OPERATIONS RESEARCH SUPPORT FOR CRITICAL INFRASTRUCTURE RESILIENCE IN THE PROVINCE OF BRITISH COLUMBIA

Lynne Genik
DRDC Centre for Security Science

Defence R&D Canada – Centre for Security Science
Scientific Literature
DRDC CSS SL 2012-016
October 2012

OPERATIONS RESEARCH SUPPORT FOR CRITICAL INFRASTRUCTURE RESILIENCE IN THE PROVINCE OF BRITISH COLUMBIA

Lynne Genik, MSc
Operations Research Scientist
DRDC Centre for Security Science
222 Nepean St, Ottawa, ON K1A0A2
1-613-943-2499, lynne.genik@drdc-rddc.gc.ca

This paper describes the Defence Research and Development Canada - Centre for Security Science (DRDC CSS) operations research (OR) support for critical infrastructure (CI) resilience in the Province of British Columbia (BC). DRDC has been providing scientific support for various aspects of CI resilience in BC since 2008, initially for the Vancouver 2010 Olympic and Paralympic Winter Games and, subsequently, for the development of Emergency Management British Columbia's (EMBC) provincial CI Assurance Program (CIAP). Guided by the NATO Code of Best Practice for C2 Assessment, a soft OR approach has been used to support the development of the CIAP. The DRDC focus has been on the first assessment stage of problem formulation and solution strategy, working in conjunction with EMBC and the multi-agency BC CI Steering Committee. Throughout the journey, a number of challenges have been identified related to governance, trust, information sharing, culture, assessment methodologies and resources. This paper outlines DRDC's goals, the CI problem (which can be characterized as a "wicked" problem), the OR approach, challenges, and progress to date, including pilot projects underway.

Key words: critical infrastructure (CI), resilience, wicked problem, NATO Code of Best Practice for C2 Assessment, soft operations research (OR), CI assessment, CI tools, emergency management, EMBC

INTRODUCTION

In 2008, the Defence Research and Development Canada – Centre for Security Science (DRDC CSS) established a project to provide scientific support for the 2010 Vancouver Olympic and Paralympic Winter Games (V2010). Under this project, DRDC provided critical infrastructure (CI) support to two groups: the Integrated Security Unit (ISU), the lead for Games security under the Royal Canadian Mounted Police (RCMP), and Integrated Public Safety (IPS), the lead for public safety under Emergency Management British Columbia (EMBC). The scientific support included a CI dependency analysis for the ISU, a separate CI dependency analysis for IPS and scientists at key operations centres during the Olympics. The author was seconded as scientific advisor to IPS from 2008-2010, working with both IPS and the ISU in CI and other domains, and was deployed to EMBC's South West Provincial Regional Emergency Operations Centre during the games.

The DRDC CI support to the ISU began in 2008 with a request to assist the ISU with the "CI problem" for the games. For the ISU, comprised mostly of police officers and responsible for venue and VIP security, CI was a new and daunting problem involving a large number of asset owners and assets. DRDC's analysis resulted in a list of prioritized CI assets for games security

and provided an objective, scientific basis for the ISU to set priorities for CI liaison, planning and preparations (1). In support of this project, IPS led a collection of data from asset owners using a modified version (2) of EMBC's Critical Infrastructure Rating Workbook that had been developed for freshet floods in 2007 (3). However, due to confidentiality concerns, asset owners insisted on a non-disclosure agreement (NDA) with the RCMP, which imposed security classifications that precluded EMBC's access to the data and analysis results, and required that the data be destroyed following the games. On behalf of the RCMP, DRDC analysed and stored data on more than 5000 assets from approximately 125 asset owners that was collected using the EMBC CI rating workbook. In the course of the analysis, DRDC identified a number of issues with the workbook (4), which had not been tested or validated. Since IPS could not access the collected CI data or analysis results, DRDC performed a subsequent analysis to identify the most critical CI service dependencies for the Emergency Management Response System for V2010 (5). Using the results of the analysis, the author coordinated efforts with the ISU and led outreach to priority asset owners on behalf of EMBC.

Under the V2010 project, DRDC had neither the mandate nor the resources to assist EMBC with addressing the issues identified with the CI rating workbook. However, following the games, DRDC and EMBC entered into a new two year project agreement for DRDC to provide scientific support to EMBC in two areas: risk assessment and CI. DRDC's goals for the project are:

- To support the client, EMBC, in achieving their objectives;
- To demonstrate the value of a scientific, structured approach for improving emergency management capabilities; and
- To develop approaches to the CI problem, including tools and assessment methodologies, that can be applied nationally.

This paper describes the CI problem, DRDC's approach to the problem, challenges and progress to date.

THE CI PROBLEM

Following the games, EMBC focused on the development of a province-wide Critical Infrastructure Assurance Program (CIAP). The purpose of the CIAP is to assist stakeholders to better prepare for, prevent and manage incidents, and to provide a framework, guidance and tools for enhancing the resilience of CI in British Columbia (BC) and reducing the risk from vulnerabilities (6). The objectives of the CIAP include enhancing public safety, developing sustainable partnerships and promoting inter-agency information sharing, promoting all hazards risk management, establishing and mapping contact information to enable situational awareness, and the provision of a common province-wide methodology for identifying and analysing CI (6). While the purpose and objectives of the program are reasonable, some are ambiguous (for example, enhancing resilience, enhancing public safety) and the means to achieve the end goal are not necessarily clear. What does it mean to enhance CI resilience and how can this be done? This is the overall problem that DRDC is trying to address in supporting the development of the CIAP. However, defining the problem and articulating goals for these types of socio-political problems can be very difficult, with good reason.

The concept of "wicked" problems was introduced by Rittel and Webber in 1973 (7) to distinguish them from problems in the natural sciences that are definable and may have solutions that can be found. They identified ten characteristics of wicked problems:

1. Wicked problems have no absolute formulation. The information required to understand the problem depends on the analyst's idea for solving it;
2. Wicked problems have no stopping rule. A better solution may be found with more effort. Work is often terminated because of a lack of time, money or patience, or when a "good enough" solution is found;
3. Solutions to wicked problems are good or bad, not true or false. Solutions may be evaluated and judged by many parties but none can confirm their correctness;
4. There is no test of a solution to a wicked problem. Any solution generates waves of additional consequences that may take time to understand;
5. Every trial solution counts since it leaves consequences that can't be undone;
6. There is no way to prove that all solutions have been identified;
7. Every wicked problem is essentially unique. Differences from other, similar problems are significantly important;
8. Every wicked problem can be thought of as a symptom of a higher-level problem that tends to be broader, more general, and more difficult to solve;
9. A discrepancy in a wicked problem can be explained in numerous ways. The analyst's world view is the strongest determinant in the choice of explanation;
10. Planners are liable for the consequences of the actions they generate since those actions can have a significant impact on others.

Enhancing CI resilience in BC can be characterized as a "wicked" problem: the problem is difficult to define; there are many interdependencies; there is no clear solution; it is socially and politically complex; while similar to the general problem of enhancing CI resilience elsewhere, it is unique to the BC environment (political, geographical, threat, governance, etc.). In addition, it has a very important characteristic of wicked problems as defined by the Australian Public Service Commission: "wicked problems hardly ever sit conveniently within the responsibility of one organization" (8). CI resilience is a multi-stakeholder problem involving government at all levels, the private sector, and individuals, with each stakeholder having their own perspective on the problem.

THE DRDC APPROACH

The DRDC team supporting this project is comprised of operational research (OR) scientists. The term "operations (or operational) research" emerged during the 1940s from the practice of attaching scientists to military operational groups to bring a scientific perspective to the planning and analysis of operations (9). Traditional OR was typically focused on physical systems, while command and control (C2) issues were regarded among the most challenging to analyse. According to Alberts and Hayes, "Command and Control applies to endeavours undertaken by collections of individuals and organizations of vastly different characteristics and sizes for many different purposes... Command and Control is about focusing the efforts of a number of entities (individuals and organizations) and resources, including information, toward the achievement of some task, objective or goal" (10). This is exactly the challenge faced by EMBC: to focus the

efforts of a number of stakeholders and resources toward the achievement of enhanced CI resilience. Thus, the CI problem can be regarded as a C2 problem.

The NATO Code of Best Practice (COBP) for C2 Assessment (11) (referred to hereafter as the COBP) was developed by the operational research and analysis (OR&A) community in response to a shift from the cold war to non-traditional operations (such as humanitarian assistance and disaster relief) coupled with advances in technology. The COBP represents more than a decade of work by the NATO OR&A community, is intended to assist the community in overcoming barriers for effective C2 analysis and has been adopted as a standard reference in the OR&A community. The approach is general enough that it can be applied to a wide range of C2 problems, such as requirements analysis, assessment of alternatives, research issues and support to operations. Therefore, the COBP has been used as a guide for this project.

The philosophy of the COBP is that the analysis of C2 involves a number of factors such as the consideration and integration of relevant stakeholders, command levels, and functions; robustness and security of information systems; human behavioural, cognitive, and physiological factors; and organizational issues. The COBP outlines four themes or stages of assessment:

1. Study dynamics, problem formulation, and solution strategy;
2. Essential elements of assessment – measures of merit, scenarios, human and organizational issues, data, and tools;
3. Risk and uncertainty;
4. Assessment products.

The DRDC work completed to date has focused heavily on the first stage, primarily on problem formulation and the development of solution strategies. Since the CI problem can be viewed as a "wicked" problem, the problem formulation is far from a trivial task. According to the COBP, "effective problem formulation is fundamental to the success of all analysis, but particularly in C2 assessment, because the problems are often ill-defined and complex, involving many dimensions and a rich context" (11). Given the importance of problem formulation as well as the associated challenges, it is an iterative process and will continue to evolve as the project progresses. In fact, it could be argued the effective problem formulation is *the* goal of the project.

OR, the application of scientific methods to the analysis of problems involving complex systems, can be further distinguished into "hard" (or classic) and "soft" OR, which rely on different perspectives of capturing and construing the perceived world. The crucial difference between the two approaches is that soft OR accepts that there are multiple, legitimate perspectives of the world. Soft OR assumes that the world can be explored using systems models, while hard OR assumes that the world contains systems that can be engineered (9). Note that the two approaches are not necessarily mutually exclusive; a soft OR approach to a problem enables multiple perspectives to be explored, and within that approach hard OR techniques can be applied where appropriate. That is essentially the approach taken by DRDC with the CIAP problem of enhancing CI resilience; that is, to explore stakeholder views using a soft OR approach, and apply hard OR, such as systems engineering and other modelling/analytical techniques, to specific aspects of the problem.

In particular, DRDC is working with the multi-stakeholder BC CI Steering Committee, chaired by EMBC, consisting of representatives from local, regional, provincial and federal government

and agencies and other stakeholders including private sector companies. For this project, the BC CI Steering Committee was consulted for feedback regarding the perceived value of the CI assessment work that had been completed and future tool development for the CIAP. As previously mentioned, the EMBC CI rating workbook had been used extensively for gathering data for V2010. The rating methodology required asset owners to assess the impact of damage to an asset across a number of factors (population, recovery cost and time, public confidence and own and other sector impact) to assign a score, and sum these scores for a final asset rating. However, through the analysis of data and scores for more than 5000 assets, DRDC identified issues with the methodology, including an inconsistent mathematical framework, correlated factors, a mix of factors making the driver of scores unclear, definition issues within factors and subjectivity in ratings (4). This led to unreliable results in the scoring. The workbook was used to a limited extent in other areas of the province, but the focus had been in the Lower Mainland of BC in preparation for the games. In order to understand the status of CI work in the various regions of the province and to solicit feedback on the development of a provincial CIAP, EMBC regional managers representing the six regions were consulted.

A preliminary CI literature review to determine best practices for CI and tools and approaches that may be applied in BC was also undertaken. This included a review of: the national CI strategies of Canada and other nations, such as the United States (US) and the United Kingdom (UK); the US National Incident Management System including the Target Capability List; academic research on CI interdependencies; risk management standards (ISO 31000); and practitioner recommendations for public-private partnerships.

The information collected from stakeholders and the literature review was analysed using the following approaches:

- Systems engineering principles (considering the CIAP as a system): to analyze the coherence, completeness and efficacy of requirements stated in the CIAP or elicited from stakeholders and to determine if the requirements were stated in a usable format for system/program development;
- Capability based planning concepts: to assess existing versus required capabilities to carry out tasks of the CIAP in terms of the required people, processes, material, and information;
- Principles for managing risk as defined in ISO 31000: to assess the CIAP against international standards for risk management.

As a result, the requirements for a cost effective, efficient CIAP, and gaps compared with existing initiatives, were identified. Given the complexity and the difficulty in defining the problem, it is not unexpected that finding the commonality among stakeholder goals and an agreed upon collective action plan is a major challenge and likely to be an ongoing, iterative process. More details on the methodology, requirements and gaps are contained in the DRDC client report for EMBC (12) and the DRDC technical memorandum describing the problem formulation and solution strategy (13).

CHALLENGES

As part of the problem formulation and understanding, a number of challenges were identified that need to be recognized in order for a successful project outcome. Several of the key challenges are outlined below (many of which are intertwined).

Governance

The responsibility to ensure CI resilience does not rest with one organization, but many. In Canada there are ten CI sectors: energy and utilities, food, finance, government, health, information and communications technology, manufacturing, safety, transportation, and water. CI assets are often owned and operated by private sector companies while government organizations are often responsible for public safety and security. Asset owners are expected to have conducted risk assessments and developed business continuity and emergency preparedness/response plans, governments are expected to provide necessary public safety and security support, and individuals are encouraged to be capable of sustaining themselves and their families for a minimum of 72 hours following an emergency incident (14). There is often regulatory control within a sector but, with the exception of the declaration of a state of emergency that grants special power to governments, the response to events is generally of a cooperative or collaborative nature. As noted by US Federal Emergency Management Agency (FEMA) Administrator Craig Fugate at the International Disaster Conference and Expo 2012, government may be able to direct the private sector in small emergency events, but this is not the case in large, complex events; it takes a team, involving the private sector (the providers of the majority of services), to manage an incident. This team philosophy is not necessarily held by all stakeholders since naturally most are concerned with their organization first.

Trust

Trust is an essential part of working relationships, particularly related to CI due to the multi-stakeholder governance structure. An initial challenge (perhaps in reality an ongoing challenge due to the number of stakeholders), was that of the DRDC team earning the trust of BC stakeholders, which generally requires establishing some degree of familiarity along with credibility. Although the author had been embedded with the IPS team in BC and had interactions with many CI stakeholders over an extended period, other DRDC team members did not have that advantage. Furthermore, DRDC's critique of the EMBC CI rating workbook was initially not well-received by some stakeholders, in particular those involved with its development. However, the support of EMBC has facilitated the development of trust with stakeholders (that is, there is some measure of trust by association) and over time trust has increased through regular interactions.

Information Sharing

Legislation varies from province to province; however, BC does not have legislation that: (a) compels CI asset owners/operators to share information for public safety/security purposes, or (b) that can protect information from access to information requests if they do share. As a result, because of concerns over proprietary information, in many cases CI information is only shared

during the response phase of an emergency incident, as deemed by the asset owner to be relevant to the situation. At the federal level there is some legislation under the federal Emergency Management Act that supports information sharing with federal organizations under specific circumstances, but again, information sharing is voluntary on behalf of the asset owners. In reality, trust based on personal relationships often plays a large part in information sharing.

Additionally, there are information sharing issues between security organizations and public safety organizations, which was apparent during V2010 (15). Security agencies generally work from a "need to know" philosophy, while public safety agencies generally work from a "need to share" philosophy. Security agencies may not appreciate the value of sharing information with the public safety community. Of course, there may be valid concerns about the appropriate handling of information. These can generally be managed by having policies, procedures and systems in place for the sharing and storage of information. However, a challenge at the provincial level is that BC does not have a protected or classified information network or undertake routine staff security clearances, which can prohibit protected/classified information sharing from federal departments and agencies, such as the RCMP.

DRDC has initiated several projects within the overarching DRDC-EMBC collaborative project, working directly with private sector companies and municipal organizations. In order to facilitate information sharing for these projects, DRDC is prepared to enter into confidentiality/non-disclosure agreements to protect sensitive information.

Culture

Each organization has their own culture and perspective. As a result, there are many cultural challenges, some of which have already been identified (for example, a "need to know" culture within security organizations that often hampers information sharing). According to Craig Fugate, FEMA Administrator, government is asking the wrong question of the private sector. Instead of asking: "What can the private sector do for government?", government officials should be asking: "What can government do to get the private sector up and running?" As more of the private sector is up and running, government is required to provide services for less of the community. This perspective represents a fundamental shift in thinking.

From a scientific perspective, scientists are trained to approach problems a certain way – that is, to state the problem, form a hypothesis, test the hypothesis, collect data, analyse data, and draw conclusions, and to subject that work to the scrutiny of others (through peer-review) for quality assurance. There seems to be an expectation of some members of the CI community to get things right the first time, which may be unrealistic. While it is important to understand the consequences of actions, the understanding and definition of the CI problem involves a learning process. People must be open to learning, willing to experiment to some degree, and accepting that things may not be perfect the first time around (but can be learned from and improved upon), in order to make progress.

Assessment Methodologies

Tested and validated CI assessment methodologies and tools are lacking in Canada. The tools that are available (for example, supported by provincial organizations) generally have not been scientifically validated, as was the case with the EMBC CI rating workbook (3). The use of such tools can lead to unreliable and/or incorrect results, which may have serious consequences. There is a desire for CI self assessment tools within the CI community, but generally for simple, straight-forward tools. However, CI is a complex problem and if tools are oversimplified, they may not provide any meaningful insight. The challenge is in creating a methodology/tool that is "simple enough" while providing value.

Multiple levels of assessment may be required depending on the scope of the problem under consideration; for example, a simple tool may be adequate to address the issues of one company, but as the problem is expanded to a sector, municipality, province, country, etc. different levels of assessment may be required. In addition, the use of more sophisticated CI assessment tools may require the facilitation of a knowledgeable analyst. The Risk Outlook CI interdependencies modelling tool developed under Emergency Management Ontario (for a province-wide CI interdependency assessment) is an example of such a tool (16).

Resources

In comparison with nations such as the US and the UK, Canada has very limited resources dedicated to CI. Moreover, Canada does not have governmental organizations with expertise (such as the UK's Centre for the Protection of National Infrastructure) and/or substantial funding (such as the US' Office of Critical Infrastructure Protection) to provide significant assessment and analysis support for CI (generally through providing expertise and/or funding, governments in return gain access to CI information). Therefore, stakeholders must be willing participants in cooperating and collaborating because they perceive a value in it.

Resources are limited at every level; for example, the DRDC team for the DRDC-EMBC collaborative project (including risk assessment) consists of 1.5 full time equivalent OR scientists, and an EMBC director and emergency management planning coordinator are responsible for the development of the CIAP, among many other responsibilities. The common message from the BC CI Steering Committee is that resources are scarce - individuals may be the sole CI representative in their organization and typically carry a heavy workload. Therefore, work undertaken as part this project must respect the limited resource availability in the CI community.

PROGRESS TO DATE

A significant amount of time has been spent on problem formulation, specifically on framing the problem and identifying requirements and gaps. This is likely to be an ongoing task as the project progresses for reasons specified previously (complexity, learning, etc.). Following the requirements and gaps analysis, DRDC proposed a number of projects that could be undertaken (by DRDC) to help minimize some of the gaps. The projects were reviewed with the BC CI Steering Committee and EMBC executive and planning staff; among the projects, work on CI assessment tools was identified as a priority. As a result, DRDC has commenced two pilot

projects, one with TransLink, Metro Vancouver's regional transportation authority, and one with the Corporation of Delta, a municipality in the Metro Vancouver region with a population of approximately 100,000. There is also a plan to do a third pilot project with a regional district comprised of rural local authorities. The purpose of the pilot projects is to understand the questions and decision processes of CI stakeholders, develop a tool (or tools) that support the decision processes and provide answers to priority CI questions, and generalize what is learned from the pilot projects in the development of tools that can be used by the broader CI community in Canada.

Several other projects are being pursued as well. A more extensive CI literature review will be undertaken by a university co-op student starting this spring. Funding has been requested to exploit work that was conducted under a DRDC technology investment fund project by the University of Ottawa on multi-agency collaboration and decision-making. The proposed project would conduct focus groups in BC to identify CI information sharing barriers, observe CI stakeholders during live events (if possible) or exercises to validate the collected information, develop and test interventions and propose guidelines in support of information sharing and collective decision-making. Pre-event information sharing is of particular interest given the current reluctance to share.

Aspects of CI resilience will likely be addressed in two DRDC contracts that are currently in the procurement process, one on the application of architecture frameworks to develop a community resilience framework, and another focusing on mission to task analysis for specific hazard scenarios within a community. These projects will be carried out by contractors under the supervision of DRDC, working with selected communities in BC. While the projects have more of a risk assessment focus, CI will be a consideration.

Finally, DRDC has developed a Major Events Security Framework (MESF), in collaboration with the RCMP, to establish a standard and comprehensive approach to major events security and safety planning. The MESF runs on open source wiki software and is a knowledge management repository including information on governance, policy, legislation, tools, best practices, lessons learned, business planning cycles, etc. It is possible to modify the MESF to provide a wiki-based, collaborative environment with a public safety focus, so that EMBC could develop a similar type of framework for CI resilience, for example. In fact, DRDC is currently undertaking a public safety adaptation of the tool for Public Safety Canada.

SUMMARY

This paper described the DRDC OR support for enhancing CI resilience in BC under the DRDC-EMBC collaborative project that commenced following V2010. The CI problem is characterized as a "wicked" problem, which means that defining the problem and solutions is a challenging and ongoing problem. DRDC has applied the first stage of the NATO COBP for C2 Assessment with a soft OR approach that considers the perspectives of multiple stakeholders, particularly those represented by the BC CI Steering Committee, along with hard OR techniques where appropriate. Stakeholders were interviewed, a literature review was performed, and the information was analysed using systems engineering, capability-based planning, and risk

management principles to identify requirements and gaps in the CIAP. Through the work of the project, a number of challenges have been identified, including working within the cooperative/collaborative multi-stakeholder governance environment, stakeholder trust, barriers to information sharing, cultural obstacles, insufficient assessment methodologies, and limited resources. DRDC is initiating a number of projects, including CI assessment pilot projects, an enhanced CI literature search, risk assessment contracts, adaptation of the MESF, and potentially multi-agency collaboration research to address some of the gaps areas. Given the "wicked" nature of the CI problem, this is a learning process for all stakeholders (including DRDC), and there are no quick solutions. The ultimate goal is shared awareness among the CI community and agreement on a way forward. While DRDC's work has been in support of BC, a goal of the project is to develop approaches, tools, and expertise for national benefit.

REFERENCES

(1) Simona Verga, Paul Chouinard and Darek Baingo, "The Critical Infrastructure Asset Ordination (CIAO) Model", DRDC CSS Technical Memorandum, DRDC CSS TM 2008-09, Confidential, 2008, 82 pages
(2) "Critical Infrastructure Identification & Rating Workbook: The 2010 Games Critical Infrastructure Initiative", EMBC, April 24, 2008 version 2, 48 pages
(3) "Critical Infrastructure Rating Workbook", Provincial Emergency Program, EMBC, May 2007 Freshet Pilot version 2, 37 pages
(4) Paul Chouinard, "Feedback on the JELC Data Collection Sheet", DRDC CSS MECSS Client Report, 3782-2008-33bd (PM MECSS), 13 May 2009
(5) Paul Chouinard, "Integrated Public Safety Urban Domain Critical Infrastructure Analysis", 8 Dec 2009, PowerPoint Presentation, 29 slides
(6) Miranda Myles and Heather Lyle, "Critical Infrastructure Assurance Program: Concept Paper", draft, Emergency Management British Columbia, September 2010
(7) Horst Rittel and Melvin Webber, "Dilemmas in a General Theory of Planning", *Policy Sciences* 4 (1973), p. 155-169
(8) "Tackling Wicked Problems: A Public Policy Perspective". Australian Public Service Commission, Commonwealth of Australia, 2007, 38 pages
(9) Peter Checkland and Sue Holwell, "'Classic' OR and "Soft" OR – An Asymmetric Complementarity", in *Systems Modelling; Theory and Practice*, Edited by Michael Pidd, John Wiley & Sons, 2004, pp. 45-60
(10) David S. Alberts and Richard E. Hayes, "Understanding Command and Control", DoD Command and Control Research Program, Library of Congress Cataloging-in-Publication Data, ISBN 1-893723-17-8, 2006, 255 pages
(11) "NATO Code of Best Practice for C2 Assessment", DoD Command and Control Research Program, Library of Congress Cataloging-in-Publication Data, ISBN 1-893723-09-7 (pbk), October 2002, 273 pages
(12) Paul Chouinard and Lynne Genik, "The Resiliency of BC's Critical Infrastructure: Requirements and Gaps Assessment and DRDC Options for Support", DRDC Letter Report to EMBC, September 2011, File 3700-1, 19 pages
(13) Lynne Genik and Paul Chouinard, "DRDC Support to Emergency Management British Columbia's (EMBC) Hazard Risk Vulnerability Analysis (HRVA) and Critical Infrastructure

(CI) Programs: Problem Formulation and Solution Strategy" DRDC CSS Technical Memorandum, DRDC CSS TM 2012-xx, 2012, to appear, 71 pages
(14) "Your Emergency Preparedness Guide. 72 Hours. Is Your Family Prepared?", Public Safety Canada, Her Majesty the Queen in Right of Canada, ISBN: 978-1-100-11290-9, 2009, 36 pages
(15) Lynne Genik and David Smith, "Command and Control Analysis of the South West Provincial Regional Emergency Operations Centre during Vancouver 2010", 16th International Command and Control Research and Technology Symposium (ICCRTS), Quebec City, June 2011, 22 pages
(16) Bruce Nelson and Phillip O'Neill, "Ontario Critical Infrastructure Assurance Program: Interdependencies Modelling Project Software Development Final Report", Emergency Management Ontario, Public Safety Canada, March 31, 2010

DOCUMENT CONTROL DATA

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

1. ORIGINATOR (The name and address of the organization preparing the document. Organizations for whom the document was prepared, e.g. Centre sponsoring a contractor's report, or tasking agency, are entered in section 8.)

Defence R&D Canada – CSS
22 Nepean St
Ottawa, Ontario K1A 0K2

2. SECURITY CLASSIFICATION (Overall security classification of the document including special warning terms if applicable.)

UNCLASSIFIED
(NON-CONTROLLED GOODS)
DMC A
REVIEW: GCEC June 2010

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.)

OPERATIONS RESEARCH SUPPORT FOR CRITICAL INFRASTRUCTURE RESILIENCE IN THE PROVINCE OF BRITISH COLUMBIA

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

Lynne Genik

5. DATE OF PUBLICATION (Month and year of publication of document.)	6a. NO. OF PAGES (Total containing information, including Annexes, Appendices, etc.)	6b. NO. OF REFS (Total cited in document.)
October 2012	11	

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.)

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

Defence R&D Canada – CSS
22 Nepean St
Ottawa, Ontario K1A 0K2

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.)	10b. OTHER DOCUMENT NO(s). (Any other numbers which may be assigned this document either by the originator or by the sponsor.)
DRDC CSS SL 2012-016	

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.))

Unlimited

13. ABSTRACT (A brief and factual summary of the document. It may also appear elsewhere in the body of the document itself. It is highly desirable
that the abstract of classified documents be unclassified. Each paragraph of the abstract shall begin with an indication of the security classification
of the information in the paragraph (unless the document itself is unclassified) represented as (S), (C), (R), or (U). It is not necessary to include
here abstracts in both official languages unless the text is bilingual.)

This paper describes the Defence Research and Development Canada - Centre for Security Science (DRDC CSS) operations research (OR) support for critical infrastructure (CI) resilience in the Province of British Columbia (BC). DRDC has been providing scientific support for various aspects of CI resilience in BC since 2008, initially for the Vancouver 2010 Olympic and Paralympic Winter Games and, subsequently, for the development of Emergency Management British Columbia's (EMBC) provincial CI Assurance Program (CIAP). Guided by the NATO Code of Best Practice for C2 Assessment, a soft OR approach has been used to support the development of the CIAP. The DRDC focus has been on the first assessment stage of problem formulation and solution strategy, working in conjunction with EMBC and the multi-agency BC CI Steering Committee. Throughout the journey, a number of challenges have been identified related to governance, trust, information sharing, culture, assessment methodologies and resources. This paper outlines DRDC's goals, the CI problem (which can be characterized as a "wicked" problem), the OR approach, challenges, and progress to date, including pilot projects underway.

Ce document décrit le soutien à la recherche opérationnelle (RO) du Centre des sciences pour la sécurité de Recherche et développement pour la défense Canada (RDDC CSS) pour la résilience des infrastructures essentielles en Colombie-Britannique (C.-B.). Depuis 2008, RDDC offre un soutien scientifique dans divers aspects de la résilience des infrastructures essentielles en C.-B., d'abord pour les Jeux olympiques et paralympiques d'hiver de 2012 à Vancouver, puis pour la mise sur pied du Programme national de fiabilité des infrastructures essentielles (PNFIE) de la gestion des urgences Colombie-Britannique (EMBC). Guidée par le Code des pratiques exemplaires d'évaluation du C2 de l'OTAN, une approche RO a été utilisée pour soutenir l'élaboration du PNFIE. RDDC a mis l'accent sur la première étape d'évaluation des stratégies de formulation et de résolution du problème, en collaboration avec l'EMBC et le comité directeur des infrastructures essentielles en C.-B. Un certain nombre de problèmes liés à la gouvernance, à la confiance, au partage de renseignements, à la culture, aux ressources et aux méthodes d'évaluation ont été identifiés au cours de cette période. Ce document donne un aperçu des objectifs de RDDC, du problème d'infrastructures essentielles (pouvant être qualifié de « pernicieux »), de l'approche RO et des progrès réalisés à ce jour, incluant les projets pilotes en cours.

14. KEYWORDS, DESCRIPTORS or IDENTIFIERS

critical infrastructure (CI), resilience; wicked problem; NATO Code of Best Practice for C2 Assessment; soft operations research (OR); CI assessment; CI tools; emergency management; EMBC