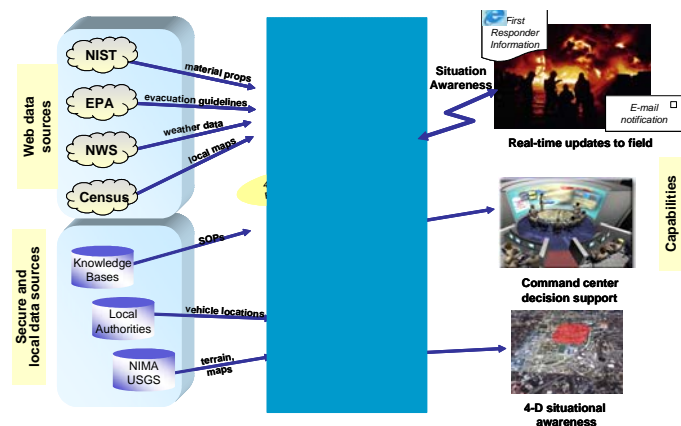


Figure 3—Instaknow-ACE™ "Talks" to All Data Sources



Figure 4—ARL Aircraft

across the globe. Integration of systems such as those developed and marketed by Outerlink Inc. (Figure 5) could be used to enable the USCG, for instance, to interrogate a vessel and obtain information about a vessel’s position, destination, cargo, number of passengers and crew, a photograph of each crew member and other relevant details. This information can then be compared with federal terrorist databases long before the vessel reaches a port of call.

Systems such as WhereNet™ provide an RF ID capability (Figure 6) that can be used to identify and/or track the contents of a container, as well as the “Skybitz” system that use satellite technology to track individual containers across the globe from factory to pier to ship to destination.

Wireless technologies and sensors such as those produced by MachineTalker™ can also be used to ensure container security. These wireless devices when placed inside a container form a kind of self-supporting network. The network is “self-forming” and when power is applied during start-up, each network goes through a discovery phase to find other wireless nodes within direct radio range. Operating in this peer-to-peer arrangement, all MachineTalker devices within radio range exchange information directly and form a “community.”

What’s more, if any member of the community goes out of radio range, the other members continue to communicate.

All MachineTalkers operate on battery power (AA batteries) and, depending on usage, have



Figure 6—Interrogation of MachineTalker Devices

a two- to five-year life. When integrated with a variety of other sensors,

MachineTalkers can provide a wealth of information about a container. They can tell if a container has been opened after it has been sealed, provide changes in temperature, humidity, carbon monoxide and dioxide, and monitor other parameters as desired. Furthermore, this data can be relayed to a ground or airborne platform (Figure 7) to be stored in a searchable database or shared with appropriate security agencies.

Needless to say, the resulting system of sensor networks and databases will generate a vast amount of information. Most of this information will be unclassified. A large portion, however, will most likely be sensitive to the parties shipping the product(s), not to mention the security agencies gathering sensor data which should remain unidentified for security reasons.

To secure this information, CACI uses Cryptsec™, a tool provided by technology partner VizorNet Technologies Inc. (Figure 8) This proprietary



Figure 5—Outerlink Provides Tracking Capabilities

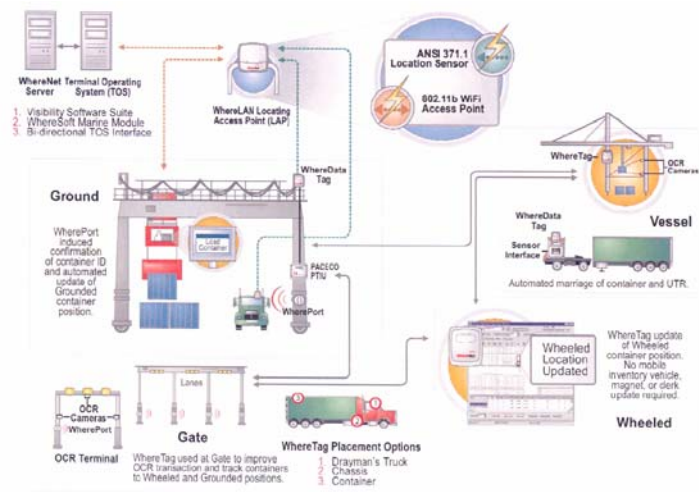


Figure 7—WhereNet's Wireless Technology Reduces Hardwire Reliance

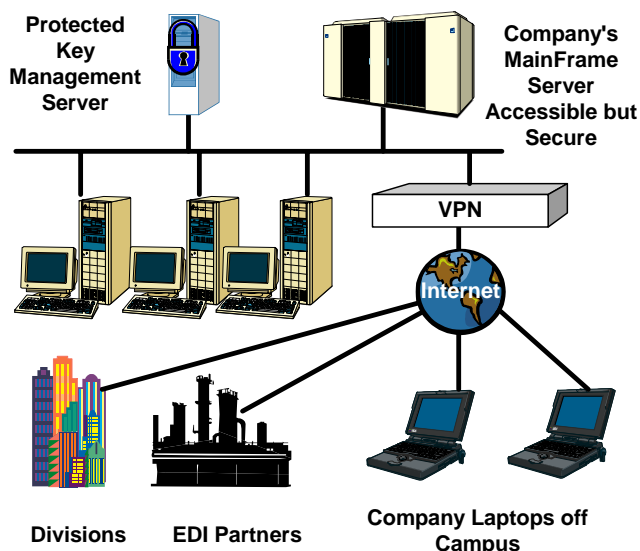


Figure 8—VizorNet Block Diagram

and patent pending split-key software encryption tool is based on the global Advanced Encryption Standard (AES). AES provides controlled client access through the use of an assigned phrase vs. a single password and/or optional access control via an ignition key or biometric device. The pass codes for the system are never stored at the work station or network storage system, and are only know by the security administrator.

The tool permanently logs all accessed data, automates and “cryptographically” enforces need-to-know access to prevent unauthorized entries (even if redistributed from a trusted source), and thereby eliminates insider threats. It allows the creation of shared groups with cross-folder boundaries, and lets the group membership to be altered without the need to redistribute encryption keys to existing members. Retroactive key revocation can be accomplished remotely by the owner or security officer. Finally, AES restricts the printing or downloading of

protected documents, thus eliminating unauthorized dissemination of information.

These are but a selected sample of sensor systems, software tools and capabilities that, when integrated with the CACI Web portal utilizing open standards and a robust and flexible architecture, can provide an affordable, feasible port security solution. CACI has over 40 years of experience developing and deploying effective processes and procedures for DoD, civilian, and commercial clients alike that have been well-tested and proven in simulated as well as real time (battlefield) situations. Innovative and evolutionary approaches such as these are key to meeting, and defeating, the new terrorist threat of the 21st Century.

For more information:

Mr. Stephen T. Makrinos
Chief Scientist
CACI Technologies Inc.
(732) 578-5214
smakrinos@caci.com