Defence Research and Development Canada | Recherche et développement pour la défense Canada

DEFENCE R&D DÉFENSE

Capability Analysis Framework:
An approach for conducting simulation-based exercises with public partners and stakeholders.

A.L. Vallerand
Director –PSTP
DRDC Centre for Security Scince, Ottawa, ON

Kristine Osgoode, Chris DeJagger
CAE Professional Services,
Ottwa, ON

Defence R&D Canada – Centre for Security Science

DRDC Centre for Security Science TM 2007-002

December 2007

Canada

Copy No: _____

Capability Analysis Framework:

An Approach for Conducting Simulation-Based Exercises with Public Security Partners and Stakeholders.

A.L Vallerand
Director – PSTP

DRDC CSS, Ottawa ON

Kristine Osgoode, Chris DeJager
CAE Professional Services,

Ottawa ON.

Department of National Defence/Defence Research & Development Canada

Centre for Security Science

Author

A.L. Vallerand

Approved by

Dr. Anthony Ashley
DRDC Centre for Security Science, Director General

Approved for release by

Dr. Mark Williamson
DRDC Centre for Security Science, Director CRTI
Document Review Panel

Abstract

This report is written for government departments and other stakeholders, who may desire science and technology (S&T) support in ensuring a horizontal approach to emergency management and public security across the government of Canada. This approach is applicable to an all hazards approach to public safety and relevant to communities with interest in CBRNE protection, Critical Infrastructure Protection (CIP), Surveillance, Intelligence and Interdiction (SI2), Emergency Management & Systems Integration (EMSI) and finally, Risk and Threat Assessment domains.

The report serves as an overview of the approach and activities conducted with stakeholders who seek to engage in S&T research in cooperation with Defence Research & Development Canada's (DRDC) Centre for Security Science and the Public Security Technical Program (PSTP). It provide an overview of the PSTP Capability Analysis process and outlines how the PSTP may use exercises to engage in capability based analyses and simulation. The report communicates how the PSTP used certain views of the Department of Defence Architecture Framework (DoDAF) to map the incident concept of operations (the actors and organizations) for a scenario that represented a high-consequence public security event.

The report documents how the PSTP conducted human centered capability analysis to identify where capability gaps exist in a response mechanism. The data obtained from using this methodology revealed a clear sequence of steps, and an output at each step that feeds into the next. Using recognizable operational architectural modeling analytical tools allowed stakeholders to produce concise outputs, ensuring clarity in the process. Conducting a realistic simulation, focused on the user's needs ensures the final assessment of capability options will operate from metric data that most closely reflects a real-life response to a high-consequence public security event. Finally, the report highlights the process the PSTP is exploring to determine critical capability gaps and draft alternative science and technology solutions that may be considered to remedy the gaps.

Résumé

Le présent rapport s'adresse aux ministères et aux autres intervenants qui voudraient obtenir du soutien en matière de sciences et de technologie en vue d'adopter une approche horizontale de gestion des urgences et de sécurité publique à l'échelle du gouvernement du Canada. Cette façon de faire convient à une approche tous risques liée à la sécurité publique et aux collectivités qui s'intéressent à la protection contre les agents CBRNE, à la protection des infrastructures essentielles (PIE), à la surveillance, au renseignement et à l'interdiction (SRI), à la gestion des urgences et à l'intégration des systèmes (GUIS), et à l'évaluation de la menace et des risques.

Le rapport donne un aperçu des méthodes mises en place et des activités menées aux intervenants qui veulent participer aux recherches en matière de sciences et de technologie en collaboration avec le Centre des sciences pour la sécurité de Recherche et développement pour la défense Canada (RDDC) dans le cadre du Programme technique de sécurité publique (PTSP). Le rapport donne une vue d'ensemble du processus d'analyse des capacités du PTSP et décrit comment le PTSP peut recourir à des exercices pour effectuer des analyses et des simulations fondées sur les capacités. Le rapport indique de quelle façon le PTSP a utilisé certains aspects du cadre d'architecture du département de la Défense pour élaborer le concept de l'opération (les acteurs et les organisations) d'un scénario qui représente un événement ayant de lourdes conséquences sur la sécurité du public.

Le rapport explique comment le PTSP a analysé les capacités centrées sur le facteur humain afin de déterminer les lacunes du mécanisme d'intervention. D'après les données ainsi obtenues, on a constaté clairement une séquence d'étapes et un résultat à chacune des étapes qui mène à l'étape suivante. Les intervenants ont utilisé des outils d'analyse identifiables de modélisation architecturale opérationnelle qui leur ont permis d'obtenir des résultats concis, assurant du coup la clarté du processus. En conduisant une simulation réaliste axée sur les besoins de l'utilisateur, on s'assure que l'évaluation finale des capacités se fondera sur les données métriques qui correspondent le mieux à une intervention réelle lors d'un événement ayant de lourdes conséquences sur la sécurité du public. Enfin, le rapport donne les grandes lignes du processus que le PTSP examine afin de déterminer les lacunes graves au niveau des capacités et de trouver de nouvelles solutions de rechange en matière de sciences et de technologie susceptibles de combler ces lacunes.

This page intentionally left blank.

Executive summary

The Defence Research and Development Canada's (DRDC) Centre for Security Science (CSS) – Public Security Technical Program (PSTP) conducted a critical telecommunications infrastructure simulation in cooperation with Industry Canada, the government partner, and a telecommunications critical infrastructure owner, as a Case Study. The project created a model that simulated the reaction to a biological contamination incident at a major communications exchange. The response involved maintenance performed by a hazardous material (HAZMAT) responder on critical telecommunications infrastructure in a contaminated environment.

The purpose of the simulation was to determine the capabilities required to maintain business continuity during this high consequence public security event. Through simulation, deficiencies were identified in the business continuity response capability to the contamination event, and possible solutions to remedy the deficiencies were presented.

The activities performed as part of the methodology were instructive for all study partners. The results of the method applied and the outcome of the study provided insight by highlighting both deficiencies and remedies, actionable through the partnership with Industry Canada, the Centre can leverage to remedy gaps. The methodology started by mapping the process using the Department of Defence (US) Architectural Framework (DODAF) to identify the actors involved in response, linkages, dependencies, and the lines of communications based on the identified scenario. The architecture views identified 'swim lanes' for multiple activities and actions performed by the actors involved in reaction and response. To confirm the framework, a task oriented live response simulation was performed at a critical telecommunications infrastructure location using HAZMAT responders to simulate the performance of routine maintenance tasks in a contaminated environment.

Capability gaps were identified throughout the simulation and were noted for post analysis. The success of the simulation was due in large part to the user-centric task focus resulting in maximum realism during the simulation and an appropriate context for validated gap analysis. The findings were summarized and a thorough description of capability improvement options was presented to the telecommunications infrastructure owner for consideration.

The methodology applied to the critical telecommunications infrastructure capability assessment will be used by the PSTP in future simulation based capability analysis with other public security and emergency management stakeholders and partners. The success of the user-centric simulation validates the effectiveness of the methodology in defining the current response process and capability, while identifying specific areas for improvement. Future simulations conducted by the PSTP will most likely follow the methodology outlined above, and conform to all additional Government of Canada regulations.

Vallerand, A.L, K Osgoode, C DeJager, 2007. Capability Analysis Framework: An Approach for Conducting Simulation-Based Exercises with Public Security Partners and Stakeholders. DRDC Centre for Security Science TM 2007-002

Sommaire

Le personnel du Programme technique de sécurité publique (PTSP) – Centre des sciences pour la sécurité de Recherche et développement pour la défense Canada (RDDC) a effectué une simulation portant sur l'infrastructure essentielle des télécommunications dans le cadre d'une étude de cas, en collaboration avec Industrie Canada, le partenaire du gouvernement, et le propriétaire d'une infrastructure essentielle de télécommunications. Le projet a permis de créer un modèle qui simulait la réaction à un incident découlant d'une contamination biologique durant un échange important. Un intervenant en cas de déversement de matières dangereuses a pris les mesures nécessaires en assurant la maintenance de l'infrastructure essentielle de télécommunications dans un environnement contaminé.

La simulation visait à déterminer les capacités requises pour assurer la continuité des opérations à la suite de cet événement ayant de lourdes conséquences sur la sécurité du public. La simulation a permis de cibler les lacunes au niveau des capacités d'intervention en matière de continuité des opérations découlant de l'incident de contamination et de trouver des solutions possibles en vue de combler les lacunes cernées.

Les activités ainsi menées se sont révélées instructives pour tous les partenaires ayant participé à l'étude. Les résultats obtenus à l'aide de la méthodologie employée et les résultats de l'étude ont fourni des indications. En effet, ils ont donné un aperçu des lacunes et des solutions possibles. Le Centre peut collaborer avec Industrie Canada pour combler les lacunes. La première étape de la méthodologie consistait à schématiser le processus au moyen du cadre d'architecture du département de la Défense (États-Unis) pour cerner les acteurs de l'intervention, les liens, les dépendances et les lignes de communications à la lumière du scénario retenu. Les vues architecturales ont repéré des couloirs pour diverses activités et actions menées par les acteurs qui participent à l'intervention. Afin de confirmer le cadre, on a procédé à une simulation d'intervention en temps réel axée sur les tâches sur les lieux d'une infrastructure essentielle de télécommunications. On a recouru aux services des intervenants en cas de déversement de matières dangereuses pour simuler la maintenance de routine dans un environnement contaminé.

On a réussi à cibler les lacunes au niveau des capacités pendant toute la durée de la simulation et on les a pris en note en vue d'effectuer des analyses postérieures. Le succès de la simulation est largement attribuable au fait qu'elle ait porté sur les tâches de l'utilisateur, assurant du coup des conditions réalistes tout au long de la simulation et contexte approprié pour analyser les lacunes validées. On a rédigé un résumé des constatations et on a remis au propriétaire de l'infrastructure des télécommunications une description détaillée des améliorations pouvant être apportées aux capacités.

Le PTSP utilisera la méthodologie appliquée à l'évaluation des capacités liées à l'infrastructure essentielle de télécommunications pour mener ses prochaines analyses des capacités fondées sur la simulation auprès d'autres intervenants et partenaires dans le domaine de la sécurité publique et de la gestion des urgences. La réussite de la simulation axée sur l'utilisateur permet de valider l'efficacité de la méthodologie à définir les capacités et le processus actuels en matière d'intervention, tout en ciblant des domaines à améliorer. Les autres simulations effectuées dans le cadre du PTSP s'appuieront vraisemblablement sur la méthodologie susmentionnée et se conformeront aux autres règlements établis par le gouvernement du Canada.

Table of contents

List of Figures and Tables

This page intentionally left blank.

Introduction

This report provides an overview of the Telecommunications Critical Infrastructure Case Study performed by Defence Research & Development Canada's (DRDC) Public Security Technical Program (PSTP)[1]. Using the PSTP's Telecommunications Critical Infrastructure Study as a case study, this report communicates how the PSTP will leverage the study's approach to provide a re-usable analysis capability to other federal department's responsible for emergency management and public security.

This analysis capability supports the Department of Public Safety Canada (PSC) and builds a horizontal approach to science and technology (S&T) that leverages DRDC's traditional expertise and develops new areas of specialty. The approach discussed applies capability analysis, scenarios, simulation and human factors engineering to the critical infrastructure domain.

It is expected that this approach be extended in the next phase of work to integrate risk and threat assessment information, and the identification of S&T solutions to solve high priority capability gaps. The extension of this analysis will position PSTP to provide reach back to similar projects across the federal government and subsequently to provide guidance to forward looking science and technology solutions. This approach is useful for capability goals associated with emergency management and public security. These capability goals are reflected in the emergency management taxonomy and include: prepare, prevent, respond and recover with respect to all hazards.

The following sections will provide the background of the PSTP and an overview of the Telecommunications Critical Infrastructure Study. It will set the Telecommunications Critical Infrastructure Study as the case-study for this report. The discussion that follows will:

- Provide reference to the idea of the capability-based approach to public security Science and Technology (S&T) Research; and
- Outline a methodology for analyzing capability deficiencies to prevent, protect, respond to and recover from high consequence public security events.

Background

The PSTP was founded in 2006 and based on an agreement between the Department of National Defence (DND) and then Public Security and Emergency Preparedness Canada (PSEPC), now Public Safety Canada (PSC). The PSTP works under the leadership of PSC to provide direct S&T support to Public Safety objectives and the bi-lateral Security and Prosperity Partnership Agreement (SPP) between the federal government and the United States. In addition, the PSTP provides science and technology related expertise, advice and services to other government department's efforts in achieving their security related roles and responsibilities outlined in the Federal Emergency Response Plan. The PSTP anticipates providing further expertise and guidance on the role S&T can play in closing capability gaps related to Bill C-12 – the Act to provide for Emergency Management assented June 22, 2007.

[1] Telecommunications Critical Infrastructure Study conducted by Public Security Technical Program in support of Industry Canada and Private Sector Critical Infrastructure Owner. (March 2007).

As a program under DRDC's Centre for Security Sciences (CSS), the PSTP works in cooperation with other federal government departments and partners to identify and remedy capability gaps. The goal of PSTP initiatives is to identify and support science and technology that closes these gaps and improves existing response mechanisms for high-consequence public security events.

To date, the CSS has a mandate to support S&T related to CBRNE, Critical Infrastructure Protection (CIP), Surveillance, Intelligence and Interdiction (SI^2) and Emergency Management & Systems Integration (EMSI). The CSS has deep knowledge in threat and risk assessment and manages a portfolio focused on foresight. Under the CSS, the CRTI program focuses on the CBRNE domain while the PSTP works across the remaining areas. The CSS coordinates the federal public S&T Strategy and resulting S&T programs with a range of federal, provincial and territorial partners including academic and industrial networks. The Centre is responsible for reach-back into the federal S&T community, including funding studies, exercises and workshops for safety and security communities.

Purpose of the Case Study

The purpose of the case study was to inform stakeholders in the critical infrastructure and incident response organizations about the business continuity requirements and capability options associated with a CBRNE incident effecting the operations of a telecommunications critical infrastructure.

The objectives of the study were two-fold. First, to determine the applicability of a simulation based capability analysis methods in the evaluation of critical infrastructure vulnerabilities. Second, to identify the challenges associated with the existing response mechanisms in the maintenance of business continuity during a biological incident recovery effort at a telecommunications critical infrastructure location.

The response elements to be assessed in the study had a variety of functions, each with different purposes, properties, responsibilities and objectives. To address the operational and managerial independence of the scenario response requirements, the study used systems of systems thinking, as depicted in figure 1 below. It also leveraged the capability based Department of Defence Architecture Framework (DODAF) to clarify the response concept of operations involved in the scenario and adapted processes from Canadian Military Standard, Mil-Std 46855 for human factors engineering to conduct specific human-centred capability analysis as it related to the conduct of functions and tasks. The goal of the analysis and use of simulation was to assess the capability of the incident response architecture to execute mission, functions and tasks response organization(s) would be required to perform to maintain business continuity of the critical infrastructure. The effectiveness of the study in identifying gaps in capability has cast it as a benchmark for future studies.

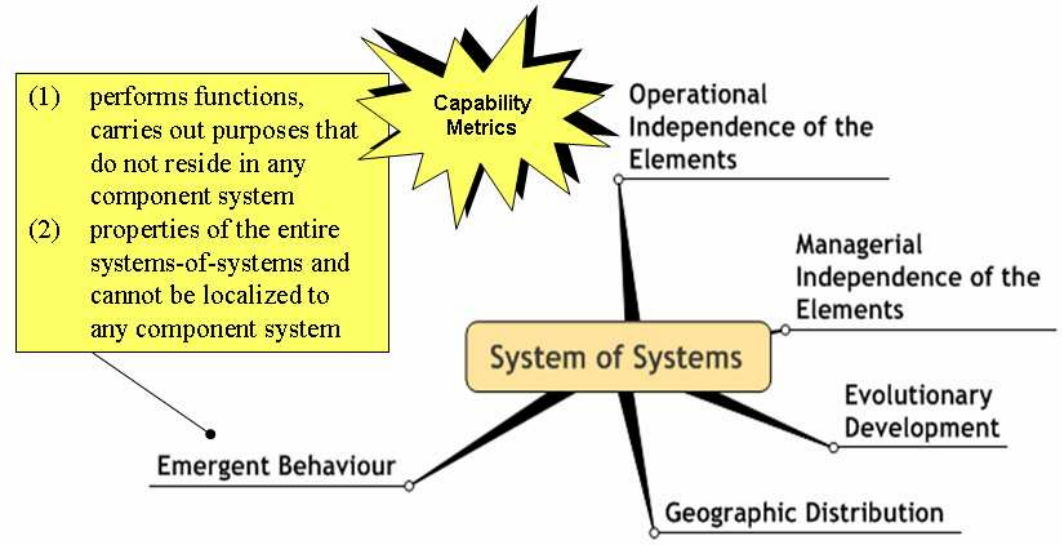

Figure 1 System of System approach

The Study

In 2007, the PSTP[2] led an exercise that conducted a simulation based capability analysis. The goal of the exercise and analysis was to test the response capability after a theoretical CBRN contamination event on a telecommunications critical infrastructure. The objective of the analysis was to determine capability gaps (if any) to ensuring business continuity after such an event.

The study was conducted in co-operation with Industry Canada[3] and a telecommunications critical infrastructure owner. The exercise was designed to provide specific guidance to Industry Canada and to inform the telecommunications community in general. Results were made available to the Canadian Telecommunications Emergency Preparedness Association (CTEPA).

The study itself provides the background of the initiative and describes the approach applied to gather information and conduct the analysis. It highlights key elements of the scenario[4] that was exercised and describes the organizational roles involved in the current incident response concept of operations.[5] The concept of operations was modeled using an operational architecture view (OV-6c) leveraged from the US. Department of Defence Architecture Framework (DoDAF). This model helped to clarify and communicate to the critical infrastructure owner, the roles of each agency responsible for a portion of the emergency response required by the scenario.

The study required the team to identify technology critical to ensuring emergency telecommunications business continuity. Considerations for selecting which technology were informal and fell across the common systems of systems taxonomy of people, process and technology. Considerations for selecting the technology included:

- likelihood of failure;
- likelihood of repair;
- location of technology (e.g. various floors, in the building, accessed only from a ladder);
- physical conditions where the technology was located (e.g. rooms with natural light, rooms no natural light, technology located in proximity to dangerous materials etc)
- variety of technology types (e.g. switches, wiring, cards);

---

[2] The PSTP is a Program under the DRDC's Centre for Security Sciences (CSS). Other programs under CSS include the CRTI.

[3] Public Security Canada, through the Federal Emergency Response Plan, delegates responsibility for emergency telecommunications to Industry Canada. As such, Industry Canada is the federal department partner responsible to ensure critical infrastructure protection [CIP] of Telecommunications infrastructure..

[4] The scenarios were identified by Industry Canada and the critical infrastructure owner. They were co-developed by all study partners in conjunction with the critical infrastructure owner. They are based on executive perception of threats to this infrastructure. In the future it is expected that the PSTP, in conjunction with public security partners, will have the capability and capacity to provide threat and risk assessment information to help determine the scenarios.

[5] The concept of operations included in the study is for the province in which the scenario was exercised. It is important to note that incident response concepts of operations vary between province and territories and potentially from municipality to municipality with the same province or territory.

- knowledge and skill requirements for repair or replacement of technology (e.g. simple to complex tasks, level of technical knowledge and/or training required);
- time required for repair or replacement (e.g. likely duration for completion of typical repair or replacement tasks on cross section of technologies); and
- availability of replacement parts (e.g. some replacement parts or entire replacement units may be kept on site while others may require advance notice to be provided from other locations).

The study then focused on the capability goals of Respond and Recover – goals that are relevant to ensuring business continuity for emergency telecommunications. The key functions required to achieve these goals were:

1. Repair Technology
2. Replace Technology

The exercise conducted a live simulation of repair and/or replacement functions and their related tasks. The exercise was conducted with the participation of Environment Canada who provided a HAZMAT response specialist, with full equipment, to simulate conducting repair and replacement tasks within the simulated conditions of a scenario.[6] The HAZMAT responder conducted appropriate repair and replacement activities for each technology. The analysis captured specific tasks and assessed the response capability to conduct these capability goals. Qualitative metrics were captured for all tasks and included:

- duration of the task,
- access and clearance requirement,
- dexterity,
- visual requirements,
- room layout,
- environmental conditions, and
- other considerations.

The study used the scenario-based approach to document the process and outcomes of the capability-based human factors analysis conducted during the simulation. Finally, the study provides recommendations and options for future consideration to the emergency response lead and the critical infrastructure owner. Findings included capability gaps in the following areas:

- Human Factors;
- Doctrine and Operations;
- Emergency Response & Command and Control;
- Communications; and
- Training and Exercises.

Three future capability options were identified and discussed for further investigation. These capability options were:

1. Identify private HAZMAT First Responder organisation(s) that are able to provide assistance,
2. Develop an in-house HAZMAT First Responder team, and
3. Utilize HAZMAT/Merit teams that have been developed at Telecommunication Organizations in the United States.

In addition to performing a capability analysis, stakeholders of the study were interested in identifying future capability options – some associated with capability options outlined above. While the

[6] Environment Canada, the response organization who would actually assist in the response architecture of the scenario, based on the exercise location (Quebec).

development of capability options is typically a phase of capability based planning that occurs after capability assessment[7] this step can be linked to capability assessment. This study investigated the option of ensuring business continuity for emergency telecommunications using the support of contracted organizations outside of the current response architecture.[8] This involved researching and compiling potential CBRNE response capabilities available within Canada, and internationally. This investigation also identified private and public organizations that provide training related to CBRN threats and/or associated technology.

[7] Technical Cooperation Program, Joint Systems and Analysis Group, Technical Panel 3, *Guide to Capability Based Planning*, *Fig-1, Generic Process Chart of Capability Based Planning*.

[8] Current response architecture and business continuity plans from the telecommunications organizations relies on the capacity of government response organizations to respond to a multi-event

Methodology: Simulation-Based Capability Analysis

The following paragraphs highlight the process used by the PSTP in the simulation based capability analysis for the telecommunications domain. The process outlines the use of the operational architecture modeling, building realistic scenarios to provide user-centric solutions, and through simulation - delivering quantifiable measures of improvement in stakeholder capability.

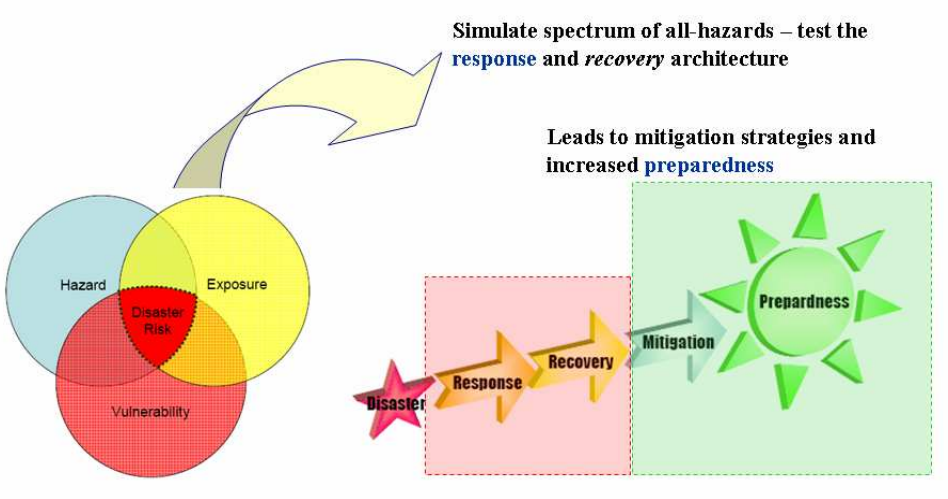

Figure 2: Simulation to test response, recovery and preparedness

The PSTP applied a standardized capability assessment methodology to identify S&T solutions to critical telecommunications infrastructure deficiencies. Future projects should follow this methodology, allowing for modifications where appropriate.

1 The use of architecture modeling principles and structures allow for a timeline of events and depicts deficiencies through the visualization of the steps required to mobilize an effective response. The purpose of modeling is to manage the complexity of the simulation environment in the initial analysis stage. Modeling views represented each step involved in the response to a contamination of a critical telecommunications facility with a biological agent. Using a standardized architecture modeling technique allows for the application of a common lexicon to defining the problem and helps manage complexity.

2 The definition of the threat ensures the simulation plan to be scenario-driven, providing maximum realism for an accurate assessment of capability deficiency. To develop new, relevant capabilities the simulation needs to represent gaps as realistic as possible.

3 The tailoring of the simulation in a user-centric manner delivers maximum value to the stakeholders and government partners.

4 The use of a simulation-based approach identifies capability gaps. Simulating the steps in the architectural model allows staff from the core response team and stakeholders to critically evaluate the relationship between actors at each step in the response. Evaluating current capabilities is critical to defining where gaps exist.

5 The application of metrics measures the current state and any improvement in capability delivered after the study. Improvement cannot be a simple statement: it must be proven quantitatively. Improved capabilities are compared to potential solutions using quantitative visualization tools. These tools clearly present what aspects of current capabilities are deficient, driving the focused

improvement of capabilities in specific areas: the comparison of 'as is' capabilities to future concepts, through decomposition.

The critical telecommunication infrastructure study established the Centre's simulation-based, capability analysis technical framework. This framework leverages DRDC's Capability Engineering to identify capability gaps with the intent of remedying them. The methodology and associated tools that support the PSTP technical framework were adapted to fit the context, scope, time and budget requirements of the study. The diagrams below are examples of required activities specific to the telecommunications critical infrastructure owner in identifying their capability deficiencies in response to a crisis affecting business continuity. The diagrams are not meant as templates for future projects, but as indication of the application of a simulation-based technical framework for the critical telecommunications infrastructure project. Figure denotes the plan, as per the PSTP technical framework; and Figure denotes the framework tailored for the telecommunications simulated scenario. Processes 3.0 and 4.0 of the PSTP technical framework can be reversed in order to denote the identification of 'to be' functional requirements thus changing how capability gaps are defined in light of more specific requirements. Defining the 'to be' functional requirements can be understood as a roadmap, directing how capability is defined, and subsequently how gaps are defined. Activity 1.1 can be considered as the business model, defining how parts of the organization interact.

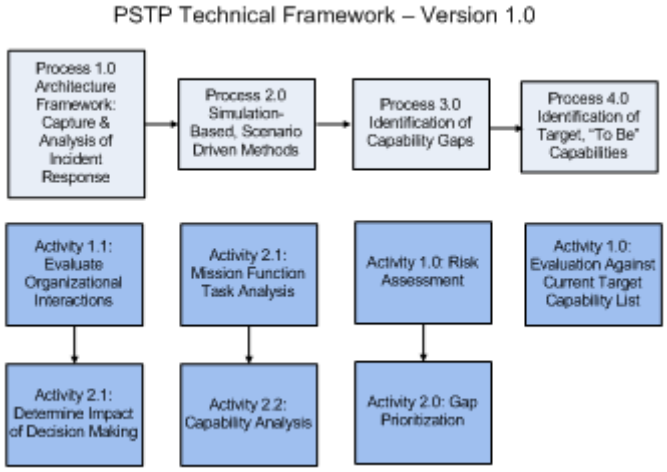

Figure 3: PSTP Technical Framework – v1.0.

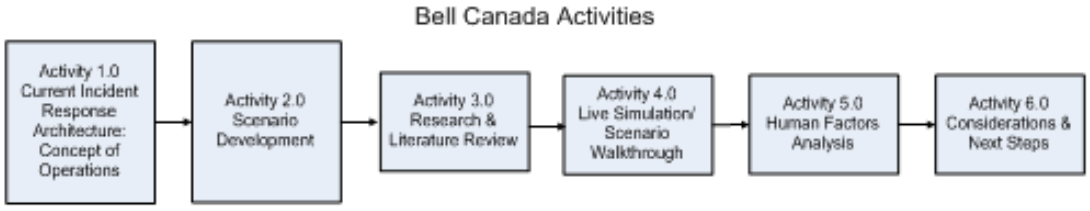

Figure 4: Bell Canada Activities

Operational Architecture Modeling

The Centre will begin its analysis using a standardized operational architecture modeling system appropriate to a project. Operational architecture modeling will identify specific capability areas that require simulation. The application of architecture modeling will build a concise analysis of capability interdependencies and linkages across all levels of command. It is the start-point for building a realistic, user-driven simulation to provide effective solutions. Visually displaying the division of activities comprising an event allows for focused analysis of where capability deficiency exists at a precise point in the overall system, and for analysis into the specific systems deficiency within the larger system of response. In applying the 'system-of-systems' approach, the Centre and stakeholders will identify specific capabilities that are driving deficiency. A listing of useful operational architecture methodologies is included in the references section of this document.

Scenario-Driven Approach

The way the scenario is defined provides context and scope to the study and resulting analysis. The scenario describes the requirements for any response and recovery operation. Requirements can be refined throughout the project as necessary to provide maximum realism. The more realistic a scenario, the more value can be translated to S&T research to remedy gaps. The parameters of the scenario will be based on the outputs from the architectural modeling diagram. A scenario is necessary to inform the initiation and context of the incident response. The scenario is based on known information about threat vectors for the threat selected in the scenario to replicate a real-life situation as closely as possible.

User-Centric

The purpose of the work of the Centre is to produce S&T solutions for its stakeholders and partners. Those solutions will only be useful if they serve the ends of the user. Simulations and scenarios are thus driven by the needs of the user, and their requirements for S&T solutions to capability deficiencies. The measures necessary to remedy capability gaps will be tailored specifically to the needs of the user, from the architectural modeling diagram to the application of metrics at the end.

Simulation Based Approach

To confirm the architectural modeling accurately reflects the response process, a simulation is necessary. Analyzing each step in the process of response and recovery to a high-consequence public security event produces applicable outcomes. The simulation based approach seeks to identify each step along to way, to assess any gaps in capability that inhibits first responders' action to critical events.

Simulations are test cases, seeking to identify specific capability deficiencies addressing a type of event and/or venue. Simulations will test response to the specific threat the stakeholder is concerned with (fire, explosives attack, chemical weapons attack, etc) and where possible, the simulation will take place at the site of the critical infrastructure to develop capabilities specifically for the target in question. If conducting a simulation at the target in question is not possible, simulation can be conducted in a synthetic environment. To better understand the challenges of each role, a simulation based analysis will be performed based on the critical tasks required to effectively respond to a high consequence public security event.

Simulating a high-consequence event permits the actors responding to a real-life scenario to test the interoperability of their existing systems, and the compatibility of the standard operating procedures

used by each. Simulation sponsored by the Centre will address only high-consequence events of national importance. Matters of purely regional or provincial impact remain the responsibility of the actors in the jurisdiction facing the incident. Simulation provides an excellent opportunity to identify where capability gaps exist prior to an event, rather than identifying gaps after a blow to Canadian public security.

Application of Metrics

All S&T solutions will improve a stakeholders' existing capability: success will be measured by applying metrics to the improvement in capability. For example, science clusters will likely measure improvement in terms of the number of people a new technology can protect from radiation or the capability to defend against more virulent strains of a disease, while a community of practice may define improvement as new capability to detect radio signals from further away than before, and with greater clarity.

A capability cannot simply be declared 'better': it must be proven. The metrics analysis will follow a similar format to the categories outlined in the operational architectural modeling overview to identify exactly where improvement is required, and to what level capability current exists. For ease of understanding and dissemination, the statement of metrics should include a visualization output, clearly showing how a prospective capability is an improvement over its predecessor. Generation of metrics to measure capability is useful to clearly identify capability improvements. Equally useful is a statement of priority, giving greater weight to improvement in a specific capability area, such as cost, detection range or persistence for example, as per the user's requirements. A clear depiction of improvement is valuable to provide clear options to stakeholders, and an explanation of the implication of each option. Quantifiable, measurable success is the responsibility of every government department as per the Results Management Accountability Framework (RMAF) guidelines maintained by the Treasury Board Secretariat (TBS).

Results

This section outlines how the steps performed in the study were applied during the critical telecommunication infrastructure project. Section 3 provided an overview of steps to be used for future projects, while this section describes the actual application of the steps in Section 3 in a successful project that identified capability gaps in the existing response mechanism to a high-consequence public security event.

Current Capability

For the critical telecommunication infrastructure project the operational architectural model selected was the Department of Defense (US) Architectural Framework (DODAF). During this stage of the exercise information was collected to provide an understanding of the existing response procedures and capabilities from both the responder organization and infrastructure owner. The output of this step was an operational level trace that identified the sequence of events during response to a high consequence public security event, and the actors involved. It identified the flow of information during a response, and developed an understanding of how the actors involved interacted. Figure is the trace of the first responder process to the biological contamination event at the critical telecommunication infrastructure facility.

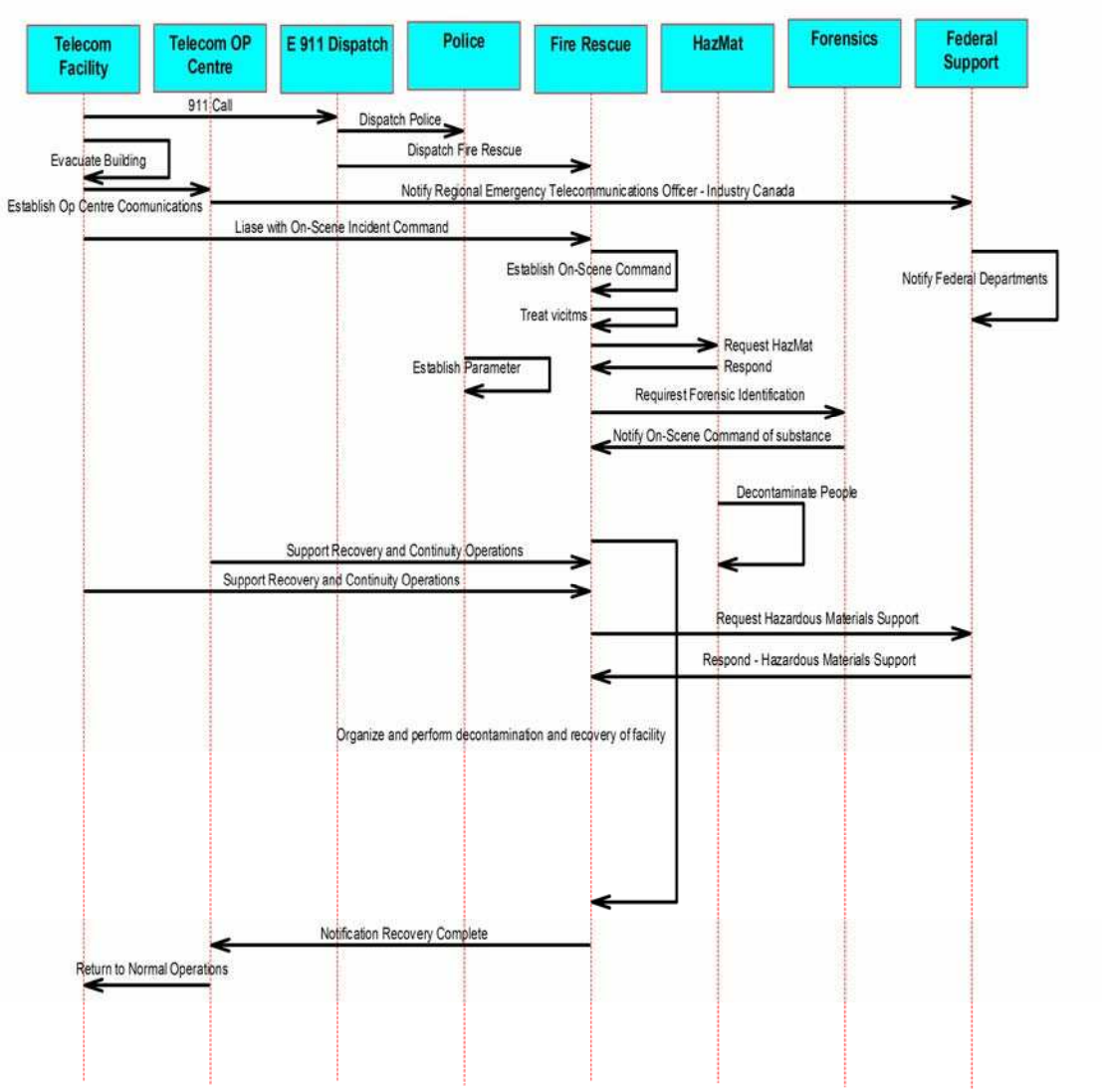

Figure 5: DODAF Event Trace (OV-6c).

Current Incident Response Capability Gaps

The capability gap in this case was the identification of two very different skills, the conducting of activities in a biologically contaminated area and the maintenance of complex telecommunications equipment, both required to affect business continuity during a biological attack on the CI.. The core staff and the stakeholders agreed, after examining the operational architecture modeling, the scenario presented was not something the critical telecommunication infrastructure was adequately prepared to respond to. With the identification of the key critical capability gap work could begin on the assessment of options to close the gap. This step is crucial to delivering applicable results. Finding out during a

real-life crisis is too late to be taking stock of capability gaps. The scenario considered known gaps and suspected gaps to test deficiency. The study outlines the estimated timeline of the response and the actors involved on site, the gaps tested and the expected output at this stage.

The critical telecommunications infrastructure study's capability improvement section provided a 'considerations' column to show the shortcoming of each available option. The considerations range from the willingness of external partners to cooperate in capability development, to labour union regulations regarding outsourcing capability from telecommunications technicians, to adding the telecommunications repair capability to trained HAZMAT responders. This is important because it provided the infrastructure owner with a list of options, and the consequences and potential obstacles associated with each option. The study did not elaborate on the specific costs associated with each option, though the considerations are sufficiently specific that each option so that subsequent analysis can consider budgetary factors.

Figure 6: HAZMAT responder during live simulation of simulated anthrax attack at a CO, attempting to perform CIP-Telecoms Business Continuity plan tasks

Following the definition of options it was determined that a live exercise should be conducted to test the overall effectiveness of HAZMAT personnel within CI facilities. It should also be noted that the exercise was conducted as realistically as possible with communications being simulated using a net-enabled technology that would link the first responder with technical experts to provide direction to the responder in conducting complex maintenance tasks. Communications on the first responder experience during the exercise were captured throughout the simulation using video feeds. A debrief after each task and sub task included discussion on the level of difficulty of each task. A representation of the results of the simulation's task/difficulty table is provided in Table 1. The level of difficulty was assessed and measured based on qualitative comments from the HAZMAT first responder and the subjective observation of human factors subject matter experts observing the task performance.

Task / Time	Level of Difficulty and/or Risk			
	1	2	3	4
Task 1: HVAC System Shut-Off (8 minutes)				
1.1. Walk from 1st Floor to HVAC Room			✓	
1.2. Identify HVAC unit	✓			
1.3. Climb up metal ladder	✓			
1.4. Pull down handle to open control panel	✓			
1.5. Pull lever to shut-off HVAC fans	✓			
Task 2: Card Replacement (15 minutes)				
2.1. Locate room			✓	
2.2. Locate blue or brown cabinets that contain replacement cards		✓		
2.3. Open cabinet		✓		
2.4. Locate card		✓		
2.5. Remove card from packaging			✓	
2.6. Find location for card replacement		✓		
2.7. Insert card			✓	
Task 3: Frame Repair/Addition (Max. 18 minutes)				
3.1. Locate frame		✓		
3.2. Locate blue and white wire reels	✓			
3.3. Grasp wires		✓		
3.4. Identify “right” side of frame		✓		
3.5. Locate box		✓		
3.6. Open box			✓	
3.7. Place wire in box at appropriate location			✓	
3.8. Obtain tool		✓		
3.9. Assemble wire in box using tool			✓	
Task 4: Tool Manipulation – Wire Cutting and Splicing (Not assessed)				
4.1. Cut Wire		✓		
4.2. Splice Wire			✓	
Task 5: Battery Repair (10 minutes)				
5.1. Locate basement			✓	
5.2. Enter room		✓		
5.3. Locate battery	✓			
5.4. Tap on battery to view whether bubbles are visible			✓	
Task 6: DMS Repair - Replace Fuse (Not assessed)				
6.1. Enter DMS room	✓			
6.2. Repair Fuse				✓

Table 1: Table of data related to the performance of necessary tasks to maintain the Critical Infrastructure. The level of difficulty 1, 2, 3 or 4 was documented using the following framework: 1 = Easy to perform / low risk, 2 = Moderate difficulty / moderate risk , 3 = Very difficult / high level of risk , 4 = Not possible under simulated exercise conditions.

The simulation exercise clearly illustrated where in the response process capability gaps existed. The critical infrastructure owner was presented a list of options to improve capabilities. The study provided

options ranging from outsourcing HAZMAT response to a critical telecommunications infrastructure event, to developing an in-house response capability.

The scenario was tailored to test the capability gaps in the existing response mechanism, identified in Figure 5: DODAF Event Trace (OV-6c). The capability gap in this case was a non-telecommunications trained HAZMAT responder called on to perform telecommunications repair tasks. The Centre staff and the stakeholder agreed after examining the operational architecture modeling the scenario presented was not something the critical telecommunication infrastructure was adequately prepared to respond to. This step is crucial to delivering applicable results. Finding out during a real-life crisis is too late to be taking stock of capability gaps. The scenario considered known gaps and suspected gaps to test deficiency. The study outlines the estimated timeline of the response and the actors involved on site, the gaps tested and the expected output at this stage.

Findings and Future Considerations

The results of the study addressed deficiencies in target capabilities identified in the operational architecture model, and those discovered during the course of the simulation. Prioritization of the gaps was guided by the severity of the consequences of an event, applied through the consolidated risk assessment. Those gaps noted most critical were addressed by the Centre in the study.

Once identified and prioritized gaps were further divided into functional categories. The purpose was to determine exactly where in the process the deficiency existed, and what further S&T research was required to help fix the deficiency. The following is a list of functional categories of capability gaps from the telecommunications study:

- Human Factors;
- Emergency Response & Command and Control;
- Communications;
- Situational Awareness; and
- Training and Exercises.

Human factors, for example, examined capability limitations with respect the responder's ability to act on the problem. Included were improper tools to complete tasks, and audio/video communication relay deficiencies. Command & Control pertained to communications overload, as all actors attempt to contact the on-scene commander simultaneously.

Capability Improvement Options

The simulation clearly illustrated where in the response process capability gaps existed. Bell Canada was presented a list of options to improve capabilities. The study provided options ranging from outsourcing HAZMAT response to a critical telecommunications infrastructure event, to developing an in-house response capability.

The nature of S&T research a stakeholder requires to remedy a capability gap is different depending on what target capabilities are required. Figure below shows the different stages of S&T development at which a stakeholder may find themselves. This chart shows the 'width' of the capability gap, or how much S&T research is required in developing the necessary capabilities. The columns on the far right indicate that the further along S&T research goes the more expensive it becomes, and the less risk tolerant.

BROAD TERMINOLOGY	Technology Readiness Level (TRL)	DESCRIPTION	Level of Risk Tolerance	Relative Cost
Basic Research	1	Basic Principals observed and reported	High	Low
	2	Technology Concept and/or application formulated through analytical studies		
Applied Research/ Research to prove feasibility	3	Analytical and experimental critical function and/or characteristic proof of concept		
	4	Concept, Process, Component and/or subsystem validation in a laboratory environment		
Experimental or Technology Development	5	Concept, Process, Component and/or subsystem validation in a relevant environment		
Demonstration and Validation/ Engineering feasibility	6	Concept, Process, System/subsystem model or prototype demonstration in a relevant, high fidelity environment		
	7	Concept, Process, or System prototype demonstration in an operational environment		
Engineering and manufacturing Development	8	Actual concept, process, or system completed and qualified through test and demonstration		
System Test & Operations/ Operational Systems Development	9	Actual concept, process or system proven through successful mission operations (operational test and evaluation).	Low	High

Figure 7: Science & Technology Readiness Level (S&TRL)

Figure 7 shows what type of research occurs at each S&TRL. The first stage of S&T research available is the proof of concept phase, or Research & Technology development phase (R&TD). Next is technology demonstration, with user involvement to verify the research will serve their desired target capabilities. Lastly is the technology acquisition phase, where the required technology for capability gap remedy is ready for commercialization and field application by first responders. The output for this section is a document outlining capability options based on urgency, and what level of S&T research is required to develop the necessary target capabilities based loosely on the guidelines in figures 4 and 5.

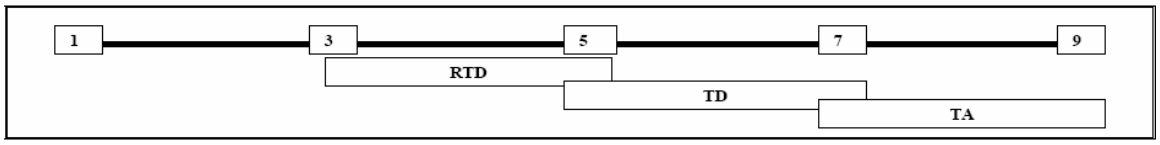

Figure 8: Linear Representation of Technological Evolution

These diagrams reinforce the concept that the wider a capability gap a user experiences, the more time, effort and resources will be required to remedy it.

Measured Results

The critical telecommunications infrastructure study provided a ‘considerations’ column to show the shortcoming of each available capability improvement option. The considerations range from the willingness of external partners to cooperate in capability development, to labour union regulations regarding outsourcing capability from Bell Canada technicians, to adding the telecommunications repair capability to trained HAZMAT responders. This is important because it provided Bell Canada with a list of options available, and the consequences and potential obstacles associated with each option. The study did not elaborate on the specific costs associated with each option, though the considerations are sufficiently specific that each option could be costed as required.

Conclusion

The capability analysis methodology defined through the PSTP Technical Framework will serve as the framework for future simulations carried out by the Centre. By applying a consistent framework the Centre creates a predictable process with clear steps for making progress toward enhancing target capabilities.

This methodology provides a clear sequence of steps, and an output at each step that feeds into the next. Using recognizable operational architectural modeling analytical tools allows stakeholders to produce concise outputs, ensuring clarity in the process. Conducting a realistic simulation, focused on the user's needs ensures the final assessment of capability options will operate from metric data that most closely reflects a real-life response to a high-consequence public security event. The capability analysis methodology is a process to clearly identify specifically where in the high-consequence public security response framework capability deficiencies exist and where the Centre can apply S&T solutions to remedy those gaps, and will be applied to future projects of the Centre.

Special thanks to Frederick Gauthier, Emergency Officer, Environmental Emergency Branch, Environment Canada, Quebec Region, for contributing expertise and participating as the HAZMAT responder for the live simulation exercise for this project.

References

Department of Defence Architectural Framework – Version 1.5; *Volume 1 – Definitions and Guidelines.* http://jitc.fhu.disa.mil/jitc_dri/pdfs/dodaf_v1v1.pdf. Published by the United States Department of Defense

Department of Defence Architectural Framework – Version 1.5; *Volume 2– Product Descriptions.* http://jitc.fhu.disa.mil/jitc_dri/pdfs/dodaf_v1v2.pdf. Published by the United States Department of Defense

Department of Defence Architectural Framework – Version 1.5; *Volume 3 – Architecture Data Description* http://jitc.fhu.disa.mil/jitc_dri/pdfs/dodaf_v1deskbook.pdf. Published by the United States Department of Defense

The MOD Architecture Framework – Version 1.1. http://www.modaf.org.uk/. Crown Corporation 2004-2007

List of symbols/abbreviations/acronyms/initialisms

CBRNE	Chemical, Biological, Radiological, Nuclear and Explosives
CIP	Critical Infrastructure Protection
CSS	Centre for Security Science
D&I	Disruption & Interdiction
DND	Department of National Defence
DODAF	Department of Defense (US) Architectural Framework
DRDC	Defence Research & Development Canada
EMSI	Emergency Management & Systems Integration
HAZMAT	Hazardous Materials
PSTP	Public Security Technical Program
PSC	Public Safety Canada
S&T	Science & Technology
S&TRL	Science & Technology Readiness Level
R&TD	Research & Technology Development
RMAF	Results Management Accountability Framework
TBS	Treasury Board Secretariat

This page intentionally left blank.

DOCUMENT CONTROL DATA

(Security classification of title, body of abstract and indexing annotation must be entered when the overall document is classified)

1. ORIGINATOR	2. SECURITY CLASSIFICATION
DRDC- Centre for Security Science- Public Safety Technical Program	(Overall security classification of the document including special warning terms if applicable.) UNCLASSIFIED

3. TITLE (The complete document title as indicated on the title page. Its classification should be indicated by the appropriate abbreviation (S, C or U) in parentheses after the title.)

Capability analysis framework: an approach for conducting simulation-based exercises with public security partners and stakeholders.

4. AUTHORS (last name, followed by initials – ranks, titles, etc. not to be used)

Vallerand, A, Osgoode, K., DeJager, C.

5. DATE OF PUBLICATION	6a. NO. OF PAGES	6b. NO. OF REFS
December 2007	(Total containing information, including Annexes, Appendices, etc.) 19	(Total cited in document.) 4

7. DESCRIPTIVE NOTES (The category of the document, e.g. technical report, technical note or memorandum. If appropriate, enter the type of report, e.g. interim, progress, summary, annual or final. Give the inclusive dates when a specific reporting period is covered.)

Technical Memorandum

8. SPONSORING ACTIVITY (The name of the department project office or laboratory sponsoring the research and development – include address.)

9a. PROJECT OR GRANT NO. (If appropriate, the applicable research and development project or grant number under which the document was written. Please specify whether project or grant.)	9b. CONTRACT NO. (If appropriate, the applicable number under which the document was written.)
10a. ORIGINATOR'S DOCUMENT NUMBER (The official document number by which the document is identified by the originating activity. This number must be unique to this document.) DRDC Centre for Security Science TM 2007-002	10b. OTHER DOCUMENT NO(s). (Any other numbers which may be assigned this document either by the originator or by the sponsor.)

11. DOCUMENT AVAILABILITY (Any limitations on further dissemination of the document, other than those imposed by security classification.)
Unclassified- Unlimited

12. DOCUMENT ANNOUNCEMENT (Any limitation to the bibliographic announcement of this document. This will normally correspond to the Document Availability (11). However, where further distribution (beyond the audience specified in (11) is possible, a wider announcement audience may be selected.))

13. ABSTRACT

This report is written for government departments and other stakeholders, who may desire science and technology (S&T) support in ensuring a horizontal approach to emergency management and public security across the government of Canada. This approach is applicable to an all hazards approach to public safety and relevant to communities with interest in CBRNE protection, Critical Infrastructure Protection (CIP), Surveillance, Intelligence and Interdiction (SI2), Emergency Management & Systems Integration (EMSI) and finally, Risk and Threat Assessment domains.

The report serves as an overview of the approach and activities conducted with stakeholders who seek to engage in S&T research in cooperation with Defence Research & Development Canada's (DRDC) Centre for Security Science and the Public Security Technical Program (PSTP). It provide an overview of the PSTP Capability Analysis process and outlines how the PSTP may use exercises to engage in capability based analyses and simulation. The report communicates how the PSTP used certain views of the Department of Defence Architecture Framework (DoDAF) to map the incident concept of operations (the actors and organizations) for a scenario that represented a high-consequence public security event.

The report documents how the PSTP conducted human centered capability analysis to identify where capability gaps exist in a response mechanism. The data obtained from using this methodology revealed a clear sequence of steps, and an output at each step that feeds into the next. Using recognizable operational architectural modeling analytical tools allowed stakeholders to produce concise outputs, ensuring clarity in the process. Conducting a realistic simulation, focused on the user's needs ensures the final assessment of capability options will operate from metric data that most closely reflects a real-life response to a high-consequence public security event. Finally, the report highlights the process the PSTP is exploring to determine critical capability gaps and draft alternative science and technology solutions that may be considered to remedy the gaps

14. KEYWORDS, DESCRIPTORS or IDENTIFIERS (Technically meaningful terms or short phrases that characterize a document and could be helpful in cataloguing the document. They should be selected so that no security classification is required. Identifiers, such as equipment model designation, trade name, military project code name, geographic location may also be included. If possible keywords should be selected from a published thesaurus, e.g. Thesaurus of Engineering and Scientific Terms (TEST) and that thesaurus identified. If it is not possible to select indexing terms which are Unclassified, the classification of each should be indicated as with the title.)

All- Hazards, Emergency Management, Public Safety. CBRNE, CIP, Risk Analysis