9th International Command and Control Research and Technology Symposium
Coalition Transformation: An Evolution of People, Processes and Technology to Enhance Interoperability

Copenhagen, Denmark, September 14 - 16, 2004

Multi-Environment Decision Support and Knowledge Exploitation in Terrorist Emergency Responses

Jean Roy

Defence Scientist
Decision Support Systems Section
Defence R&D Canada – Valcartier
2459 Pie-XI Blvd. North
Val-Belair, Quebec
Canada, G3J 1X5

Tel. 1-418-844-4000 / Ext. 4379
Cell. 1-418-955-0409
Fax 1-418-844-4538

jean.roy@drdc-rddc.gc.ca
Roy.JMJ@forces.gc.ca
www.valcartier.drdc-rddc.gc.ca

Relevant ICCRTS Topics

Decision Making & Cognitive Analysis
C4ISR/C2 Architecture

Multi-Environment Decision Support and Knowledge Exploitation in Terrorist Emergency Responses

Jean Roy

Defence R&D Canada – Valcartier
2459 Pie-XI Blvd. North, Val-Belair, Quebec, Canada, G3J 1X5
Tel. 1-418-844-4000, Fax 1-418-844-4538
jean.roy@drdc-rddc.gc.ca

Abstract

The post 9/11 new security paradigm requires military forces to be prepared with robust capabilities to support the response to terrorist attacks against people and critical infrastructures. This paper describes a new R&D program, called MUSKETEER, that will develop decision support and knowledge exploitation tools and demonstrate how these tool sets can significantly improve the military forces ability to respond to terrorist attacks. MUSKETEER will create a collaborative workspace aiding military experts to work together effectively (and also aiding the military forces to coordinate with federal government departments and agencies, other civil authorities at all levels, and international allies when required) in order to integrate perspectives to better interpret the situation and the problem, identify candidate actions, formulate evaluation criteria, decide on what to do, and synchronize a diverse set of plans and actions. The paper discusses asymmetric threat and terrorism, outlines the perspective and responsibilities of the Department of National Defence (DND) regarding these important issues, considers the need for decision support and knowledge exploitation systems, and describes the main aspects of the MUSKETEER program, including the well-structured development process that has been identified to build the appropriate decision support system.

1. Introduction

We live in an increasingly interconnected, complex and often dangerous world. The increase in terrorist acts and the threat of rapid, globalized spread of infectious disease all challenge our society and the sense of security that is so critical to our quality of life [PCO, 2004]. Clearly, the events of September 11, 2001 moved the issues of anti- and counter-terrorism, national/public security, and collective emergency response (both crisis and consequence management) to the fore of concerns of many nations. The post 9/11 new security paradigm requires military forces to be prepared with robust capabilities to support the response to terrorist attacks against people and critical infrastructures.

Given the nature of the threats, often labelled “asymmetric” in the military domain, the military forces must strive to reduce the time they needs to identify any such threats to operations, personnel, systems and facilities, and effect the appropriate response to counter them. In some cases, they must prepare themselves to respond to requests for assistance from civil authorities. Military organizations must develop a greater ability to protect units, formations and installations against non-conventional attacks, e.g., chemical, biological, radiological and nuclear (CBRN) attacks.

This paper describes a new R&D program called MUSKETEER (Multi-Environment Decision Support and Knowledge Exploitation in Terrorist Emergency Responses) that has recently been undertaken at Defence R&D Canada – Valcartier (DRDC Valcartier). MUSKETEER will identify, refine, develop and integrate decision support and knowledge exploitation tools and demonstrate how these tool sets can significantly improve the military forces ability to respond to terrorist attacks. The paper first discusses the nature of asymmetric threat and terrorism, providing a few definitions along the way. It also outlines some elements of the perspective of the Department of National Defence (DND) regarding these important issues, and the responsibilities of the DND related to this domain. Section 4 talks about the need for computer-based systems to support decision-making and also discusses decision quality with respect to the availability of critical information. The main aspects of the MUSKETEER program are presented in Section 5, while Section 6 describes the well-structured development process adopted and followed in MUSKETEER to build the appropriate decision support system.

2. Asymmetric Threat and Terrorism

The world is a dangerous place, even if the relative safety of life in Canada sometimes obscures just how dangerous it is [PCO, 2004]. As recent events have highlighted, there is a wide range of threats facing Canada, from pandemics to terrorism. These threats, often labelled “asymmetric” in the military domain, can have a serious impact on the safety of Canadians and on the effective functioning of our society. Defence Planning Guidance (DPG) 2000 initiated an ambitious programme of strategic transformation within the Department [DND, 1999]. DPG 2000 sets out a number of change objectives, including Change Objective Three (CO3), Modernize, that identifies five inter-related goals associated with modernizing the Canadian Forces (CF). One of these goals, Goal Three, pertains to asymmetric threats: *Develop new task-tailored capabilities to deal with asymmetric threats and weapons of mass destruction*.

DPG 2000 assigned the Deputy Chief of the Defence Staff (DCDS) responsibility for the development of Goal Three and directed the DCDS to determine the capabilities and force structure required to meet future asymmetric threats and to substantiate the resources needed to provide the required capabilities. In this context, [Ajilon, 2001] examined the full range of asymmetric threats and Weapons of Mass Destruction (WMDs) to determine the types of military response required to support Canadian security and interests. The four phases of the study were: scope definition, roles and responsibilities definition, determine capability requirements, prepare force development plan for asymmetric threats.

2.1 Defining Asymmetry

Asymmetric threats or techniques describe weapons and tactics that opponents could use to foil or circumvent the technological superiority of Western nations. They can include the use of surprise, and the use of weapons and tactics in ways that are unplanned or unexpected. An asymmetric attack avoids strength and exploits vulnerabilities and could include the prospect of an opponent designing a strategy that fundamentally alters the battlespace on which a conflict is fought. Opponents could, for example, choose to operate in environments, such as large cities or towns, that degrade the capacity of their enemy to find and attack militarily significant targets. Tactics could include conducting acts of aggression that purposely blur boundaries between actions considered crimes and those viewed as warfare. The aspect of opponents conducting asymmetric operations outside of the accepted norms of warfare and the law of armed conflict poses a moral dilemma to Western nations bound by these restrictions.

For the purposes of the study reported in [Ajilon, 2001]: "The asymmetric threat is a term used to describe attempts to circumvent or undermine an opponent's strengths while exploiting his weaknesses, using methods that differ significantly from the opponent's usual mode of operations." Defence Planning Guide (DPG) 2000 defined three broad approaches that potential opponents might employ to gain an asymmetric advantage: use of WMDs, use of cyber warfare, or choosing to fight only in complex terrain. For the purposes of the [Ajilon, 2001] study, the three broad approaches that may be used by opponents have been amended to Information Operations (IO), WMDs, and Non-Conventional Operations (NCO). The impact of an asymmetric attack could be enhanced significantly and synergy created by combining various asymmetric threats in a co-ordinated fashion.

Asymmetry can be manifested in the ends to be achieved, or the ways and means of achieving them. Asymmetric attacks can have a strategic impact, especially in the psychological plane, and may include exploiting the fears and beliefs of the civilian population to weaken support for the democratic process, to undermine the government and its national security forces or, in alliances and coalitions, to compromise the cohesion of the partners. Methods could include information system attacks, exploiting sensitivity to casualties, misinformation, psychological operations, the use of Weapons of Mass Destruction, disrupting complex economies, civil disobedience and terrorism. At the operational and tactical levels, opponents may interdict lines of communications, attempt to maximize casualties to erode resolve, fight in complex terrain such as cities, or take hostages.

The potential for asymmetric attacks on deployed operations or on citizens, property or territory will increase the demand for flexible and unconventional Canadian Forces (CF) contributions to the security of deployed forces, peace support missions, and Canadian interests, and also for improved intelligence capability.

2.2 Terrorism

Terrorism is an important aspect of asymmetric threats having significant potential to affect people security. It can be defined as the calculated use of violence or the threat of violence to inculcate fear, intended to coerce or intimidate governments or societies in pursuit of goals that are generally political, religious or ideological (US DoD Joint Pub 1-02) [Ajilon, 2001]. [DHS, 2004] states that, under the Homeland Security Act of 2002, terrorism is defined as an activity that involves an act dangerous to human life or potentially destructive of critical infrastructure or key resources and is a violation of the criminal laws of the United States or of any State or other subdivision of the United States in which it occurs and is intended to intimidate or coerce the civilian population or influence a government or affect the conduct of a government by mass destruction, assassination, or kidnapping.

Terrorism may be motivated by a variety of causes that can be intermingled [PCO, 2004]: religious extremism, violent secessionist movements, state-sponsored terrorism, and domestic extremism. Anti-terrorism can be defined as defensive measures used to reduce the vulnerability of individuals and property to terrorism (attacks on populations, territory, infrastructure, and information and communications systems), while counter-terrorism can be defined as offensive measures taken to track down, prevent, deter, interdict and respond to terrorists activities.

2.3 Asymmetric Threat Impact and Security Challenge

All of these threats pose a real security challenge for Canada [PCO, 2004]. Often, they do not exist in isolation from one another. For example, the proliferation of WMDs is a problem in itself, but when terrorism is involved, the threat increases dramatically. The danger of pandemics is amplified if groups seek to spread disease deliberately.

DPG 2000 contains a scenario-based capability planning process that enables the analysis of future requirements. Although the DND scenario framework is still in development, the work achieved to date was used to review and rate the likelihood of, and the circumstances under which, an asymmetric threat could develop. The Defence Planning Guidance outlines eleven scenarios which span the spectrum of conflict and operations envisioned for the CF. The CF intent is for the scenarios to continuously evolve, thus ensuring that they reflect the latest strategic environment and Canada's defence perspectives. An initial review of the eleven scenarios indicated that seven offered possibilities for asymmetric threats that could be manifested on Canadian territory or against CF units deployed abroad [Ajilon, 2001].

3. Some Responsibilities of the Department of National Defence

The asymmetric threat study [Ajilon, 2001] examined existing and potential future responsibilities and roles, both international and domestic, for the DND to deal with the asymmetric threat. The currently accepted DND responsibilities were determined by examining the various acts, orders-in-council and government policy directives that apply to DND and the responsibilities of other federal government departments and the provinces.

The responsibilities outlined below are unlikely to change significantly in the foreseeable future [Ajilon, 2001]. These responsibilities are mandated by federal law and long-term government policies, are deeply engrained in our federal democratic system of government and its civil-military relationship, and have existed for some time.

3.1 International Responsibilities

DND may be required to provide military response to direct and indirect threats to Canadian interests, and will deal with threats to DND operations, including the provision of force protection measures during collective defence and peace support operations. The Department of Foreign Affairs and International Trade (DFAIT) will retain primary responsibility for the security of Canadian citizens and interests abroad and, when requested by DFAIT, DND will provide armed or unarmed assistance for the protection and evacuation of Canadians from areas threatened by imminent conflict.

3.2 Domestic Responsibilities

Domestically, the provinces and other federal government departments and agencies have the responsibility for preventing, deterring, crisis managing and consequence managing an asymmetric attack on Canada. If called upon, DND will need to respond to requests for assistance from these organizations and will function in a supporting role. Regardless of which government department has the lead, the inherent flexibility of military units makes DND a potential source of assistance in all domestic emergencies and civil disturbances. However, the DND response is bound by legal considerations. Typically, DND is the Canadian government’s instrument of last resort. This being said, DND may be required to respond to a domestic attack designed to delay or hinder the deployment of Canadian forces overseas. The following broad government responsibilities assist in defining current and future DND domestic roles [Ajilon, 2001].

DND will be required to provide military response to direct and indirect threats to Canadian sovereignty. It will deal with threats to DND assets, installations and operations and will provide communications security support to all government departments. The Solicitor General will retain primary responsibility for terrorist incidents in Canada and DND will provide armed or unarmed assistance when requested. Provincial and territorial governments are responsible for law enforcement and public safety within their jurisdiction, and DND will be required to respond to requests from the provinces for Aid of the Civil Power to assist law enforcement agencies during riots or disturbances of the peace. Other federal government departments (OGD) and the provinces retain responsibility for domestic economic threats and for broader health and criminal issues, and DND will provide armed or unarmed assistance when requested. In many cases this assistance will be discretionary. The provinces and territories have the primary responsibility for emergency preparedness and consequence management during a domestic emergency, and the Minister responsible for emergency preparedness will be required to coordinate federal assistance.

DND is responsible for maintaining an immediate response capability to any terrorist incident in Canada in support of the civil authorities and, in each Land Force Area, a unit to provide an early, planned response to an internal security emergency. DND responsibilities include: operation of the National Defence Command Centre (NDCC), co-operation with the national intelligence community to maintain threat assessments, development of mutually agreed operational procedures with police services, provision of armed assistance in the resolution of a terrorist incident in support of the Royal Canadian Mounted Police (RCMP), provision of nuclear, biological and chemical technical assistance and response capability, including determination and the measures necessary to isolate, contain, assess and dispose of NBC hazards and assisting with the decontamination of persons and property.

4. Decision Support Systems

Operational trends in warfare and the collective response to large-scale terrorist emergency events put the command and control (C2) process under pressure. The technological evolution constantly increases the scope of the operational theatre and the tempo of the response. Moreover, a huge load of uncertain data and information is generated about the environment. Clearly, all these data and information may exceed the human information processing capabilities. Yet, the military community typically maintains that the dominant requirement to counter the threat and ensure the survivability of people, or of a critical infrastructure, is the ability to perform the C2 activities quicker and better than the adversary.

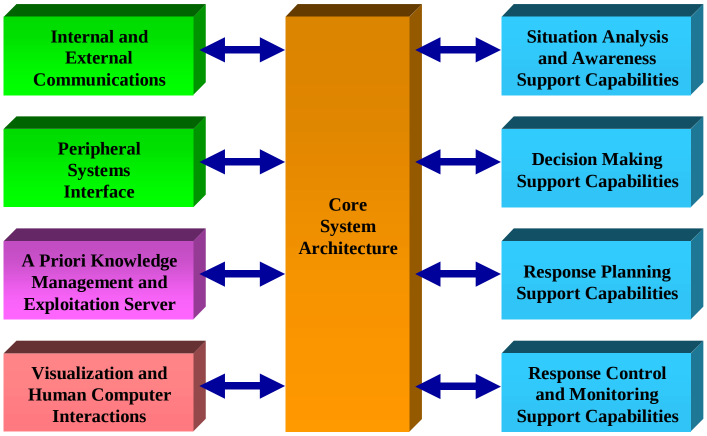

Internal and External Communications
Peripheral Systems Interface
A Priori Knowledge Management and Exploitation Server
Visualization and Human Computer Interactions
Core System Architecture
Situation Analysis and Awareness Support Capabilities
Decision Making Support Capabilities
Response Planning Support Capabilities
Response Control and Monitoring Support Capabilities

Figure 1. A generic decision support and knowledge exploitation system

Information technology support is thus typically required to cope with the human limitations in such complex environments. This emphasizes the need for real-time, computer-based Decision Support Systems (DSSs) to bridge the gap between the cognitive demands inherent to the accomplishment of the C2 process and the human limitations. A DSS is a computerized system that is intended to interact with and complement a human decision maker [Elm, Potter, Gualtieri, Roth, Easter, 2002]. Whatever the nature of the DSS, the objective is to develop DSS features that intuitively fit the perceptual and cognitive processes of the human user. The ideal DSS is one that provides the information needed by the human decision maker as opposed to raw data, can be controlled effortlessly by the human, complements the cognitive power of the human mind, and supports a wide variety of problem solving strategies. Effective DSSs are the ones that "make the problem transparent to the user". Figure 1 shows a generic decision support and knowledge exploitation system. On the right-hand side are the capabilities supporting the C2 activities per se. On the left-hand side are the necessary ancillary capabilities. All these heterogeneous capabilities are glued together through the core system architecture.

4.1 All Information? The Right Information?

In her model, [Endsley, 1995] presents Situation Awareness (SAW) as a stage separate from Decision Making (DM) and action. SAW is described as the decision maker's internal model of the state of the environment. Based on that representation, the decision maker can decide what to do about the situation and carry out any necessary actions. There is thus a strong link between SAW and the decision making processes. SAW is represented as the main precursor to decision making, and is the key factor determining decision quality. Enhancing SAW improves the probability of selecting the appropriate course of actions in most of the situations. Consequently, SAW is considered essential for commanders to conduct DM activities, and the improvement of the human DM process can be seen as highly related to the enhancement of SAW.

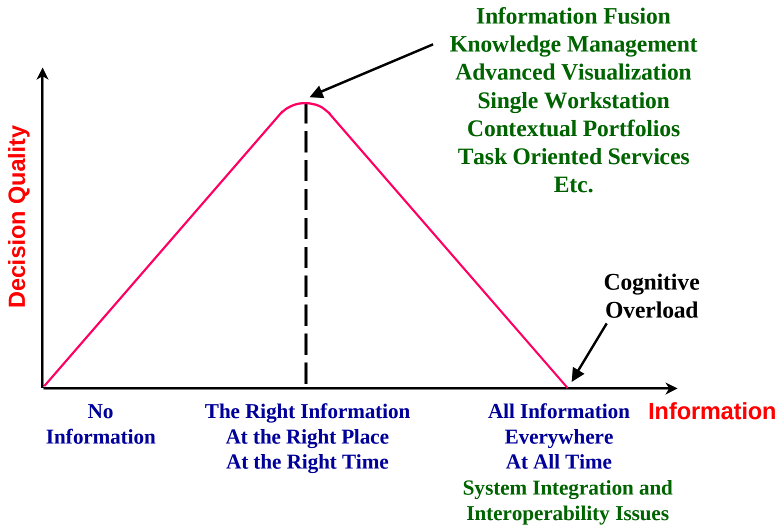


Figure 2. The right information?

In the same line of thoughts, SAW quality can be related to the amount of information available to an individual. Clearly, circumstances where no information is available should result in poor SAW, leading with high probability to very low decision quality. In such a case, a natural reaction would be to provide mechanisms to increase the amount of information available to the decision makers in order to improve SAW quality. One could even claim that a good approach to reach optimal SAW and DM would be to provide as much information as possible. However, this does not necessarily represent the best solution, as more information does not automatically mean better SAW to ensure a better human performance. First, all this information may exceed the human information processing capabilities, leading to cognitive overload. Second, it is not all of the data and information available in the environment that is relevant and useful for reaching an optimal decision. In fact, in some situations, most of the data can be seen as distracters and noise for the decision maker, and may thus reduce his/her level of SAW. The decision maker must detect and use only a specific fraction of this information to enhance his/her SAW and DM processes. Such considerations lead to the concept of "the right information, at the right place, at the right time", as opposed to "all information, everywhere, at all time". This is illustrated in Fig. 2.

Clearly however, research and technological advancements toward providing "all information, everywhere, at all time" are necessary, as such progresses ensure that "the right information, at the right place, at the right time" will actually be available to the decision-makers. Figure 3 presents a different perspective of a generic DSS that takes into account these issues. In Fig. 3, the support capabilities of Fig. 1 are represented as a set of independent system tools and services supporting situation analysis, decision making, knowledge exploitation, etc. Part of the necessary interactions between these tools/services is enabled by the system integration and interoperability layer. However, the system also requires the appropriate mechanisms, based on technological enablers such as information fusion and knowledge management, to provide "the right information, to the right person, at the right time.

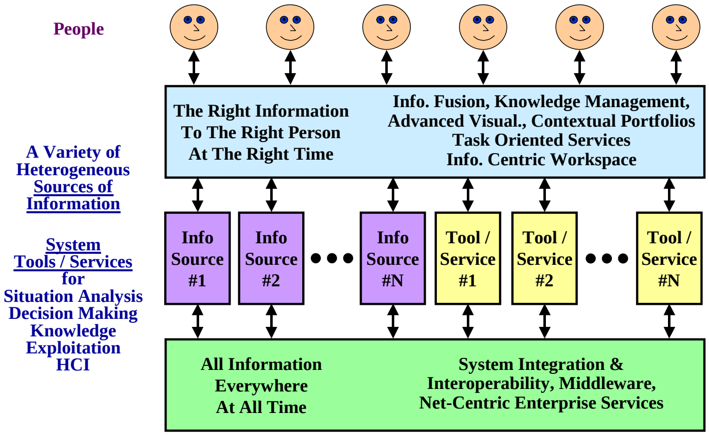


Figure 3. Exploiting information sources and tools/services

5. MUSKETEER

A new R&D program, called MUSKETEER (Multi-Environment Decision Support and Knowledge Exploitation in Terrorist Emergency Responses), has recently been undertaken at Defence R&D Canada – Valcartier (DRDC Valcartier). MUSKETEER will identify, refine, develop and integrate decision support and knowledge exploitation tools and demonstrate how these tool sets can improve the military forces ability to respond to terrorist attacks.

Exploiting distributed collaboration technologies, MUSKETEER will create a collaborative workspace aiding military experts to work together effectively (and also aiding the military forces to coordinate with federal government departments and agencies, civil authorities and international allies when required) in order to integrate perspectives to better interpret the situation and the problem, identify candidate actions, formulate evaluation criteria, decide on what to do, and synchronize a diverse set of plans and actions. DRDC Valcartier will build a computer-based system to support the creation, maintenance and sharing of situational awareness (i.e., a common operational picture), and to assist joint problem solving and decision making at multiple echelons from responders through commanders, and through a set of disparate agencies at different locations. This will require taking advantage of cutting edge ontology-based knowledge management technologies to provide tools to capture and exploit lessons learned, to make inferences that turn data and assumptions into information, and for data/information classification, categorization, clustering, search, etc.

Current work on contextualized user-centric task-oriented knowledge services (based on web services and portal technologies), and on innovative visualisation and human-computer interaction devices, will be leveraged. A compliant architecture will be developed, along with information management concepts and sufficient mechanisms for military forces to effectively interoperate with information system technology (across a wide range of disparate hardware/software systems) between the land/air/sea/joint environments, and also with other government departments, civil authorities at all levels and international allies. Many critical issues, such as common data and service access, information exchange/sharing, data formats, system and data security, privacy and confidentiality and authentication, will be addressed.

6. Approach and Development Process

To build the appropriate DSS, a well-structured development process needs to be adopted and followed. Figure 4 illustrates such a development process. Many aspects of this process are discussed in [Breton, Paradis, Roy, 2002]. An important challenge is to develop a DSS that, on one hand, takes advantage of all the technological opportunities but, on the other hand, is totally compatible with the way the human executes the tasks to be supported. The development of decision support systems thus includes the participation of experts from the application domain, i.e., the Subject Matter Experts (SMEs) in Fig. 4, system designers and human factor specialists to ensure the cognitive fit between the DSS and the decision-makers, in order to maximize decision-making effectiveness.

The DSS development process begins with the identification of SMEs (mostly decision-makers) from the operational community. Then, it proceeds with the capture and understanding of the requirements of the particular application domain of interest. This is a fundamental step, as the application domain characteristics will define the fundamental skeleton of the DSS and ultimately the form of the DSS knowledge model communicated to the human practitioner controlling the domain. This step can be initiated through reading appropriate documentation of the domain, through an analysis of documented lessons learned, and through an active participation in training courses and/or exercises/demonstrations with end users. However, a serious DSS development process must include formal interview of SMEs, following cognitive engineering methods. This step includes the use of current cognitive theories and models to interpret and understand the impact of the results and findings from a human factor perspective.

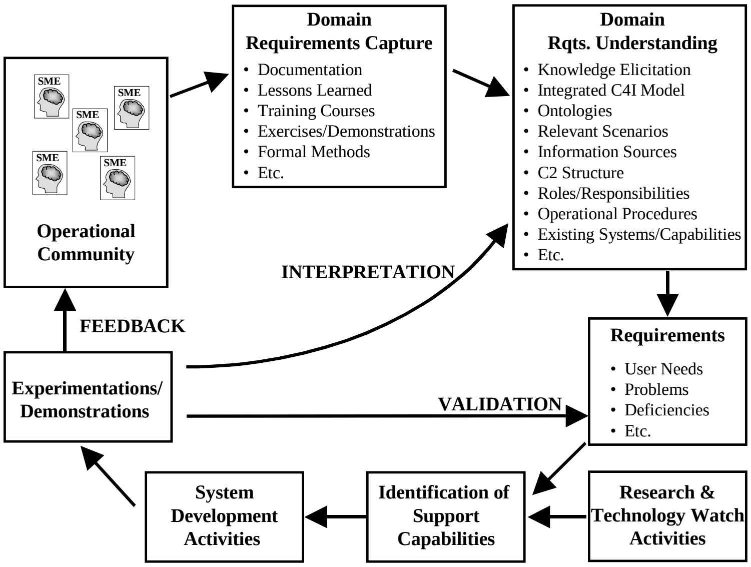
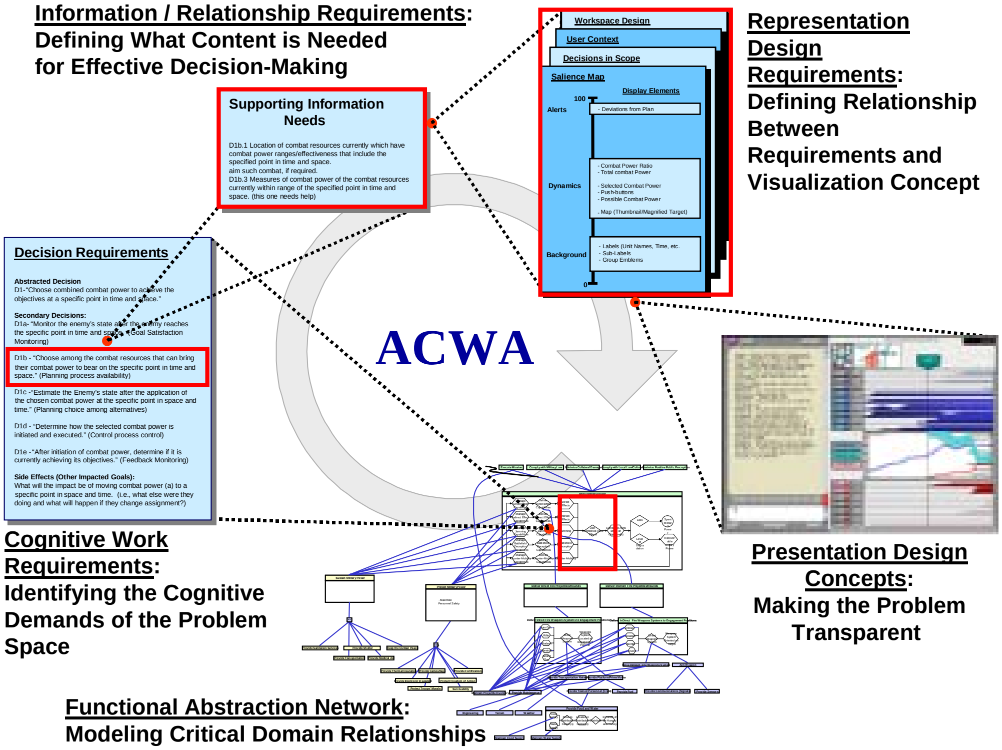


Figure 4. DSS development process

The analyses above lead to the identification of user needs, problems and deficiencies in the form of explicit system/software requirements. Then, technological solutions are identified to address the requirements, taking into account findings of research and technology watch activities, leading to system development activities. A serious system development process, if the project timeframe and appropriate resources permit, should follow formal software engineering methodologies. Testing procedures and demonstrations/experimentations are required to validate the technological solutions from the human performance and operational perspectives. Transparency must be one characteristic of the development process. With testing/demonstration/experimentation results presented as a feedback, the SMEs can understand the link between their requirements and the solutions provided at the end of the development process to answer these requirements. Moreover, discussions around these results may lead to the identification of other problems experienced by the SMEs, or potential problems created by the new DSS. On one hand, being more involved into the development process through the feedback process allows the SMEs to develop a better understanding about the way the DSS is built, which can result in a better acceptation and a higher level of confidence about the DSS. On the other hand, having more contacts with the SMEs helps the team members to be more aware of the SME reality, which can lead to the development of a more appropriate DSS.

6.1 Cognitive Engineering

To efficiently support humans in their situation analysis and decision-making processes, the technology has to be designed to provide only the critical information required for these processes, i.e., the data and information that enhance the decision maker's SAW, which in turn increases the probability of an efficient DM process [Roy, Breton, Paradis, 2001]. From a DSS design perspective, the identification of the critical information can be done through the application of cognitive theories and cognitive system engineering (CSE) techniques.


Information / Relationship Requirements:
Defining What Content is Needed
for Effective Decision-Making
Representation Design Requirements:
Defining Relationship Between Requirements and Visualization Concept
ACWA
Cognitive Work Requirements:
Identifying the Cognitive Demands of the Problem Space
Presentation Design Concepts:
Making the Problem Transparent
Functional Abstraction Network:
Modeling Critical Domain Relationships
Workspace Design
User Context
Decisions in Scope
Salience Map
Display Elements
100
0
Alerts
Dynamics
Background

Supporting Information Needs

D1b.1 Location of combat resources currently which have combat power ranges/effectiveness that include the specified point in time and space.
aim such combat, if required.
D1b.3 Measures of combat power of the combat resources currently within range of the specified point in time and space. (this one needs help)

Decision Requirements

Abstracted Decision
D1-"Choose combined combat power to achieve the objectives at a specific point in time and space."

Secondary Decisions:
D1a- "Monitor the enemy's state after the enemy reaches the specific point in time and space." (Goal Satisfaction Monitoring)

D1b - "Choose among the combat resources that can bring their combat power to bear on the specific point in time and space." (Planning process availability)

D1c -"Estimate the Enemy's state after the application of the chosen combat power at the specific point in space and time." (Planning choice among alternatives)

D1d - "Determine how the selected combat power is initiated and executed." (Control process control)

D1e -"After initiation of combat power, determine if it is currently achieving its objectives." (Feedback Monitoring)

Side Effects (Other Impacted Goals):
What will the impact be of moving combat power (a) to a specific point in space and time. (i.e., what else were they doing and what will happen if they change assignment?)

- Deviations from Plan

- Combat Power Ratio
- Total combat Power

- Selected Combat Power
- Push-buttons
- Possible Combat Power

- Map (Thumbnail/Magnified Target)

- Labels (Unit Names, Time, etc.
- Sub-Labels
- Group Emblems

Figure 5. Applied Cognitive Work Analysis (ACWA)

Cognitive Task Analysis (CTA) and Cognitive Work Analysis (CWA) are both often put forward as techniques that can provide, via interviews with SMEs, the set of critical information that must be made available to reach optimal decisions. Unfortunately, these approaches are well suited to deal with decision support issues but are in practice very expensive to conduct, time consuming and more importantly, generally inefficient from a design process perspective. With the latter limitations in mind, a pragmatic CSE approach, known as the Applied Cognitive Work Analysis (ACWA), has been developed to bridge, in a structured, efficient and converging way, the gap between cognitive analysis and design [Paradis, Breton, Bossé, Elm, Potter, 2002]. This ACWA modeling method is a pragmatic adaptation of the CWA method in order to cope with the limitations related to applying CWA. As a result, the cost to conduct CSE analyses using the ACWA approach is reduced and the analysis-design efficiency is significantly improved, therefore making easier the identification of decision-aiding concepts suited to provide effective decision support. Figure 5 provides a visual depiction of the sequence of methodological steps and their associated output artefacts, as well as an indication that the process is typically repeated in several expanding spirals, each resulting in an improved DSS. [Elm, Potter, Gualtieri, Roth, Easter, 2002] describes each step of this approach in detail.

6.2 Software Engineering

Developing a computer-based decision support system ultimately has to do with developing software. Hence, as for any large-scale software system, the development of a large-scale DSS should follow an appropriate software development methodology for the creation and management of the required software. This section briefly discusses two such methodologies often put forward by the software development communities.

6.2.1 ISO/IEC 12207 International Standard

As discussed in [IEEE, 1998-A], software is an integral part of information technology and conventional systems, such as transportation, military, medical care, and finance. Over many years, there's been a proliferation of standards, procedures, methods, tools, and environments for developing and managing software. This proliferation has created difficulties in software management and engineering, especially in integrating products and services. The software discipline needed to migrate from this proliferation to a common framework that could be used by software practitioners to "speak the same language" to create and manage software. The ISO/IEC 12207 international standard, published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), provides such a common framework for software life cycle processes, with well-defined terminology, that can be referenced by the software industry.

The processes in ISO/IEC 12207 form a comprehensive set. An organization, depending on its purpose, can select an appropriate subset to fulfill that purpose. The standard is, therefore, designed to be tailored for an individual organization, project, or application. The tailoring process has to do with the deletion of non-applicable processes, activities, and tasks. The standard is also designed to be used when software is a stand-alone entity, or an embedded or integral part of the total system.

6.2.2 Rational Unified Process (RUP)

The Rational Unified Process (RUP) is a software engineering process [Rational, 1998]. It provides a disciplined approach to assigning tasks and responsibilities within a development organization. Its goal is to ensure the production of high-quality software that meets the needs of its end-users, within a predictable schedule and budget. It captures many of the best practices in modern software development in a form that is suitable for a wide range of projects and organizations.

The RUP activities create and maintain models. Rather than focusing on the production of large amount of paper documents, the unified process emphasizes the development and maintenance of models—semantically rich representations of the software system under development. RUP is supported by tools, which automate large parts of the process. These tools are used to create and maintain the various artefacts—models in particular—of the software engineering process: visual modeling, programming, testing, etc. The unified process is a configurable process that fits small development teams as well as large development organizations, and is founded on a simple and clear process architecture that provides commonality across a family of processes. Yet, it can be varied to accommodate different situations. Details of the Rational Unified Process can be found in [Rational, 1998] or in [Kruchten, 2000].

6.3 Combining Cognitive and Software Engineering Methodologies

Figure 6 illustrates the approach proposed to develop highly effective decision support systems, based on combining cognitive and software engineering methodologies into an integrated approach.

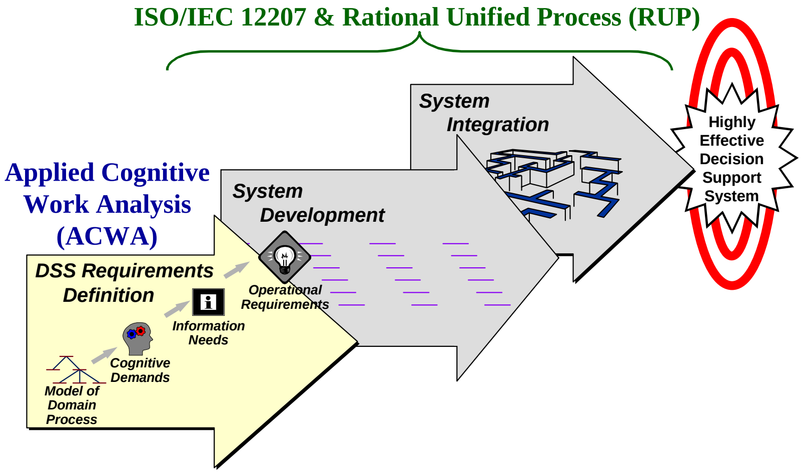

ISO/IEC 12207 & Rational Unified Process (RUP)
Applied Cognitive Work Analysis (ACWA)
DSS Requirements Definition
Model of Domain Process
Cognitive Demands
Information Needs
Operational Requirements
System Development
System Integration
Highly Effective Decision Support System

Figure 6. DSS development methodology

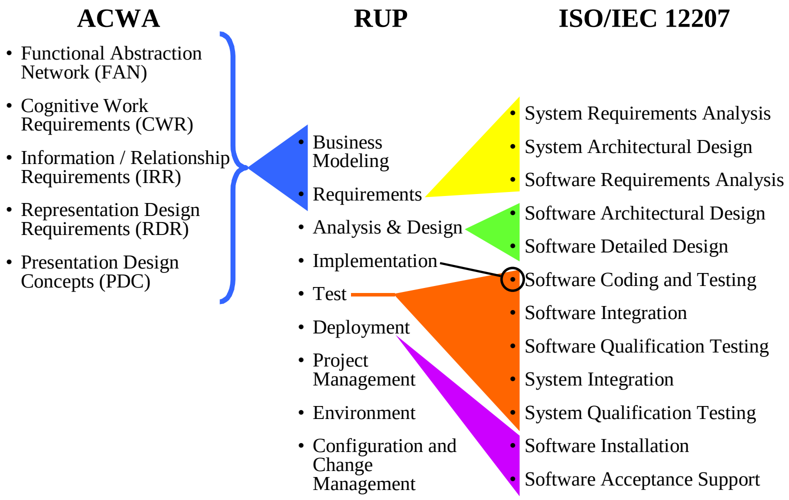

ACWA
Functional Abstraction Network (FAN)
Cognitive Work Requirements (CWR)
Information / Relationship Requirements (IRR)
Representation Design Requirements (RDR)
Presentation Design Concepts (PDC)
RUP
Business Modeling
Requirements
Analysis & Design
Implementation
Test
Deployment
Project Management
Environment
Configuration and Change Management
ISO/IEC 12207
System Requirements Analysis
System Architectural Design
Software Requirements Analysis
Software Architectural Design
Software Detailed Design
Software Coding and Testing
Software Integration
Software Qualification Testing
System Integration
System Qualification Testing
Software Installation
Software Acceptance Support

Figure 7. DSS development activities

As previously mentioned, the development of a large-scale DSS should follow an appropriate software engineering methodology for the creation and management of the required software. We propose to use an appropriate mix of two methodologies often put forward by important software development teams, i.e., ISO/IEC 12207 and the Rational Unified Process. These methodologies will be adapted and tailored to create an hybrid approach that will meet the needs and scope of the DSS development process. Clearly, using ISO/IEC 12207, RUP, or a clever combination of both methodologies would provide good results for most software development projects. However, this is not sufficient for the development of an effective decision support system. Hence, we propose to combine the software engineering methodology with a cognitive engineering methodology. In this regard, Applied Cognitive Work Analysis seems to be an appropriate candidate. Figure 7 shows the relationships between the various development activities put forward by these three methodologies.

6.4 Capturing and Documenting the DSS Requirements

Figure 8 shows how the three methodologies will be combined and used to derive the requirements for the MUSKETEER project.

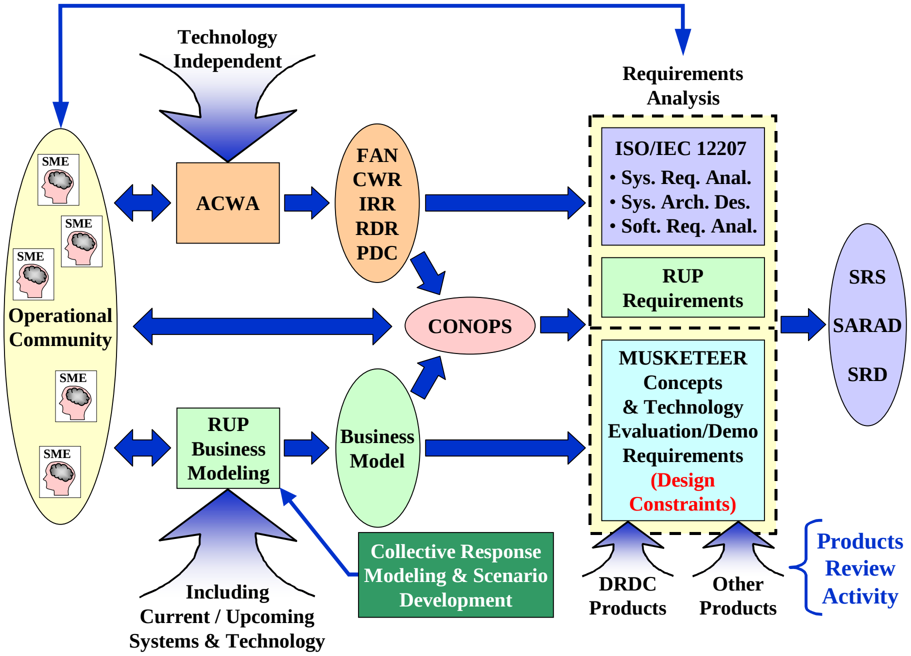


Figure 8. DSS requirements identification

The proposed approach for the identification of the DSS requirements includes the modeling of the application domain from a cognitive, decision-making perspective (i.e., the capture, grasp and documentation of the goals, analysis processes, critical decisions and corresponding information requirements). Combined with formal business modeling activities, this approach will examine and help sort out the decision-support challenges, leading to the identification and definition of proper support capabilities, and their documentation expressed as system and software requirements.

Based on the results of the ACWA and business modeling activities, and working with the SMEs from the operational community, a Concept of Operations (CONOPS) will be developed to describe, in users' terminology, how the system should operate to meet the users' needs for the system. The concept of operations description should include elements such as a description of the current situation or system, a justification for and the nature of changes, concepts for the proposed system, operational scenarios, summary of impacts, etc. [IEEE, 1998-B]. Building on the artefacts of the ACWA, the business model and the CONOPS, the requirement analysis activity will identify and document the system and software requirements for the DSS (system requirements specification, software requirements description, etc.) following guidelines provided by the ISO/IEC 12207 and the RUP.

6.4.1 Collective Response Modeling and Scenario Development

Among other things, MUSKETEER will create a collaborative workspace aiding the military forces to coordinate with other government departments and agencies, civil authorities and international allies when required. It is thus important to obtain a deep understanding of the roles and responsibilities of DND in the collective response to large-scale emergencies, especially those involving terrorism. Indeed, it is important to understand the relationships between all of the players involved. In that sense, the approach of Fig. 8 for the identification of the DSS requirements includes the development of a model of the collective response, developed mainly through an in depth review of the many emergency response plans and scenarios available.

6.4.1.1 Reviewing Emergency Response Plans

This activity will identify documents (especially Emergency Response Plans (ERPs), Standing Operating Procedures (SOPs) and Tactics, Training and Procedures (TTPs)) that could be used to understand and describe the collective response to large-scale terrorist attacks, i.e., emergency responses involving many different participants (e.g., the CF, other government departments (OGDs), civil authorities at all levels, first responders, international allies, etc.). A particular care will be given to any information pertinent to the description of processes (activities), the interaction between these processes/activities, the information flow, the existing strategic, operational and tactical C2 processes associated with the different roles of the participants, etc. Key ERPs and procedures will be reviewed and analysed. This analysis will be documented in order to provide the MUSKETEER project with a deep understanding of the extent and limitations of these plans.

6.4.1.2 Reviewing Emergency Response Scenarios

This activity will begin with a search for relevant existing scenario material from appropriate Canadian and US organizations. Key Emergency Response Scenarios (ERSs) will be reviewed and analysed to obtain a deep understanding of the extent of these scenarios, including any restrictions or limitations. Typical basic scenario components relevant to the emergency response domain will be identified from the review. In particular, the typical terrorism and asymmetric threat elements present within these scenarios will be identified.

6.4.1.3 Characteristics of Asymmetric Threats and Terrorist Activities

Based on the review and analysis described above of the ERPs and ERSs, and the analysis of recent real world events (e.g., the information available on www.terrorism.com), the typical, common characteristics of asymmetric threats and terrorist related activities will be identified and described. In particular, the nature and characteristics of terrorist events and asymmetric threats will be documented, along with the common characteristics or trends of the scenarios, either in their nature, sequence of events/activities, preparation and impact analysis of any such terrorist events/activities. The nature and general characteristics of complex situations (complex operations in complex environments) resulting from asymmetric threats and terrorist activities will also be identified, along with potential complex situations (e.g., asymmetric threats, natural disasters, peace support operations, etc.) that the CFs may encounter.

6.4.1.4 Developing a Collective Response Model

A unified model of the collective response to emergencies caused by terrorist attacks and other asymmetric threat situations will be developed. This model (a generic emergency response framework) will be a synthesis of the reference ER and scenario documents that summarizes and integrates their main characteristics (in order to give an integrated view of all activities that could be involved in a generic collective ER). This synthesis will clearly identify and highlight the different roles/responsibilities of the various responders, as discussed in the key national emergency response plans. In particular, the synthesis will focus on and emphasize the roles and responsibilities of the DND. The different Emergency Operation Centres (EOCs) that can and will be used to support the collective response will be identified, along with the challenges in inter-agency co-operation, co-ordination, interoperability and decision making. The C2 requirements of the operational communities at federal, provincial and municipal levels will be documented (potentially leading to the development of an integrated C2 model for national planning, alert, prevention and response). The actual role and issues pertaining to information system technologies used in collective response situations will be highlighted.

The model will identify and describe the processes associated with each role, the activities occurring within each process, and the aspects relevant to the realization of each activity. This will include the information/data flow in and out of each process/activity (including the format, the intent, the destination etc.), controls and mechanisms (including the systems actually involved) associated with each process/activity, the knowledge (implicit and explicit, declarative and procedural) needed to realize them, the interactions among the activities, the contextual aspects of the realization of the activities (including the dynamic of the different activities, the identification of the participants/contributors realizing the activities, and the constraints imposed by the environment).

6.4.1.5 Developing Generic Scenarios of Emergency Response

Based on the review and analysis of the ERPs and ERSs, the typical characteristics of asymmetric threats and terrorist events/activities, and the model of the collective response, this activity will develop four generic, baseline scenarios of emergency response to terrorist attacks and asymmetric threats, focusing on and emphasizing the roles and responsibilities of the CFs. The main themes for these generic scenarios could be "domestic operations: high-density urban area / DND assets and CF operations" and "international operations: CA-US cross-border emergency / CF deployment abroad". For each scenario, a time-stamped storyboard and a detailed description of the scenario will be developed.

6.4.2 Products and Systems Review Activity

The MUSKETEER project will not develop and build a DSS starting from a blank sheet; it will rather harness existing capabilities to achieve some level of leveraging. In particular, it will capitalize on many relevant and unique concepts and products already developed by DRDC and elsewhere, and that will be considered for refinement, adaptation, incremental integration and use. As illustrated in Fig. 8, the analysis of the system and software requirements for the DSS will have to take this into account, since the integration of existing products will create design constraints for the development of the DSS.

In order to identify the products or systems that should be considered for MUSKETEER, the project team will conduct an in depth review of products and systems in the field of computer-assisted decision support and knowledge exploitation, and relevant to terrorist emergency response. A detailed search for relevant products and systems that are available in the industry, the military domain, and the academic domain will be performed. This phase will include a review and positioning of the decision support and knowledge exploitation technologies, and then the actual inventory of products and systems (including an overview of major research projects around the world, and the review of emerging commercial products/ systems). A Products and Systems Master List (PSML) will be generated, including a list of all contacts relevant to the PSML.

Then, a review and description of the products and systems of the PSML will be performed in terms of technical specifications, features, system requirements, and other relevant description items. This will generate a Products and Systems Review Matrix (PSRM). A Global Capability Matrix (GCM) will next be created, covering all capabilities offered by all of the reviewed products and systems. The identified capabilities will be regrouped in functional categories (e.g., situation analysis, decision support, visualisation, etc.). Finally, an analysis and a synthesis of the review activity above will be performed, including but not limited to trends (commercial and academic), outstanding findings, user satisfaction, most promising products and systems (and those that should be avoided), products and systems evolution (foreseen development), etc.

6.4.2.1 Products Investigated and Developed by DRDC Valcartier

A number of existing products investigated and developed at DRDC Valcartier have already been identified as good candidate for refinement, adaptation, incremental integration and use in MUSKETEER. Examples of such products are listed in Table 1. Discussing all of these products is clearly out of the scope of this document; some of them are shown on Fig. 9.

Figure 9. Examples of existing products/systems developed at DRDC Valcartier

TABLE 1 - Examples of existing products/systems developed at DRDC Valcartier

Products / Systems	**Reference(s)**
Common Operational Picture 21^{st} Century (COP 21) Technology Demonstration Project (TDP) Situational Awareness Portal	[Gouin, Gauvin, Woodliffe, 2003], [Gauvin, Boury-Brisset, Auger, 2004], [Gauvin, Boury-Brisset, Garnier-Waddell, 2002]
COPlanS (Collaborative Operations Planning System)	[Guitouni, 2003]
ADAC (Automatic Documents Analyzer and Classifier)	[Guitouni, Boury-Brisset, Belfares, Tiliki, Belacel, Poirier, Bilodeau, 2002]
ToMaDi (Topographical Map Display)	[Fortin, 2001]
KNOWMES (Knowledge Management and Exploitation Server)	[Boury-Brisset, 2001], [Boury-Brisset, 2003]

CODSI (Command Decision Support Interface)	[Roy, Breton, Paradis, 2001], [Breton, Paradis, Roy, 2002]
Results from the "Lessons Learned" projects	[Boury-Brisset, Gauvin, Champoux, 2002], [Champoux, Thibault, Trudel, 2003]
3D Urban Models	[Létourneau, 2002]
Information-Centric Workspace	[Thibault, Le May, 2003]
OPERA (Operational Planning Environment and Reference Application)	[St-Jacques, 2001]
AIThink / Optipath	[Pigeon, Bergeron, 2003]

6.5 Demonstrations and Field Experiments

The work plan for the MUSKETEER program includes field experiments, as the program is directed towards the validation of concepts, technologies and response processes, in order to provide both timely and directed systems input to military planners and acquisition managers. The activities below, sequentially progressing from a workshop to a large-scale field experiment, will be conducted with the end users to validate the findings and results of the MUSKETEER program.

Activity 1 – Organize and conduct a counter terrorism/asymmetric threat workshop involving key organisations and personnel identified by the project sponsor to identify critical issues, processes, ERPs, etc., through short scenario-based case studies.

Activity 2 – Participate to a major existing experiment/exercise to capture domain specific joint operational requirements and demonstrate initial MUSKETEER prototype functionalities.

Activity 3 – Participate to a counter terrorism/asymmetric threat exercise aimed at developing the MUSKETEER target operational architecture (concepts, sources, organisations, business processes) and demonstrate the initial MUSKETEER Command Environment (MCE) capabilities.

Activity 4 – Simulation-based, combined laboratory tests aimed at validating MCE functionalities supporting the C2 process of a Unified Command Center (UCC).

Activity 5 – Limited Objective Experiment (LOE) to capture and validate functional and operational requirements for the development of advanced decision support and knowledge exploitation tools for MUSKETEER.

Activity 6 – Evaluate and measure within a suitable experimental context the validity and effectiveness of the decision support and knowledge exploitation tools provided within a UCC.

7. Conclusion

The post 9/11 new security paradigm requires military forces to be prepared with robust capabilities to support the response to terrorist attacks against people and critical infrastructures. This paper described a new R&D program, called MUSKETEER, that will develop decision support and knowledge exploitation tools and demonstrate how these tool sets can significantly improve the military forces ability to respond to terrorist attacks.

The nature of asymmetric threat and terrorism was briefly discussed. Some elements of the perspective of the DND regarding these important issues, and the responsibilities of the DND related to this domain were outlined. The need for computer-based systems to support decision-making was discussed, along with issues regarding decision quality with respect to the availability of critical information. The main aspects of the MUSKETEER program were presented. The well-structured development process adopted and followed in MUSKETEER to build the appropriate decision support system was described. This included a brief discussion on cognitive and software engineering methodologies, and on a proposition to combine such methodologies in order to develop highly effective decision support systems. The proposed approach for the identification, capture and documentation of the DSS requirements was presented. This approach includes the development of a model of the collective response to large-scale emergencies caused by terrorism, and the development of appropriate emergency response scenarios for the MUSKETEER program, mainly through an in depth review of the many emergency response plans and existing scenarios available. The approach also includes an in depth review of products and systems in the field of computer-assisted decision support and knowledge exploitation, and relevant to terrorist emergency response. Finally, the validation of the findings and results of the MUSKETEER program through demonstrations and field experiments was briefly discussed.

8. References

[Ajilon, 2001], Ajilon Canada, The Asymmetric Threat, Report Number 2001-1, Prepared for DND/DCDS, August 2001.

[Boury-Brisset, 2001], 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.

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

[Boury-Brisset, Gauvin, Champoux, 2002], 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.

[Breton, Paradis, Roy, 2002], 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.

[Champoux, Thibault, Trudel, 2003], 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.

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

[DND, 1999], Department of National Defence, Defence Planning Guidance 2000 (DPG 2000), 5 August 1999.

[Elm, Potter, Gualtieri, Roth, Easter, 2002], Elm, W.C., Potter, S.S., Gualtieri, J.W., Roth, E.M. and Easter, J.R., Applied Cognitive Work Analysis: A Pragmatic Methodology for Designing Revolutionary Cognitive Affordances, Chapter in preparation, To appear in Hollnagel, E. (Ed). *Handbook of Cognitive Task Design*, 2002.

[Endsley, 1995], Endsley, M. R., Toward a Theory of Situation Awareness in Dynamic Systems, Human Factors Journal, 37(1) , pages 32-64, March 1995.

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

[Gauvin, Boury-Brisset, Auger, 2004], 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.

[Gauvin, Boury-Brisset, Garnier-Waddell, 2002], 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.

[Gouin, Gauvin, Woodliffe, 2003], 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.

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

[Guitouni, Boury-Brisset, Belfares, Tiliki, Belacel, Poirier, Bilodeau, 2002], 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.

[IEEE, 1998-A], IEEE, Industry Implementation of International Standard ISO/IEC 12207 : 1995 (ISO/IEC 12207) Standard for Information Technology - Software life cycle processes, IEEE/EIA Standard, IEEE/EIA 12207.0-1996, March 1998.

[IEEE, 1998-B], IEEE, Industry Implementation of International Standard ISO/IEC I2207: 1995 (ISO/IEC 12207) Standard for Information Technology - Software life cycle processes - Life cycle data, IEEE/EIA Guide, IEEE/EIA 12207.1-1997, April 1998.

[Kruchten, 2000], Kruchten, P., The Rational Unified Process – An Introduction, Second Edition, Addison-Wesley, Reading, Massachusetts, 2000.

[Létourneau, 2002], Létourneau, F., Different Approaches for the Creation and Exploitation of 3D Urban Models, 7th ICCRST, Quebec City, September 2002.

[Paradis, Breton, Bossé, Elm, Potter, 2002], Paradis, S., Breton, R., Bossé, É., Elm, W.C., and Potter, S., A Pragmatic Cognitive System Engineering Approach to Model Dynamic Human Decision-Making Activities in Intelligent and Automated Systems, NATO HFM, 2002.

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

[Pigeon, Bergeron, 2003], 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.

[Rational, 1998], Rational Software Corporation, Rational Unified Process - Best Practices for Software Development Teams, White Paper, 1998.

[Roy, Breton, Paradis, 2001], 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.

[St-Jacques, 2001], St-Jacques, J.-C., OPERA – Operational Planning Environment and Reference Application, Fact Sheet IS-218-A, DRDC Valcartier 2002-04.

[Thibault, Le May, 2003], 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.