Crisis Response Interoperability System: Enabling Multi-National and Multi-Agency Defence Against Terrorism

Jean Roy, Dany Dessureault, François Létourneau
Defence R&D Canada – Valcartier
2459 Pie-XI Blvd. North
Val-Belair, Quebec
Canada, G3J 1X5
Fax: 1-418-844-4538
www.valcartier.drdc-rddc.gc.ca

jean.roy@drdc-rddc.gc.ca / dany.dessureault@drdc-rddc.gc.ca / francois.letourneau@drdc-rddc.gc.ca

ABSTRACT

We live in an increasingly interconnected, complex and often dangerous world, and recent events have moved the issues of anti- and counter-terrorism, national/public security, and collective emergency response to the fore of concerns of many nations. Large-scale terrorist emergency situations necessitate the ability to coordinate multi-agency and multi-national operations. Advanced information management technology is required to enable the emergency response communities to timely and securely access data, information, services, etc. relevant to their roles and responsibilities. In this regard, this paper described a new R&D project, called Crisis Response Interoperability System (CRIS). A brief review of Canada's national security policy is presented. Key concepts of emergency management are outlined. An analysis of the characteristics of emergency management, and also of the information management requirements associated with the collective response to emergencies, is presented. Highlights are presented of a vision to structure a knowledge environment framework capable of laying the foundations of a situational awareness knowledge portal. The specific objectives of the CRIS project are summarized, and a number of system requirements are listed. Then, some enabling technologies for the project are discussed. Finally, the R&D methodology used for the CRIS project is described.

1.0 INTRODUCTION

The military viewpoint alone is not sufficient to meet the increase in terrorist threat that is diverse and unpredictable, as such threat requires a consideration of collective security that expands to cooperation with multiple non-military organisations. Actually, working effectively in terrorist emergency situations requires the ability to communicate and to coordinate multi-national and multi-agency operations in a seamless environment. There are vast quantities of data and information requiring weeding, sorting, and analysis. Clearly, advanced information management technology is required to enable the emergency response communities to timely and securely access data, information, services, etc. relevant to their roles and responsibilities, regardless of what agency operates the facilities where the critical data and services reside.

This paper describes a new R&D project, called Crisis Response Interoperability System (CRIS), that has recently been undertaken at Defence R&D Canada – Valcartier (DRDC Valcartier). Section 2 presents a brief review of the relevant aspects of Canada's national security policy. The scope of the policy is discussed, followed by an outline of the proposed integrated security system. Consequence management and emergency

Paper presented at the RTO SCI Symposium on "Systems, Concepts and Integration (SCI) Methods and Technologies for Defence Against Terrorism," held in London, United Kingdom, 25-27 October 2004, and published in RTO-MP-SCI-158.

planning and management, are then examined. The key concepts of emergency management, with some emphasis given to the collective management of large-scale terrorist events, are outlined in Section 3. Definitions are provided, and the response phase of the emergency management cycle is described. The key primary responsibilities for crisis and consequence management are summarized, and the National Support Structure (NSS) in Canada is explained, leading to the notion of multiple interacting jurisdictions. Section 4 provides a coarse analysis of the characteristics of the emergency management domain, and of the high-level information management requirements associated with the collective response to emergencies. Section 5 presents highlights of a vision that has been developed, for an ongoing technology demonstration project at DRDC, to structure a high-level knowledge environment framework capable of laying the foundations of a situational awareness knowledge portal. A model supporting the knowledge environment is presented, introducing the important concepts of context, ontology and portfolio.

The specific objectives of the CRIS project are summarized in Section 6, and a number of system requirements are listed. The CRIS Horseshoe Architecture Concept (CHAC) that shows, at a conceptual level, the interaction between the end-users and the CRIS is described, and a service-oriented architecture framework is briefly discussed. Section 7 is about some enabling technologies for the project. Portal and web services technologies are considered. Geospatial data and geospatial visualisation and analysis services, and advanced representation techniques and visualization approaches are also of particular importance to the CRIS project. The R&D methodology used for the CRIS project addresses end-user requirements, needs and interests. It can be viewed from two perspectives: top-down (end-user business process and requirements) and bottom-up (building on existing relevant products). These perspectives are discussed in Section 8, along with the technological demonstrations planned for the project for the evaluation and validation of the resulting system during some exercises or joint demonstrations with the project partners coming from the operational community. Finally, some concluding remarks are provided in Section 9.

2.0 CANADA'S NATIONAL SECURITY POLICY

Canada’s first-ever comprehensive statement of national security policy is presented in [1]. The document outlines the integrated security system the Government of Canada (GoC) will build. Addressing many of the threats requires a more integrated, co-ordinated approach to national security, integrated inside the GoC and with key partners (i.e., provinces, territories, communities, the private sector and allies). The focus of the policy is on events and circumstances that generally require a national response as they are beyond the capacity of individuals, communities or provinces to address alone. The policy adopts an integrated approach to security issues across government. It contains several measures to help build a more integrated security system in a way that is consistent with the goals of the policy.

2.1 The Scope of the National Security Policy

National security deals with threats that have the potential to undermine the security of the state or society. These threats generally require a national response, as they are beyond the capacity of individuals, communities or provinces to address alone. National security is closely linked to both personal and international security. While most criminal offences, for example, may threaten personal security, they do not generally have the same capacity to undermine the security of the state or society as do activities such as terrorism or some forms of organized crime. Given the international nature of many of the threats affecting Canadians, national security also intersects with international security. At the same time, there are a growing number of international security threats that impact directly on Canadian security and are addressed in this strategy. Figure 1 illustrates these concepts.

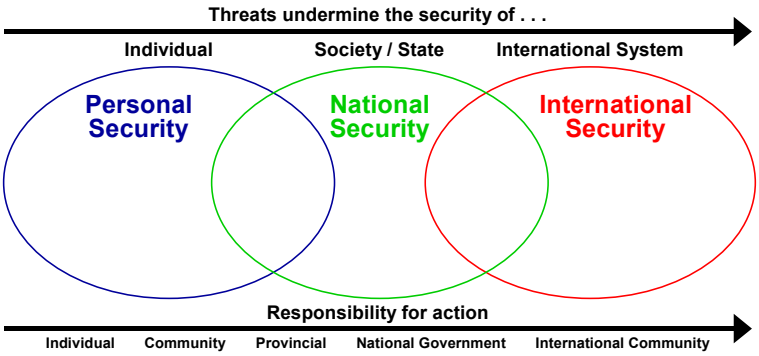

Figure 1: Personal-national-international security [1]

The middle ellipse in the chart of Fig. 1 delineates the focus of the national security strategy. The security environment includes a wide range of often interrelated threats. While all threats ultimately impact on individuals, threats to national security have the capacity to seriously impair the security of Canada. A growing number of international security threats impact directly on the national security of Canada. The type of response required also differs as one moves along the continuum. Individuals have a primary role in taking responsibility for their personal security. Their efforts can be amplified when they work in communities to address challenges in their midst. As threats become more significant, they may require the assistance of the local police, a provincial government, a national government or the wider international community to address them effectively. While the Government has a role to play in all three areas of security, the National Security Policy focuses on national security threats.

2.2 Building an Integrated Security System

The increasing complexity of the threats facing Canada requires an integrated national security framework to address them. Figure 2 articulates the integrated security system that the GoC is developing.

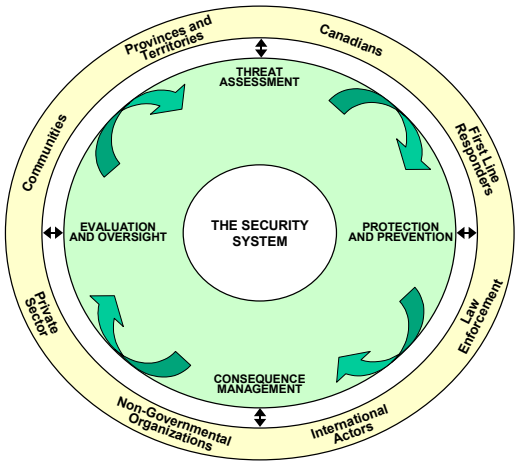

Figure 2: The integrated security system [1]

It is critical for our key security instruments to work together in a fully integrated way to address the security interests of Canadians. The lack of integration in our current system is a key gap that has been recognized by the Auditor General of Canada. The GoC agrees that the key to providing greater security for Canadians and

to getting the most out of our security expenditures is to co-ordinate and better integrate our efforts. The Government is committed to providing the leadership, resources and structures necessary to build a fully integrated and effective security system. The Government is building a fully integrated security system that ensures that we can more effectively respond to existing threats and quickly adapt to new ones. The evolving nature of threats to Canadians requires a fully integrated government approach that ensures that issues and information do not fall between the different parts of our security system. This system needs to be fully connected to key partners, i.e., provinces, territories, communities, first line responders, the private sector and Canadians. It will help to ensure that all of the necessary government resources are brought to bear in a more co-ordinated way to ensure the security of Canadians.

2.2.1 Consequence Management

While much of Canada's national security effort is directed at preventing events from occurring, the system needs to be able to respond to incidents and their consequences. This can range from providing emergency medical assistance to prosecuting individuals for committing security offences. While the national strategy is being collectively developed, there are important tangible steps that can be taken immediately to enhance co-operation. To this end, the Government is working to co-locate federal, provincial, territorial and municipal emergency operations centres to ensure that officials build strong practices of collaboration and can operate seamlessly during emergencies.

2.3 Emergency Planning and Management

The diverse array of emergencies in Canada in recent years shows the importance of transforming the national emergency management system to meet the challenges of protecting modern Canadian society from the effects of increasingly complex emergencies. This increased complexity is a function of several factors:

- trans-national threats, including international terrorism, globalized disease outbreaks and natural disasters, many of which have significant economic and health impacts;
- the near simultaneous engagement of multiple government departments and jurisdictions, often in more than one country; and
- the need for quick responses to minimize human and economic losses.

Canada’s current approach to emergencies is based on a highly decentralized and distributed division of responsibilities among first line responders, provinces and territories, and lead departments at the federal level. There is currently an urgent need for a more modern, integrated national support system for first line responders. Interoperability of policies, systems and personnel is also a major national challenge that must be tackled. Effective emergency management comprises several phases, including mitigation, prevention, preparedness, detection, response, recovery, and evaluation. In all of these phases, the national capacity in Canada must be bolstered, and the policies and operations made seamless across jurisdictions. In saying this, the Government of Canada recognizes that first line responders lie at the heart of the emergency management system and that the federal Government will often play only a supporting role in emergency management to provinces and territories, communities and the private sector.

3.0 EMERGENCY MANAGEMENT

This section briefly outlines the key concepts of emergency management with some emphasis given to the management of large-scale terrorist events. Reference [2] defines an emergency as any incident(s), human-caused or natural, that requires responsive action to protect life or property. It also defines an incident as an occurrence or event, natural or human-caused, that requires an emergency response to protect life or property.

Incidents can, for example, include major disasters, emergencies, terrorist attacks, terrorist threats, wild land and urban fires, floods, hazardous materials spills, nuclear accidents, aircraft accidents, earthquakes, hurricanes, tornadoes, tropical storms, war-related disasters, public health and medical emergencies, and other occurrences requiring an emergency response.

3.1 Crisis and Consequence Management

Crisis management, also referred to as incident management, is defined as the government-led coordination of efforts to contain, alleviate or terminate an apprehended terrorist incident, to identify and bring to account the terrorist agents, and to gather information and preserve evidence to that end, primarily through the intervention and resources of law enforcement and related security agencies. Consequence management is defined as measures to mitigate the damage, loss, hardship, and suffering caused by acts of terrorism. It also includes measures to restore essential government services, protect public health and safety, and provide emergency relief to affected governments, businesses and populations. Coordinated crisis and consequence management is a modern approach recognizing that crisis and consequence management often need to be addressed concurrently rather than sequentially. The approach blends crisis and consequence management to create a more coordinated and effective response.

3.2 Emergency Management Cycle

Figure 3, adapted from [3], shows the emergency management (EM) cycle.

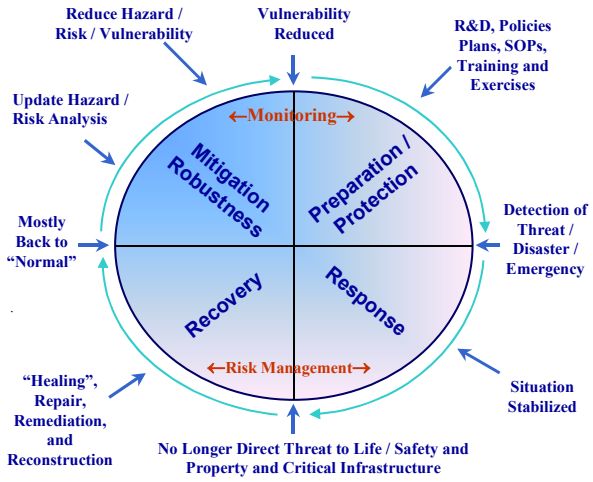

Figure 3: Emergency management cycle (adapted from [3])

Aspects of this cycle that are relevant to this paper are described next, using a mix of the definitions provided in [2, 4, and 5].

3.2.1 Response

The response phase refers to those measures and activities undertaken immediately after an emergency has occurred, and for a limited period thereafter, that address the short-term, direct effects of an incident. Response includes immediate actions primarily to save human lives, treat the injured (e.g., contaminated and overexposed persons), protect property, meet basic human needs, and prevent and minimize further injury and other forms of loss, impacts and unfavourable outcomes. These actions may necessitate the activation and

execution of emergency operations plans, opening and staffing of emergency operations centres, mobilization of resources, issuance of warnings, advisories and directions, provision of aid, and may include declaration of states of emergency. As indicated by the situation, response activities may also include applying intelligence and other information to lessen the effects or consequences of an incident; increased security operations; continuing investigations into nature and source of the threat; ongoing public health and agricultural surveillance and testing processes; immunizations, isolation, or quarantine; and specific law enforcement operations aimed at pre-empting, interdicting, or disrupting illegal activity, and apprehending actual perpetrators and bringing them to justice. This phase may last from a few hours to several weeks after the commencement of the emergency and would be followed by a recovery phase, as necessary. The time frame for recovery begins as soon as a reduction in critical response activities permits the re-allocation of some resources to longer-term recovery activities. Recovery measures can begin within the initial response phase and may last up to several years after the emergency.

3.3 Collective Response to Large-Scale Emergencies

This section briefly outlines the collective response to large-scale emergencies in Canada. The description focuses on large-scale Chemical-Biological-Radiological-Nuclear (CBRN) emergencies, as these represent a major response challenge involving many key players at all levels. A number of assumptions can be made about such emergencies:

- No single federal, provincial-territorial (P/T) or local government agency has the capability or requisite authority to respond independently to handle all crisis and consequence management aspects of a CBRN terrorist incident.
- Given the wide-ranging implications of a CBRN terrorist incident, municipal governments, P/Ts and the federal government will almost certainly all be involved in the management of the event.
- Municipal and P/T response capabilities vary across the country and within different regions of each province/territory.
- A terrorist attack may occur at any time, with little or no warning, may involve more than one geographic area and may result in mass casualties.
- The time and place of a biological attack may be impossible to determine. The subsequent spread of contamination is likely to progress exponentially. The lack of temporal and spatial boundaries of a biological attack may dictate an imposed, multi-community quarantine based on appropriate legal authorities.
- While the consequences of a chemical incident could likely be managed at the local or provincial level, a biological incident such as a smallpox outbreak would require a swift national and international response from the onset.
- Communicating between GoC departments, with other levels of government, international partners, the media, private sector and public to prevent and respond to CBRN incidents is a significant challenge.

3.3.1 Key Crisis and Consequence Management Primary Responsibilities

The federal government bears primary responsibility for the policy and operational response (crisis management) to the criminal aspects of a terrorist incident, but recognizes that local and P/T authorities will likely be the first to respond. The federal government also has lead responsibilities in managing CBRN incidents that occur on federal property (e.g., federal building or aboriginal reserve) or related to federal jurisdiction (e.g., maritime approaches). The federal government will work closely with the P/T jurisdictions

in its response. Public Safety and Emergency Preparedness (PSEPC) is the designated federal lead responsible for coordinating Canada's preparedness for, and response to, terrorist incidents occurring within Canada. The operational response to domestic terrorist incidents is the primary responsibility of the Royal Canadian Mounted Police (RCMP). P/T governments, and their respective police services, are responsible for law enforcement and public safety within their jurisdiction. The federal government's crisis management actions will occur in accordance with the implementation of a national plan (i.e., the National Counter-Terrorism Plan, [6]).

Consequence management differs from crisis management in that the province or territory in which a CBRN terrorist event occurs has primary, overall responsibility for managing its consequences, assisted, as necessary and when requested, and to the full extent possible, by the federal government. Provinces and territories have overall responsibility for determining what type(s) of assistance they might require. The federal government has primary responsibility for coordinating the international aspects of a CBRN incident affecting Canada, but will work with provinces and territories to ensure that interests and issues are appropriately represented when dealing with the international community. Clearly, effective preparedness and response to a large-scale CBRN terrorist event requires rapid, accurate and channelled communications between all levels of government.

3.3.2 The National Support Structure

Figure 4 illustrates some aspects of the National Support Structure (NSS) in Canada [4]. A disaster Area is an area designated by a provincial government(s) as having been directly affected severely by a disaster. Distribution points are locations within the disaster area where commodities moved from the advanced holding zones can be issued to officials of the affected province. They can also be used for the gathering and processing for transportation of evacuees. Advanced holding zones are locations in the affected province where resources can be received for movement to distribution points within the designated disaster area, and where evacuees may be gathered and processed for transport. Staging areas are locations where resources can be received for appropriate handling prior to onward shipment to the affected area and where evacuees, injured and uninjured, can be received.

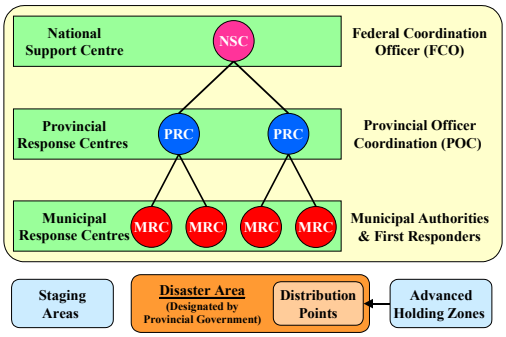

Figure 4: National Support Structure (NSS) in Canada

The occurrence of an emergency will lead to a sequence of early response actions focussing on casualty and damage assessment, the determination of the specific resource capabilities and quantities needed to respond, and the putting in place of adequate response management structures and procedures. The fundamental principle governing planning for and reaction to emergencies affecting Canadians is that initial response begins at the lowest level (e.g., individual, family, neighbour) and is escalated through levels of government until the emergency is effectively resolved.

3.3.3 Multiple Interacting Jurisdictions

Reference [2] defines a jurisdiction as a range or sphere of authority. Public agencies have jurisdiction at an incident related to their legal responsibilities and authority. Jurisdictional authority at an incident can be political or geographical (e.g., city, county, tribal, State, or Federal boundary lines) or functional (e.g., law enforcement, public health). As illustrated in Fig. 5, the collective response to a large-scale terrorist emergency typically involves numerous jurisdictions.

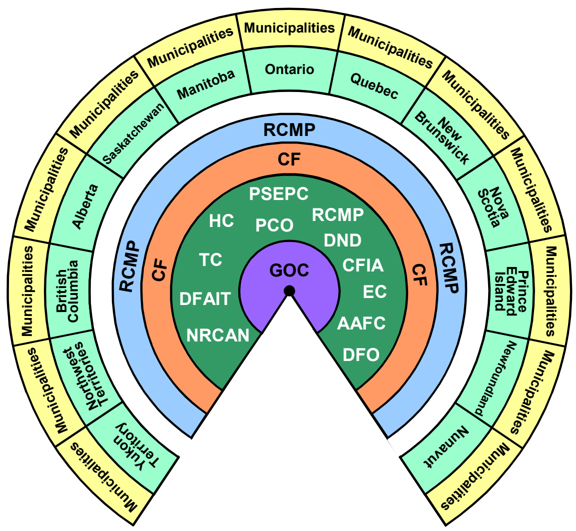

Figure 5: Collective response typically involves numerous jurisdictions

4.0 EM DOMAIN CHARACTERISTICS AND HIGH-LEVEL REQUIREMENTS

Thinking about emergency management, and especially the collective response to large-scale emergencies caused by terrorism, one can identify a number of characteristics of this domain:

- Diversity in the nature of operations.
- Geographically dispersed operations.
- Large number and diversity of data, information and knowledge types and sources.
- Large number and diversity of services, applications, tools and products types and sources.
- Staff resources to perform EM functions have remained basically stable over the years.
- EM workers possess an increasing level of information technology literacy.
- The EM environment continually adjusts to expanding information technology capabilities.

Operating in the EM environment, the decision makers at all levels (e.g., incident commanders) and their staff need:

- to rapidly develop situational awareness (e.g., understand how a situation has developed and is expected to develop);
- to rapidly develop shared understandings of the operational environment;

- to plan operations;
- to monitor the situation and the execution of the plans;
- to ensure that each individual worker is productive and concentrated in its assigned roles and tasks;
- to deal with complex crises;
- to deal with multiple, simultaneous crises (e.g., multiple operations monitoring);
- to perform routine office tasks.

Initial discussions with members of the emergency management operational communities reveal that there is a need to address some limitations very similar to those identified in [7] in a different context:

- The required data, information and knowledge and the services, applications, tools and products originate from various stovepipe systems.
- The information is not provided or accessed in a timely fashion because of the high operational tempo.
- There is a significant information overload (e.g., a huge quantity of messages at a high rate of message reception).
- There are limitations in timely fusing the information of different natures.
- There are information management constraints because of different security domains.
- There is a lack of tools to understand how a situation has developed and is expected to develop.
- There are limited visualization capabilities.
- There are limited decision-aid / planning tools.
- Decisions are being made on incomplete / unreliable information

4.1 Data, Information, Knowledge, Expertise, Services, Applications, Tools, Products. . .

Multitudes of vital data, information, knowledge, expertise, services, applications, tools and/or products for disaster management exist and are maintained up-to-date by the different individual organizations that are responsible for them. As information production and maintenance are costly and require particular expertise, it is natural to designate several organisations responsible to create and maintain critical information and provide mechanisms to distribute efficiently the information. The tool sets include many kinds of data, information, knowledge, expertise, services, applications, tools and/or products that help in many ways during emergency response situations.

Examples of data, information, knowledge and expertise include documents, e-mails, queries, working-track history, lessons learned, personal comments, maps, geospatial imagery, socio-political/cultural context (historical evolution of boundaries and political contexts, religious and cultural factions, organizational links, personality profiles), resources, infrastructures, terrain, 3D urban and building models, weather (e.g., past and present meteorological observations, and weather/atmospheric information available for a particular area that could be relevant for a crisis response), intelligence, etc. These data, information, knowledge and expertise are provided from a wide variety of sources (including open sources such as internet, TV channels, commercial, human). There are dynamic sources, providing real-time data and information, and sources of a priori data, information, and knowledge. Examples of services, applications, tools and products include electronic messaging, chatting, conferencing, message processing, document management, federated/contextual search

and retrieval, knowledge discovery, user assistance/assistant wizard, briefing production, lessons learned, alerting/ triggering, situation analysis/assessment, information fusion, decision-aid, course of actions development, numerical weather prediction, optimal path computation (e.g., vehicle path optimization for VIP evacuation purposes as infrastructures are being disrupted), crowd phenomena simulation, etc.

Of particular importance are leading edge numerical models, algorithms and technology that are able to simulate (in a quasi-real time mode) the past/present/future 3D dispersion plumes of toxic matters. Precisely knowing the contaminated region helps save time and lives. With such numerical models working with meteorological data, it is also possible to precisely trace the source of a contaminant by doing a backward simulation in time.

4.2 Information Management Requirements

In view of the discussions above, working effectively in terrorist emergency situations requires the ability to communicate and coordinate multi-national and multi-agency operations in a seamless environment. There are vast quantities of data and information requiring weeding, sorting, and analysis. Clearly, advanced information management technology is required to enable the emergency response communities to timely and securely access data, information, services, etc. relevant to their roles and responsibilities, within and across jurisdiction boundaries, regardless of what agency operates the facilities where these critical assets reside. The objective is to achieve what the authors call "Contextual Information Management for Distributed Operations Support (CIMDOS)".

Unfortunately, the current situation limits the integration of the assets from different sources, thereby limiting their impact on efficient emergency interventions. Broad integration has yet to be achieved in Canada, or within other nations, and would constitute a breakthrough. Interoperability between systems and data is also a major problem in many information technology (IT) projects. One would like to better exploit the existing legacy IT systems through synergistic integration, without the need for extensive re-engineering or major alteration to the business process of each individual participant. This is a key problem currently faced by governments and industries. In this regard, one objective of the CRIS project is to implement the necessary message and data exchange mechanisms for the ever-increasing amount of digital information that need to be exchanged within and across jurisdiction boundaries. Clearly, this must be achieved with low overhead, and with member agencies retaining autonomy of business practice & technology.

4.3 Organizational and Information Technology Issues

There are a number of organizational issues that must be taken into account regarding the development of supporting systems for the emergency management domain, similar to those identified in [8] in a different context:

- The sponsors, stakeholders and end-users belong to different services.
- The end-users might be individuals (of various ranks), communities or groups, from a variety of parent organizations, fulfilling different roles and responsibilities in different assignments.
- The tasks to be performed are highly specialized and specific to each end-user.
- The task-related knowledge is often explicitly embedded in procedures.
- The mission related knowledge remains tacit for a significant part.
- The business rules are not all formulated.
- The organisational culture and values are to be considered.

Moreover, from an information system technology point of view, the numerous jurisdictions involved in the collective response to large-scale terrorist events represent multiple continuums/scales (see Table 1) that also have to be taken into account.

Table 1: Multiple continuums/scales for information system technology

Jurisdiction	First responders, municipal, provincial ministries, provincial Emergency Operation Centres (EOCs), federal departments, federal EOCs, international.
Time	Minutes, hours, days, weeks, months --- Past, present, future.
Space	Buildings, streets, cities, regions, provinces/territories, countries, global.
Computer processing power	PDAs, tablet PCs, laptops, desktops, workstations, mainframe, supercomputer.
Computer memory (RAM) capacity	Megabytes, gigabytes, terabytes.
Computer memory (long-term mass storage) capacity	Flash cards, CDROMs, hard disks, data warehouses.
Visualization, Human-Computer Interface (HCI) capacity	PDAs, tablet PCs, laptops, desktops, workstations, projectors, knowledge walls.
Communication / network bandwidth	Wireless, high-capacity networks.
Security levels	Unclassified, sensitive, protected, confidential, secret, top secret.
Training levels	Low, medium, high.
Number of client units required	100000, 10000, 1000, 100, 10, 1.
Financial resources	Municipal, provincial, federal.

5.0 A KNOWLEDGE ENVIRONMENT FRAMEWORK

The COP 21 (Common Operational Picture for the 21st Century) Technology Demonstration Project (TDP) is a DRDC project, described in [7], that has already developed a portal capability similar to the one proposed for the CRIS. A vision has been developed for the COP 21 TDP to structure a high-level knowledge environment framework capable of laying the foundations of a situational awareness knowledge portal, towards the shared objectives of information superiority [8]. Given its high relevance to the CRIS project, highlights of this vision are provided here. Further details can be found in the references.

5.1 A Model Supporting the Knowledge Environment Concept

A series of functional principles has been established to guide the modeling of the knowledge environment framework [9]. These principles provide elements to structure a model supporting the knowledge environment [8]. This model, illustrated in Fig. 6, is composed of ten entities or concepts.

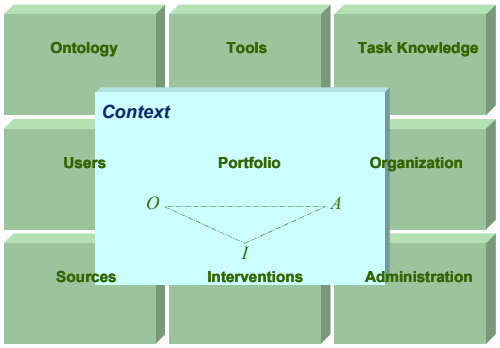

Figure 6: The knowledge environment model [8]

Three entities distinguish the proposed model, and the subsequent knowledge environment framework, from the usual information technology (IT) environment. These entities form a series of new intertwined fundamental concepts, different in their purposes from the usual ones pertaining to the organizational universe and portal system universe, that were defined to satisfy the principles previously mentioned [9]. These are the Context, Ontology and Portfolio entities (or the "C-O-P trilogy").

5.1.1 The Portfolio Concept

A portfolio is the working space (actually, a virtual container of the work material) of a user, or groups of users, to perform all the work related to a long-term, task-oriented activity or assignment (e.g., monitoring, planning) within a particular domain of intervention (i.e., in relation to a specific operation, mission, exercise, etc.). The portfolio contains all the representative material needed to perform the work (e.g., documents, annotated maps, preferences, emails, queries, work-tracking history, personal comments, etc.), as well as all the links to the required external elements (e.g., the list of relevant sources, reference documents, groups of experts, subscriptions, task-oriented tools, specialized applications, thesaurus views, organizational work layouts, etc.).

Delimiting the portfolio against three dimensions: long-term task-oriented activities, intervention, and ownership will ensure flexibility in the organization of the work and allow individual or group customization of the environment. When working, a user (or a group of users) selects, within its assignment, responsibility and security parameters, the portfolio in which it wants to work and has access to all services and sources related to this portfolio. The delimitation of the work into well-scoped portfolios allows, to a certain extent, to confine or grasp the knowledge handled within them as well as the know-how. The exploitation of that knowledge and know-how, by the means of appropriate ontologies, is then feasible and brings powerful possibilities, such as providing contextual assistance in various ways to the work performed within portfolios.

5.1.2 The Context Concept

The context, as defined in the work of [9], is the set of all elements (internal or external) surrounding the work being performed in a portfolio, and that contributes to bring light on its meaning and its value. Typically, the context entity operates in background on the portfolio, as a transparent agent. It monitors the parameters of the portfolio and keeps track of their evolution as actions are performed within the portfolio.

The context is user dependent and is really related to the work being done. From a functional point of view, it determines what information is relevant. When working within a portfolio, the user has access to numerous tools and information from various sources to help manage its work. With an active context entity, all of these tools will be available with optimal settings, in a manner that the user is familiar, as a function of the tasks to be performed. The information will be made available according to the domain of knowledge, the official assignment and security privileges of the user. The context circumscribes and reinforces the meaning of the information, strengthens its understanding and its processing by providing the right tools to do so, and giving access to the right sources.

5.2 The Knowledge Environment Framework

A knowledge environment framework integrating a set of tools and services has been defined for the COP 21 TDP to support the knowledge management environment [8]. Figure 7 is a conceptual representation of this framework decomposed into three tiers [7].

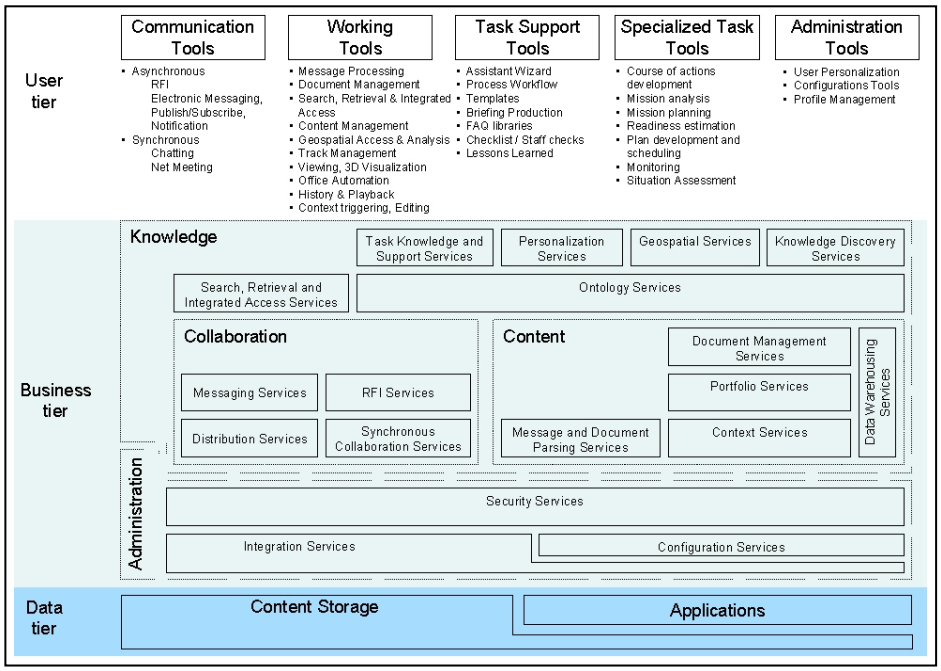

Figure 7: The COP 21 knowledge environment framework [7]

The user tier section of the framework is structured around five main tools families: communication tools, working tools, task-support tools, specialized task tools and administration tools. In order to be supported by the environment, these tools imply in turn, the structuring of services in the business tier that contains the business rules and logic. Aiming at delivering an integrated access to information and tools required to perform various tasks within the broad situation assessment process, the system should provide a reference platform for the development of interoperable services across a wide range of environments. These services share business/military logic, data and processes through a programmatic interface across networks. They should allow military organisations to communicate data without intimate knowledge of each other's IT systems behind firewalls. These services must be seen as loosely coupled. The data tier actually consists of the applications and content storage. The later refers to a collection of data organized so that it can be easily access, managed and updated.

6.0 THE CRISIS RESPONSE INTEROPERABILITY SYSTEM (CRIS)

A new R&D project, called Crisis Response Interoperability System (CRIS), has recently been undertaken at Defence R&D Canada – Valcartier (DRDC Valcartier). The aim of this project is to enable the members of the operational communities at all levels (from first responders through upper-level management) to work together effectively in large-scale terrorist emergency situations, when engaged in crisis response and consequence management. The numerous objectives of the project can be summarized as:

1) Enhance the collective C4I capabilities:
   a) Support the users in achieving information superiority:
      i) Improve the situation analysis support to enhance the situation awareness of the responders.
      ii) Provide the emergency situation picture tailored to the user's needs.
      iii) Provide users with the specific information required to perform their functional responsibilities during crisis or conflict.
      iv) Support the development, maintenance and sharing of the collective "battle space knowledge".
      v) Exchange information within and across jurisdiction boundaries.
   b) Improve decision support to enhance the critical decision-making of the responders regarding scarce response resources.
   c) Support rapid incident assessment and management (immediate reaction and near-term consequence management).
2) Improve the effectiveness and efficiency of inter-agency co-operation, co-ordination, interoperability and decision-making:
   a) Coordinate multi-national and multi-agency operations in a seamless environment.
   b) Provide a solid collaborative solution to the many participating organizations and individuals across multiple jurisdictions.
   c) Link jurisdictions into a trusted federation (with low overhead, and with member agencies retaining autonomy of business practice & technology).
   d) Facilitate secure interaction between jurisdictions while leaving access control decisions under each jurisdictional authority.
   e) Better exploit critical data, information, knowledge, services, applications, tools and products offered by the legacy systems of the operational community
   f) Improve the integration of existing operational information systems of the emergency response community (the CRIS will not replace these systems)
   g) At multiple scales regarding time, space, computer capacity, visualization and human-computer interface capacity, bandwidth, security levels, training levels, financial resources, etc.
   h) Support scenario rehearsal, exercises, training, readiness assessment, post-event reconstruction (i.e., other segments of the emergency management cycle) to enhance collective readiness.
3) Support the different needs of the various actors.

4) Improve the efficiency of the emergency response workers:
   a) As individual workers, as communities and as groups.
   b) Independently from their computer literacy level.
   c) Without revolutionizing organisation values, business rules and work layouts.
5) Reduce the response time.
6) Enable more efficient and effective collaboration among cluster members of the CBRN Research and Technology Initiative (CRTI), and enhanced cluster participation in the response to CBRN events (laboratory cluster management and operations)
   a) Enable the capture and sharing of knowledge and expertise with first responders and operational communities.
   b) Enable the exchange of secure data and information before and during an operation to support cluster operations.

6.1 The CRIS Requirements

The CRIS is not a new incident command system. It is also far more than just a database that can be efficiently queried through a web-based portal. The CRIS is an innovative information management and integration system (providing the information management technological glue) developed to meet requirements such as the ones listed below:

1) Allow a timely and secure integrated/federated access:
   a) to multiple types of data, information, knowledge and expertise;
   b) to multiple types of services, applications, tools and products;
   c) from wide variety of heterogeneous, distributed sources and disparate providers;
   d) to data, services, etc., maintained by their owners;
   e) from any media;
   f) from multiple formats;
   g) from varying levels of abstraction;
   h) within and across jurisdiction boundaries, regardless of what agency operates the facilities where the critical data, information, knowledge, expertise, services, applications, tools and/or products reside.
2) Allow arbitrary navigation, from a single workstation, on the sources of data, information, knowledge, expertise, services, tools and products.
3) Timely find and provide the users with the right, trustable data, information, knowledge and expertise:
   a) Allow semantic connections on sources of data, information, knowledge, expertise, services, applications, tools and products.
   b) Allow searching and extracting information that is truly relevant to the work and to what is needed at the time where the search is performed.
   c) Integrate/aggregate/fuse the data, information and knowledge:
      i) Allow various forms of aggregation/fusion depending on users' preference and/or true value of the results.

ii) Create new products on the fly through combining different datasets.

d) Provide data, information, knowledge and expertise relevant to the various user roles and responsibilities in tailorable views, with adaptable and flexible tools.

e) In context of the work:

i) Take into account individual user interests and group constraints within a dynamic and evolving task context (in a changing environment)

4) Manage the data, information, knowledge, expertise, services, applications, tools and products.

5) Distribute/exchange/share the data, information, knowledge, expertise, services, applications, tools and products:

a) Rapid dissemination toward the intervention site.

b) In the appropriate form and level of detail.

c) To users at all echelons.

d) Allow easy contribution to the collective “battle space knowledge”.

e) Allow easy contribution to the collective response.

6) Provide services for synchronous and asynchronous collaboration among a variety of responders:

a) Interact with other people.

b) Expertise grouping.

7) Make relevant task support tools readily/easily available to users, according to the task being performed, and according to the preferred ways of working, skills and community of practice.

8) Provide personalization capabilities in terms of data, information, and knowledge content and expertise, services, applications, tools and products:

a) Provide users with designated working spaces, called portfolios.

b) Display, manage or produce documents related to user’s assignment and responsibility.

c) Tap on task-specific tools (templates, wizards, lessons learned, etc.).

d) Access specific specialized tools such as systems or applications (e.g., a planning application).

9) Allow smart navigation from any elements of the portfolio universe. For instance, to jump from a particular paragraph in a working document into the appropriate section of an external system source corresponding to the meaning of that paragraph.

10) Allow the activation or deactivation of the contextual assistant in certain fuzzy scoped areas.

11) Allow a continuous formulation of the contextual meaning of the work as actions are performed.

12) Keep track of all documents and actions taken when assuming the duty.

13) Tackle many critical issues regarding system and data security, privacy and confidentiality, and authentication:

a) Provide fine grain user management and access control.

b) Allow a security strategy that matches the nodal network and information pull approach.

6.2 The CRIS Horseshoe Architecture Concept (CHAC)

Figure 8 presents the CRIS Horseshoe Architecture Concept (CHAC). The CHAC shows, at a conceptual level, the interaction between the end-users, represented by "*roles*", and CRIS. The proposed CRIS project is based on a web portal solution that can be simply accessed by an Internet client by means of standard communication protocols such as http or https. A CRIS end-user, such as a first responder or an incident commander, will be able to operate CRIS from a simple web browser engine, from its client station. CRIS will provide a wide variety of end-users with a transparent and highly powerful operational service point for a variety of services ranging from portal core services, such as a "Data Organizer" and a "Data Viewer", to more specialized CBRN emergency data and processing services. CRIS will be characterized by its facility to exploit the CBRN data, information and knowledge by the emergency staff before, during and after a CBRN incident.

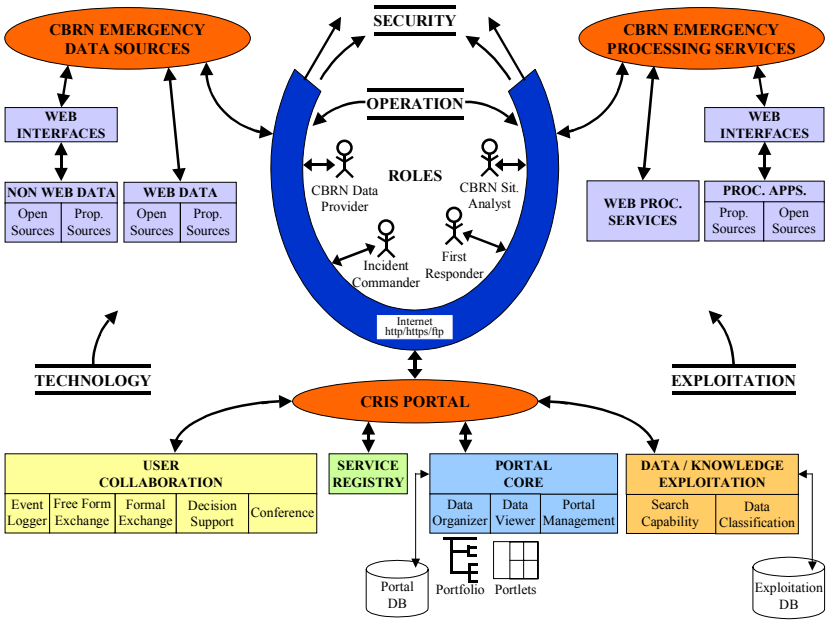

Figure 8: CRIS Horseshoe Architecture Concept (CHAC)

The CHAC highlights the fact that four main thrusts will drive the development and the demonstration capability of CRIS: the "*operation*", the "*exploitation*", the "*technology*" and the "*security*" thrusts. A proper balance between these four thrusts during the evolution of the project will ensure that the "horseshoe concept" will be preserved. As someone can expect, the *operation* thrust has to do with the various roles of the CRIS operational community. As for the *technology* thrust, one can simply deduce that a large number of technology solutions/products will be used in order to render the CRIS portal and available services. The *exploitation* thrust is related to the means offered to the CRIS end-users to exploit the capabilities of the system. For instance, having a knowledge database with a large relevant CBRN emergency content, but poor operating mechanisms to access this valuable information, is an example of a weak exploitation thrust. Finally, in the context of the proposed CRIS project, where a large number of organizations of different types and from various jurisdictions are participating, the *security* issue shall be considered as a major driving thrust as well.

One can still ask why the horseshoe? Having a system like CRIS that is deployed on the Internet means that an almost infinite number of resources can collaborate to the capability of the system. Thus, with this sole

consideration in mind, an image like an infinite straight line would have been more appropriate than a horseshoe one. However, it is required to apply some access control mechanisms to protect the valuable resources of the main collaborators involved in this project, without limiting the access to the large potential of the Internet. Having this extra consideration in mind, the reader can better appreciate the horseshoe form.

Another aspect shown by the CHAC is that the technological environment is composed of three main groups of components: the *CRIS portal*, the *CBRN emergency data sources* and the *CBRN emergency processing services* groups. Each group contains its specific technological stream of components. It is important to note that it is a main objective of the CRIS project to render, at least partially, the user front end of the technology components from the *CBRN emergency data sources* and the *CBRN emergency processing services* groups into the *portal core data viewer* under the *CRIS portal* group. Doing so will ensure that the end-users of CRIS will have a single point of access to the various capabilities of CRIS from the *CRIS portal*. This approach has already been tested successfully in other Technology Demonstration Programs (TDPs) such as the ongoing COP 21 (Common Operational Picture for the 21st Century) TDP developed at DRDC Valcartier with some of the CRIS project team members. It is the intent of the CRIS project team to reuse this approach.

6.3 A Service-Oriented Architecture (SOA) Framework

The development of the CRIS will be based on a service-oriented architecture (SOA) framework providing the foundation of a sound enterprise reference architecture that presents a number of benefits discussed in [10]: ability to rapidly adapt to changes in business conditions, ability to reduce the amount of time spent developing custom code, and cost savings as more of an organization's existing investments in technology are leveraged. The end goal of a service-oriented architecture is to provide easy and secure access to enterprise technology and process resources, maximizing re-use and minimizing cost, while improving the performance and reliability of the systems. The organizations involved in the development of an enterprise system can think about a phased approach to the implementation, ensuring the success of the project.

Unlike traditional architecture approaches, the enterprise reference architecture promotes the use of a mechanism for systems to take action when pre-determined or unplanned events arise, such as the failure of a business process to reach completion within a specified timeframe. When considering this additional mechanism, the architecture is said to be event-driven and, consequently, more dynamic than non-event driven architectures. For the development of a system such as the CRIS, the implementation of an event driven architecture is truly important in order to ensure a responsive system to the end users during crisis periods. One main challenge about developing the CRIS is the ability to leverage the many technology infrastructures (hardware and network infrastructures) and application systems own by the many organizations participating in the development of the CRIS enterprise system. To address this challenge, the architecture should provide a clear approach for the integration of and the access to the application systems.

7.0 ENABLING TECHNOLOGIES

The CRIS will mainly be based on portal and web services technologies, as these have become effective means of enabling organizations to access, share, exchange and manage data, information and knowledge of pertinence to the organizations. Geospatial data and geospatial visualisation and analysis services, and advanced representation techniques and visualization approaches are also of particular importance to the CRIS project. These aspects are briefly discussed next. One should note, however, that the success of the CRIS project also relies on numerous technologies not discussed here. Some examples are: collaborative environments, knowledge management, modeling and simulation (e.g., toxic matter dispersion prediction), identity management services (security technologies), etc.

7.1 Network-Centric Enterprise Services (NCES)

The Defense Information Systems Agency (DISA) has recently announced a new, multi-billion dollar technology initiative, the NCES program [7 and 11]. In a network-centric environment, data would be made available as quickly as possible to those who need it across the organization or on the battlefield. This would enable the military and intelligence communities to access information relevant to their missions regardless of what agency operates the network where the data resides. The NCES pilot program currently includes nine core enterprise services that the Department of Defense (DoD) has identified as being critical to supporting the business and warfighting sides of the enterprise: collaboration, messaging, security, discovery, mediation, enterprise systems management, user assistance, storage of the massive amounts of information already on the networks and collected in the future, and application - an infrastructure to host and organize the data.

7.2 Portal Technology

The system requirements for the CRIS calls for a portal concept in the widest definition of the concept. Several military organizations are rapidly adopting the portal approach. As discussed in [7], the enterprise portal technology constitutes a good foundation to implement Network Centric Enterprise Services. Portals can be seen as a natural evolution from the desktop and the web page. With the desktop (e.g., the Windows platform), a user (or group of users) is able to configure its environment, in particular the set of icons corresponding to applications to be launched, to file folders or documents. However, the desktop is a local capability. The web page provides users with a capability to access information on a remote web server. Like the desktop, the web page can be customized to support the special interests of a user community and an individual user can personalize the browser options and set bookmarks to facilitate access to frequently used or special interest sites.

The portal is a window to the World Wide Web extending the user's access beyond the web server, to multiple sources of information, finding the information the user needs to do its job without hunting for it. The user can personalize its portal to display specific information content from a variety of sources such as local weather and local events. David Morrison defines a portal as "an application that provides a personalized and adaptive interface enabling people to discover, track, and interact with other people, applications, and information relevant to their interests [12]." He summarizes the unique, distinguishing features of a portal in the following meaningful list:

- Personalization for end users. Tailoring of appearance, content, and application interface to each user.
- Organization of the desktop. Consolidate access to important applications and information.
- Resource division. Separation of some portal features into layers.
- Tracking of activities. Personalize the portal as affinities of the user are confirmed or evolve over time.
- Access and display of information. From multiple heterogeneous data stores.
- Location of important people and things. Discover and locate the experts, communities, and content related to a particular topic.

Some interesting features are [8]: cascading portals, abstraction layers, person-to-person (P2P). Gerry Murray distinguishes four kinds of corporate portals, that can be seen as four stages of portal evolution in general, based on the type of content and tools that are exposed to the user [13]:

- Enterprise information portals that connect people with information.

- Enterprise collaborative portals that provide collaborative computing capabilities of all kinds (e.g., such as chat, conferencing, calendaring, workflow, document management, and forms processing).
- Enterprise expertise portals that connect people with other people based on their abilities, expertise, and interests.
- Enterprise knowledge portals that combine all of the above to deliver personalized content based on what each user is actually doing.

Enterprise portal technology is rapidly evolving. One of the trends is its evolution towards knowledge portals where the information content is customized to suit the needs of the user [7]. Since the beginning of 2002, the main providers of portal solutions have introduced the concept of "a unique desktop" into their implementation environments and they offer functionalities such as: customized information access according to user profiling, basic collaborative tools, online application, and wireless support. However, although portal technology exists, the combination of all requirements for the CRIS system is a challenge. The off-the-shelves solutions do not address all previously stated requirements. Even if some of the missing components are conceptually well advanced and exist as a prototype or are even commercialized, none of the off-the-shelves integrated solutions found in the market would address the totality of the requirements. As a result, the system architecture for the CRIS must bridge between numerous standalone applications, systems and networks.

7.3 Geomatics

Geospatial data and geospatial visualisation and analysis services are core components that constitute the basis of any crisis response system that has a relation with the territory. Because of the nature and the diversity of the different responders involved in the response phase, it is highly recommended that any geospatial components supports open standards and specifications. Indeed, as there is a very heterogeneous variety of geospatial data formats and access mechanisms, it is important that crisis response systems supports the geospatial data standards and interoperability specifications that are the mostly used, in order to enable a better interoperability with the geospatial data and services maintained by the various responders. While it might be argued that proprietary formats and data structures are usually offering better performance for indexing and visualisation, these benefits should not be, in our opinion, considered as the driving factor for selecting a particular architecture or a geospatial data management system that would not at least supports the various OGC, OGDI, DIGEST, W3C and ISO metadata standards and specifications. All the geospatial components proposed for the CRIS system will be defined, specified and designed in relation with this strong commitment to support these standards and specifications. Examples of such geospatial-based components include datasets, distributed geomatics services, distributed spatial analysis, cartographic representation, document and report generation, exportation of geographical views, geospatial peer-to-peer sharing infrastructure and alerting, and advanced geospatial data visualisation, in 2D and 3D.

7.4 Representation Techniques and Visualization

The CRIS portal must be carefully designed and must exploit meaningful representation techniques and visualization approaches. The nature of emergency response operations constitutes a significant challenge in terms of information visualization. For example, urban operations bring a requirement to rapidly understand the morphology of an urban landscape in order to support a range of functions from strategic situation awareness to tactical mission rehearsal [7].

So far, the most commonly used technique to generate the Common Operational Picture (COP) has been the use of electronic maps superimposed with symbology [7]. Especially in the military domain, the predominance of this technique will remain. However, a wide range of visualization tools and approaches are

worth exploiting in the CRIS portal in order to enhance situation awareness. The TTCP C3I Action Group on Information Visualization has conducted a survey of visualization techniques and approaches used in allied command and control systems or being examined as applied R&D activities [14]. Among these techniques and approaches are the following:

- Playback capability. Animated playback / forward capability to visualize and understand how a situation has been evolving and how it is expected to evolve.
- Urban models. 3D modeling and visualization (developed from photographs and inputs from other sensors) to represent urban environments with various degrees of granularity and realism [15].
- Socio-political information. Visualization of socio-political information such as historical evolution of boundaries and political contexts, religious and cultural factions, organizational links, personality profiles.
- Visualization of Uncertainty. Representation of uncertain or incomplete information using clues or highlighting techniques.
- Abstract information. Use of abstract representations techniques to convey information such as commander's intent, morale of the troops and asymmetric threats.
- Visualization customization. Capability to filter the quantity of information presented according to the task being performed.
- Alerting / triggering. Use of subscription, notification and triggering services to get access to the required information.

8.0 R&D METHODOLOGY

The R&D methodology proposed for the CRIS project addresses end-user requirements, needs and interests. It can be viewed from two perspectives: top-down and bottom-up. These perspectives are further discussed next.

8.1 Top-Down Perspective: End-User Business Process and Requirements

An important objective for DRDC Valcartier is that the various end-users develop a firm intent to adopt the CRIS capability after a successful demonstration. In line with this objective, the project team includes as partners many key representatives from the emergency management operational communities at the municipal, provincial and federal jurisdiction levels, as expert advisors to bring key expertise and experience to the project (since they best know the application domain). These representatives form a manageable set of participants with expertise/roles that collectively covers many facets pertaining to the preparedness and response to very large-scale terrorist events. Moreover, according to the emergency response plans, some of them clearly have a decision-making role to play in emergency response, while the others mainly have a supporting role. Without a doubt, it is of the utmost importance that the project team has direct access to first responder expertise and experience.

A strong and active participation of all these end-users is necessary during the overall CRIS development process for the definition of the requirements, to help detailing the targeted business process, to guide the development of the CRIS, and for the planning and execution of the technological demonstrations required for the evaluation and validation of the resulting CRIS during some exercises or joint demonstrations to be identified or defined with them. The CRIS capabilities will be designed in consultation with them to fit the current and future systems, architecture and infrastructure of operational units. This is the top-down perspective.

A major aspect of this top-down perspective is the capture and documentation of the end user business process with respect to the emergency management cycle. This is an aspect that clearly requires end-users participation. Regarding this issue, the CRIS project plan takes into account some significant leveraging from an ongoing DRDC Technology Demonstration Project (TDP) called JCDS (Joint Command Decision Support). The JCDS TDP is currently conducting a major activity on the characterization of complex situations resulting from terrorist activities and asymmetric threats. This activity includes a review and analysis of Emergency Response Plans (ERPs), the development of a model of the collective response to large-scale terrorist events, a review and analysis of Emergency Response Scenarios (ERSs), and the characterization of asymmetric threats and terrorist activities. This activity will produce results of direct interest to the CRIS project. These results will provide a solid foundation for the capture and definition of the end-user business process. Then, working with the members of the project team having an operational role in emergency response, this foundation work will be augmented through meetings and interviews to capture and documents the specifics of these participants.

From the end-users point of view, the CRIS project can also take advantage from the results of another ongoing TDP. The COP 21 TDP has already developed a portal capability similar to the one proposed for CRIS. The project team intends to exploit the availability of this existing portal component to initiate, very early in the project implementation, the development of a concept of operations for such a product in the context of the emergency management cycle. Access to the COP 21 portal capability can easily be given to the partners coming from the operational communities, as such an access only requires a web browser and a PC workstation. Similarly, the COP 21 portal will be exploited with the end-users to support early requirements capture.

8.2 Bottom-Up Perspective: Building on Existing Relevant Products

The top-down perspective described above is extremely important for the success of the CRIS project. However, even with the best intent of the world, the project plan cannot be based exclusively on a top-down approach. There would then be a high risk that the scope of the project quickly becomes too large. There is also the notion that the CRIS project cannot develop from scratch all of the required components, as such an approach would certainly be too expensive. Such considerations lead the project team to the bottom-up perspective, i.e., building on existing relevant products. In this regard, the CRIS project will seek to capitalize on many relevant, mature and unique products already developed by DRDC and the other members of the project team, and on those currently available off the shelve on the market. It will focus on the incremental integration of such existing capabilities (i.e., a set of largely autonomous capabilities that must be integrated and interleaved into an overall process flow relevant to the operational community) and new technology requiring some degree of adaptation or development. Examples of products that will be considered for refinement, adaptation, integration and use are listed in Table 2. Discussing all of these products is clearly out of the scope of this document.

Table 2: Examples of existing products/systems to be considered for the CRIS project

Products / Systems	Reference(s)
Common Operational Picture 21st Century (COP 21) Technology Demonstration Project (TDP) Situational Awareness Portal	[7], [8], [9]
COPlanS (Collaborative Operations Planning System)	[16]
ADAC (Automatic Documents Analyzer and Classifier)	[17]
ToMaDi (Topographical Map Display)	[18]
KNOWMES (Knowledge Management and Exploitation Server)	[19], [20]
CODSI (Command Decision Support Interface)	[21], [22]
Results from the "Lessons Learned" projects	[23], [24]
3D Urban Models	[15]
Information-Centric Workspace	[25]
OPERA (Operational Planning Environment and Reference Application)	[26]
Orbat Browser	[26], [27]
AIThink / Optipath	[28]
National Infrastructure Database (NIDB)	[27]
National Topographic Data Base (NTDB)	[29]
GeoServNet	[30]
EM/2000 Software	[31]
Urban Dispersion Models	[32]

The state of maturity of these many products and the strong experience of DRDC Valcartier in system integration make the bottom-up approach appealing for the CRIS project. However, the integration of any such product will have to be carefully analyzed with respect to the technical feasibility, the level of effort required and, most importantly, the relevance and benefits to the end-users of the operational community.

8.3 Leveraging Other Projects and Products

The CRIS project will harness existing capabilities, building on existing projects and products already in line with the needs and interests of first responders and other operational units. As mentioned above, the project will capitalize on many existing products from DRDC and the members of the project team. In particular, the project will leverage from the DRDC COP 21 TDP that has already developed a portal capability similar to the one proposed for CRIS. Actually, the COP 21 TDP portal could form a large part of the CRIS foundation. This portal component will be exploited very early in the project, with the end-users, to initiate the development of a concept of operations for such a product. The development methodology, knowledge and expertise acquired during the COP 21 TDP will also be directly reused for CRIS.

8.4 Technological Demonstration with the End-Users

To complete the user-centric approach and work plan proposed for the CRIS project, the project partners coming from the operational communities will participate in technological demonstrations for the evaluation and validation of the resulting system during some exercises or joint demonstrations to be identified and/or

defined with them. The project plan proposes both interim and full-scale technological demonstrations of the science and technology, capability and knowledge of the project partners. During the final demonstration, the real impact of the CRIS on the end-users will be assessed with a deployed and completed CRIS capability that will be accessed by all of the project participants and stakeholders, for end-user experimentation with the system, to achieve significant validation and testing. These demonstrations, including the requisite training and technology transfer, will be carried out by the project team, including first responder organizations, using facilities provided by operational units and agencies.

It is worth noting that there are opportunities to use the CRIS system in international-level anti-terrorism training exercises. For example, DRDC Valcartier already played in many Coalition Interoperability Trials of the Joint Warrior Interoperability Demonstrations (JWIDs) 2004 [33] with the situation awareness portal of the COP 21 TDP. A similar participation to JWID 2005, with the JCDS TDP, is currently being planned. This is highly relevant as NORTHCOM is bringing a Homeland Security/Defense focus to JWIDs 04/05. There is also a possibility to experiment with CRIS in TOPOFF 3 [34], but this remains to be explored.

8.5 Research Methodology Suitability

The proposed R&D methodology is based upon the specific project needs and constraints. It will allow the CRIS project team to concurrently address the two ways of viewing the project (top-down and bottom-up) and will help ensure consistency in the deliverables. The R&D associated with the conception, the development, the integration, and the implementation of the CRIS capability requires a number of incremental iterations (from each individual development team) in order to lower, as early as possible, all associated risks. The main cycles of refinement proposed for the CRIS capability, and the integrated technological demonstrations will also minimize risks in the project. All results from developments and tests will be used as a feedback for subsequent R&D steps in order to realign on the fly, with minimum impact, all processes toward a unified view. The overall effort in this project is relatively complex as it implies many peoples, processes and technologies that, a priori, are not always coordinated in their works. The proposed methodology will maximize the coordination between organizations, unifying all participant efforts toward a highly focused product development cycle all along the project.

The project participants from the emergency management operational communities are quite pleased with the proposed R&D methodology, as our approach based on frequent consultations with the end-users will provide rich benefits to both the CRIS project and these communities as well. It augment the likelihood that the project results will be well aligned with their requirements, addressing priorities and gaps. While new capabilities will be created to fill some identified gaps, the project is not targeting the creation of new technology to be pushed to end-users; the R&D methodology is rather driven by some S&T “pull” that addresses end-user requirements. The commitment of the end users to provide personnel (for testing and validation) and to use some of their facilities during the demonstrations is a key factor for achieving successful outcomes that will benefit the end-user community, and for which there is an urgent requirement to improve terrorism preparedness and response. This greatly lowers the risk of leaving behind capabilities that would not be used by end users. The interaction with multiple partners with various responsibilities will reduce the risk of developing stovepipe systems not generic enough to be adopted by heterogeneous user communities. Finally, the active participation of the end-users in all project phases add a lot of credibility to the proposed project. There is a strong potential that the CRIS elements will be used eventually in an operational capability, as the end-user community (especially first responders and operational units) is deeply involved in the project

9.0 CONCLUSION

This paper described a new R&D project, called Crisis Response Interoperability System (CRIS), that has recently been undertaken at DRDC Valcartier. It discussed all aspects of the CRIS project. A brief review of Canada's national security policy was presented. The key concepts of emergency management, with some emphasis given to the collective management of large-scale terrorist events, were outlined, along with a coarse analysis of the characteristics of the emergency management domain, and of the high-level information management requirements associated with the collective response to emergencies. Highlights of a vision developed to structure a high-level knowledge environment framework capable of laying the foundations of a situational awareness knowledge portal were presented. The specific objectives of the CRIS project were summarized, and a number of system requirements were listed. Then, some enabling technologies for the project were discussed. Finally, The R&D methodology used for the CRIS project was described.

The project will leave behind the portal infrastructure, a series of distributed geomatics services linking meteorological phenomena and dispersion of toxic matter with 2D/3D cartographic views and urban environments, an infrastructure database (to track the status of critical infrastructures, provide points of contact, provide risk assessment capabilities on utilities, services, transportation, communications, etc.), browsers for easy access to relevant data and information on organizations, equipment and resources, and planning and calculation tools for supply, staff check, tasking and assignments, logistic, movement, lift, etc. Although the development of the initial CRIS capability and the set up of a central server for the core services of CRIS are somewhat expensive, the proposed approach, based on portal and web technologies, will actually be highly affordable form the end-user perspective. The CRIS portal can be simply accessed by an internet client by means of standard communication protocols. The end-users will be able to operate the CRIS from a simple web browser engine, from their client stations. Clients will thus exploit the CRIS protal server through their particular field units that will use a familiar web-style interface minimizing the need for special training.

The CRIS will have significant social, economic and operational impacts on emergency preparedness and response, as the project rightly addresses some needs and interests already expressed by the end-user community, targeting maximum effectiveness and efficiency of the responder partnerships. It will significantly improve the effectiveness and efficiency of emergency response operations by addressing a number of deficiencies. It will add to the capabilities of first responders and other frontline personnel to protect, mitigate and contain large-scale terrorist emergency events and reduce the response time (faster incident assessment and management for immediate reaction and near-term consequence management). Finally, the CRIS links to a broad range of terrorist events as it relates to all anticipated scenarios that would have catastrophic/critical impact and rated as extreme/high risk and immediate/high preparedness prioritization. It will enhance collective readiness and the safety of people and critical infrastructures.

10.0 REFERENCES

[1] PCO, Securing an Open Society: Canada's National Security Policy, Canada - Privy Council Office, www.pco-bcp.gc.ca, April 2004.

[2] U.S. Department of Homeland Security, National Incident Management System, March 1, 2004.

[3] Tucker, C., Canada – United States CIP R&D Roundtable, Presentation at the Canada – United States CIP R&D Roundtable, Ottawa, Canada, October 2002.

[4] Emergency Preparedness Canada, National Support Plan - Part I, Emergency Preparedness Canada, 15 February 1999.

[5] Health Canada, Federal Nuclear Emergency Plan - Part 1: Master Plan, 4th Edition, Nuclear Emergency Preparedness and Response Division, Radiation Protection Bureau, Health Canada, May 2002.

[6] Solicitor General Canada, The National Counter-Terrorism Plan, 30 May 2000.

[7] Gouin, D., Gauvin, M. and Woodliffe, E., COP 21 TD – Towards a Situational Awareness Knowledge Portal, Proceedings of SPIE 2003 - Aerosense/Defence Sensing, Simulation and Controls, Orlando, 21-25 April 2003 Vol. 5101 - Battlespace Digitization and Network-Centric Systems III.

[8] Gauvin, M., Boury-Brisset, A.-C. and Garnier-Waddell, F., Contextual User-Centric, Mission-Oriented Knowledge Portal: Principles, Framework and Illustration, 7th ICCRST, Quebec City, September 2002.

[9] Gauvin, M., Boury-Brisset, A.-C. and Auger, A., Context, Ontology and Portfolio: Key Concepts for a Situational Awareness Knowledge Portal, HICSS-37: 37th Annual Hawaii's International Conference on System Sciences, Hawaii, US, 5-8 January, 2004.

[10] Doculabs, Planning and Building an Architecture that Lasts: The Dynamic Enterprise Reference Architecture, Marketfocus Report, 2003, 39 pages.

[11] Caterinicchia, D., DOD net-centric pilot making progress, Federal Computer Week, 12 Feb 2003, http://www.fcw.com/fcw/articles/2003/0210/web-nces-02-12-03.asp

[12] Morrison, D., Building Successful Portals, May 2000, Article Id: 110, in http://e-proMag.com

[13] Murray, G., The Portal Is the Desktop, May 1999, Article ID: 166, in http://e-proMag.com

[14] Gouin et al, D. Gouin (Ed.), Information Visualization in C3I: Final Report of TTCP C3I AG-3, TTCP C3I AG-3, July 2002.

[15] Létourneau, F., Different Approaches for the Creation and Exploitation of 3D Urban Models, 7th International Command and Control Research Technology Symposium, Quebec City, 16-20 Sep 2002.

[16] Guitouni, A., COPlanS - Collabarative Operations Planning System, Fact Sheet IS-228-A, DRDC Valcartier 2003-10, 2003.

[17] Guitouni, A., Boury-Brisset, A.-C., Belfares, L., Tiliki, k., Belacel, N., Poirier, C. and Bilodeau, P., Automatic Documents Analyzer and Classifier, 7th International Command and Control Research and Technology Symposium (ICCRTS), Quebec City, 16-20 September 2002.

[18] Fortin, R., Novel Display Devices for Command & Control Applications, SPIE Proceedings, Orlando, 16-18 April 2001.

[19] Boury-Brisset, A.-C., Towards a Knowledge Server to Support the Situation Analysis Process, Proceedings of the Fourth International Conference on Information Fusion (FUSION 2001), Montreal, Canada, August 7-10, 2001.

[20] Boury-Brisset, A.-C., Ontology-based Approach for Information Fusion, International Conference on Information Fusion, Cairns, Australia, July 2003.

[21] Roy, J., Breton, R. and Paradis, S., Human-Computer Interface for the Study of Information Fusion Concepts in Situation Analysis and Command Decision Support Systems, SPIE Proceedings, Vol. 4380, Signal Processing, Sensor Fusion, and Target Recognition X, Orlando, 16-18 April 2001.

[22] Breton, R., Paradis, S. and Roy, J., Command Decision Support Interface (CODSI) for Human Factors and Display Concept Validation, Proceedings of Fusion 2002, Annapolis, MD, July 2002.

[23] Boury-Brisset, A.-C., Gauvin, M. and Champoux, P., A Knowledge Management Approach to the Creation and Sharing of Canadian Forces Lessons Learned, 7th ICCRST, Quebec City, September 2002.

[24] Champoux, P., Thibault, G. and Trudel, M., A Lessons Learned Knowledge Warehouse to Support the Army Knowledge Management Command-Centric, NATO RTO Military Data and Information Fusion Symposium, Prague, CZ, 20-22 October 2003.

[25] Thibault, G. and Le May, F., Introducing the Canadian Information-Centric Workspace Concept, NATO RTO Military Data and Information Fusion Symposium, Prague, CZ, 20-22 October 2003.

[26] St-Jacques, J.-C., OPERA – Operational Planning Environment and Reference Application, Fact Sheet IS-218-A, DRDC Valcartier 2002-04.

[27] CGI, NIDB & Orbat Browser COP-21 Integration - System Requirements Analysis, Technical Report, Document version 0.5, 22 January 2004.

[28] Pigeon, L. and Bergeron, A., Urban Operations - AIThink: Intelligent system to support command and control within complex environments, Fact Sheet IS-220-A, DRDC Valcartier 2003-11, 2003.

[29] Natural Resources Canada, National Topographic Data Base (NTDB), http://www.cits.rncan.gc.ca/cit/servlet/CIT/site_id=01&page_id=1-005-002-001.html, 2004.

[30] GeoTango, GeoServNet, http://www.geotango.com/productsV2/gsn/, 2004

[31] EMIS Technologies, EM/200, http://www.emistech.com/em2000.asp, 2004.

[32] Jean, M., Advanced Emergency Response System for CBRN Hazard Prediction and Assessment for the Urban Environment, Proceedings of the 2004 CRTI Summer Symposium, Gatineau, Quebec, 15-16 June 2004.

[33] Joint Warrior Interoperability Demonstrations (JWIDs), http://www.jwid.js.mil/, 2004.

[34] US Department of Homeland Security, TOPOFF 3, http://www.dhs.gov/dhspublic, 2004.