

Defence Interoperability for Crisis Management

It is a simple fact that intelligence-gathering and operating agencies do not like to share. Irrespective of this reality, the events of 9/11 are forcing greater sharing of critical information and imposing major cultural changes within these communities. There is now a near universal call for increased sharing of intelligence and situational awareness information among these International, Federal, Provincial (State) and Municipal agencies.

The most detailed recommendations came from the *Congressional Joint Inquiry Into 9/11* that recommended:

“full utilization of existing and future technologies to better exploit terrorist communications; to improve and expand the use of data mining and other cutting edge analytical tools; and to develop a multi-level security capability to facilitate the timely and complete sharing of relevant intelligence information both within the Intelligence Community and with other appropriate federal, state, and local authorities” – *Final Report of the Congressional Joint Inquiry Into 9/11*

Although a statement of US intent, many of these objectives are mirrored by statements and initiatives within Canada's federal, provincial and municipal governments. In the current environment of terrorist threats, the desire and need to share information among first responders, various law enforcement agencies, and the military is growing rapidly. Let us not forget - customs, immigration, law enforcement, fire services, health services, and government planners that all need to be able to contribute and access information.

Looking beyond the war on terrorism, there has and continues to be a growing need for information across the broader community of organizations responsible for the protection of territory, sovereignty, population, and/or infrastructure from both man-made emergencies, such as chemical spills, and for such natural disas-

ters as floods, ice storms and earth quakes. The challenge is “establishing information interoperability within existing communication infrastructure and information assets”, while protecting the privacy, confidentiality and security of these assets. With the focus on existing assets and technology revolving around a reality of resource limitations and the prohibitive cost of the alternative - transforming the culture and IT infrastructure of a large cross section of government organizations and agencies.

It used to be simple stuff, like voice over radio – but the advent and deployment of increasing numbers information gathering technologies, large databases of highly sensitive information are being created, often encrypted, and often unique to the domain where the systems are being employed. It is the information from these evolving sources that needs to be shared among a wider community of interest without breaching legislated privacy and security requirements.

Not to be forgotten, as governments, organizations and agencies increasingly rely on technology to track, analyze, store and communicate their information, they are increasing the challenges of less developed countries, non-government organizations (NGOs) and private volunteer organizations (PVOs). It is these countries where one finds many of the operational deployments, the lack of needed infrastructure and most of the NGOs and PVOs. Solutions developed to deliver interoperability must factor in the needs of the operational environments and the capabilities of the developing world. This has both technical and legal implications that need to be resolved, first nationally, then with regard international sharing of data.

Challenges

The challenges are considerable and rise from the cultures of the organizations being asked to address the requirements to

more effectively share information. The basic challenges have been documented in numerous reports:

- Solutions must address the different information and technology needs of this diverse community of interest.
- The wholesale replacement of existing information technology and communication infrastructure is impractical based on financial and cultural considerations.
- The requirements for interoperability are not well understood by the community at large and will evolve over the course of years – static, proprietary solutions will not cope with the complexities and transforms needed for interoperability.
- The systemic aversion to sharing information and the perceived uniqueness of information within each community must be addressed in order for any technological solution to be effective.
- Cultural, social and legislative challenges such as language of interoperability, freedom of information and information Privacy.

It all seems overwhelming, but there is some light at the end of the tunnel!

Successful Approach – MIP

Though relatively new to many federal, provincial and municipal government organizations and agencies – the need for inter-agency and international communication and information interoperability is not new to the department of National Defence (DND) and the North Atlantic Treaty Organization (NATO).

DND and its allies have been investigating numerous procedural and technological solutions with varying degrees of success. One initiative that appears to hold significant promise is the *Multilateral Interoperability Programme* (MIP) programme, which includes the participation of more than 20 nations. DND has been a leading contributor to the success of MIP, which has as its objective:

“To achieve international interoperability of Command and Control Information Systems (C2IS) at all levels from corps to battalion, or lowest appropriate level, in order to support multinational (including NATO), combined and joint operations and the advancement of digitization in the international arena.”

MIP conducts annual testing and demonstration of this evolving system with each of the participating nations. Each nation is

responsible the development and testing of a MIP solution and its integration into their national infrastructure and procedures.

The MIP specifications effectively define a coalition standard for the sharing of situational awareness, planning, and other operational information assets that enhances coalition (multi-nation, multi-organization or multi-agency) capability and flexibility beyond the legacy of structured messaging. These enhanced capabilities are only limited by the coalition's ability to agree on semantics (content and structure) for information exchange, and each partner's ability to convert information to a common database structure and security infrastructure. The MIP community is continually enhancing and extending the MIP specifications on a two year cycle which is published on an open Web site (www.mip-site.org/).

MIP interoperability is delivered through two primary specifications – the C2IEDM (Command and Control Information Exchange Data Model, which defines information structure and rules for exchange of information within a coalition), and the Data Exchange Mechanism which delivers a common infrastructure for the exchange of shared information. The purpose of the programme is to deliver information interoperability while allowing participating nations to choose technology that best meets its own national objectives.

Crisis Management

Of the MIP successes, the one most applicable to the broader Crisis Management/Response Community is the C2IEDM which provides and universal expression of the information sharing requirements for:

- Situational awareness;
- Operations management and control, reporting; and planning.

Crisis Management organizations face many of the same challenges the nations and organizations participating in MIP:

- Dynamically evolving requirements for information exchange, integration, interoperability, security, privacy and confidentiality;
- Deployed operations employing limited technology and challenge communication links (e.g., High Frequency Radio);
- Inability to centrally mandate operating policy to the responding organizations and agencies; and

- Inability to centrally mandate technology solutions to the responding organizations and agencies.

Based on the similarities in the two environments, it would appear many of the MIP concepts and approaches (such as retention of data ownership) can be readily adapted to information sharing for crisis prevention, management and response. As a minimum, a crisis management/response organizations and agencies could leverage and reuse: MIP's common data structure; its approach to database management and ownership; the framework for defining exchange agreements and semantics; and the MIP framework for contract based information exchange.

Why reinvent the wheel?

It is becoming more and more important to fully integrate crisis management system interoperability with other Crisis Response Organizations that include:

- First responders;
- Emergency Medical Personnel;
- International, Federal, Provincial, and Municipal Government Organizations and agencies;
- Non-government Organizations;
- Utilities;
- Private Venture Organizations; and
- Military Organizations.

The MIP can be adapted to enable interoperability between military and non-military organizations involved in planning for, responding to, or managing national and/or international crisis situations.

There exists an opportunity for Crisis Management/Response Organizations to leverage on-going military and commercial initiatives. The most effective way to do this is directly participate in the development of these specifications and standards. We don't need to reinvent the wheel in order to accomplish the complete integration of crisis management services and intelligence. **FI**

Michael Abramson is a founder and CEO of Advanced Systems Management Group Ltd. (www.asmg-ltd.com), has been a consultant to government and private sector organizations for more than 20 years, and is currently the Co-chair of the OMG C4I Domain Task Force (www.omg.org). He can be reached at (613) 567-7097 or abramson@asmg-ltd.com

Allen-Vanguard

The new name in CBRNE



Two of the best known names in dealing with improvised terrorist devices have combined to create one company with an integrated set of solutions against all hazardous devices and materials, whether *chemical, biological, radiological, nuclear or explosive* (CBRNE).

PW Allen, of Tewkesbury, UK, is long established in providing specialist equipment for dealing with improvised explosive devices. **Vanguard Response Systems**, headquartered in Ottawa, Canada, has the world's leading technologies and products for neutralizing and mitigating toxic devices and materials, including bio-chemical devices and "dirty" (radiological) bombs.

Both Allen and Vanguard develop and manufacture innovative technology solutions in close collaboration with users to address the ever-evolving threat of CBRNE devices. Now, branding under **Allen-Vanguard**, their combined expertise and product suite ensure that specialists dealing with terrorist devices can turn to one company focused exclusively on ensuring the most advanced solutions for a safe resolution to the whole range of CBRNE threats.

Signature products include: the Universal Containment System™; BombTec™ EOD/IEDD systems; a full suite of small, medium and large ROV's – the Vanguard™, Defender and Responder robots; SearchTec™ security search equipment; and, Electronic Counter-Measures equipment.

Allen-Vanguard is committed to supporting the life-and-death mission of CBRNE specialists with training and technical support, including advice on optimal use of equipment.

Contact: Jonathan Chapple,
VP Sales & Marketing (North America)
613-747-3590 jchapple@pwallen.com

www.allen-vanguard.com