Toward a Comprehensive National Incident Management System:

"What Is" Versus "What Could Be"

By Mr. Norm Mueller and Ms. Mary Bergeron

The progress associated with using technology to collect and store data has far outpaced the ability to process or convert that data into useful or, more precisely, actionable information. Closing this dangerous knowledge gap (the proverbial example of "what is" versus "what could be") was at the heart of a recent award-winning project conducted at the Coalition Warrior Interoperability Demonstration (CWID) 2007. The project demonstrated how the gap, precipitated by the breakdown in communication between those who hold useful information and those who are in a position to act on that information, could be successfully closed during an emergency pursuit to save lives, preserve property and infrastructure, and protect the environment.

On an annual basis, CWID provides a globally networked environment where military commanders investigate command, control, communications, computers, intelligence, surveillance, and reconnaissance solutions that can be used by military and civilian organizations. At CWID 2007, key military and emergency management decision makers witnessed, for the first time, the Integrated Information Management System (IIMS)—a truly interoperable system and a watershed in domestic security. A broad spectrum of public and private-sector organizations participated in the demonstration. The coordinated technologies of IIMS offered military and civilian leaders an improved common operational picture (COP) for use in critical decision making.

The Challenge

The key to creating and sharing actionable information in support of domestic defense and security missions lies in the ability of the defense domain to shepherd accurate data into and out of the civilian emergency management arena in a timely manner. This is of particular interest to the Chemical community, which is responsible for preparing for and monitoring potentially hazardous chemical, biological, radiological, and nuclear events. By leveraging science and technology, the defense Chemical community collects and evaluates critical data using sophisticated tools such as field sensors and predictive dispersion modeling. But then what? Is there more that could be done?

The technical structure of computer messages within the Department of Defense (DOD) is governed by the U.S. message text format (USMTF). Until recently, however, there was no overarching agency to create and mandate standards for data formats and messaging within the civilian emergency management community. Non-DOD data formats and messages were independently determined by a variety of vendors who were trying to support the civilian emergency management community.

These independent development efforts resulted in dissimilar emergency message formats and a variety of human interfaces, creating confusion among military and civilian emergency personnel during potentially life-threatening situations and undermining efforts to create common standards and interoperability.

Civilian Background

In October 2002—with the interoperability problems that surfaced during the tragic events of 11 September 2001 in mind—the Emergency Interoperability Consortium (EIC) was formed to focus on issues related to interoperability standards for emergency and incident management. The EIC provided a means for public agencies, private companies, and nonprofit organizations to unite in a public forum, address the absence of interoperability standards, offer solutions, and create standards that would represent best practices and consensus.

From its early days, EIC worked closely with the Emergency Management Technical Committee of the Organization for the Advancement of Structured Information Standards (OASIS). Their combined goal was to begin creating requirements for standards. In January 2005, EIC formed a partnership with the Department of Homeland Security (DHS) Disaster Management Program

to encourage and provide guidance for the development of standards.

As a result of wide industry input, the first OASIS message format—Common Alerting Protocol (CAP) Version 1.1—was created. By developing a message translator that maps applicable civilian CAP information fields to similar USMTF fields and vice versa, nonmilitary and military groups could "talk" to each other to develop a COP in the midst of an emergency situation.

Military Background

In October 2006, the Nuclear, Biological, and Chemical Battlefield Management Team at Edgewood Chemical and Biological Center (ECBC) and the Air Force Research Laboratory Information Technology Division joined forces to address the need for accurately passing military messages to civilian emergency managers. Their goal was to develop an interoperability tool and demonstrate it at CWID 2007.

For eight months, participants planned the configuration and established objectives to be met. These objectives included demonstrating interoperability among various military and civilian hardware and software systems and sharing CAP 1.1 messages and polygons across civilian, DHS, and DOD domains. Polygons, which are shapes (rather than text) that represent important places or conditions on a map, are particularly important but challenging to communicate. Examples of typical polygons include roadblocks, staging areas, and hazard outlines.

In addition to fulfilling the stated objectives, the group had bigger ambitions. They sought to uncover additional areas for improvement so that they could make recommendations for the future. Two significant issues surfaced.

First, because CAP 1.1 is the only approved message standard and not all systems support this standard, stakeholders were forced to find work-arounds. This encouraged collaborative problem solving among a variety of organizations and likely influenced the direction of future development efforts, prompting organizations to develop technical specifications that would accommodate future standards.

Secondly, arriving at commonality on even simple matters, such as units of time and organizational labels, proved challenging. In IIMS, which was tailored to address the needs of local response teams, minutes and hours are used to measure process milestones. However, it may take seventy-two hours for a federal response to commence; so in those cases, time must be measured in larger units. Also, a single point on a postdisaster timeline may simultaneously represent a federal response and a local recovery.

Preparation for the CWID 2007 demonstration helped uncover these issues, which in turn, encouraged the spiral development process used in defense transformation efforts. Vendors also benefited from the process. They received feedback and suggestions regarding their products and processes. As a result, many systems were reprogrammed, incorporating new capabilities and more user-friendly screens and processes.

Preparation and Demonstration

In March 2007, ECBC conducted a laboratory trial to test message translators and message-passing capabilities. One of the key findings of the project was made during the laboratory trial.

Each of the CAP-compliant software platforms used in the trial had been developed independently using different business models and delivering different interpretations and implementations of the CAP standard. The potential existed for these independently developed graphic user interfaces to display CAP messages differently—and they did. So, even though the message data followed a standard format, the presentation of the data was not standard.

This discovery, which was considered critical by the emergency management community, was presented at a special briefing to the EIC. As a result of the briefing and pressure from the emergency management community, numerous commercial software platforms were modified to address the problem.

As technical development and testing progressed, steps were taken to more closely replicate the CWID environment. A simulated emergency operations center (EOC) was mobilized aboard a large motor home. It provided a nonmapped workflow platform representing multiple local and state jurisdictions using a variety of emergency management software applications. The EOC contained ten laptop workstations and multiple briefing/status areas.

The mobile unit was able to take advantage of local power and internet infrastructure or operate autonomously via onboard diesel generators and its own satellite dish. The information technology architecture of the EOC was also adaptable. It operated on thin client user interfaces with a central processing server, but was also set up to support internet connectivity for standard thick client laptops and thin client applications.

In addition to technical testing, scenario testing was also conducted. ECBC directed that the scenarios be as credible as possible to ensure that each message made operational sense to the players and simultaneously

proved technical success. Software manuals and player guidebooks were put through the paces, and the group's ability to maintain "controlled confusion" in the pursuit of effective problem solving was tested. ECBC wanted to observe how the players in an unscripted environment would use the military and civilian software platforms to communicate and share actionable data. The hope was that in such a near real-world scenario, user needs would be revealed. Such scenario testing is indicative of the type of forward thinking that continues to support ongoing Homeland Security Exercise and Evaluation Program-compliant tabletop exercises.

CWID itself held a number of planning and coordination meetings, some of which involved adjustments to the proposed configuration for the demonstration. Final CWID preparations included the shipment and delivery of hardware to the Naval Surface Warfare Center, Dahlgren, Virginia.

During the actual CWID exercise, IIMS demonstrated dynamic data sharing, enabled on-the-fly collaboration between military and civilian sectors, and demonstrated increased efficiency and effectiveness of responses to simulated events ranging from earthquakes, wildfires, and other natural events to acts of chemical, biological, and radiological terrorism. The demonstration paved the way for a practical, affordable approach to the data-sharing aspect of the National Incident Management System (NIMS).

Key Players

The success of IIMS can be attributed to the joint cooperative effort among the military, state and local emergency responders, and the private sector. Approximately sixty people from a variety of organizations contributed to the success of this project.

Movement Toward a Best Practices Solution

IIMS is a software tool that assists the installation commander in the efficient deployment of the observe, orient, decide, and act (OODA) loop during an emergency.[1] IIMS addresses the *observe* role of the OODA loop by providing the near real-time operational status of the installation and surrounding area. With IIMS, seemingly unconnected incidental data and events can prove to be critical information as the commander properly orients to the threat.

IIMS can display disparate observations in its COP—a potential clue that an adversary might be trying to disrupt the ongoing mission. In the event that a continuum of these types of asymmetric threats is encountered, multiple observations can be made and input into IIMS, further strengthening the *observe* element of OODA. If managed manually, the input of data could be labor-intensive. And without warning, an additional follow-on disaster such as a new attack or infrastructure failure could occur. This would increase the amount of data to be analyzed, rendering manual information processing completely ineffective.

In addition to assisting with the deployment of the OODA loop, IIMS provides operational recordkeeping in support of postevent analysis. Not only does the electronic record contribute to the creation of a valuable resource for studying lessons learned, but it also provides an official government record that could be used in a court of law.

The IIMS also helps support the installation commander's decision-making process for determining the appropriate mission-oriented protective posture (MOPP). IIMS contains specific elements designed to quickly assimilate chemical warfare agent contamination data and orient the commander to the threat. Continuously updated information provides a current COP, orients the commander to the near real-time threat, and assists in decisions to reduce MOPP levels in uncontaminated and unthreatened areas of the installation.

From a purely technical perspective, IIMS serves as a research and development software platform, aiding in the development and testing of new concepts at operational installations. The system provides a reliable test bed configuration for evaluating components and transitioning successful elements into programs of record.

Conclusion

The success of the IIMS project at CWID 2007 positively affects our Nation's domestic security and emergency management efforts by—

- Bridging the data exchange between critical and historically untethered organizations (such as DOD and civilian security agencies) with affordable, available technologies.
- Considering communications and interoperability standards as more than action items for the long term—proving them to be doable, affordable options for today.
- Encouraging emergency management software vendors to consider modifying software to reflect standards and guidelines.
- Encouraging emergency planners to promote interoperability immediately by using informally approved data formats to create temporary, voluntary standards in lieu of formal standards.

- Showcasing best practices for vendors cooperatively working to improve offerings to defense and emergency management sectors.
- Raising emergency managers' expectations of CAP messages, thereby increasing the demand for clear, understandable headers and content.
- Promoting CWID and its offerings, including ambitious objectives such as determining relevant technologies; quickly and affordably demonstrating and fielding effective solutions; and identifying gaps in service, cooperation, and coordination.
- Creating a catalyst for change. Presenting IIMS at CWID 2007 encouraged industry leaders to begin taking cooperative steps in support of a comprehensive NIMS.

Endnote:

[1]The OODA loop, developed by John Boyd, is a well-tested, well-accepted combat assessment process that exercises the following tasks in a cyclical fashion: observe, orient, decide, and act. The cycle continually repeats until victory or defeat is declared. It has been demonstrated that engagements are typically won by those employing the fastest assessment and decision cycle. Due to its deployment record in exercises and combat, the OODA loop has been embraced within DOD.

Mr. Mueller, a former Army Chemical officer, is the associate manager of chemical, biological, radiological, nuclear, and high-yield explosives at IEM, Incorporated. He holds a bachelor's degree in mechanical engineering from Michigan Technical University and a master's degree in public administration of emergency management from Jacksonville State Univeristy, Alabama.

Ms. Bergeron is a marketing specialist with IEM, Incorporated. She holds a bachelor's degree in arts and sciences from Louisiana State University.

Address Corrections Requested

If your military unit has experienced difficulties receiving *Army Chemical Review*, please send us your correct, complete mailing address. We frequently receive returns when no street address is listed for the organization, so **please include a street address for your office**. E-mail <*leon.mdotacr@conus.army.mil*> with "Address Correction" in the subject line. If you prefer regular mail, our address is:

Army Chemical Review
464 MANSCEN Loop
Building 3201, Suite 2661
Fort Leonard Wood, Missouri 65473-8926

Address changes for personal subscriptions should be sent to Superintendent of Documents, ATTN: Mail List Branch, Mail Stop: SSOM, Washington, D.C. 20402.

Chemical Knowledge Network Web Site

Do you need up-to-date information about chemical career management, courses, equipment, doctrine, and training development? All of this information and more is available at the Chemical Knowlege Network Web site. To visit the CKN, go to the Fort Leonard Wood Web site <*http://www.wood.army.mil/*> and select *Maneuver Support Knowledge Network (MSKN)* in the lower left-hand corner of the home page. At the Army Knowledge Online (AKO) portal, log in using your user name and password. Under *MANSCEN [Center of Excellence] CoE Links,* select *CBRN* to check out this great resource.