Defence Research and
Development Canada

Recherche et développement
pour la défense Canada

DEFENCE R&D DÉFENSE

MODELLING, SIMULATION AND ANALYSIS (MS&A): POTENT ENABLING TOOLS FOR PLANNING AND EXECUTING COMPLEX MAJOR NATIONAL EVENTS

Anthony Masys
DRDC Centre for Security Science

Andrew Vallerand
DRDC Centre for Security Science

Defence R&D Canada – Centre for Security Science

Canada

MODELLING, SIMULATION AND ANALYSIS (MS&A): POTENT ENABLING TOOLS FOR PLANNING AND EXECUTING COMPLEX MAJOR NATIONAL EVENTS

Anthony Masys
DRDC Centre for Security Science

Andrew Vallerand
DRDC Centre for Security Science

Defence R&D Canada – CSS

Anthony MASYS

Original signed by Anthony Masys

Anthony Masys

DRDC Centre for Security Science (CSS)

Approved by

Original signed by Paul Chouinard

Paul Chouinard

DRDC Centre for Security Science (CSS)

Approved for release by

Original signed by Dr. Mark Williamson

Dr, Mark Williamson

DRDC Centre for Security Science (CSS) DRP Chair

Abstract

Modelling, Simulation & Analysis (MS&A) are known as crucial, effective and efficient enablers of Defence Communities from Concept Development & Experimentation (CD&E) to Training. In Public Safety and Security in general and in particular in recent complex major national events such as the Vancouver 2010 Olympics, the impact of MS&A has been significant, though far less known. Drawing upon case studies, this report argues that MS&A is a potent enabling tool for Defence & Security Communities not only from CD&E to Training, but in all aspects of Capability, from Strategy/Policy to Capability Development, Capability Generation, Capability Employment and Network Enabled Capability (NEC). The methodologies by which MS&A became a crucial enabler to ensure safe and secure conduct of the Vancouver 2010 Olympics and G8/G20 Summits are highlighted in this report. Given the recurrent nature of complex major national events as well as the growing requirement to efficiently test and validate Emergency Management Plans and Business Continuity Plans, a persistent capability framework to support (National and International) Major Events security and safety planning and operations has been undertaken that includes a persistent and credible S&T and MS&A capability. This persistent capability is in many ways comparable with the DoD Information Analysis Centers (IACs; http://iac.dtic.mil/) and the DHS Simulation and Analysis Center (http://www.dhs.gov/xabout/structure/gc_1257535800821.shtm). MS&A products and lessons learned, in particular when they are leveraged in the Major Event Security Framework, could provide efficient analysis, insight and support to other Major Events including, London 2012 Olympics, 2015 Commonwealth Games in Toronto as well as the Cross-border Management of Emergencies, such as earthquakes, floods and forest fires. In conclusion, though at first brush the use of MS&A in Public Safety and Security does not seem to be as wide and deep and does not seem to be similarly "crowned" by large International distributed simulated training like in Defence, their valued-use was documented as clearly growing. This Report concludes that MS&A represent significant potent enabling tools that contribute significant value and impact as well as efficiency and effectiveness to Public Safety and Security in general and in particular to support safety and security at complex major national events. Decision makers seeking efficiency and effectiveness are thus encouraged to increasingly use or re-use Public Safety and Security M&S in their analyses.

Résumé

La modélisation, la simulation et l'analyse (MS & A) s'avèrent être un outil habilitant des milieux de la défense, connu pour son efficacité et sa nécessité dans l'élaboration et l'expérimentation de concepts (EEC) ainsi que dans l'instruction. Quoique moins connues, les répercussions de la MS & A sur la sécurité publique en général et lors d'événements complexes d'envergure nationale tels que les Jeux olympiques de 2010 à Vancouver sont importantes. Suite à une recherche factuelle, les auteurs de ce rapport soutiennent que la MS & A est un outil habilitant utile aux communautés de la sécurité et de la défense, que ce soit pour l'EEC, l'instruction ou tout aspect de la capacité (stratégie, politiques, développement, production, emploi, opérations facilitées par réseaux [OFR]). Ils y énoncent les méthodologies qui ont fait du MS & A un élément essentiel pour la sécurité des Jeux olympiques de 2010 à Vancouver et des sommets du G8 et du G20. En raison du caractère récurrent des événements complexes d'envergure nationale et des besoins croissants d'évaluation et de validation des plans de gestion des mesures d'urgence et de continuité des opérations, une structure permanente a été mise sur pied afin de soutenir la planification et les opérations de sécurité lors d'événements d'envergure nationale et internationale. Cette structure comprend une capacité constante et fiable en matière de S & T et de MS & A. À plusieurs niveaux, cette capacité récurrente est comparable aux centres d'analyse de l'information du DoD (http://iac.dtic.mil/) ainsi qu'au centre d'analyse et de simulation du DHS (http://www.dhs.gov/xabout/structure/gc_1257535800821.shtm). Les résultats de la MS & A de même que les leçons retenues, surtout au niveau du cadre de sécurité des événements d'envergure, pourraient permettre une analyse, un aperçu et un appui efficaces lors d'autres événements tels que les Jeux olympiques de 2012 à Londres, les Jeux du Commonwealth de 2015 à Toronto et la gestion des cas d'urgence transfrontaliers (tremblements de terre, inondations, feux de forêt). Les auteurs de ce rapport ont conclu que la MS & A et sa grande utilité ont de la valeur et des effets sur : 1) la sécurité publique générale et spécifique et 2) l'appui à la sécurité lors d'événements complexes d'envergure nationale.

Executive summary

MODELLING, SIMULATION AND ANALYSIS (MS&A): POTENT ENABLING TOOLS FOR PLANNING AND EXCECUTING COMPLEX MAJOR NATIONAL EVENTS

Anthony Masys; Andrew Vallerand, DRDC CSS TM 2011-20; Defence R&D Canada – CSS.

Modelling, Simulation & Analysis (MS&A) are known as crucial, effective and efficient enablers of Defence Communities from Concept Development & Experimentation (CD&E) to Training. The impact of MS&A in Homeland Security in general and in particular "Major Events" such as the Olympics, has been significant. The management of the safety and security of Major Events, such as Vancouver 2010 Olympics (V2010) and G8/G20 Summits is a complex multidisciplinary, multi-jurisdictional issue that necessitates an integrated planning and response mechanism to ensure seamless operational management in the event that a safety and security issue would arise. Drawing upon the lessons learned from the Defence domain, MS&A is shown as a crucial enabler that supported the safe and secure conduct of the Vancouver 2010 Olympics and G8/G20 Summits. Further it is proposed that a persistent capability framework to support (National and International) Major Events includes a persistent and credible MS&A capability. The Lessons Learned from the above case studies and others, are well positioned to support other Major Events including, London 2012 Olympics and the 2015 Commonwealth Games in Toronto.

The case studies-based approach applied in the development of numerous multiple Technology Demonstration projects, the 'Guide to M&S for NATO NEC' and the lessons learned from the application of M&S in support of Vancouver 2010 Olympics and G8/G20 Summits demonstrates the enabling power of M&S and Analysis in both the safety and security domains and supports the argument for the establishment of a persistent S&T capability to support the public security environment. The application of MS&A within the safety, security and defence domains is thus demonstrated and supports the institutionalization of S&T contributions to safety and security planning and operations.

In conclusion, though at first brush the use of MS&A in Public Safety and Security does not seem to be as wide and deep and does not seem to be similarly "crowned" by large International distributed simulated training like in Defence, their valued-use was documented as clearly growing. This report concludes that MS&A represent significant potent enabling tools that contribute significant value and impact as well as efficiency and effectiveness to Public Security in general and in particular to support safety and security at complex major national events. Decision makers seeking efficiency and effectiveness are thus encouraged to increasingly use or re-use Public Safety and Security M&S in their analyses
.

Sommaire

MODÉLISATION, SIMULATION ET ANALYSE (MS & A) : OUTIL EFFICACE PERMETTANT LA PLANIFICATION ET LA RÉALISATION D'ÉVÉNEMENTS COMPLEXES D'ENVERGURE NATIONALE

Anthony Masys; Andrew Vallerand; DRDC CSS TM 2011-20; R & D pour la défense Canada – CSS; octobre 2011.

La modélisation, la simulation et l'analyse (MS & A) s'avèrent être un outil habilitant des milieux de la défense, connu pour son efficacité et sa nécessité dans l'élaboration et l'expérimentation de concepts (EEC) ainsi que dans l'instruction. La MS & A a eu de grandes répercussions sur la sécurité intérieure en général et lors d'événements d'envergure tels que les Jeux olympiques. La gestion de la sécurité lors d'événements comme Vancouver 2010 et les sommets du G8 et du G20 est un enjeu pluridisciplinaire et intergouvernemental complexe qui exige une planification intégrée et des moyens d'intervention pour une gestion opérationnelle en continu en cas d'incident de sécurité. Les leçons retenues dans le domaine de la défense ont permis de démontrer la nature essentielle de la MS & A en matière de sécurité lors de Vancouver 2010 et des sommets du G8 et du G20. Cette recherche factuelle met en évidence l'efficacité, la rentabilité et la nécessité de la MS & A en ce qui a trait à la sécurité intérieure. Il est suggéré qu'une structure permanente comprenant une capacité MS & A fiable et constante serve à appuyer les événements d'envergure nationale et internationale. Les leçons retenues lors des études de cas (susmentionnées et autres) permettront d'offrir un soutien lors de futurs événements d'envergure tels les Jeux olympiques de 2012 à Londres et les Jeux du Commonwealth de 2015 à Toronto.

L'approche factuelle adoptée pour l'élaboration de nombreux projets de plusieurs millions de dollars sur les démonstrations de technologies, ainsi que du « Guide de M & S pour le NEC de l'OTAN » et des leçons retenues lors de l'utilisation de la M & S en appui aux Jeux olympiques de 2010 de Vancouver et aux sommets du G8 et du G20, démontre le pouvoir habilitant de cet outil en matière de sécurité. Cette approche soutient également la mise en place d'une capacité en S & T pour assurer la sécurité intérieure.

Ce travail est d'une grande importance. Il démontre clairement l'application de la MS & A dans les domaines de la sécurité et de la défense et il soutient l'institutionnalisation des apports de la S & T en ce qui a trait à la planification et aux opérations de sécurité. Les auteurs de ce rapport concluent que la MS & A est un outil habilitant grandement efficace ayant de la valeur et des effets importants sur la sécurité lors d'événements complexes d'envergure nationale. Les résultats de cette étude ont permis d'établir des points d'intervention clés qui serviront à élaborer un **programme de résilience** faisant appel à la MS & A en tant que S & T qui s'imposent dans le domaine de la défense pour appuyer la sécurité.

List of figures

This page intentionally left blank

Table of Contents

Acknowledgements

1 Introduction

> **"Science used to be composed of
> two endeavours:
> Theory and Experiment.**
>
> **Now,
> it has a third component:
> Computer Simulation,
> which links the other two!"**
>
> *Dr. Rita Colwell, Director National Science Foundation,
> speaking to yhe National Press Club, April 29, 1999*

Globalization is a term that describes a process by which distinct national boundaries become increasingly blurred and regional economies, societies, and cultures become more integrated through global communications, transportation, trade and financial networks. Advanced communications and information technology has provided almost immediate awareness of events regardless of location which has in turn provided an ever increasing number of windows of opportunity to influence associated outcomes. Advances in transportation technologies have increased the reach, speed and volume of traffic exponentially to many parts of the world. International trade and financial networks have provided opportunities in the form of global markets for both goods and investment capital. The process of globalization through these increasingly pervasive networks has provided an increased number of windows of opportunity to exercise instruments of national or coalition influence (diplomatic, military, economic and social/cultural) to attempt to affect advantageous outcomes.

This system of growing global connections and interdependencies has also permitted the rapid transfer of technologies around the globe. Where new scientific breakthroughs and related technologies may have taken months or years to be heard of in distant parts of the world, through the global digital infrastructure they can now be available for study in seconds. The same detailed and rapid transmission is true for changes in social and cultural values, norms and beliefs. Some have referred to this aspect as the "McDonaldization" or "Americanization" of the world with "western" countries pushing their opinion over the digital infrastructure which has become so prevalent in these societies.

Yet with all this increased connectivity, the world is increasingly more polarized and continuously presents extremes in views, in weathers, in resources and in power. National economies instantaneously shift to buffer shocks in reaction to global political and economic upheavals. Events in the Middle East cause oil prices to jump everywhere. Stock markets dance in tandem. Currencies fluctuate in relation to each other fracturing into groups of winners and losers. So many diseases - Ebola, mad cow disease, AIDS, influenza, SARS - have been globalized due to the rapid movement of people and products across national boundaries and even continental divides. Differences in population, wealth, poverty, hunger, ideologies, cultures, values, war and violence in some parts of the world spill over and threaten entire regions and global stability.

Nowhere is this paradox of concurrent globalization and polarization more evident than in the area of international security and defence which produces a constant churn in the Defence, Security and Safety environment: We are all living in a complex adaptive international security system characterized by an environment populated by a great many agents conducting seemingly "independent" actions attempting to actively gain competitive advantage that at the same time produce interdependent consequences or effects which are quite difficult to effectively influence let alone manage or control. Whether related to IED or Cyber, we see an alarming rise of Asymmetric Threats that innovatively combine relatively simple technologies to create complex problems for our own defensive security capabilities. The threats often provide significant competitive advantage for short periods of time and because of the simplicity of the components, are easily modified and highly adaptive to change.

These types of problems can be characterized as "complex and adaptive" which do not lend themselves to well-bounded, linear problem-solving approaches, nor to the design of interventions based on historical and empirical evidence alone. These problems require approaches that acknowledge the challenges of complex adaptive systems and respond by facilitating collaboration across multiple domains and seek to discover interdependencies and emergent behaviour. In this sense uncertainty emerges as a key characteristic of the problem space. The ability of groups and organizations to appreciate and take action in relation to 'complex adaptive' problems often drive them to seek the benefits from Modelling, Simulation and Analysis as a potent enabling tool for investigation of the complex problem space associated with security threats.

Modeling and Simulation (M&S) has long been known as a potent analytic tool enabling Defence Communities to conduct effective Concept Development & Experimentation (CD&E) and Training, particularly in the Joint realm as the spheres of influence of land, sea, air and cyber increasingly overlap becoming increasingly interdependent. Explicitly linking modelling and simulation tools with the analytical process (MS&A) as a facilitator for decision-making, provides a potent methodology for gaining insights into problem spaces characterized by complexity and provides a viable means to reduce their

inherent uncertainty.   However, as with all powerful tools, M&S[1] must be used appropriately or the user risks an unfavorable outcome and so their weaknesses and strengths must be fully understood as well as how and when they should be properly applied. In a similar vein, there is an important distinction between "simulation for formal experiments" (using an hypothesis, an experimental design and statistical analysis of the quantitative data) and "simulation for knowledge generation" (small number of representative simulations, collecting sometimes qualitative data) and both bring value but differently.

Complex dynamic feedback can emerge within simulations stemming from the interdependencies that reside within and between individual entities in the model thereby leading to emergent behaviour. High complexity is the critical factor without which we could easily predict the outcomes of simple interactions. However, as a result of the high complexity, our internal mental modelling ability can easily become overwhelmed, and we may expect results that are simple (linear) extrapolations of observed behaviours rather than consider the possibility of emergent behaviour.

Although the application of M&S within the defence domain as an analytic tool for decision support across the entire capability lifecycle is well documented, the **impact of MS&A in Public Safety and Security in general and in particular in "Complex Major National Events" such as the 2010 Olympics, has not been thoroughly explored,** documented and exploited.   It will be argued in this paper that due to the asymmetric nature of new security threats, military and non-military threats are becoming more similar in their complexity; it follows that military and domestic civil responses are themselves becoming more similar in the complexity of the response by combining a

---

[1] A **model** is a physical, mathematical or otherwise logical representation of a system, entity, phenomenon or process that has been designed for a specific purpose.   The strength as well as the weakness of a model derives from the fact that they are simplified representations entities that intentionally exclude certain aspects of the real things they represent. Thus, models are abstractions that reduce the complexity of an entity to enable a better understanding of the specific aspects of interest and their impact. They must be constructed in such a way that all aspects of significance will be actively considered.

It is for this reason that there are often multiple models for any entity operating within an environment. The selection and use of a specific model must be based upon the aspect of the entity's behaviour under investigation as well as the level of aggregation of individual agents and /or their effects. For example, an aircraft may be represented by a complex high fidelity physical model that runs non-real time for engineering test and evaluation purposes or it can be represented by a lower fidelity performance model that runs in real-time for human-in-the-loop decision training. Similarly, aircraft can be modelled as individual entities, flights, sections, packages or even entire fleets of aircraft depending on the granularity required of the investigation. Care must be taken to ensure that the model selected is appropriate to meet the requirements of the user, a mismatch may provide what appear to be reasonable results but in fact are completely misleading.

A **simulation** is the manipulation of a model in such a way that it represents the expected behaviour over time. Simulations can be run real-time, near-real-time or non-real-time depending on the user's requirements and objectives for running the simulation as well as the number and complexity of the modelled entities in the system and the available processing power.

number of specialized capabilities together from potentially different source organizations.

It is therefore argued that MS&A is a potent enabling tool not only for Defence but also for Safety and Security Communities. This applies not only for CD&E and Training, but also across the entire Capability lifecycle from Strategy/Policy, to Capability Development, Generation and Employment including aspects related to Network Enabled Capabilities. Since many of the same attributes applicable to International Security and Defence planning and execution are equally applicable to Domestic Security and Public Safety relating to Complex Major National Events such as 2010 Olympics, then the evidence would support that MS&A is a crucial enabler for this community as well.

2   MS&A in support of Defence

2.1 Introduction

M&S has been used as an analytical tool for many years by scientists, engineers and economists to address a wide variety of complex technical issues. Defence has been able to benefit from many new developments in this technology that have significantly enhanced Defence Capability modernization/transformation across Naval, Land and Air Forces capabilities and these benefits were obtained by the use of Constructive M&S, Virtual M&S, as well as Live M&S[2].

Recent advances in computer processing, data capture, storage, retrieval and manipulation through distributed interactive networking as well as computer-generated imagery (visuals) employed in synthetic environments have literally transformed the way business in force development, material acquisition, as well as training and exercise supporting the delivery of Military Capabilities are conducted.

Simulation is increasingly used by the Canadian DND/CF to leverage existing capabilities and to focus future investments by supporting the following areas of activity:

  a. Concept development and experimentation;
  b. Capability requirements development, definition and capture;
  c. Equipment and subsystem specification;
  d. Developmental Test and Evaluation (DT&E);
  e. Operational Test and Evaluation (OT&E);
  f. Education and Training requirements and support;
  g. Operational mission rehearsal; and
  h. Optimizing platform and weapon system upgrades.

The cost-benefit analyses extracted from the published literature in these areas indicate that savings have been achieved through the structured and balanced employment of modern M&S practices and procedures. Many examples of cost and time savings

---

[2] **Constructive M&S** involves simulated people operating simulated systems. **Virtual M&S** involves real people operating simulated systems. Such simulations are often known as "Human-in-the-Loop" type of simulation as they inject a human into a central role by exercising motor control skills (e.g., flying an aircraft), decision making skills (e.g., committing people to action), or communication skills (e.g., as Communicating to Commander). Finally, **Live M&S** involves real people operating real systems, e.g. a pilot flying a jet in a simulated conflict. Prior to *computer-based* simulation, a **Table Top** *"paper-based"* **simulation** is sometimes used to get the scenario details and order of events right. At a Table Top effort, agencies sit around a table and step through a vignette, an emergency situation or the entire scenario and, verbally or in writing, respond to the scripted events as they occur.

(including Cost Avoided) realized by Canada and Canada's allies have been documented through hundreds of robust Case Studies, regarding the exploitation of MS&A (Vallerand et al, 2009; Vallerand et al, 2005).

In addition, recent case studies described below have revealed how MS&A has also been a crucial enabler across an entire Capability lifecycle. The next sections address how MS&A support Capability Development, Generation and Employment respectively.

2.2 MS&A for Strategy/Policy and Capability Development

Policies, like individual capabilities, are normally applied within a collective framework. The modelling of policies and policy frameworks has been used to identify conflicts, overlaps and gaps in the overall framework as well as a wide variety of supporting capabilities required for their collective implementation. The defence community has also started to use modelling and simulation to identify emerging technologies, potential technology applications, technology trends, social behaviours, social demands, business potential and measures of potential impact related to the required capabilities. Policy/Strategy modelling is also capable of identifying emerging research directions in the domain and providing a means to develop policy options and investigate their downrange implications. There are thus immense benefits in being able - *"To see the Finish before the Start[TM]*[3]*"* - i.e. the impact of policy/strategy before the Organization commits to it.

Application of such MS&A contributing to **Strategy/Policy and Capability Development** include such projects as:

- Robust Canadian Forces Defence Strategy (CFDS) Capability Based Planning supporting Defence Planning Procedures;

- Understanding and modelling the Human Dimension of the Comprehensive Approach.

- Identifying and modelling the benefits of Network Enabled Capabilities in a synthetic environment.

- Future weapon systems conceptualization and effectiveness assessments

- Predictive modeling of Adversarial Intent

- Physics-based MS&A to evaluate Arctic surveillance solutions and comparative analysis to determine their cost-effectiveness

---

[3] http://www.cae.com/en/military/_pdf/datasheet.project.management.pdf

- Test Bed to develop C2 processes for multi-agency domestic security missions
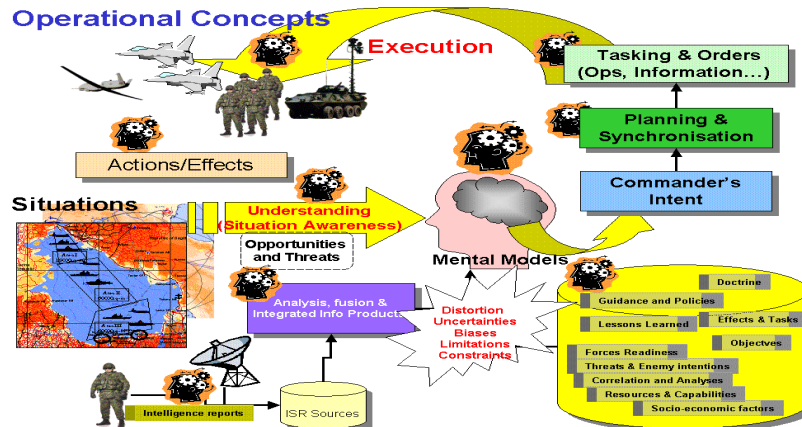
Figure 1 Joint Command Decision Support for the 21st Century (JCDS 21) Hales & Scipione, 2008

- Coalition Joint Fires Tech demo and M&S Test Bed

-
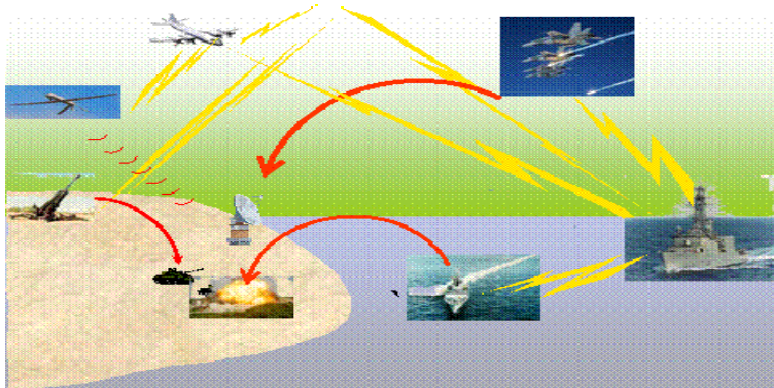
Figure 2 Joint Fire Support Technology Demonstration, Abdellaoui et al, 2008

- Evaluation of new distributed sensor architectures;
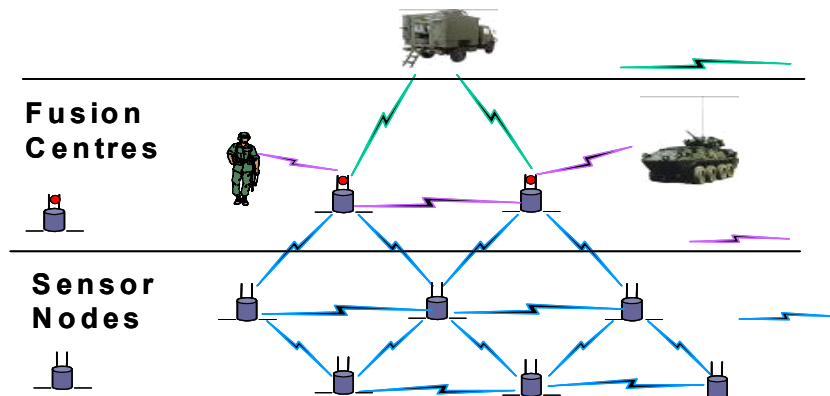
Figure 3 SASNet TDP Project 12PK: Self Healing Autonomous Sensor Network TDP , Li, L. 2008

These examples represent a subset chosen from DRDC Technology Demonstration Projects (TDP).

2.3 M&S for Capability Generation and Capability Employment:

Capability Generation is the means by which Material or Equipment Capability is made into useable Military Capability by the combined activity of all Defence Lines of activities. Capability Generation is a critical part of ensuring that the User expectations are met and achieving the benefits identified are within an individual project and programs. Ultimately, this serves to meet the required level of Capability Integration. Once integrated into a useable Capability that gets employed in Operations, we have achieved Capability Employment. It is very exciting to analyze the set of projects that have benefited from the use of M&S for Capability Generation and Capability Employment. These include the following:

- Synthetic environment to develop, test and verify electro-optic countermeasures

- Deployable simulation system with ultra-high resolution for mission planning and rehearsal
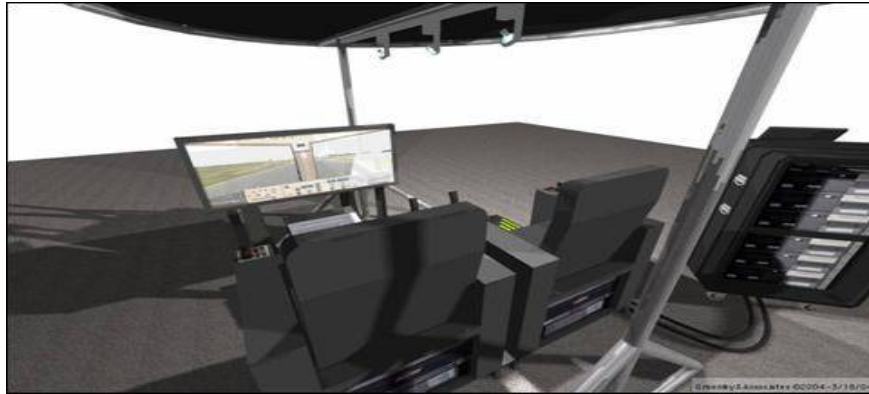
Figure 4 Project 16bg Advanced Deployable Day/Night Simulation; Niall, 2009

- Synthetic Environment for rapid scenario analysis for maritime air littoral operations (MALO TDP Project; Hassaine, Vallerand & Hubbard, 2005);
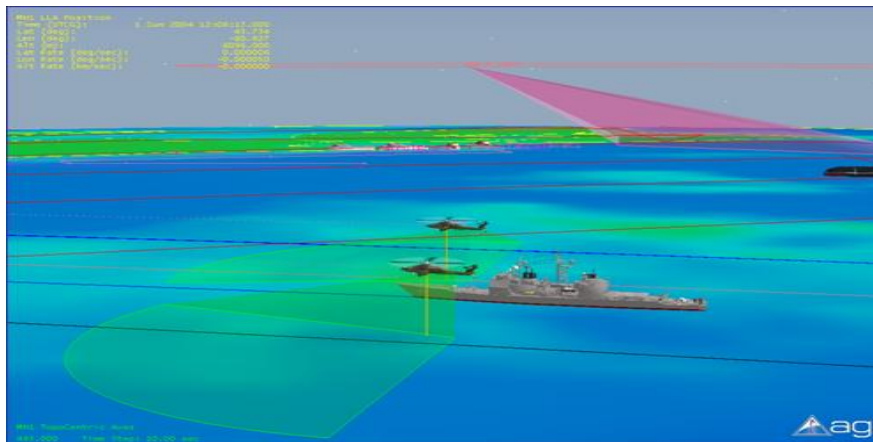
Figure 5 ScreenCapture of MALO using STK^{TM} under license by AGI Inc for MALO TDP

- M&S enabled tools to defeat the IED System (McGroder, 2011)

- Process models to assess and improve the Vancouver 2010 Olympic Integrated Security Unit design and staffing of Vehicle Screening Areas and Pedestrian Screening Areas (see later in this manuscript)

- Geographic Information System Capability to support CF recruitment strategies (Tongco and Vapos 2011)

2.4 M&S in Support of Defence Capabilities that are Network-Enabled Capability (NEC)

M&S is well known in NATO as well as in NATO NEC[4]. NEC can be described as the realization of a robust, globally interconnected, network environment (including infrastructure, systems, processes, and people) in which data are shared in a timely and seamless way among users, applications, and platforms, during all phases of civil and military cooperation (CIMIC) and war-fighting efforts. By securely interconnecting people and systems, independent of time or location, net-centric capabilities enable substantially improved military situational awareness and significantly shortened decision-making cycles.

Through several dozens NATO Case Studies, M&S has been demonstrated as significantly enhancing the desirable advancement of Network Enabled Capabilities (NEC) across: Through-Life Management, Concept Development & Experimentation (CD&E), Acquisition, Test & Evaluation, Logistics, Human Dimension of NEC, Training/Exercises, Agile Operations.
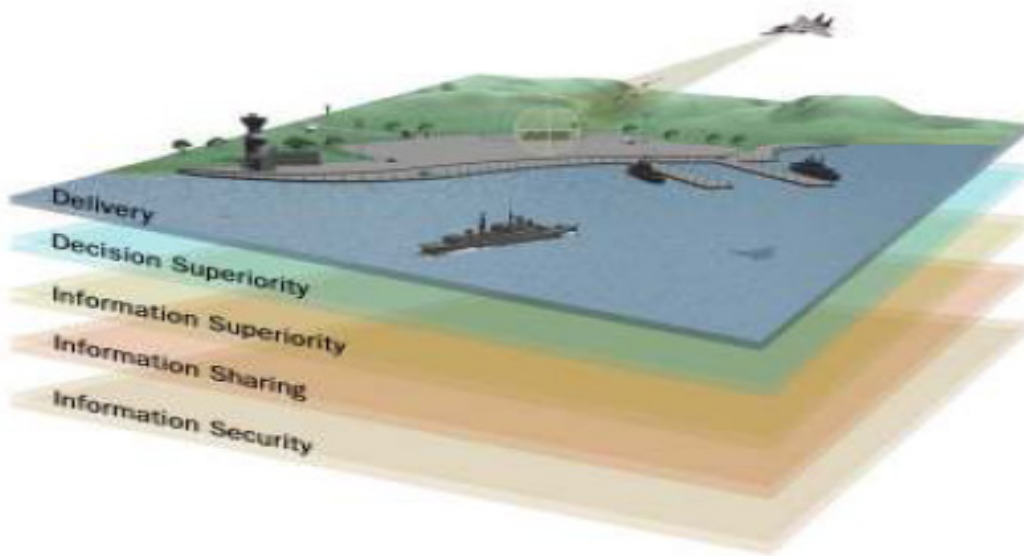
Figure 6 M&S supports all the fundamental building blocks required to achieve NATO NEC (from Hayat et al., 2006)

---

[4] ALL seven of NATO Research Technology Organization S&T Panels use M&S and one of which, NATO Modelling and Simulation Group (MSG) is uniquely devoted in supporting the NATO Defence communities with M&S tools, technologies, best practices, portals and standards (www.rta.nato.int)

2.5 Guidance in the application of M&S to NEC

A recent NATO MSG report has documented, using an evidence-based approach and a Case Study based approach, the best practices or the M&S Principles by which M&S enables the generation, the development and the employment of smart network enabled capabilities not only in Defence but in Homeland Security (Vallerand et al, 2009).

The best practices/Guidance was structured around 24 Key "M&S principles" or "Gold Nuggets" and was derived from in excess of 20 NATO nations Case Studies. The NATO report concludes that M&S is a powerful enabler to achieving NEC. Some recent documented best principles/ best practices include:

a. Systems-of-Systems Architectural Modelling underpins the successful Through-Life Management of NNEC.

b. M&S allows for CD&E that would otherwise be too dangerous, too expensive, time consuming or even completely impossible.

c. Case Studies confirm M&S as a potent lead investment for risk reduction supporting Acquisition of Defence and Security NECs.

d. M&S provides a low risk/low consequence Training environment that better represents the complexity, flexibility & adaptability of the real-world.

e. All aspects of "agile operations" - from planning/rehearsal to real-time monitoring/post operational analysis – can be enhanced by M&S support.

f. M&S supports Human development for NEC by providing "people-to-people" training that changes how people think and work together in NEC.

g. Changing demographics are increasing the "Operational Pull" for M&S support and driving an acceleration of the Evolution of M&S technologies.

The list of 24 best practices is contained at Annex A. It is proposed that a lot of the benefits and value added of MS&A seen in Defence is directly transposable to Public Safety and Security in an effort to improve address such gaps. This is addressed in the next Chapters.

3　MS&A Support to Public Safety and Security

With consideration of the safety and security domain, black swans represent the unpredictable. They represent '…our misunderstanding of the likelihood of surprises' (Taleb, 2007:2). A black swan is described by Taleb (2007) as that which is an outlier, that which is outside the realm of regular expectations which carries with it an extreme impact such as natural disasters, market crashes, catastrophic failure of complex socio-technical systems and terrorist events such as 9/11. These 'surprising events' reflect an organization inability to recognize evidence of new vulnerabilities or ineffective countermeasures (Woods, 2006). This necessitates the requirement to readjust to their existence and thereby the need to consider the extremes (Taleb, 2007).

With consideration of emerging and systemic risks and inherent uncertainty associated with surprising events, planning for and managing risk, crisis and disasters requires understanding of the space of possibilities in order to avoid unrealistic expectations that can influence the management of disasters and catastrophes. Many of the systemic risks that characterize the safety and security problem space often arise from unanticipated consequences of interactions within and between different types of systems. MS&A are tools to facilitate insights into the problem space associated with the safety and security domains.

From the Defence domain, we know that M&S has a large spectrum of applications which range from concept development and analysis, through experimentation, measurement and verification & validation, all the way to Ops analysis and eventually disposal analysis. Projects, programs and units use hundreds of different simulations, simulators and model analysis tools. Figure 7 below highlights well the integrated benefits of M&S in the continuum of defence activities. It is the thesis of this manuscript that similar benefits can be applied to Public security, in particular with respect to the use of M&S from Policy development, CD&E, Tech/Platform Demo, Testing, to Ops, training and Disposal.

This section leverages evidence-based research to illustrate the impact MS&A has had within the safety and security domains in particular Critical Infrastructure, CBRNE, command and control, exercises and experiments, security screening, interoperability and process modeling[5] (note: a list of new, short "Letter Reports" are documented as a whole to avoid repetitions and to show the recent trend).

---

[5] Allen, (2009),2009, 2010); ; Baingo et al , (2008, 2010);Baker, et al (2010) ; Beaudoin, et al (2009, 2010); Bélanger, et al (2008); Billyard, et al (2008); Boury-Brisset, et al (2009); CAE (2008, 2009); Carson, et al (2009, 2010); Cazzolato, et al (2009); Chouinard, (2008, 2009, 2009); Coateset al. (2009); Couillard et al. (2010); Crowe (2010); Desharnais, et al. (2010); Dixson, et al. (2008, 2008, 2009, 2010); Dooley, (2007, 2008, 2009, 2010); Duncan, et al (2008); EMBC (2009, 2010); Erhardt, (2009, 2009); Fujitsu (2009, 2010);); Funk, et al (2008, 2009); Gauthier,
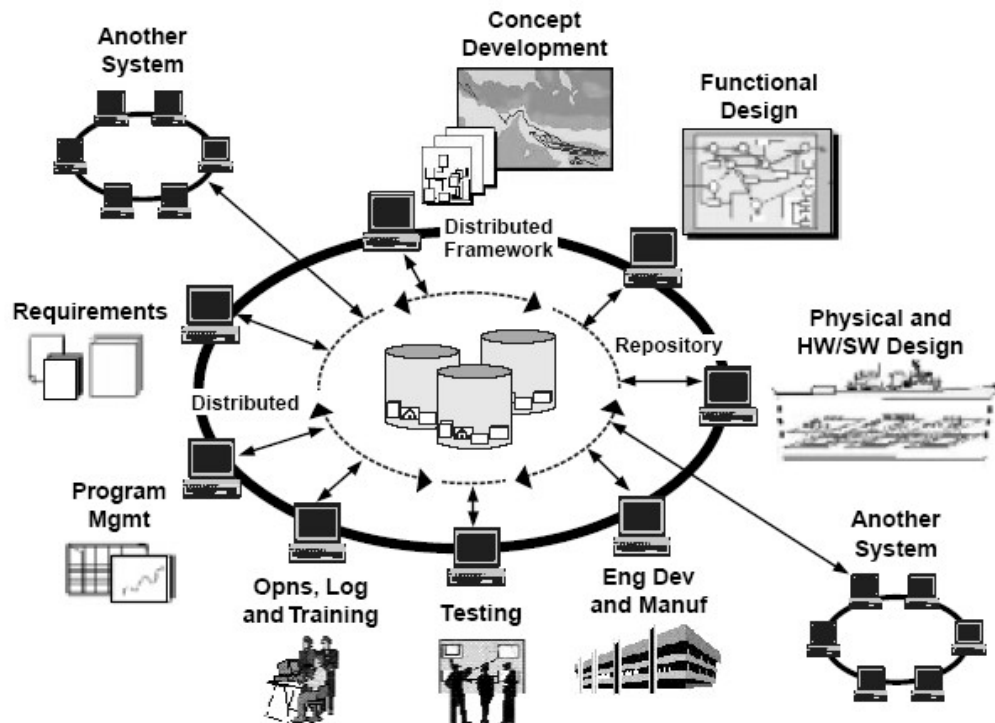
Figure 7 Excellent example of the integrated use of M&S in Defence life cycle management. The M&S is represented in the center with the 3 containers that are re-used in various instances. This is transposable from Defence to Security. (from Systems Engineering Fundamentals. Defense Acquisition University Press, 2003.)

(2009,2010); Genik, et al (2009); Gerber, et al (2010); Goodman (2010); Gouin, et al (2008);Guitouni, (2010) ; Hales, et al (2008, 2008,2009, 2010); Hewitt, et al (2009); Hill, et al (2009, 2010) ; IBM (2008, 2009); Jaurez, et al (2009) ; Jones, et al (2010) ; Jong, (2009); Kaluzny, et al (2010); Keefe, et al (2009); Khouj et al (2010); Larsson, (2009, 2010) ; Lauder, et al (2010); Lavigne, et al (2009) ; Lee (2008) ; Lemyre, (2008); Martec (2009) ; Masys, et al (2009) ; Maxwell, et al. (2010) ; McIntyre, (2008) ; McLellan, et al (2010) ; Mitrovic-Minic,et al (2010); Nadeau, et al (2009) ; Pourian, I. (2009); Quayle, D. (2009); Reedel, et al. (2009); Rehak, et al (2008); Saunders (2008); Smith, et al (2008, 2009, 2010); Steele, (2009, 2010); Sykes, (2010); Verga, et al. (2008); Wang, (2009); Wood, (2009); Yee (2010); Yee, et al (2010); Zegers, (2008); Zegers, et al (2008, 2009, 2010).

3.1 Modelling of Risk and Analysis of Emergency/Business Continuity Plans

Modeling and simulation are an integral part of management, planning, and stewardship of any Critical Infrastructure (CI) sector. In Canada, there are 10 such CI Sectors, mainly owned by Industry, and they are the Sectors of Energy, Telecommunications, Finance, Transport, Health Care, Food, Water, Safety, Government, and Manufacturing.

A survey of the M&S literature has revealed numerous tools available to support such efforts. A recent RAND Corporation report identified 37 separate tools that could be used to support risk assessment and disaster planning (Moore et al, 2010). Sandia National Labs (as other US Natl Labs) have developed and made available a suite of several risk assessment methodology to support Critical Infrastructure and Business Continuity analysis. Detailed simulation work has been done to examine both the phenomenology of terror attacks or natural disasters and the likely impact of such attacks (i.e.: "Mass Egress and Post-disaster Responses).

Modeling and simulation are used by a diverse set of stakeholders for a diverse set of local and national applications. Despite the value of a Sector's modeling activities, such models are rather severely dependent on having access to large data sets (usually a proprietary issue of significance), dependent on having been narrow in scope and have not provided an integrated, comprehensive capability. As a consequence, gaps remain in addressing the important national-scale sector challenges, such as:

- Wide-area disruptive events, including natural or All Hazards;
- Improvement of existing simulation methods and their interoperability with others;
  Planning and designing scenarios for the Sector, including wide-scale deployment of intermittent capability or Cross border events;
- Interdependencies between critical infrastructures sectors, creating tipping points with potentially devastating domino effects. The modelling of coordinated cyber and physical attacks and related impact on emergency plans and business continuity plans is relatively new asymmetric threat and falls on that category and further highlights the importance of M&S in CI interdependencies to analyze the vulnerabilities, to gain insight into the options or the future, and to mitigate related risks.

3.2 Modelling of National Critical Infrastructure Interdependencies and Risk

As described in Rahman, Beznosov and Marti (2006), modern Telecommunications provides key links and services to many other critical infrastructures, such as telecommunication, electricity, water supply, oil and gas networks, transportation, financial services, etc. Over the years, integration of these infrastructures with IT infrastructure has become pervasive, extensive, and complex. As such, failure in Telecommunications, either due to an accident or caused by a malicious attack, can propagate to other infrastructures and can degrade or disrupt their functionalities. By studying the origin of the infrastructure related failures and their propagation patterns, we can develop a better understanding of their interdependencies and thereby better support safety and security planning and operations (Vallerand, et al., 2007).

As discussed in Johnson (2008), understanding the origin of infrastructure failures and their propagation patterns in critical infrastructures can provide important information for secure and reliable infrastructure design as well as for the security of Major Events in a Nation. Among the 10 Sectors of CI, the Energy, Telecommunication and Information Technology Infrastructure (cyber) are crucial, as they provide the basic mechanism for sharing information among all infrastructures. Failures in Telecoms, cyber and energy can disrupt the effective functionality of the other critical infrastructures. Conversely, failures in the other infrastructures (Water, food, and transport as examples) can also propagate to Telecommunications, cyber and energy, and hence disrupt the operation of all systems.

In the course of our work, we have identified four broad modelling paradigms (adapted from Ciancamerla and Minichino, 2007) used to model critical infrastructure interdependencies, in order to act on those:

    i. Network Models and Derivatives
    ii. Input-Output Models
    iii. Architecture Framework or System Dynamics Models
    iv. Agent-Based Models

What seems to be emerging from this, is that the inherent interdependencies that reside within the critical infrastructure domain, could be supporting the requirement for the application of MS&A.

Network Models and Derivatives

CI is represented as a network of interconnected nodes. This is useful in showing how the network would look if a node was added or removed. One approach is to develop an interdisciplinary model to simulate the extensive human and multi-infrastructure

interdependencies that need to be coordinated to cope with large disaster scenarios in order to maximize the survivability of Canadians. This method requires a sophisticated model and a large data set to run the model. This method also helps to determine the causes of infrastructure failures and their impact on CI and other critical infrastructures in a number of dimensions, such as the origin of failures, impacts of failures in spatial and temporal dimensions, their effect on public safety and how failures propagate from one infrastructure to another. This is comparable to the approach used by several of the US National Labs. Key network models in Canada are found in the Industries who are capability owners of the sector as well as the Federal Depts with a mandate for a particular sector. It should be noted however, there are difficulties and limitations of using public domain data in academic research.

Indeed, obtaining the data to run the model or to explore different aspects of the model is a hard problem that has refused to go away. (Hollman & Marti, 2003; Ventura et al, 2008). Prof Marti of University of B.C. in Vancouver BC has built and advanced "I2SIM", a well known and capable model of such interconnected nodes and has been successfully applied to several complex related scenarios (Hollman and Marti, 2003; Ventura et al., 2008).

Input-Output Models

These models consider the presence of CI and the flow of resources between them. When dealing with protecting critical infrastructures such as: Energy, Telecoms, Cyber, Drinking Water/Wastewater, Transportation, Food & Agriculture, or Chemical, some view it as critical to take into account the multi-events, multi-threats and cascading effects by taking a different approach , an approach that identifies geographic interdependencies among critical infrastructures, without the need of sensitive and difficult to get data. Addressing such complex threat structure presents a tremendous challenge—M&S has proven to be a powerful technique for effectively addressing this challenge.

Interdependencies among Critical Infrastructures (CIs) are the basis for domino effects that may have serious consequences for society. Especially in urban areas, the high density of these infrastructures and their geographic proximity may result in failures due to geographic interdependencies, one of the four types of interdependencies that exist among CIs. Studying the issue of geographic interdependencies raises a specific problem that must be addressed. Such a study necessarily requires information on the location of system infrastructures in order to determine their proximity. Access to this kind of information is one of the major difficulties associated with the study of geographic interdependencies. Because this kind of information is confidential, systems owners are normally not willing to share it. A new approach makes it possible to study geographic interdependencies among CIs but requires only a minimum of information on the specific location of system infrastructures. Based on the concept of so-called flexible cartography, this approach models relevant results for the processing of interdependencies, while

respecting organizations confidentiality constraints. In essence this methodology is a method of risk management based interdependencies between "Lifeline Networks" (Robert & Morabito 2010; Robert, 2004)

Input Output modelling was further advanced by Chouinard et al (2010) employing essentially a "Critical Infrastructure Asset Ordination" model, as an enhanced method of addressing the most crippling upstream and downstream dependencies during complex Major National events. In this model, criticality was taken as an index of dependency risk. Since data sharing had remained problematic even for such events, the success of this method relied on one organization being entrusted as a "data safe heaven", thus enabling appropriate analyses and supporting informed decision making (Chouinard et al., 2010).

Architecture Frameworks / System Dynamics Models:

Architecture Frameworks / System Dynamics models can represent socio-technical systems, consisting of human, organizational, and technological parts. While building "UK Resilience", a new "Gold Standard" has been developed for the Simulation of Catastrophic Disaster Emergency Management Exercises at the strategic level (LeGallais, 2009). It relies on modeling of Architecture Frameworks better known as DoDAF for the US or MoDAF in the UK. Figure 8A shows an MoDAF 'OV1' in the community ('who does what, where and when') while Figure 8B shows the stakeholders' benefits and outcomes of modeling via architecture framework the infrastructure dependencies in a regional space. This is a novel way of modelling sometimes crippling dependencies. It is sometimes referred to as the "UK Home Office CPNI approach: St Pancras case study" **(**LeGallais, 2009).
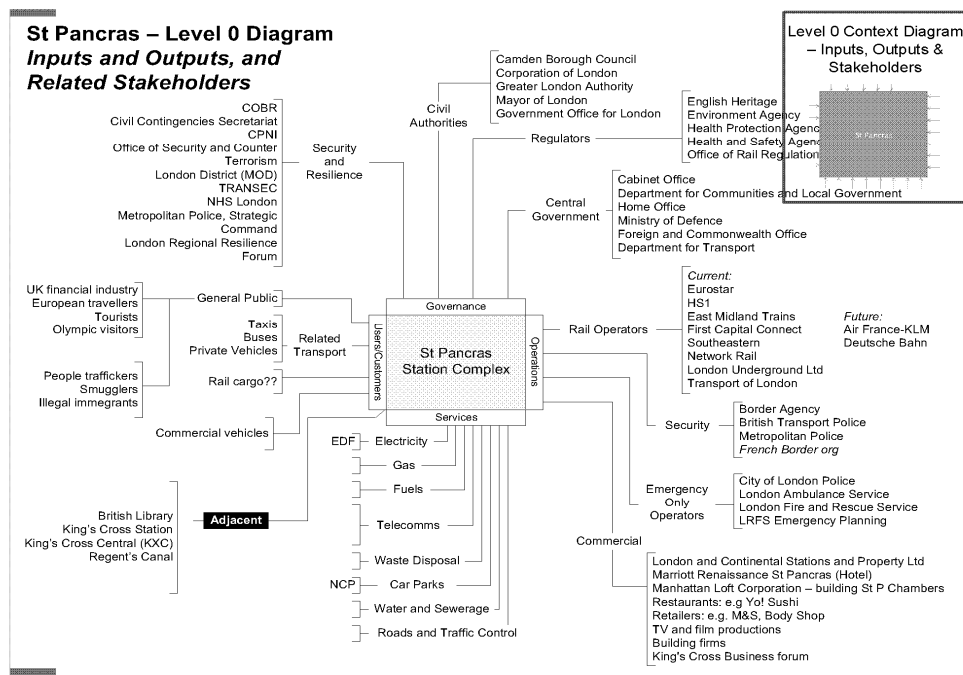
Figure 8A *(Top) UK National Infrastructure dependencies project, showing a diagram of St Pancras – Level 0 Inputs and Outputs, and Related Stakeholders .* **Figure 8B** *(Bottom). Diagram depicting Stakeholders benefits and outcomes. (LeGallais, 2009).*

This is further supported by Johnson (2008) who argues for the requirement to better understand the interdependencies associated CI. With regards to failures within CI, Johnson (2008) shows how 'latent causes can be traced back through the decisions of local management teams to higher-levels of public policy'. He argues that the 2003 blackout of areas of Canada and the USA was triggered by 'flash overs' that occurred when distribution lines sagged too close to the surrounding vegetation. The causes of this failure can also be traced back to longer term problems in regulating competitive and reliable energy markets, thereby highlighting how public policy and managerial decision making impact CI.

Agent-Based Models:

Agent Based modelling represent complex system behavior as the consequence of local interactions between agents and their environment. As Complex systems modelling is improving, it is now possible to understand tipping points between order and chaos in aerospace engineering, which may have applications to public safety and security (Cardellini et al, 2007; Bicocchi et al, 2010; Ulieru et al, 2009). When one is in a position to predict the tipping point when laminar flow becomes turbulent flow over an aircraft wing with the right parameters such as the Reynolds number, it is then reasonable to conceive that it is possible to model the tipping point: 1) in social radicalization, 2) in political unrest, 3) in critical infrastructure interdependencies, etc. Thus it would be possible to model the tipping point when 'order' falls into 'chaos' in public safety and security, and that would become rich information for smart decision making. Currently there are limitations in the behaviour of computer generated agents, forces or responders.

3.3 MS& A: CBRNE Decision Support

As described earlier, the complex and fragmented worldview has given rise to the realization of CBR threats. As articulated in Yee and Ji (2010), the release of Chemical. Biological or Radiological (CBR) agents by terrorist or rogue states in a North American city (densely populated urban center) and the subsequent exposure, deposition and contamination are emerging threats in an uncertain world. The extent of the region in a built-up environment that might be contaminated following an airborne (accidental or deliberate) release of toxic gases and aerosols and knowledge of the subsequent downwind transport, diffusion, deposition and fate of the contaminant is of great importance for emergency response planning and management, as well as for training personnel (first-responders).

The physical complexity of the urban environment is invariably characterized by particularly complex flow patterns that include curved mean streamlines, sharp velocity discontinuities, large velocity gradients, flow separations and reattachments, cavity regions, recirculating zones, and strongly non-stationary and inhomogeneous turbulence. As a consequence, the urban environment can significantly alter the transport and dispersion of a pollutant plume and provide non-intuitive concentration distributions. Although high-resolution, three-dimensional Computational Fluid Dynamics (CFD)

models can accurately simulate complex, highly-disturbed dynamic flows in and around arbitrary building configurations in an urban area, they are unfortunately not appropriate for applications where a timely response is required.

To support this problem space, Yee and Ji (2010) described a wind field library consisting of pre-computed building-aware mean wind and turbulence fields obtained from a high-resolution, high-fidelity CFD model for a specific urban area (Vancouver). This modelling output facilitated on-demand CFD in support of emergency response applications for 2010 Winter Olympic Games where timely response was an essential safety and security requirement.

This work demonstrates for the first time the feasibility of using a building-induced wind field library for a specific (pre-determined) urban area to enable 'on-demand' CFD predictions of urban dispersion for emergency response applications.
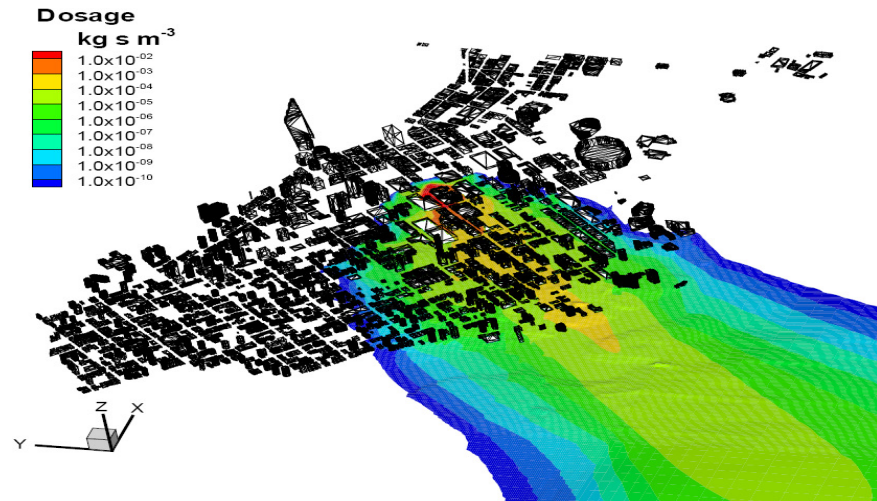
(a) Large area
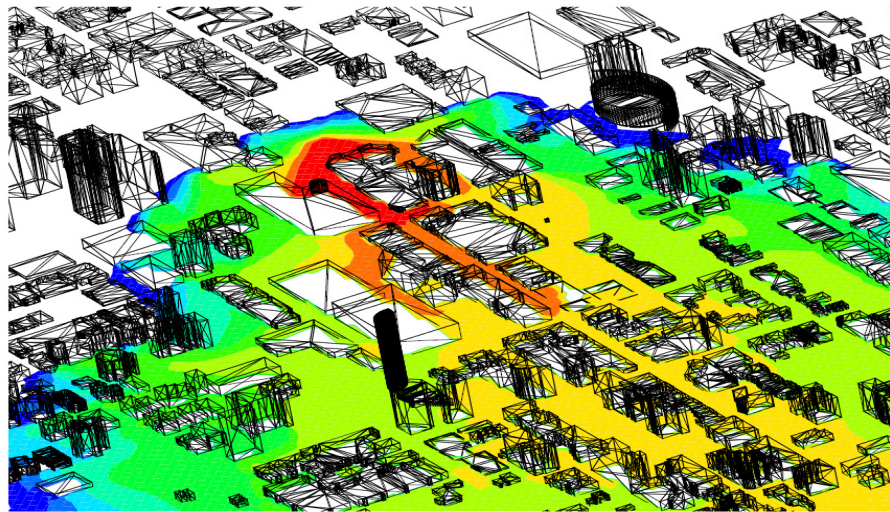
(b) Small area

Figure 9 Isopleths of the surface deposition density on the ground surface, as well as on the roofs and walls of the buildings for (a) a large area in the building-aware region and (b) an expanded view over a smaller area of the building-aware region of downtown Vancouver. The results are obtained for a prevailing wind direction of 45 degrees (Yee, 2010).

Another MS&A support initiative focuses on CBRNE sensor driven event reconstruction (Yee, 2010). Atmospheric dispersion modeling is important to public security as it provides emergency managers and responders with predictions for plume direction, coverage and lethality required to direct efforts for managing the consequences of a toxic agent release. However, before plume dispersion modeling can be applied, knowledge of the characteristics of the toxic release (e.g., location, emission rate, time of release) is

required thereby necessitating the ability to determine the characteristics of the unknown source following the detection of the event by a network of CBRN sensors. This is the so-called source reconstruction problem (which has also been referred to as the source characterization or source inversion problem in various studies). Yee (2010) describes how the operational implementation of a source reconstruction capability in 'urbanSOURCE' will enable the rapid estimation of an unknown source term associated with a covert (clandestine) release of a CBRN agent, using the available concentration data measured in real-time by a sensor network. The capability provided by 'urbanSOURCE' can provide significant improvements in the situational awareness for security operations.

The incorporation of this capability into a government operations facility will give it the key-enabling tools to provide a 'whole-of-government' (comprehensive) single authoritative source for expert quality-assured sensor-driven CBRN hazard predictions and concomitant decision-support aids, which will form the basis for making significantly improved decisions for responding to and mitigating hazardous release incidents. These products can be used by emergency managers, planners and first responders (civil and military) in various federal, provincial and municipal agencies for informed response decision making in both domestic and international operations, as well as for support of major events of national and international significance [e.g., Vancouver Winter Olympics, G8/G20 Summits, Francophonie Summit].

3.4 Real-time, In-Situ Chemical, Biological, Radiological-Nuclear and Explosives (CBRNE) Analysis Support

Science and Technology: Overview

As new threats and risks emerge, whether from terrorists, natural disasters, or human-caused accidents, first-responders must be equipped to respond quickly and effectively, while ensuring their own safety and the safety of those they are trying to help.
The Chemical, Biological, Radiological, and Nuclear (CBRN) domain leverages existing S&T activities under the CRTI Program as well as other CBRN activity within the national S&T community. In support of V2010 and G8/G20 Summits, MECSS coordinated and exploited projects within the CRTI program to meet the required timelines and operational requirements of V2010. During the preparation for V2010, numerous CBRNE activities and exercises have been conducted whereby MECSS contributed to the deployment of specific capabilities such as the: Chemical, Biological, Nuclear mobile labs; and CBRN Triage lab. The CBRNE support to Vancouver 2010 and G8/G20 was developed and validated through MS&A table-top, command post and live play exercises.

S&T in Context: Support to Vancouver 2010 and G8/G20 Summits

Major events pose unique security challenges because of mass gatherings, multiple venues, the presence of V.I.P.s, and an intense focus by the media and public. S&T can play an important role in addressing these challenges by providing analytical and technological support in planning and operations.

The Vancouver 2010 Olympic and Paralympic Winter Games (V2010) offered an opportunity for Canada's S&T community to be engaged and support public security and safety partners in addressing some of the more complex and non-traditional security challenges associated with an event of this magnitude.

The scope of S&T support included: Critical Infrastructure, Command and Control, CBRNE, Surveillance, Psychosocial, and Operations support. Scientific Advisors (SA) were embedded within the key security and safety organizations to facilitate the identification of operational requirements, as well as ensure the effective exploitation of S&T outcomes within the operational domain.

To facilitate the S&T support, an S&T reach back network was positioned to deliver expert advice from within a 24/7 posture. This network included Scientific Advisors at each of the primary Operations Centres within the Integrated Security Unit, Emergency Management BC, and the Government of Canada Operations Centre, who had contact access to expertise through centralized reach back coordination within the Centre for Security Science. A similar S&T deployment strategy was employed for the 2010 G8/G20 summits.

Science Town

Science Town is the term used to describe the totality of CBRNE science and technology (S&T) support to security operations for the Vancouver 2010 Olympic and Paralympic Games (V2010). This support included a collection of Canada's mobile laboratory capabilities together with the mobilization , thus leveraging of S&T Communities as well as reachback mechanisms into the broader Government of Canada S&T community across the country. This innovative concept was developed by the federal S&T community through the Chemical, Biological, Radiological-Nuclear and Explosives (CBRNE) Research and Technology Initiative (CRTI) and the Major Events Coordinated Security Solutions (MECSS) project.

Many of the advanced skill sets needed by the RCMP's National CBRNE Response Team exist in the larger public service and it was recognized that leveraging existing capabilities was far more efficient and cost effective than trying to build them within the RCMP. This also makes sense in light of the current low-threat environment, which allows the scientists to support the RCMP, as needed, while maintaining their regular full-time positions. Over the last several years, the CRTI has been working towards the

operationalization of S&T support to the National CBRNE Response Team. These efforts culminated in the development of the Science Town concept, with oversight provided by the MECSS project, an initiative which aimed to provide S&T support to assist functional authorities in reducing the security risk associated with V2010, as well as to contribute to the development of the RCMP's Major Event Framework.

Defeating CBRN Threats

The use of CBRNE devices continues to represent a significant threat globally. In Budget 2001, the Government of Canada announced new programs to address public security and antiterrorism issues. One of these was the CRTI, which has a mandate to strengthen Canada's ability to prevent, prepare for, respond to, and recover from incidents involving CBRNE agents.

CRTI executes its mandate through coordination of S&T investments across a partnership of over 20 federal departments and agencies as well as industry, other levels of government, end users and academia. These investments have served to mobilize the S&T community in addressing real CBRNE issues which have been prioritized through application of a systematic approach to risk and capability gap analysis. Several years ago, one such capability gap was defined relating to the ability to deploy sophisticated analytical equipment, normally housed in national laboratories across the nation, to major events across the country. Thus the notion of mobile laboratories was developed which eventually led to the science town support to V2010 and to the G8/20.

Mobile Laboratories: "S&T On the Go"

As described in the Science Town Fact Sheet (2010), the federal government of Canada houses an impressive array of S&T subject matter experts, including owners and operators of 10 mobile laboratories: two bio labs (Public Health Agency of Canada); two Chem labs (Environment Canada and Defence R&D Canada (DRDC) Suffield; five mobile nuclear labs (DRDC Ottawa, DRDC Suffield, Atomic Energy of Canada Limited and two at Health Canada); and a forensic lab (RCMP). These labs are fully operational, self-sufficient facilities that can be pre-deployed to a major event site as part of planned security operations. They provide the capability for on-site, rapid triage and identification of CBRNE agents, as well as the ability to recover and render safe contaminated evidence for the RCMP Forensic Laboratory Services.

Figure 10 Support to the major events was realized in part through the deployment of Science Town. (Pictures taken during Exercise Gold in support of V2010 (2-6 Nov 09); Sykes et al, 2010.)

3.5 Exercise and Experimentation

The development of security and safety scenarios and the establishment of a threat-based view of a major event steers the focus of major events security toward a capability-based planning approach. Since the problem space of security and safety involve an inherent uncertainty, it is important to explore and build capabilities that can be applied to a wide variety of incidents. Capability-based planning is all-hazards planning that identify a baseline assessment of safety and security efforts.

The capability-based planning approach that is inherent in analysis of readiness and validation exercises help to answer the following questions:

- How prepared are we?
- How prepared do we need to be?
- How do we prioritize efforts to close the gap?

The CRTI initiative designed series of exercises, each becoming increasingly complex and involving more players from Emergency Response and Management communities (Sykes, et al., 2010). The outcome has consisted in the integration of S&T support and "operationalization" of CRTI Clusters, as described below:

- **Exercise "AS IS"** – 7&8 Oct 03: AECL, DRDC-O, NRCan, CNSC + OGD Observers
- **Exercise "Unified Defense"** – Mar 04: USA DHS/Northcom field EX + CAN Observers
- **Nuclear Smuggling LabEx** – Apr 04: ITWG: Five Fed Labs plus UofA
- **Exercise "Follow-On"** – 23-25 Feb 05: First ex with "Federal Field Teams"
- **Exercise "Maritime Response"** -27 to 31 Mar 06: 1st Integrated CT EX in CAN – 9 Depts + NB
- **Medical Nuclear Emergency Exercise**-11 Oct 06: First exercise with medical community
- **Bi-Ex-West** – 18-19 Oct 07: Bioterrorism
- **Exercise Initial Thunder** -18-21 Feb 08: Largest CBRNE field exercise to date
- **Exercises Bronze, Silver, Gold for V2010 prep**: Heavy focus on CBRNE and integration of S&T

Three major exercises Bronze, Silver and Gold were planned by the Integrated Security Unit (ISU) to support their preparation for the Final Operating Capability. The MECSS project provided support to facilitate the integration of select S&T technologies into the existing exercise framework, and to support dedicated experimentation. Work included the development of scenarios and data sets to support experimentation, coordination of S&T resources, as well as collection and analysis of results.

Figure 11 Exercise Gold in support of V2010 (2-6 Nov 09)

Through the application of MS&A, Exercise Bronze aim was to examine the problem space associated with the Vancouver 2010 Olympics security posture. It included over 70 agencies, 550 participants and was designed using a table top methodology to establish a common, baseline understanding of interagency plans, procedures and their linkages. Exercise Silver was a functional exercise employing scenarios and injects to practice the interagency plans and procedures. Exercise Gold was a full play, live play scenario based exercise, designed to confirm the concepts of operations, processes and procedures highlighting shared situational awareness thereby providing an integrated local, regional, federal and international response to threats or emergencies.

The objectives of the GOLD exercise were designed specifically to *confirm* various existing V2010 CBRNE response plans and Concept of Operations (ConOps) as well as the joint command, control and communications processes within both the urban and Olympic domains. Over the course of five days, organizations at every level (municipal, provincial, federal, and international) participated in a series of command post exercises (CPX) and two live-play events resulting in the largest exercise of its kind in Canadian history. The V2010 live play portion of GOLD was composed of two carefully constructed scenarios designed specifically for "boots on the ground" CBRNE response. In addition to many exercise benefits, various response gaps and issues became evident during the course of both exercises. Organizations were afforded an exceptional opportunity to test interoperability and identify any gaps within departments and between participating agencies. In addition, each agency was able to test their own response protocols and strategic preparedness, while having the opportunity to rectify any gaps and issues prior to the V2010 Games. One of the primary exercise objectives, the activation of the Civil Assistance Plan (CAP), was achieved by successfully creating a scenario that presented the criteria required to initiate the request for additional resources from municipal to provincial and then provincial to federal levels. The exercise also highlighted the complex decision making triggers required for such activation. The lessons learned from this exercise will be carried forward in an effort to improve the effectiveness of targeted training in multi-organizational response protocols, roles and

responsibilities, and interoperability in a large scale CBRNE event. In addition to showcasing some of the available capabilities and resources of participating organizations, the exercise demonstrated the value of continued education and training in CBRNE response.

3.6 Security Screening

As described in Dooley (2010), during the Olympic Games, the V2010 ISU operated Vehicle Screening Areas (VSAs) and Pedestrian Screening Areas (PSAs) to reduce the risk of vehicle-borne and person-borne prohibited items (e.g., weapons) entering V2010 venues. Given the context of the Olympic games it was expected that there would be approximately 2 million pedestrian screenings at PSAs alone which by virtue of the magnitude and 'no fail' posture of the games would thereby require balancing the requirements with scope, security workforce and budget.

To support this initiative, the V2010 ISU requested S&T support from DRDC in August 2007 and March 2008 for VSAs and PSAs, respectively. DRDC support commenced almost immediately in each case and was provided continuously on a full-time basis during a 2.5 year period that included the Games. During that interval, DRDC provided V2010 ISU planners and decision makers with a multitude of practical and timely, science-based advice that arose from two comprehensive VSA and PSA development campaigns.

Software-based models were developed in each case to:
a) deepen planners' qualitative understanding of screening area dynamics and
b) translate planning assumptions rigorously into quantitative projections of screening area performance, based on the existing concept of operations and modified versions thereof.

Quantitative analyses of the model data were then conducted to identify the most promising potential approaches in each case for further study. Such approaches were later investigated and compared during a series of experiments and field trials, under conditions that were increasingly representative of the anticipated V2010 environment. Whereas early experiments were designed to help ascertain the most productive and feasible screening approaches, subsequent field trials aimed to elucidate, in detail, the manner in which the V2010 ISU might best implement its chosen VSA and PSA concepts during the Games. Finally, dedicated troubleshooting personnel operated during the Games to adjust VSA and PSA operations to real-world circumstances when the latter differed from anticipated conditions.

3.7 Information Management and Process Modeling, Simulation and Analysis

In support of Command and Control, MS&A had been instrumental in supporting the development of the physical and operational design of the Integrated Security Unit for V2010. As well, advice and support in the following areas have been conducted:

- Development and deployment of a Mobile Command Post for Joint Task Force Games;
- Concept of Operations (CONOPS) validation;
- Course of Action analysis;
- Federated Information Request manager; and
- Collaboration/information sharing

Through efforts of Allen et al (2010), an overall experimental campaign plan was designed to investigate the concept of Integrated Security Unit (ISU) and the relevant processes required to support the activities within the command centre of an ISU in charge of public security during a major event (international cultural or sporting event, G8 summit, etc.). The overall experimental campaign, called Pegasus Guardian, included: work analyses; the modeling and simulation of the processes of interest; and, a human-in-the-loop experiment to validate and investigate the modeled processes. The modeled processes focused on the tasks and activities within the Integrated Command Centre (ICC) for V2010 as they were envisaged in November 2007.

In support of MECSS, Allen (2009) describes nine information management processes that were selected for the modeling efforts during a working group meeting composed of representatives from the RCMP, the CF, PSC, British Columbia Public Emergency Preparedness (BC PEP), the Vancouver Police Department (VPD) and the West Vancouver Police Department (WVPD). These nine processes are:

1. **Situation Report Process**: Scheduled process where the games venues report the current situation to the command centre. The command centre uses this information as well as generic situational awareness (SA) to develop a situation brief and the Commander's directions.
2. **Maintains Situation Awareness Process**: Regular process used to classify and prioritize incoming information. Within this process specific information will also be selected for its display on the real-time board (electronic easel).
3. **Request for Information Process**: Formalized process used to request specific information. Anyone within the ISU can fill out a request for information form. The reception of such a form by the IM staff within the command centre will trigger the process.
4. **Public Affairs Process**: Regular process used to develop the media lines, which specifies the information that will be provided to the public. This process is an

important one that specifies the interface between the command centre and the public.

5. **Incident Report Process**: Process through which a given games venue reports about an incident to the command centre.
6. **Incident Response Planning**: Process performed within the command centre in response to an incident report from a given venue. The command centre will keep monitoring the situation at the venue and if it is assumed that the resources at the venue are insufficient to respond to the incident, immediate tasks will be performed to dispatch additional ISU resources. Furthermore, detailed courses of action will be developed if requested.
7. **Request for Assistance Process**: Rare process that will be used by the ISU to request assistance from a federal agency if it is assessed that the ISU resources will be insufficient to respond to a given threat.
8. **Transfer of Authority Process**: Rare process used when an incident goes beyond the games venues and it is assessed that the lead of the response shall be given to a higher entity (e.g., the RCMP National Operational Centre).
9. **Handover Process**: Occasional process used when the ISU has completed the crisis management in response to an incident and the lead for the consequence management is transferred to another agency.

The modeling effort consisted of detailing all the tasks required to fulfill each of the nine processes including the time and resources associated with each of these tasks. Based on estimated rates of occurrence for each process, the model was run by selecting a given set of ISU resources. The runs were analyzed by evaluating the likelihood that given task delays be observed given the size of the ISU resources.

3.8 Capability Analysis

Events such as V2010 provide an impetus for integrated planning and operations. In fact, new organisations were created for this purpose, such as the Integrated Security Unit (ISU), led by the RCMP, and Integrated Public Safety, led by EMBC. Exercise Gold, the final, large-scale exercise in preparation for V2010, provided an indication of the scale of the planning and integration of operations required to support security and EM for a major planned event such as the Olympics. The complexity associated with operating the games in conjunction with providing safety and security necessitated the requirement to clearly develop an organizational design that supported collaboration, coordination and direction

As described in Funk (2009), Dixson and Genik (2010), implementing Architectural Frameworks (AF) as a way to help manage the complexity of security and emergency management operations requires a strategy for best extracting the relevant data and generating useful products. In preparation, the objectives must first be defined and, based

on those objectives, the products of interest can then be chosen. For the V2010 application, with various groups from the ISU and EMBC, the AF concept was utilized to support planning and exercise preparation activities, contributing to these three main objectives:

1. Facilitate the integration, planning and operations of selected organizations involved in security and emergency management for the Games.
2. Track the progress of planning and integration.
3. Measure the effectiveness of the coalition of organizations.

3.9 M&S Best Practices for Public Safety and Security

Derived from the best practices for M&S supporting NEC and evidence-based evaluation of M&S within the safety and security domain, the following best practices have been contextualized for the safety and security domain.

1. M&S that uses architectural techniques to measure interoperability provides a key decision support tool for managing investment in systems that contribute to safety and security.

2. The way to explore the way ahead for safety and security domain is by CD&E, which should be based on a campaign of experiments that use Live, Virtual, and Constructive simulations in an iterative, and scientific way.

3. Simulation allows for experiments that would otherwise be too dangerous, expensive, time consuming, or even impossible.

4. Simulation development should not start from scratch, but instead reuse assets that are part of a permanent simulation capability.

5. Managing a persistent simulation capability can benefit from Capability Maturity Model Integration (CMMI) with M&S key process extensions.

6. M&S provides the potential to create a more comprehensive analytical environment from a financial and risk perspective, thus enabling informed decision making and resulting in a better understanding of the total cost, both from a financial and risk perspective.

7. M&S provides a synthetic environment representing the safety and security domain within which safety and security stakeholders can test and evaluate any proposed capability acquisitions for ease of connection to the network.

8. Use of M&S at the front end of the dedicated acquisition activity should flow logically from any efforts that were made during the earlier stages of capability development, such as complex CD&E.

9. M&S allows users to explore new concepts, procedures, and technologies within a synthetic operating space, without depending on any operational resources.

10. A single system cannot meet the needs of safety and security training. The safety and security domain training capability must mirror the flexibility and agility found in the safety and security domain environment itself,

11. M&S provides a training environment that realistically represents the complexity, flexibility, and adaptability of an actual safety and security real-world operating environment.

12. Use standards whenever possible – for example: a) when simulation systems are developed; b) for technical architectures; c) for verification and validation; d) for data representation; e) and synthetic environments and scenarios.

13. The development of training and exercise capabilities requires an incremental and evolutionary approach, supported by an architecture framework such as DNDAF, DODAF or NATO Architecture Framework (NAF).

14. M&S must be aligned to the technical capability of the supporting safety and security Information Infrastructure.

15. The use of M&S will be increasingly important to support current and future operations, particularly with safety and security stakeholders.

16. A holistic approach is needed, covering all aspects from training to post-operational analysis which will allow the full re-use of M&S tools and data.

17. Use of M&S to support complex operations needs to be seen by all concerned as 'business as usual' through the Major Event Security Framework

18. It is important to focus on "people-to-people" Training and Experimentation to change how people think and work together.

3.10 Two Key MS&A Gaps Remaining in Public Safety and Security

The present data suggest so far that Models and Simulations are available in Public Safety and Security to address in a meaningful ways the following:

- Threat and risk analysis;
- CI sector modeling and analysis;
- Supply chain analysis;
- CI Interdepedencies;
- Optimization modeling;
- Capability based planning modeling;
- Asset prioritization modeling
- Advanced modeling for investigation /forensics purposes;
- Advanced visual analytics.

Some gaps remain. The first one in Public Security appears to be an Integrative and comprehensive M&S capability, outside of the essential - though large, expensive and people intensive Live simulations. Defence Communities have known for years the value of integrating many models, many simulations, from many areas into one distributed venue reuniting Live, Constructive and even Virtual simulations that can be used as test/re-test scenarios as appropriate. Experiments and exercises have been conducted with such comprehensive M&S capabilities such as EMERGEO, ADMS Command, CAE EM-Sim, Hydra/Mynerva (Web-based), EDMSIm, and others. What is not clear is how the above M&S capabilities enabled the connectivity with others via TCP/IP protocols, or by DIS Protocol (IEEE 1278 standard), or by HLA protocol (IEEE 1516 standard) or by TENA protocol.

A second gap that surfaces is the ability to benefit from a Portal that supports and enables the community in the journey to get to the objectives efficiently through the smart use of MS&A. In the defence sector one will find a large list of Information and Analysis Centers. In DoD, there are ten IACs : AMMTIAC CBRNIAC CPIAC DACS IATAC MSIAC RIAC SENSIAC SURVIAC WSTIAC (http://iac.dtic.mil/). Of clear interest is the M&S IAC, the portal to support Modelists and Simulationists in the Defence domain (http://www.dod-msiac.org/). In DHS, the closest to the above portal capability is the DHS National Infrastructure Simulation and Analysis Center (http://www.dhs.gov/xabout/structure/gc_1257535800821.shtm). In Public Safety and Security, an emerging persistent capability to support Public safety and Security M&S is the "Major Events Security framework on GCPedia (GoC wiki at http://196.303.185.144/MESF.xxxxx.html)

4   MS&A in Support to Public Security Operations - Creating a Persistent S&T Capability

A Major Event is defined as an event of national or international significance, where the overall responsibility for the security rests with the federal government of Canada. Examples of such major events include major summits, conferences, and meetings when the participants are heads of states/governments (G8) and international sporting events (Vancouver Olympics). Given the high profile nature of these events, natural and man-made disruptions to these events can have significant safety and security implications that can cross local, national and international boundaries. The management of the safety and security of these events is a multidisciplinary, multi-jurisdictional issue that necessitates an integrated planning and response mechanism to ensure seamless operational management in the event that a safety and security issue would arise.
S&T is an enabler that informs the various stakeholders with respect to major event safety and security issues such as those stemming from Vancouver 2010 (V2010) Olympics and G8/G20 Summits.

Canada's experience and associated challenges with security preparations for major events such as V2010 and G8/G20 have illustrated opportunities for a stronger alignment of planning activities across the domestic security domain. Challenges associated with integrated planning, communications, and interoperability, are elements of deeply rooted issues that can be attributed to dissimilar organizational cultures and security doctrine. The existing challenges are compounded by a national safety and security infrastructure that is challenged to fully exploit collective learning opportunities between agencies and across jurisdictions. The level of effort and the degree of investment in establishing an effective security posture for upcoming major events warrants serious consideration into how new knowledge, practices, and protocols can be captured and institutionalized to support an enhanced degree of national resiliency as a function of a more robust 'whole of government' approach to future security events in Canada.

The planning and execution of major events security operations is not a new discipline. Over the past four decades Canadian authorities have planned for, and executed, complex operations in support of major events accounting for both the security and safety dimensions. Such major events include:
- 1976 Montréal Summer Olympic Games;
- 1986 Vancouver World's Fair (Expo 86);
- 1987 Vancouver Commonwealth Heads of Government Meeting (CHGM);
- 1988 Calgary Winter Olympic Games;
- 1993 Vancouver Clinton-Yeltsin Peace Summit;
- 1994 Victoria Commonwealth Games;
- 1996 Vancouver Asia Pacific Economic Conference (APEC);

- 1999 Winnipeg Pan American Games;
- 2001 Québec City Summit of the Americas;
- 2002 Kananaski, Alberta G8 Summit;
- 2008 Sommet de la Francophonie à Québec City.
- 2010 Vancouver Winter Olympics
- 2010 G8/ G20 Summits
- 2012 London Olympic Games
- 2015 Pan Am Games (Toronto)

Major events vary in scope and thereby shape the requirements for resources and planning. For example, the resources and planning required for a short visit of an international dignitary is much different from the resources and planning required for Vancouver 2010 Olympics. The scope of the events with respect to resources and planning are well articulated in Johnson (2006). Of note:

> 'The security operation for the Athens Summer Games of 2004 had to protect more than 11,000 athletes who came from 201 National Olympic Committees and who participated in 296 events. The Games sold more than 3.2 million tickets; only Sydney sold more with 5 million in 2000. There were more than 21,500 media representatives in Athens. The US NBC network had more than 3,000 people. Media representatives were spread across 19 sports venues, 102 hotels and 7 media villages. The Games were broadcast to a worldwide television audience of up to 3.9 billion. Protecting these potential targets requires enormous resources. Athens was the most expensive Games costing approximately €9 billion ($11.6bn; £6.3bn)…. security arrangements are estimated to have cost the Greek government more than €1bn' (Johnson, 2006).

4.1 MECSS

Recognizing the recurrent requirements to manage the security for major events across departments and leveraging the Vancouver 2010 (V2010) Olympic experience, the Major Events Coordinated Security Solutions (MECSS) initiative was established. MECSS reflects a multi-agency collaborative partnership, established to reduce the security risk associated with V2010 through the coordinated application of S&T.
There are two high-level objectives associated with the project:

1. Assist the functional authorities in reducing the security risk associated with V2010 through the coordinated application of science and technology; and

2. Contribute to the establishment of an enduring Major Event security framework that can be applied to future Major Events in Canada.

MECSS derives its mandate and support from the Public Security Technical Program (PSTP). PSTP is a federally funded S&T program managed by DRDC Centre for Security Science (CSS) on behalf of the Government of Canada.

The PSTP program consists of four theme areas: 1) Chemical, Biological, Radiological-Nuclear and Explosives (CBRNE) Threats; 2) Critical Infrastructure (CI) Protection; 3) Surveillance, Intelligence, and Interdiction (SII); and 4) Emergency Management and Systems Interoperability (EMSI).

Whole-of-government, industry, and academic collaboration is promoted in each theme area through activities that are identified and prioritized by expert groups and stakeholders, defined for PSTP purposes as "Communities of Practice" (CoP) or Science Clusters. The vision of PSTP sees each CoP generating collaborative project teams to reduce capability deficiencies by integrating leading-edge S&T to meet the needs of end-user clients. A systems-of-systems approach underlies much of the contributions of PSTP (Figure 12).

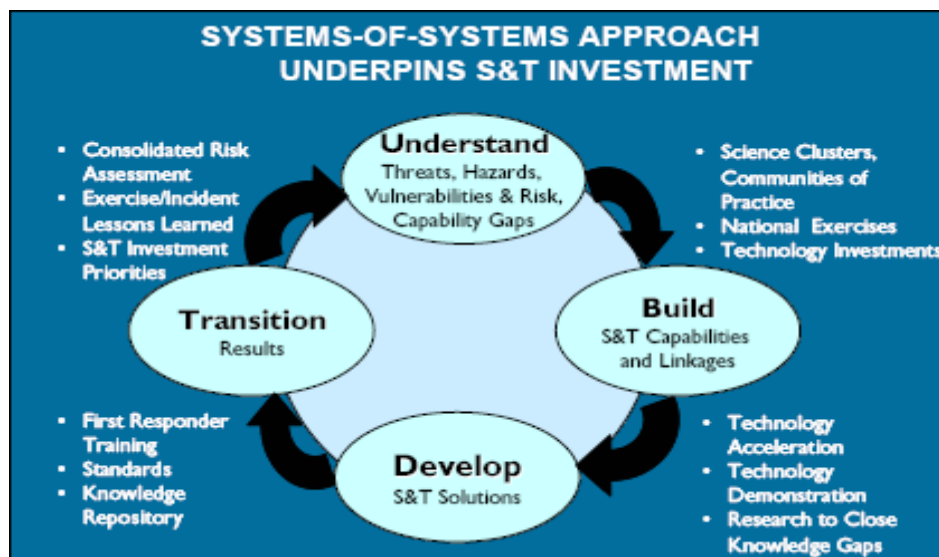*Figure 12 Systems-of-Systems Approach to S&T Investment*

The complexity associated with planning for major events safety and security resonates with Weick (1987) and Sitkin (1992) who argue that actors in high-hazard organizations cannot learn by trial and error in the same way as can those in other organizations because the risks of error are too high; instead they must draw many lessons from many

more minor incidents (Carroll, 1995). Within the security domain, MS&A can facilitate the exploration of the problem space thereby providing insights that can shape the design of the security. In support of the first MECSS objective, to reduce the security threat associated with V2010, a number of initiatives that derive from the PSTP have been exploited to support the safety and security domains.

4.2 Creating a Persistent S&T Capability Supporting the Safety and Decurity Domains: Major Events Security Framework

In support of the second MECSS objective regarding the establishment of an enduring Major Event security framework, DRDC has been working with the RCMP, academia and industry in developing a 'whole of government' planning process for Major Events. The Major Events Security Framework is an 'integrated' generic planning process that is 'tailorable' with regards to the scope of the major event. The framework facilitates a logical, analytical problem solving process that results in the development of products ,leading to a synchronized plan that addresses both security and safety dimensions. The Major Event Security Framework focuses on 3 key deliverables:

1. Integrated planning capability for major events in Canada across federal departments and agencies;

2. Institutionalization of Science and Technology (S&T) support within the public security domain pertinent to major event security; and

3. Resiliency-Based Public Security Capabilities, facilitated through Strategic Safety and Security Capability-based planning.

Characteristics of the framework
The strategic vision of the "Whole of Government' Major Events Security Framework is to further enhance the preparedness of the Canadian Government through its security and safety stakeholders by formally establishing a standard and comprehensive approach to major event security and safety planning. With this in mind, the framework is defined by its purpose in:
* Facilitating an overarching guide for Major Events Security Outcome Management
* Providing standardized planning process
* Ensuring control of strategic & operational planning
* Enabling strategic goals to be translated to operational level security objectives
* Enabling stakeholders to guide development of the plan, and to synchronize & integrate joint operational security functions
* Maximizing effective and efficient use of resources

The development of the framework is based on 2 key assumptions. First, it is recognized that current planning approaches do not provide for sufficient levels of information sharing and collaboration to achieve the necessary shared awareness. Second, that collaborative planning allows all levels of government to plan together to synchronize their efforts. As such the corner stone of the framework realizes that a sound planning process should be orderly, analytical, and consist of logical steps to identify a mission or requirement; develop, analyze, and compare alternative courses of action; select the best course of action (COA); and produce a plan.

In line with the vision and given that effective networking of people, organizations and technologies is key to managing planning for major events security, the proposed framework encompasses the following:

- 'whole of government' forum that guides the collaborative planning and execution of security capabilities;
- knowledge management system that identifies best practices, captures lessons, effects change, and champions innovation;
- repository of value-added tools and technologies; and
- Governance, with the authority to link 'policy, legislation and mandates' with 'functions, tasks, and expertise', within the business planning cycle.

Thus governance, culture and interoperability characterize the foundation of the Major Events Security Framework.

WEB 2.0
To facilitate the development of requirements and vision of the MESF, the Treasury Board's GCPEDIA (MediaWiki) site was leveraged as it is accessible to all of the government users across Canada. It is also a great enabling environment for a free and user-friendly Repository. The new art and science of wikinomics is based on four powerful new ideas: openness, peering, sharing and acting globally.' (Tapscott and Williams, 2006: 20)[i]
One of the most powerful emergent features of the web 2.0 environment is the inherent knowledge management (KM) and Organizational Learning (OL) capability. Knowledge management is defined as the art of creating value from an organizations intangible knowledge asset. Moreover, it is the process through which organizations generate value from the intellectual and knowledge based assets. More often, generating value form such assets involves sharing them among employees, departments and even with other organizations.

The web 2.0 paradigm affords the capability:
- To make knowledge observable and visible the role of knowledge in an organization, mostly using hypertext tools

- To develop a knowledge culture by encouraging behaviours such as knowledge sharing and searching and offering knowledge
- To construct a knowledge foundation not only as a technical system, but as a web of interconnections among people given space, time, tools and inspiration to interact and cooperate. Essentially bringing people, processes and technology together.

The backbone of GCPedia (a wiki) is more that just software for enabling multiple people to edit web sites. It is a metaphor for a new era of collaboration and participation. As described in Tapscott and Williams (2006: 18), 'the new promise of collaboration is that with peer production we will harness human skill, ingenuity, and intelligence more efficiently and effectively than anything we have witnessed previously. …Collective knowledge, capability and resources embodied within a broad horizontal network of participants can be mobilized to accomplish much more. …the ability to integrate the talents of dispersed individuals and organizations is becoming the defining competency for organizations'. Collaboration is a cooperative relationship in which participants' differences are leveraged and divergent stakeholder concerns are balanced (Hardy, Lawrence, & Grant, 2005). Collaboration is especially important in complex, dynamic situations that impact community public security and safety.

Through leveraging GCPedia, the MESF design facilitates transparent planning that is tailorable and scalable; it facilitates collaborative planning and co-creation through collaborative efforts thereby harnessing the collective intelligence.

The hallmark of the Major Event Security Framework regarding successful knowledge sharing and collaboration is most readily associated with three outcomes:
- Improved organizational learning
- New knowledge creation and innovation
- Knowledge reuse

The main advantage of a people-focused strategy is that it enables the sharing of more relevant tacit knowledge (Polanyi, 1983), such as employees' experiences, know-how, and other similar or complementary expertise that cannot be captures in documents. Today's organizations require the capability to access timely expertise and this is most likely done through employees' personal or social networks- the informal connections and relationships among people where much knowledge sharing occurs and very often where critical work gets accomplished…Work in organizations has become much more relational, interdependent and collaborative in nature' (Parise, 2007:360).

According to Senge (2006), a learning organization is an organization that is continually expanding its capacity to create its future. The creation of a learning culture not only facilitates the creation of new knowledge but also prevents much of the knowledge loss' (Loermans, 2002). Organizational learning is the vehicle for utilizing past experiences,

adapting to environmental changes and enabling future options' (Berends et al., 2003: 1036).

The MESF recognizes and embraces that when individual and group learning becomes institutionalized, organizational learning occurs and knowledge is embedded in non-human repositories such as routines, systems, structures, culture and strategy (Crossan et al., 1999; Nelson and Winter, 1982; Walsh and Rivera, 1991).
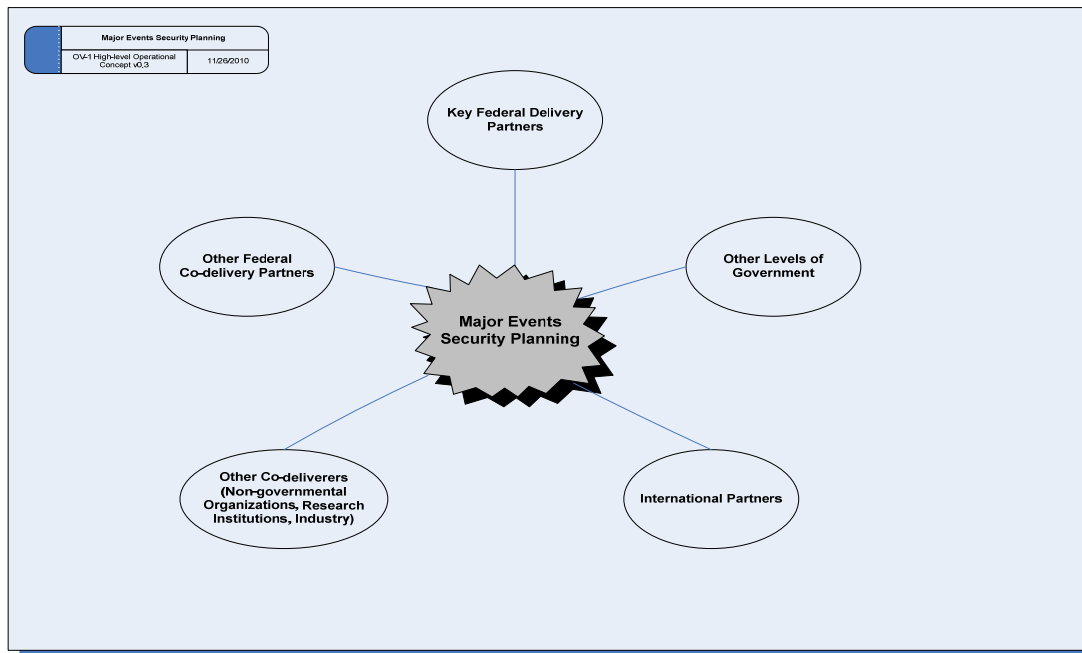
Figure13 Connecting Distributed knowledge

Persistent MS&A Capability

Embedded within the MESF are a collection of tools and guidance regarding the application of S&T (Modelling, Simulation and Analysis) to the safety and security problem space. Available to the community are an overview of existing M&S tools, their capabilities, requirements, and points of contacts.

The following tool categories were prioritized:
- Tools for predicting the potential consequences of natural disasters such as storms, hurricanes, floods, earthquakes, tsunamis, forest fires, or other disasters.
- Tools for predicting the potential consequences of man-made disasters such as Chemical, Biological, Radiological, Nuclear and High-Yield Explosives (CBRNE) attacks or non-intentional releases.

- Tools for assessing the relative importance of critical infrastructures, their interdependencies, and the possible consequences of their failures.
- Tools for predicting the potential consequences of pandemics and preparing response plans.
- Tools for planning major event security, including tools that can model the behaviour of large crowds in urban environments.
- Tools for modelling domestic Intelligence, Surveillance, and Reconnaissance (ISR) activities and measuring their effectiveness.
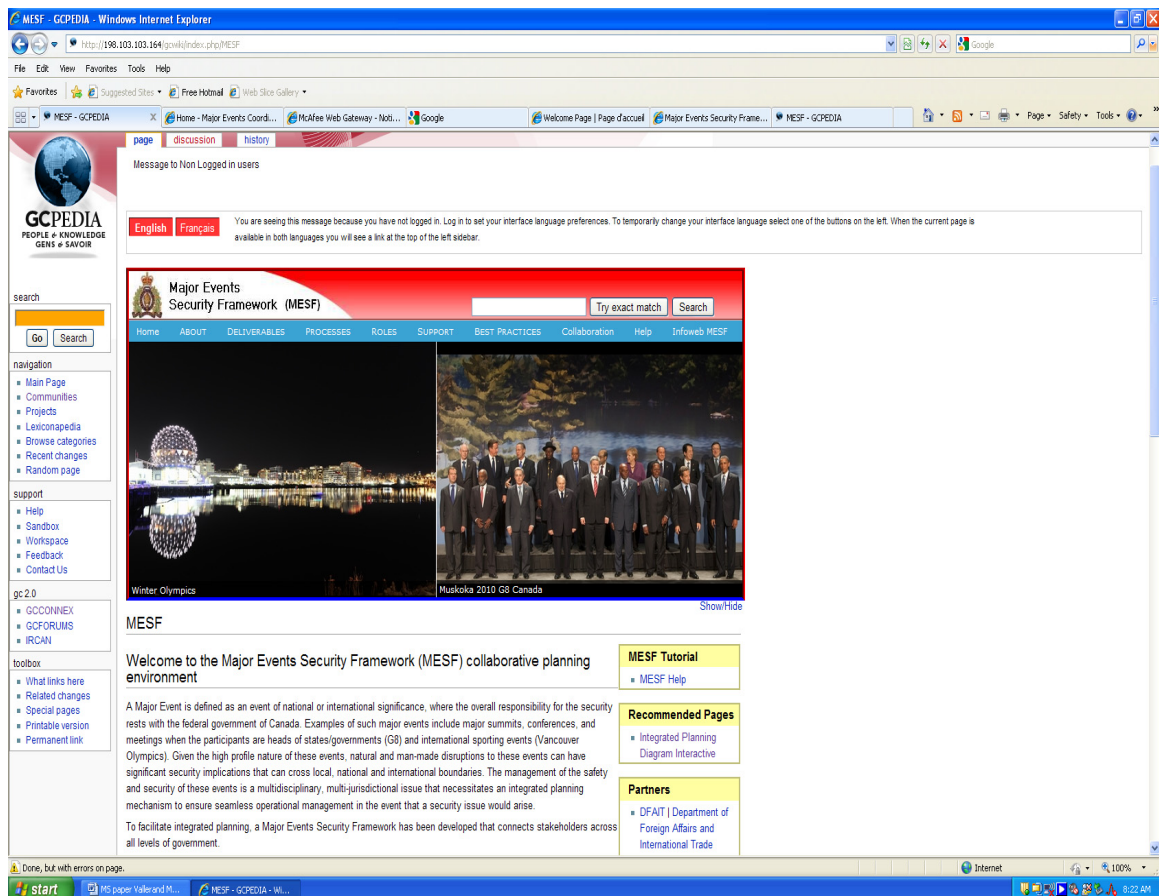
Figure 14 MESF Home Page

Figure 15 MESF home page depicting M&S tools set links.

5   Conclusions and Recommendations

The Defence, Security and Safety environments can be characterized as "complex and adaptive". Such environments do not lend themselves to well-bounded, linear problem-solving approaches, nor to the design of interventions based on historical and empirical evidence alone. These problems require approaches that acknowledge the challenges of complex adaptive systems and respond by facilitating collaboration across multiple domains and seek to discover interdependencies and emergent behaviour. The ability of groups and organizations to appreciate and take action in relation to 'complex adaptive' problems often drive them to seek the benefits from M&S as a potent enabling tool for investigation and analysis.

Through a case studies-based argument, this report demonstrates the success of explicitly linking M&S tools with the analytical process (MS&A) as a facilitator for decision-making to provide a potent methodology for gaining insights into complex problem spaces. In particular, based upon the success of M&S within the defence domain, this report highlights the growing use and impact of MS&A in the Public Safety and Security domain in general and in particular to supporting "Complex Major National Events" such as the Vancouver 2010 Olympics. We therefore argue that MS&A is indeed a potent enabling tool not only for Defence but also for Safety and Security Communities. Indeed, a multitude of Defence case studies demonstrated that this concept was not only applied for CD&E and Training, but also applied across the entire Capability lifecycle from Strategy/Policy, to Capability Development, Generation and Employment including aspects related to Network Enabled Capabilities. Since many of the same attributes applicable to International Security and Defence planning and execution are equally applicable to Domestic Security and Public Safety relating to Complex Major National Events such as Vancouver 2010 Olympics, then the evidence would support that MS&A is a crucial enabler for this community as well.

Further, it was argued in this paper that due to the asymmetric nature of new security threats, military and non-military threats are becoming more similar in their complexity. By consequence, both military and domestic civil responses are themselves becoming more similar in the complexity of the response by combining a number of specialized capabilities together from potentially different source organizations. Conversely, the ability to 're-use " M&S tools, technologies, protocols, portals and standards from Defence to Public Security and Safety becomes even better supported. Drawing from a compilation of over several dozens of new reports produced in support of Vancouver 2010 and G8/G20 Summits and others, MS&A emerges as a crucial, effective and efficient enabler to Public Security and Safety. It is specifically due to the value and the contribution of such tools to various Defence and Public Security and Safety capabilities, that a persistent MS&A capability framework has been developed to facilitate, to enable reuse and to better support the multi-jurisdictional communities engaged in both National and International complex Major Events.

In conclusion, though at first brush the use of MS&A in Public Safety and Security does not seem to be as wide and deep and does not seem to be similarly "crowned" by large International distributed simulated training like in Defence, their valued-use was documented as clearly growing This report concludes that MS&A represent significant potent enabling tools that contribute significant value and impact as well as efficiency and effectiveness to Public Safety and Security in general and in particular to support safety and security at complex major national events. Decision makers seeking efficiency and effectiveness are thus encouraged to increasingly use or re-use Public Safety and Security M&S in their analyses.

Annex A 24 Key M&S Principles in support of NEC

•**M&S Using Systems Architectures in Support of Through-Life Management for NNEC**
1. M&S that uses architectural techniques to measure interoperability – a fundamental property of NEC – provides a key decision support tool for managing investment in systems that contribute to NEC mission threads.
2. NEC is a Systems-of-Systems (SoS) problem that can be understood through effective use of enterprise architectures.
3. SoS Architectural Modelling underpins the through-life management of NNEC.
• **M&S in Support of Concept Development and Experimentation Supporting NEC**
4. The way to explore the way ahead of a NEC is by CD&E, which should be based on a campaign of experiments that use Live, Virtual, and Constructive simulations in an iterative, scientific way.
5. Simulation allows for experiments that would otherwise be too dangerous, expensive, time consuming, or even impossible.
6. Simulation development should not start from scratch, but instead reuse assets that are part of a permanent simulation capability.
7. Managing a persistent simulation capability can benefit from Capability Maturity Model Integration (CMMI) with M&S key process extensions.
• **M&S Support to Acquisition, Test and Evaluation, and Logistics for NNEC**
8. M&S provides the potential to create a more comprehensive analytical environment from a financial and risk perspective, thus enabling informed decision making and resulting in a better understanding of the total cost, both from a financial and risk perspective.
9. M&S provides a synthetic environment representing the NNEC framework within which member nations can test and evaluate any proposed capability acquisitions for ease of connection to the network.
10. Use of M&S at the front end of the dedicated acquisition activity should flow logically from any efforts that were made during the earlier stages of capability development, such as complex CD&E.
11. M&S allows users to explore new concepts, procedures, and technologies within a synthetic operating space, without depending on any operational resources.
• **M&S Support to Training and Exercises for NNEC**
12. A single system cannot meet the needs of NEC training. The NEC training capability must mirror the flexibility and agility found in the NEC environment itself, i. e. the NEC training and exercises environment (and the supporting M&S) must themselves be network enabled.
13. M&S provides a training environment that realistically represent the complexity, flexibility, and adaptability of an actual NEC real-world operating environment.
14. Use standards whenever possible – for example: a) when simulation systems are developed; b) for technical architectures; c) for verification and validation; d) for data representation; e) and synthetic environments and scenarios.
15. The development of training and exercise capabilities requires an incremental and evolutionary approach, supported by an architecture framework such as NATO Architecture Framework (NAF).
16. M&S must be aligned to the technical capability of the supporting NATO Information Infrastructure (NII) for NEC.
• **M&S Support to Agile Operations and Command for NNEC**

17. The use of M&S will be increasingly important to support current and future Operations, particularly in coalitions.

18. A holistic approach is needed, covering all aspects from training to post-operational analysis, which will allow the full re-use of M&S tools and data.

19. Integration of M&S in Command, Control, Communications, Computers, and Intelligence (C4I) is essential to permit the optimum benefit to be obtained and while immature, ongoing research needs to be maintained.

20. Use of M&S to support Complex Operations needs to be seen by all concerned as 'business as usual'.

• M&S to Enable the Human Dimension of NNEC

21. There is a range of new Human Dimension (HD) challenges related to both central NNEC ideas and the wide spectrum and variety of Operations today. Addressing such HD issues requires the use of more "light weight" technologies such as gaming/massively multi-player gaming for cheaper, more easily accessible experimentation and training.

22. It is important to focus on "people-to-people" Training and Experimentation to change how people think and work together. Accelerating the pace of HD (how quickly people work together to achieve a common goal) in NNEC requires the use of all aspects of simulation-based technologies available today (and in the future) to accelerate the pace of the HD in NNEC.

• Evolution of M&S in the NNEC Context

23. M&S as a formal discipline has rapidly expanded into new roles and provides unthought-of new abilities to support the commander. This expansion is in part as a result of significant developments in computing power and evolution of computer programming knowledge and capability.

24. Due to six key reasons, the "Operational Pull" for M&S is escalating significantly and is requiring M&S technologies to change and evolve.

References

Abdellaoui, N. , K. Wheaton, and D. Allen, The Role of Modeling and Simulation in the Canadian Joint Fire Support Technology Demonstration . Proceedings of NATO Conference Potent enabling Tools for Planning and Executing Complex Major Events, 11-1-11-14, 2008;

Allen, D. (2009). *Comparison of Planned and Observed Processes for Major Event Security - Results from Pegasus Guardian 1* (Technical Note).

Allen, D. (2009). *Modeling Information Management Processes for Major Event Security* (Technical Report).

Allen, D., Bélanger, M., & Goodman, L. (2010). *Feedback on the ISU 2010 Summits Command and Control Document Version 0.3* (Letter Report - PA).

Allen, D., Breton, R., & Hancock, J. (2009). *Initial Analysis of ISU Whistler Area Command Centre (WACC) Operations during Exercises Pegasus Guardian 3 and Gold* (Letter Report - PB).

Allen, D., Farrell, P., Chow, R., & Trinh, K. (2009). *Pegasus Guardian Experiment Analysis Report* (Technical Report).

Allen, D., Maceda, E., Smith, D., Wood, D., Gouin, D., Jobidon, M.-E., et al. (2009). *Initial Analysis of ISU Vancouver Area Command Centre (VACC) Operations During Exercises Pegasus Guardian 2-2 and Silver* (Letter Report - PB).

Baingo, D. (2010). *Blast Effects Analysis in Support of Security Operations for the Vancouver 2010 Winter Olympic Games* (DRAFT Technical Report).

Baingo, D., & Chouinard, P. (2008). *Briefing Note to the ISU on Interim Analysis of Games Related CI Assets* (Letter Report - S).

Baker, K., & Hales, D. (2008). *V2010 Command and Control Architecture - Initial Data Collection at the Integrated Security Unit* (Contractor Report).

Baker, K., & Hales, D. (2010). *Vancouver 2010 Command and Control Architecture: Initial Needs Analysis* (Contractor Report - PB).

Beaudoin, L., & Genik, L. (2009). *Cyber Incident Communication Structure* (Power Point Presentation).

Beaudoin, L., & Genik, L. (2010). *Review and Coordination of Cyber Security for Vancouver 2010*. Paper presented at the Knowledge Systems for Coalition Operations 2010

Beaudoin, L., & Genik, L. (2010). *Vancouver 2010 Key Cyber Stakeholders* (Power Point Presentation).

Beaudoin, L., Scheurkogel, N., & Genik, L. (2010). *Vancouver 2010 Cyber Security Review* (Letter Report).

Bélanger, M., Sahi, A., & Guitouni, A. (2008). *Synthesis: Lessons Learned From CIS Deployments* (PowerPoint Presentation - S).

Berends, H., Boersma, K., Weggeman, M. (2003) The structuration of organizational learning. Human Relations, 56(9): 1035-1056.

Bicocchi, N., William Ross, Mihaela Ulieru. An Agent-Based Approach for Collaboratively Modelling and Simulating Emergency-Response Organizations, 2010. http://www.cs.unb.ca/~ulieru/Publications/Bicocchi_CRIS2010.pdf

Billyard, A. P., & Collin, I. A. (2008). *Vancouver 2010 Olympics: Identifying CF Communication Issues Associated with the CH-146 Acting as Interceptor (not yet received)* (Technical Memorandum - S(CEO)).

Boury-Brisset, A.-C., Dessureault, D., Gagnon, M., & Gouin, D. (2009). *Information Sharing Option Analysis* (External Client Report).

CAE (2008). *IR Manager - Federation Requirements* (Contractor Report).

CAE (2008). *IR Manager - Functional Requirements* (Contractor Report).

CAE (2008). *IR Manager - Security Requirements* (Contractor Report).

CAE (2008). *IR Manager- JCDS 21 Integration Requirements* (Contractor Report).

CAE (2008). *JCDS TDP TA21 IR Manager 3.8 - System Design Specification (SDS) Design Changes* (Contractor Report).

CAE (2009). Information Request Manager (Version 4.0.0) [Installation Disks].

CAE (2009). *Information Request Manager 4.0 - Configuration Plan* (Contractor Report).

CAE (2009). *Information Request Manager 4.0 - System Administrator Guide* (Contractor Report).

CAE (2009). *Information Request Manager 4.0 Software Installation Plan* (Contractor Report).

CAE (2009). *Information Request Manager (IRM) Administrator Training* (Power Point Presentation).

CAE (2009). *Information Request Manager (IRM) User Training* (PowerPoint Presentation).

CAE (2009). *IR Manager Federation Deployment - Test Plan* (Contractor Report).

CAE (2009). *IR Manager Federation Deployment - Test Report* (Contractor Report).

Cardellini, V., E Casalicchio, E Galli, Agent based modelling of critical infrastructures interdependencies through UML. SpringSim 2007. Proceedings of the 2007 spring simulation multiconference - Volume 2. Society for Computer Simulation International 2007.

Carroll, J.S. (1995) Incident Reviews in High-Hazard Industries: Sense Making and Learning Under Ambiguity and Accountability. Organization and Environment, Vol 9 (2): 175-197.

Carson, N., & Caron, J.-D. (2010). *Vancouver 2010 Olympics: Collateral Damage Considerations (not yet received)* (Letter report - S (CEO)).

Carson, N., & Caron, J.-D. (2010). *Vancouver 2010 Winter Olympics - Intercept and Engagement Platform Options Analysis (not yet received)* (Technical Memorandum).

Carson, N., Caron, J.-D., & Bourdon, S. (2009). *Vancouver 2010: Defence Against the Asymmetric Air Threat (not yet received)* (Scientific Literature - S).

Carson, N., Caron, J.-D., Bourdon, S., & de Jong, P. (2010). *Vancouver 2010 Winter Olympics - A Spatial and Temporal Analysis of the Asymmetric Air Threat (not yet received)* (Technical Report - S (CA/US Eyes Only)).

Cazzolato, F., Dooley, P. W., & Henderson, M. D. (2009). *Ex BLUE Magnetometer Sensitivity Tests: Preliminary Findings* (Power Point Presentation - PB).

Chouinard, P. (2008). *Briefing to the Office of the Coordinator for 2010 Olympics and G8 Security* (Power Point Presentation).

Chouinard, P. (2009). *Feedback on the Joint Emergency Liaison Committee (JELC) Data Collection Spreadsheet* (Letter Report).

Chouinard, P. (2009). *Overview of the V2010 Infrastructure Criticality Study* (Letter Report).

Chouinard, P., & Genik, L. (2009). *Vancouver 2010 Olympics Critical Infrastructure - Final Criticality Assessment* (Letter Report - PB).

Chouinard, P., Verga, S., & Baingo, D. (2009). *Vancouver 2010 Olympics Critical Infrastructure - Final Criticality Assessment* (Letter Report - S).

Chouinard, P , et al. Modeling of CI interdependencies, Grand Challenges in Modeling, Simulation, and Analysis for Homeland Security, MSAHS-2010, Washington DC , March 17-18, 2010.

Ciancamerla E and M Minichino, Tools and techniques for interdependency analysis. IRRISS Report D 2.2.2, 2007

Coates, C., & Perlin, M. (2009). *Ergonomic and Layout Analysis of the Joint Task Force (Games) Operations Centre* (Contractor Report-PB).

Coates, C., Perlin, M., & Stewart, A. (2009). *Ergonomic and Layout Analysis of the Integrated Command Centre* (Contractor Report).

Couillard, M., & Saunders, P. *Vancouver 2010 Burrard Inlet Patrol Boat Requirements* (PowerPoint Presentation).

Couillard, M., & Saunders, P. (2010). *Vancouver 2010" Burrard Inlet Patrol Boat Requirements (not yet received)* (Letter Report).

Crowe, V. (2010). *MFP-TDP Canadian Underwater Protection System trials - September 14-30, 2009* (Letter Report).

Desharnais, F. *Options Analysis for the Waterside Security of the Olympic Village* (Letter Report - PB).

Desharnais, F., Crowe, V., Hazen, M., Chaisson, S., Crawford, A., Labbe, J.-N., et al. (2010). *Options Analysis for Waterside Security (DRAFT - PB)* (External Client Report).

Dixson, M. (2008). *Analysis of Integrated Command Centre C2 Network Architecture Options - Results from the 9 May 2008 Video Teleconference* (Lettter Report).

Dixson, M., Funk, R., Allen, D., Desrosiers, M., Goodman, L., Gouin, D., et al. (2009). *Exercise Gold: DRDC Analysis Quick Look* (Letter Report - PB).

Dixson, M., & Genik, L. (2010). *Application of Command and Control Architecture Frameworks for Security and Emergency Management Planning*. Paper presented at the NATO MSG 082 Workshop, 3-5 May 2010.

Dixson, M., Genik, L., Baingo, D., & Bureaux, J. (2008). *DRDC Validation Support Team - Observations and Lessons Identified: Exercise Bronze* (Technical Note).

Dooley, P. W. (2007). *Vancouver 2010 Vehicle Search Area Process Model: Preliminary Development* (Power Point Presentation).

Dooley, P. W. (2008). *Mock Area Screening Exercise (Ex MOCKASIN) Quicklook Report 1* (Letter Report -PB).

Dooley, P. W. (2008). *PSA Calculator v3.1.2: A Tool for Best-Case V2010 Pedestrian Screening Area Estimates* (Letter Report - PB).

Dooley, P. W. (2008). *Simplified Ambient Air Heating Calculation* (Working Document).

Dooley, P. W. (2008). *Vancouver 2010 VISTA-VSA Model: Interim Development* (Power Point Presentation - PB).

Dooley, P. W. (2009). *Exercise BLUE Analysis 1: Walk-Through Magnetometer Characterization* (Power Point Presentation - PB).

Dooley, P. W. (2009). *Exercise BLUE Analysis 2: Pedestrian Screening Area Operations* (Power Point Presentation - PB).

Dooley, P. W. (2009). *Instrument Configuration & Evaluation Exercise (Ex ICE): Quicklook Results* (Power Point Presentation - PB).

Dooley, P. W. (2010). *Aides-Memoire for V2010 Vehicle Screening Area Personnel* (14 Working Documents - PB).

Dooley, P. W. (2010). *Potential Planning Considerations for G8 and G20 Summits (Draft)* (Working Document - PB).

Dooley, P. W. (2010). *Science-Based Planning Support to Vancouver 2010 Security: Two Case Studies*. Paper presented at the Knowledge Systems for Coalition Operations 2010 Conference.

Dooley, P. W. (2010). *Vancouver 2010 Vehicle Screening Area Experimentation 1 - Mock Area Screening Exercise (Ex MOCKASIN)* (Draft Technical Report).

Dooley, P. W., Cazzolato, F., Drolet, F., Henderson, M. D., Keefe, A., Terhaar, P., et al. (2009). *Exercise Blue Analysis 1: Characterization of the Walk-Through Magnetometer Response* (Letter Report - PB).

Dooley, P. W., Dixson, M., Evans, J., & Naprstek, T. (2010). *Exercise Blue Analysis 3: Vehicle Screening Area Operations* (Letter Report - PB).

Dooley, P. W., Terhaar, P., Cazzolato, F., Drolet, F., Henderson, M. D., Keefe, A., et al. (2009). *Exercise Blue Analysis 2: Pedestrian Screening Area Operations* (Letter Report - PB).

Duncan, P., Lombardi, B., Saunders, P., & Zegers, A. (2008). *Force Protection Matrix Game - Marine One: Post-Game Observations* (Letter Report - PB).

EMBC (2009). *British Columbia Chemical, Biological, Radiologica, Nuclear and Explosives Terrorism Response Plan (DRAFT)* (Contractor Report).

Emergency Management BC (2010). Vancouver 2010 Integrated Connectivity Schematic. In EMBC_C2_V2010ConnectivitySchematic (Ed.).

Erhardt, L. S. (2009). *Canadian RN Deployment for Vancouver 2010 in Support of CBRN Security*. Paper presented at the NATO RNDSG Meeting.

Erhardt, L. S., Sparkes, S., Quayle, D., Ellaschuk, B., Kenny, P., Morris, R., et al. (2009). *Canadian Radiological Emergency Response Exercise Scenarios Using Both Sealed and Unsealed Radioactive Sources*. Paper presented at the 54th Annual Meeting of the Health Physics Society.

Fujitsu (2009). *Major Events Coordinated Security Solutions (MECSS) - Framework Options Analysis* (Contractor Report).

Fujitsu (2010). *IRM Deployment Options* (Contractor Report).

Fujitsu (2010). *IRM Deployment Recommendation* (Contractor Report).

Fujitsu (2010). *Major Events Coordinated Security Solutions (MECSS) - Functional Requirements V1.1* (Contractor Report).

Fujitsu (2010). *Major Events Coordinated Security Solutions (MECSS) - MESF Framework Content - Document Descriptions V1.1* (Contractor Report).

Fujitsu (2010). *Major Events Coordinated Security Solutions (MECSS) - MESF Framework Content - Process Descriptions V1.1* (Contractor Report).

Fujitsu (2010). *Major Events Coordinated Security Solutions (MECSS) - MESF Framework Content - Role Descriptions V1.1* (Contractor Report).

Fujitsu (2010). *Major Events Coordinated Security Solutions (MECSS) - MESF Operational Task Analysis V1.1* (Contractor Report).

Fujitsu (2010). *Major Events Coordinated Security Solutions (MECSS) - MESF Work Plans V1.2* (Contractor Report).

Fujitsu (2010). *Sustaining and Evolving GC2.0 Internal Collaborative Tools* (Contractor Report).

Funk, R. (2008). *Observations on Pegasus Guardian II and the V2010 C2 Framework* (Power Point Presentation).

Funk, R. (2008). *V2010 Vehicle Search Area Capacity: Review of Modeling and Planning Assumptions* (Power Point Presentation - PB).

Funk, R. (2009). *Integrated Security Architecture Modeling and Process Mapping - Extract from Full Version* (Contractor Report).

Funk, R., Breton, R., & Maceda, E. (2008). *Initial Analysis of JTFG GJOC Pegasus Guardian 2 CPX During Ex Bronze in Richmond, BC* (Letter Report - PB).

Funk, R., & Dooley, P. W. (2008). *Quicklook Analysis of V2010 Vehicle Search Area Capacity based on VANOC Planning Assumptions* (Power Point Presentation - PB).

Funk, R., Zegers, A., Breton, R., & Hazen, M. (2009). *Initial Analysis of JTFG Participation in Pegasus Guardian 2.2 Command Post Exercise and Ex Silver at Richmond, BC* (Letter Report - PB).

Gauthier, Y., & Adamsson, J. (2010). *Modelling and Simulation Tools for Decision Support to Canada Command* (DRAFT Technical Report).

Gauthier, Y., & Gammon, M. (2009). *Analytical Support to Canada Command During Exercises Silver and Staunch Maple 09 (February 9-12, 2009)* (Letter Report).

Genik, L., & Lauder, M. (2009). *Analysis of Provincial Regional Operations Centre (PREOC) Operations During Exercise Silver February 9-12, 2009* (Letter Report).

Genik, L., Lauder, M., & Maceda, E. (2009). *Analysis of EMBC's South West Provincial Regional Operations Centre (PREOC) Operations during Exercise Gold* (Letter Report).

Gerber, J. D., Carson, N., & Caron, J.-D. (2010). *Analytic Visualization Tool (AVT) Vancouver 2010 Olympics Air Defence Case Study* (Contractor Report - S (CA/US Eyes Only)).

Goodman, L. (2010). *Outbrief - Scientific Advisor to RCMP G8/G20 Sumits Integrated Security Unit* (Letter Report).

Gouin, D., & Trinh, K. (2008). *Battle Rhythm Requirements* (Power Point Presentation).

Gouin, D., & Trinh, K. (2008). *TCC Layout Recommendations* (Letter Report - PB).

Gouin, D., & Trinh, K. (2008). *Theatre Command Centre - Bridge Layout Options* (Power Point Presentation).

Gouin, D., & Trinh, K. (2008). *Theatre Command Centre Layout* (Power Point Presentation).

Gouin, D., & Trinh, K. (2008). *Trip Report from Meeting with the ISU/JTFG - BattleRhythm* (Trip Report).

Guitouni, A. (2010). *C4ISR Mobile Lab Specs* (Power Point Presentation).

Hales, D. (2008). *Vancouver 2010 Olympic Security Unit: Concept of Operations Summary Presentation* (Power Point Presentation).

Hales, D., & Miller, J. (2008). *Vancouver 2010 Integrated Security - Command and Control Concept of Operations* (Contractor Report).

Hales, D., & Miller, J. (2008). Vancouver 2010 Integrated Security: Command and Control Concept of Operations Narrative (Contractor Report).

Hales D. and Andrea Scipione, Joint Command Decision Support for the 21st Century (JCDS 21) Technology Demonstration (TD) Project Concept of Operations (CONOPs), DRDC Corporate DRDC-CR-2008-002, 2008.

Hales, D., & Miller, J. (2010). *Vancouver 2010 Integrated Security Command and Control Architecture: Concept of Operations Stakeholders' Analysis and Narrative* (Contractor Report - PB).

Hales, D., Miller, J., & Poursina, S. (2009). *Integrated Security Architecture Modelling and Process Mapping: Analysis of Vancouver 2010 Olympics Integrated Security Process* (Contractor Report).

Hales, D., Miller, J., & Poursina, S. (2010). *Vancouver 2010 Integrated Security Command and Control Architecture - Modeling and Process Mapping* (Contractor Report - PB).

Hassaine, F, Andrew Vallerand and Paul Hubbard, Concept, Architecture, and Design of a Stand-Alone Physics-Based Simulation Capability to Support Maritime-Air Littoral Tactics Development, DRDC Ottawa TR 2005-229, 2005.

Hayat, Z., Reeve, J., Boutle, C. Electronic Security Implications of NEC: A Tactical Battlefield Scenario, RUSI Conf, UK, http://eprints.ecs.soton.ac.uk/12274/1/RUSI_pi_nec2.pdf

Hewitt, A., & Crowe, V. (2009). *Maritime Force Protection TDP Underwater Component build 3 Trial SITREP* (Letter Report).

Hill, A., & Kaluzny, B. L. (2009). *DRDC CORA SUPPORT TO VANCOUVER 2010 OLYMPICS: SCHEDULING OF INTEGRATED SECURITY UNIT PERSONNEL* (Letter Report - PB).

Hill, A., & Kaluzny, B. L. (2009). *SCHEDULING V2010-ISU SECURITY PERSONNEL: A CASE STUDY* (Letter Report - PB No. 3553-1 (DMGOR AST).

Hill, A., & Kaluzny, B. L. (2010). *Scheduling Security Personnel for Vancouver 2010 Olympic Venues* (Technical Report).

Hollman, J. A. , J. R. Martí, Real Time Network Simulation with PC-Clusters, IEEE Transactions on Power Systems, Vol. 18, No. 2, pp. 563-569, May 2003.;

IBM (2009). *ILOG OPL Development Studio: Scheduling of Personnel Workshifts User Guide* (Contractor Report).

ISR Inc (2008). *V2010 Federal CBRNE Capabilities* (Contractor Report).

ISR Inc (2008). *Vancouver 2010 Olympics - V2010 Federal CBRNE Technical Assistance Team Concept of Operations* (Contractor Report).

ISR Inc (2009). *BC First Responder CBRNE Refresher Course* (Power Point Presentation).

ISR Inc (2009). *BC Mass Decontamination Concept of Operations (CONOPS)* (Contractor Report).

ISR Inc (2009). *C2010 - Live CBRNE Exercises: Guide for Players* (Contractor Report).

ISR Inc (2009). *CSS/MECSS V2010 CBRNE Sensor Suite Plan: Accommodation Vessels* (Contractor Report).

ISR Inc (2009). *CSS/MECSS V2010 Gold Training and Exercise Plan* (Contractor Report).

ISR Inc (2009). *Gold - CBRNE Exercises: Controller's Manual* (Contractor Report).

ISR (2009). *Gold Live CBRNE Exercises 2009: Source Management Plan* (Contractor Report).

ISR Inc (2009). *V2010 BC CBRNE Capability Analysis: Part 1 - Summary and Gap Identification* (Contractor Report).

ISR Inc (2009). *V2010 BC CBRNE Capability Analysis: Part II - Assessment Data* (Contractor Report).

ISR Inc (2009). *V2010 CBRNE Tabletop Exercise (TTX) Concept of Operations (CONOPS)* (Contractor Report).

Jaurez, H., & Marti, J. R. (2009). *Case Study: Transportation & Treatment of BC Place Victims During V2010 Olympics* (Contractor Report).

Jones, T., & Larsson, C. L. (2010). *Training Workshop on the Sensitive Directional Gamma-Ray Probe* (Power Point Presentation).

Jong, P. d. (2009). *Exercise Silver TPS-70 Electromagnetic Interference Problem: An OR Perspective* (Letter Report).

Johnson, C. W. (2006). A Brief Overview of Technical and Organizational Security at Olympic Events. Glasgow: University of Glasgow.

Johnson, C.W. (2008), "Understanding failures in International Safety Infrastructure: A Comparison of European and North American Power failures", *Proceedings of the 26th International Conference on System Safety*, Vancouver, BC, Canada, August 2008.

Kaluzny, B. L., & Hill, A. (2010). Scheduling Security Personnel for the Vancouver 2010 Winter Olympic Games. [DRAFT Journal Article]. *Journal of Scheduling*.

Kaluzny, B. L., & Hill, A. (2010). *Security Scheduling and a Qualitative MCDA Method (not yet received)* (Powerpoint Presentation).

Karthaus, C. L. F., Hall, C. D. T., & Martin, L. B. (2009). *Analysis of Collaboration Among Operational Teams Involved in Security During the Vancouver 2010 Olympic Games* (Contractor Report - PB).

Keefe, A., Lamb, M., Terhaar, P., Au, H., & Maceda, E. (2009). *Human Factors Issues Affecting Security Personnel Working at the Vehicle Screening Areas (VSA) and Pedestrian Screening Areas (PSA)* (Letter Report - PB).

Khouj, M. T., & Marti, J. R. (2010). *Modeling Critical Infrastructure Interdependencies in Support of the Security Operations for the Vancouver 2010 Olympics* (Technical Report).

Larsson, C. L. (2009). *Canadian Radiological Field Exercise*. Paper presented at the ITWG Nuclear Forensic Laboratories Meeting.

Larsson, C. L. (2009). *Radiological and Nuclear Terrorism Overview for the vancouver Police Department Radiological Roensic Exercise Training (Power Point Presentation)* (Power POint Presentation).

Larsson, C. L. (2010). *Radiological and Nuclear Detection Architecture for V2010*. Paper presented at the STIG Meeting.

Lauder, M., McIntyre, S., Zegers, A., & Funk, R. (2010). *Exercise Laurel Wreath 1001 Results for Games Red Team* (Letter Report - PB).

Lavigne, S., Kitching, F., McCall, M., & Sykes, T. (2009). *V2010 CBRNE Tabletop Exercise 2009 (TTX-09)*.

Lavigne, S., Morris, R., McCall, M., & Sykes, T. (2009). *V2010 CBRNE Live Play Exercise 2009: After Action Report* (Contractor Report - PB).

Lavigne, S., Nguyen, T., McCall, M., & Sykes, T. (2009). *Exercise Initial Thunder 2008: After Action Report* (Technical Note).

Lee, J. J. (2008). *Underwater Explosion Threat Assessment for the False Creek Inlet in the Athlete's Olympic Village* (Letter Report - PB).

LeGallais, General C, Defining UK National Security and Resilience Issues , UK Cabinet Office Brief, Institute of Water Conference, 2009. http://www.instituteofwater.org.uk/images/eventImages/CharlesLeGallais1126.pdf

Lemyre, L. (2008). Orientation Notes on Evidence-based Guidance For Promoting Psychosocial Preparedness (Letter Report).

Li, L., Localization in self-healing autonomous sensor networks (SASNet), DRDC Ottawa TR 2008-020 2008,

Loermans, J. (2002) Synerfizing the learning organization and knowledge management. Journal of Knowledge Management. Volume 6, Number 3, 2002.pp. 285-294

Martec (2009). *Approach Report for BC/GMP and Athletes' Village Blast Modeling* (Contractor Report - S).

Martec (2009). *CSS Support - Site 1 Report: Summary of BC/GM Place Modelling Results* (Contractor Report - S).

Martec (2009). *CSS Support - Site 2 Report: Summary of Athlete's Village Modeling Results* (Contractor Report - S).

Martec (2009). *Large Scale Facility Modeling - BC Place Roof Analysis* (Contractor Report - S).

Marti, J. R. (2009). *I2Sim to Support CoV Emergency Response* (Contractor Report).

Marti, J. R. (2009). *Vulnerabilities and Mitigation Strategies: Downtown Vancouver, 2010* (Contractor Report).

Masys, A. (2009). *Exercise Gold After Action Report: National Operations Centre (NOC)* (Letter Report - PA).

Masys, A. J., Belanger, M., Gouin, D., & Wood, D. (2009). *National Operations Centre (NOC) Table-Top Exercise (TTX): After Action Report* (Letter Report - PB).

Maxwell, D., Silva, D. D., Shubaly, D., & Ltd., M. S. (2010). *Underwater Component Support for OP PODIUM (DRAFT)* (Contractor Report).

McGroder, D.P. An Emerging DoD M&S Enterprise Data

Strategy 2011 Spring SIW Paper 11S-SIW-029, 2011.

McIntyre, S. (2008). *CAPEX08: Lessons Learned* (Letter Report - PB).

McLellan, T., & Paul, M. (2010). *Guidance for Heat Stress and Sleep for G8/G20* (Power Point Presentation).

Mitrovic-Minic, S., Guitouni, A., & Zwick, H. (2010). *Risk Aggregation Methodology for Emergency Management*. Paper presented at the FIRST REGIONAL CONFERENCE OF THE EUROPEAN DECISION SCIENCES INSTITUTE.

Moore, Wermuth, et al, "Bridging the Gap: Developing a Tool to Support Local Civilian and Military Disaster Preparedness," RAND Center for Military Health Policy Research, April 2010.

Nadeau, C., & Wood, S. (2009). *Major Events Security Framework: Information Sharing and Knowledge Management Final Report* (Contractor Report).

Niall, K., A summary of proceedings for the Advanced Deployable Day/Night Simulation Symposium, Niall, K.K., DRDC-TORONTO-TR-2009-121

Parise, S. (2007) Knowledge Management and Human Resource Development: An Application in Social Network Analysis Methods. Advances in Developing Human Resources Vol. 9, No. 3 August 2007. pp.359-383.

Pourian, I. (2009). *New Thinking on Major Event Safety and Security* (Contractor Report).

Quayle, D. (2009). *Observations on the Employment of CBRN Scientific Advisors in Support of the National CBRNE Response Team During Exercise Silver Febrary 9-12, 2009* (Letter Report - PB).

Rahman, Beznosov and Marti (2006

Reedel, G., & Nadeau, C. (2009). *Development of an Ontology in Support of JCDS 21 Final Report* (Contractor Report).

Rehak, L., McDermott, K., Famewo, J., & Martin, L. B. (2008). *Final Synthesis Report for Social Network Analysis of Joint Interagency Multinational & Public (JIMP) Operations* (Contractor Report).

Robert , B and Luciano Morabito. An approach to identifying geographic interdependencies among critical infrastructures. International Journal of Critical Infrastructures Volume 6, Number 1 , 17-30, 2010.

Robert, B. A method for the study of Cascading effects within lifeline networks Int J Critical infrastructure 1,1 2004.

Saunders, P. (2008). *Marine Security Technology Survey* (Letter Report).

Senge, P. (2006) *The Fifth Discipline: The Art and Practice of the Learning Organization*, New York: Doubleday Currency.

Sitkin, S. B. (1992). Learning through failure: The strategy of small losses. In B. M. Staw & L.L. Cummings (Eds.), Research in organizational behavior (pp. 231-266). Greenwich, CT: JAI.

Smith, D., Allen, D., Dooley, P. W., Hawton, A., & Pavlovic, N. (2008). *Initial Analysis of ISU Theatre Command Centre (TCC) Operations During Exercise Pegasus Guardian II (November 12-14, 2008)* (Letter Report - PB).

Smith, D., Allen, D., Hawton, A., & Dixson, M. (2009). *Initial Analysis of ISU Theatre Command Centre (TCC) Operations During Exercise Pegasus Guardian 2-2 and Exercise Silver (February 2-12, 2009)* (Letter Report - PB).

Smith, D., & Chow, R. (2008). *Analysis of Responses to the OMOC Information Sharing Questionnaire* (Letter Report).

Smith, D., Genik, L., Maceda, E., & Masys, A. (2010). *Vancouver 2010 PREOC Operations Report* (Letter Report).

Steele, J. (2009). *On Observations and Assessment of Joint Interface Control Cell (JICC) Operations During Ex Staunch Maple* (Letter Report - S).

Steele, J. (2010). *On CF Tactical Data Link Capability Development* (Letter Report).

Sykes, T. (2010). Science Town Fact Sheet English.

Sykes, T. (2010). Science Town Fact Sheet French.

Systems Engineering Fundamentals. Defense Acquisition University Press, 2003.)

Taleb, N.N. (2007), *The Black Swan: The impact of the highly improbable,* Penguin Books Ltd., London.

Tapscott, D. and Williams, A.D. (2006) Wikinomics: How mass collaboration changes everything. Portfolio, New York.

Ulieru, Mihaela . UNB Canada Research Chair, Enabling the Self Organizing Security Network . Proceeding report, 2009.
http://www.cs.unb.ca/~ulieru/Publications/Ulieru-Formatted-Final-sos.pdf

Vallerand, A.L., Kim, B., Youssef, R. , Hubbard, P., Skinner, D., Murray, B., Poursina, S, Herdman, C.M., Gamble, M., Hagen, L., Bleichman, D., Kurts, D., Kruk, R., Lavoie, R., Gladstone. K.G. SYNTHETIC ENVIRONMENTS AT THE ENTREPRISE LEVEL: OVERVIEW OF A GOVERNMENT OF CANADA (GOC), ACADEMIA and INDUSTRY DISTRIBUTED SYNTHETIC ENVIRONMENT INITIATIVE, DRDC Ottawa Technical Memorandum 2005-130, 2005.

Vallerand, A.L., Osgoode, K., De Jager C. Defence Against Terrorism Case Study: Simulation-Based Technical Framework to Address Changes In Capability Deficiency NATO Modelling & Simulation Group (MSG) Conference MSG 056-09, 1-9, 2007

Vallerand, A.L., et al. Guide to Modelling and Simulation for NATO Network enabled capability. NATO Modelling and Simulation Group MSG-062. Report, AC/323(MSG-062)RTG-039, RTO-TR-MSG-062, Jun 2009

TONGCO A., G. V. JAPOS Integration of Geographic Information Systems (GIS) to Enhance Academic Capability of Philippine Higher Education Institutions Asian Journal of Business and Governance Vol. 1 No. 1 January 2011 ISSN: 2094-9251 pp. 1-18

Ventura,, C.E., H. Juarez Garcia, K. M. Thibert, J. Martí and J. Hollman. Mapping of interdependencies through integrated hazard analysis: study case of a Canadian university campus. The 14th World Conference on Earthquake Engineering October 12-17, Beijing, China, 2008.

Vera, D., Crossan, M. (2005). Organizational Learning and Knowledge Management: Toward an Integrative Framework.

Verga, S., Chouinard, P., & Baingo, D. (2008). *The Critical Infrastructure Asset Ordination (CIAO) Model* (Technical Memorandum).

Wang, W. (2009). *Joint Command Support through Workspace Analysis, Design and Optimization* (Technical Report).

Weick, K. E. (1987, Winter). Organizational culture as a source of high reliability. California Management Review, pp. 112-127.

Woods, D.D. (2006), "Essential Characteristics of Resilience", In Hollnagel, E., Woods, D.D., Leveson, N. (Eds), *Resilience Engineering: Concepts and Precepts*. Ashgate Publishing. Aldershot, Hampshire England, pp. 21-34.

Wood, D. (2009). *Analysis Report Pegasus Guardian III - NOC Observations* (Letter Report - PB).

Xwave Inc (2009). Information Request Manager (Version 3.8.0) [Source Code].

Yee, E. (2010). *An Operational Implementation of a CBRN Sensor-Driven Modeling paradigm for Stochastic Event Reconstruction: Technical Description of an Advanced Modeling Component of CRTI PRoject 07-0196TD)* (DRDC Suffield TR 2010-999, 2010).

Yee, E., Lien, F.-S., & Ji, H. (2010). *A Building-Resolved Wind Field Library for Vancouver: Facilitating CBRN Emergency Response for the 2010 Winter Olympic Games (DRAFT)* (Technical Memorandum).

Zegers, A. (2008). *Trip Report to Force Protection Matrix Game Darwin Australia - 23-30 June 2008* (Trip Report).

Zegers, A. (2009). *Analysis of OMOC Participation in Exercise Gold* (Letter Report - PB).

Zegers, a. (2010). *Matrix Game Methodology Development and Employment for Vancouver 2010 Olympics Marine Security Planning (not received yet)* (Scientific Literature).

Zegers, A., & Hazen, M. (2009). *Analysis of OMOC Participation in Exercise Pegasus Guardian 3* (Letter Report - PB).

Zegers, A., & Saunders, P. (2008). *Force Protection Matrix Game - Marine Two: After Action Report* (Letter Report - PB).

Zegers, A., Saunders, P., Rudd, D., & Sand, M. B. (2009). *Integrated Safety/Security Matrix Game - Marine III: After Action Report* (Letter Report - PB).

This page intentionally left blank.

DOCUMENT CONTROL DATA		
(Unclassified)		
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.) CSS		2. SECURITY CLASSIFICATION (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.) MODELLING, SIMULATION AND ANALYSIS (MS&A): POTENT ENABLING TOOLS FOR PLANNING AND EXECUTING COMPLEX MAJOR NATIONAL EVENTS		
4. AUTHORS (last name, followed by initials – ranks, titles, etc. not to be used) Masys, Anthony; Vallerand, Andrew		
5. DATE OF PUBLICATION (Month and year of publication of document.) October 2011	6a. NO. OF PAGES (Total containing information, including Annexes, Appendices, etc.) 61	6b. NO. OF REFS (Total cited in document.) 109
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.) CSS		
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 CSS TM 2011-20		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.) UNCLASS, UNLIMITEDUnlimited		
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.)

Modelling, Simulation & Analysis (MS&A) are known as crucial, effective and efficient enablers of Defence Communities from Concept Development & Experimentation (CD&E) to Training. In Public Safety and Security in general and in particular in recent complex major national events such as the Vancouver 2010 Olympics, the impact of MS&A has been significant, though far less known. Drawing upon case studies, this report argues that MS&A is a potent enabling tool for Defence & Security Communities not only from CD&E to Training, but in all aspects of Capability, from Strategy/Policy to Capability Development, Capability Generation, Capability Employment and Network Enabled Capability (NEC). The methodologies by which MS&A became a crucial enabler to ensure safe and secure conduct of the Vancouver 2010 Olympics and G8/G20 Summits are highlighted in this report. Given the recurrent nature of complex major national events as well as the growing requirement to efficiently test and validate Emergency Management Plans and Business Continuity Plans, a persistent capability framework to support (National and International) Major Events security and safety planning and operations has been undertaken that includes a persistent and credible S&T and MS&A capability. This persistent capability is in many ways comparable with the DoD Information Analysis Centers (IACs; http://iac.dtic.mil/) and the DHS Simulation and Analysis Center (http://www.dhs.gov/xabout/structure/gc_1257535800821.shtm). MS&A products and lessons learned, in particular when they are leveraged in the Major Event Security Framework, could provide efficient analysis, insight and support to other Major Events including, London 2012 Olympics, 2015 Commonwealth Games in Toronto as well as the Cross-border Management of Emergencies, such as earthquakes, floods and forest fires. In conclusion, though at first brush the use of MS&A in Public Safety and Security does not seem to be as wide and deep and does not seem to be similarly "crowned" by large International distributed simulated training like in Defence, their valued-use was documented as clearly growing. This Report concludes that MS&A represent significant potent enabling tools that contribute significant value and impact as well as efficiency and effectiveness to Public Safety and Security in general and in particular to support safety and security at complex major national events. Decision makers seeking efficiency and effectiveness are thus encouraged to increasingly use or re-use Public Safety and Security M&S in their analyses.

La modélisation, la simulation et l'analyse (MS & A) s'avèrent être un outil habilitant des milieux de la défense, connu pour son efficacité et sa nécessité dans l'élaboration et l'expérimentation de concepts (EEC) ainsi que dans l'instruction. Quoique moins connues, les répercussions de la MS & A sur la sécurité publique en général et lors d'événements complexes d'envergure nationale tels que les Jeux olympiques de 2010 à Vancouver sont importantes. Suite à une recherche factuelle, les auteurs de ce rapport soutiennent que la MS & A est un outil habilitant utile aux communautés de la sécurité et de la défense, que ce soit pour l'EEC, l'instruction ou tout aspect de la capacité (stratégie, politiques, développement, production, emploi, opérations facilitées par réseaux [OFR]). Ils y énoncent les méthodologies qui ont fait du MS & A un élément essentiel pour la sécurité des Jeux olympiques de 2010 à Vancouver et des sommets du G8 et du G20. En raison du caractère récurrent des événements complexes d'envergure nationale et des besoins croissants d'évaluation et de validation des plans de gestion des mesures d'urgence et de continuité des opérations, une structure permanente a été mise sur pied afin de soutenir la planification et les opérations de sécurité lors d'événements d'envergure nationale et internationale. Cette structure comprend une capacité constante et fiable en matière de S & T et de MS & A. À plusieurs niveaux, cette capacité récurrente est comparable aux centres d'analyse de l'information du DoD (http://iac.dtic.mil/) ainsi qu'au centre d'analyse et de simulation du DHS (http://www.dhs.gov/xabout/structure/gc_1257535800821.shtm). Les résultats de la MS & A de

même que les leçons retenues, surtout au niveau du cadre de sécurité des événements d'envergure, pourraient permettre une analyse, un aperçu et un appui efficaces lors d'autres événements tels que les Jeux olympiques de 2012 à Londres, les Jeux du Commonwealth de 2015 à Toronto et la gestion des cas d'urgence transfrontaliers (tremblements de terre, inondations, feux de forêt). Les auteurs de ce rapport ont conclu que la MS & A et sa grande utilité ont de la valeur et des effets sur : 1) la sécurité publique générale et spécifique et 2) l'appui à la sécurité lors d'événements complexes d'envergure nationale.

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.)

M&S; modeling, simulation, analysis, CD&E, training; security, network-enabled capability, NEC, strategy, policy, capability development, capability generation, capability employment , Olympics; safety; security, defence, complex national major events