LAW ENFORCEMENT TECHNOLOGY FOR MARITIME INTERDICTION

Samuel A. Musa and Thomas J. Calabro

National Defense University and Computer Deductions, Inc.

The application of the Chicago Citizen and Law Enforcement Analysis Reporting (CLEAR) system to Maritime interdiction operations and port security has been demonstrated in several exercises. The CLEAR system leverages information technology in prosecuting law enforcement operations against gangs, drug cartels, and other crime. The system provides instantaneous access to information on criminals and tracks criminal trends. Biometric identification using high-resolution hand and facial scanning capability is used to identify criminals at the beat cop level. In addition, it mines multiple databases for link analysis and operational planning. The system consists of a database/data correlation/data mining/knowledge system based on Oracle's commercially available 9i database and associated Developer suite, and biometric collection units.

The objective of the Maritime field experiments was to evaluate the capability of collaboration and data sharing between several boarding parties engaged in the interception and search of multiple small craft penetrating metropolitan areas. The identification of the intercepted individuals in the geographically distributed areas coupled with the link analysis among the individuals is of great value to Maritime interdiction operations. The test assessed the ability of a CLEAR like system with its communication architecture and layered database to produce actionable intelligence during such operations. A specially configured biometric collection unit (MV-100) was used to take two fingerprints, a mug shot, and other demographic data. The unit has three modes of operation, chosen by the operator in the field as needed, Full Encounter ID (collection of full demographic and location information including voice recordings, multiple fingers, GPS readings and person & affiliations), Fast ID (collect simply two fingers and a GPS location to check for known person) and QUICK ID (Check only the local Fingerprint database of up to 10k records in the handheld device). All three modes include a local "Bad Guy" fingerprint search on the handheld device, which takes seconds to complete. A number of records were stored in the device for potential initial matching. If there was no match, then the data was transmitted to a Tactical Operations Center where the second match took place at the server (laptop). The server had a much larger database. The data was then transmitted via a virtual private network to a Fusion Center for access to a significantly larger database for matching. The response from the Center was then transmitted to the server and then returned to the handheld device for action. This response to the field device contained information including but not limited to, prior "Encounters" (locations) that this individual was at, known affiliates, and prior information collected in the field, including notes, photos and voice recordings. The response is presented in a WEB like format directly on and within the handheld device, allowing the field operator to navigate through the multiple response messages as needed. The most recent experiment extends this capability to multinational locations for biometric collection, data correlation and link analysis.

The CLEAR like system can accept inputs simultaneously from multiple devices with different technologies and can process the information in a matter of seconds. The devices can provide instantaneous identification based on the stored database. It can also provide link analysis and associations among the collected information. This capability has been proven based on commercially available technology.