Defence Against Terrorism Case Study:

Simulation-Based Technical Framework to Address Changes in Capability Deficiency

Dr. Andrew L Vallerand
Director, Public Security Technical Program
Defence Research & Development Canada -Centre for Security Science,
344 Wellington St, Ottawa, ON, K1A-0K2,
Canada

Andrew.Vallerand@drdc-rddc.gc.ca

Ms Kristine Osgoode & Mr Chris DeJager
CAE Professional Services Inc
300-1135 Innovation Drive
Ottawa, ON K2K 3G7
Canada

Kristine.Osgoode@cae.com , Chris.DeJager@cae.com

ABSTRACT

The events of 9/11, subsequent anthrax incidents, as well as attacks in London, Spain and elsewhere, have brought increasing attention to the probability of NATO nations becoming a target of a terrorist threat. While telecommunications infrastructures may not be a specific target for attack, the consequences of a Chemical, Biological, Radiological, Nuclear, Explosive (CBRNE) incident on such Critical Infrastructures (CI) are debilitating, in part due to interdependencies with other CI. Improving CBRNE emergency preparedness, readiness and response capabilities is critical for both defence and security partners involved in domestic security. This report documents the results of a simulation based – framework for capability assessment of the emergency response Capability to a CBRNE threat at a Telecommunications CI location in Canada. The assessment reviewed the options for address a capability deficiency related to ensuring business continuity of a highly technical environment that would become a contained site after a biological attack, while still requiring maintenance tasks to be performed due to its CI nature. An agile analytical/technical framework methodology associated with Capability options was developed and tested. The assessment captured the as-is emergency response architecture which helped stakeholders understand their role in the incident and displayed the variety of emergency response organizations and levels of government would play a role during such an incident. A scenario was developed to provide context and a structure for identification and evaluation of CBRNE emergency response processes and procedures for CI. The simulation conducted for the study included live simulation with fully trained HAZMAT responders from a Government Department who performed a cross selection of tasks required for business continuity. The tasks were conducted in a Telecommunications central office that was hypothetically sealed off due to the simulated anthrax attack.

Vallerand, A.L.; Osgoode, K.; DeJager, C. (2007) Defence Against Terrorism Case Study: Simulation-Based Technical Framework to Address Changes in Capability Deficiency. In *Improving M&S Interoperability, Reuse and Efficiency in Support of Current and Future Forces* (pp. 9-1 – 9-10). Meeting Proceedings RTO-MP-MSG-056, Paper 9. Neuilly-sur-Seine, France: RTO. Available from: http://www.rto.nato.int.

Remote camera technology was used and evaluated during the scenario walkthrough. A mission, function, task, analysis and human factors evaluation of the overall space was applied. The results revealed that private sector owner of the CI should work with government to leverage existing knowledge that can be shared about existing threats, about risk assessment and about what is most likely to fail in various "emergency scenarios" related to physical security of CI protection. The camera technology proved to be key to providing detailed performance instructions, technical support and building directions to the first responders The data also revealed that special procedures may have to be developed for infrastructure components that are considered a high failure risk or infrastructure that is open to risk, particularly if business continuity is critical to prevent a cascade of interdependent failures. It was concluded that a simulation-based, scenario-driven and user-centric approach supports well many elements of a valid, credible and reproducible capability assessment including the analysis of an "as is" capability, the "target or to be" capability as well as the options to remediate capability gaps while ensuring business continuity of the critical infrastructure in support of security partners.

1.0 INTRODUCTION

DND [1], DoD, MoD, and DHS [2] are all organizations that have embraced a capability-based approach versus a technology-based approach for their respective mandates. In Canada, capability analysis supports the Department of Public Safety Canada (PSC) and Public Security partners in building a horizontal approach to science and technology (S&T) that leverages DRDC's traditional expertise in capability analysis. The technical framework involves a simulation-based, scenario-driven, user-centric capability analysis methodology. In the public security mission area of Critical Infrastructure Protection, there are 10 Sectors, as defined in the CI Protection Strategy [3]. The events of 9/11, subsequent anthrax incidents, as well as attacks in London, Spain and elsewhere, have brought increasing attention to the probability of NATO nations becoming a target of a terrorist threat. While telecommunications infrastructures may not be a specific target for attack, the consequences of a Chemical, Biological, Radiological, Nuclear, Explosive (CBRNE) incident on such Critical Infrastructures (CI) are debilitating in part due to interdependencies with other CI. Using the CI Protection - Telecommunications Community of Practice as a Sector eager to be considered as a case study, the report documents and communicates the technical framework approach used to provide an analysis of public security capability that can also be re-used with other federal departments with an emergency management and public security mandate.

This report provides the background of the PSTP technical framework approach and an overview of the Telecommunications CI community Case Study used to test it. It also:

- Provides a documented reference to the concept of the capability-based approach as the framework to bring Public Security Science and Technology (S&T) support to Public Security partners' capability gaps; and
- Outlines a methodology for analyzing capability deficiencies to prevent, protect, respond to and recover from high consequence public security events and to introduce capability metrics as an index of how to measure during S&T analysis and quantify success of S&T solutions to remediate the deficiencies.

2.0 METHODOLOGY

The following paragraphs describe the current capability assessment methodology. 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. Five key observations were made in the application of the methodology:

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 demonstrated 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 diagrams below are examples of required activities specific to the telecommunications CI 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 1 denotes the plan, as per the PSTP framework; and Figure 2 denotes the framework tailored for the telecommunications simulated scenario. Processes 3.0 and 4.0 of the PST framework can be reversed in order to denote the identification of ‘to be’ functional requirements, 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.

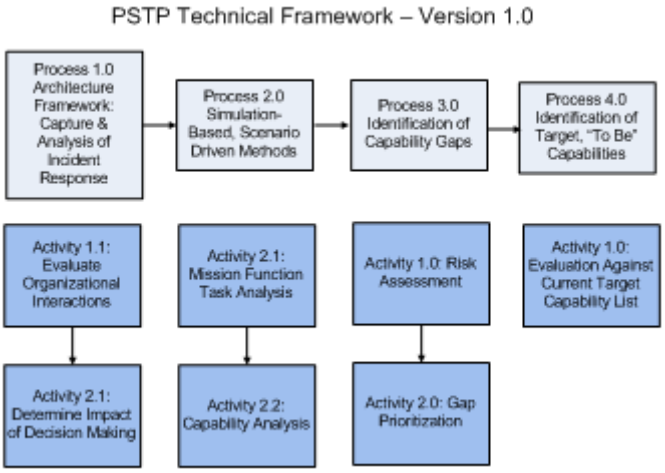

Figure 1: PSTP Technical Framework – v1.0.

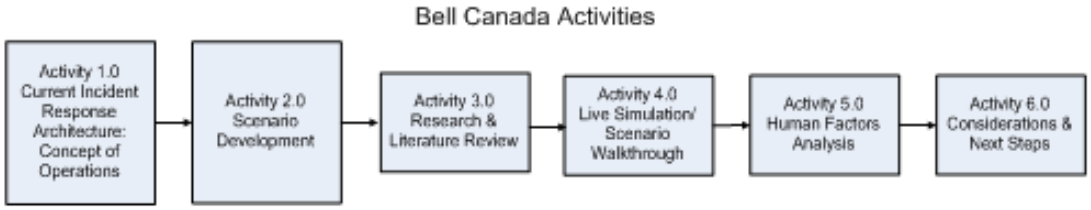

Figure 2: CIP Telecoms end user Activities

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 development of capability options is typically a phase of capability based planning that occurs after capability assessment [4] this step can be completed as part of a specific 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[1]. for the purpose of engaging expert resources in the conducting activities within biologically contaminated facilities. This involved researching and compiling potential CBRNE response capabilities available within Canada, and internationally and resulted in the identification of private and public organizations that provide training related to CBRNE threats and/or services and technology to conduct a response.

3.0 RESULTS

For the CI Telecommunication project the operational architectural model selected was the Department of Defense (US) Architectural Framework (DODAF) [5-8]. During this stage the exercise information was collected to provide an understanding of the existing response procedures and capabilities from both the emergency management response organizations and the infrastructure owner. The output of this step was an operational activity trace that identified the sequence of events during response to a high consequence public

[1] 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

security event, and the operational nodes involved. It identified the flow of information during a response, and developed an understanding of how the actors interacted during critical activities. Figure 3 is the trace of the first responder process to the biological contamination event at the CI Telecommunication facility.

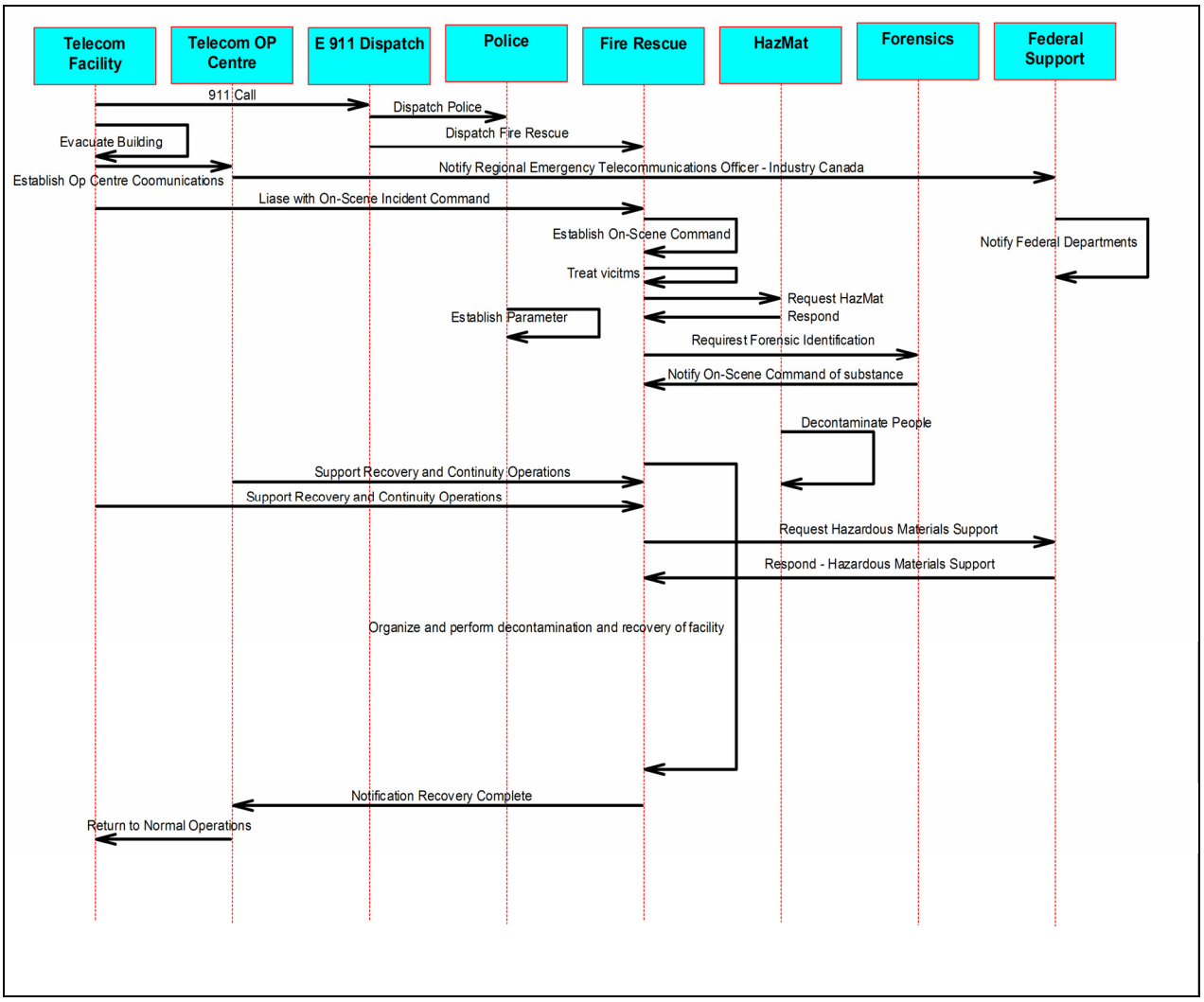

Figure 3: DODAF OV-6c event trace.

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 CI telecommunications 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 4: HAZMAT responder during live simulation exercise of simulated anthrax attack at a Critical Infrastructure, 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.

Table 1: Table of data related to the performance of necessary tasks to maintain the Critical Infrastructure in the simulation exercise. 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

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				✓

The simulation exercise clearly illustrated where in the response process capability gaps existed. The CI 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.

4.0 CONCLUSION

Improving CBRNE emergency preparedness, readiness and response capabilities is critical for both defence and security partners involved in domestic security. This report documents the results of a simulation based – framework for capability assessment of the emergency response Capability to a CBRNE attack at a Telecommunications CI location in Canada. The assessment reviewed the options for addressing a capability deficiency related to ensuring business continuity of a highly technical environment that would become a contained site after a biological attack, while still requiring maintenance tasks to be performed due to its CI nature. An agile analytical/technical framework methodology associated with Capability options was developed, documented in terms of architecture, scenario, simulation, tasks, and tested. First, the assessment captured the as-is emergency response architecture which helped stakeholders understand their role in the incident and displayed the variety of emergency response organizations and levels of government would play a role during such an incident. Secondly, a scenario was developed to provide context and a structure for identification and evaluation of CBRNE emergency response processes and procedures for CI. Third, the simulation conducted for the study included live simulation with fully trained and experienced HAZMAT responders from a Government Department who performed a cross selection of tasks required for business continuity. Fourth, the tasks were conducted in a Telecommunications central office that was hypothetically sealed off due to the simulated anthrax attack. Remote camera technology was used and evaluated during the scenario walkthrough. A mission, function, task analysis and human factors evaluation of the overall space was applied.

The results revealed that private sector owner of the CI should work with government to leverage existing knowledge that can be shared about existing threats, about risk assessment and about what is most likely to fail in various “emergency scenarios” related to physical security of CI protection. The camera technology proved to be key to providing detailed performance instructions, technical support and building directions to the first responders The data also revealed that special procedures may have to be developed for infrastructure components that are considered a high failure risk or infrastructure that is open to risk, particularly if business continuity if critical to prevent a cascade of interdependent failures. It was concluded that a simulation-based, scenario-driven and user-centric approach supports well many elements of a valid, credible and reproducible capability assessment including the analysis of an “as is” capability, the “target or to be” capability as well as the options to remediate capability gaps.

Special thanks to Mr 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.

5.0 REFERENCES

[1] Strategic Capability Based Planning for the Canadian Forces, http://www.vcds.forces.gc.ca/dgsp/pubs/dp_m/cbp_e.asp

[2] Caudle, S.L. Homeland Security Capability-based planning: lessons from defense community. http://www.hsaj.org/pages/volume1/issue2/pdfs/1.2.2.pdf , 2005

[3] Government of Canada Position paper on National Strategy for Critical Infrastructure protection. http://www.ps-sp.gc.ca/prg/em/nciap/NSCIP_e.pdf , 2004.

[4] The Technical Cooperation Program, Joint Systems and Analysis Group, Technical Panel 3, *Guide to Capability Based Planning*, TR-JSA-TP3-2-2004, http://www.mors.org/meetings/cbp/read/TP-3_CBP.pdf , 2004

[5] 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

[6] 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

[7] 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

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