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

DEFENCE R&D DÉFENSE

Implementing Capability Based Planning within the Public Safety and Security Sector

Lessons from the Defence Experience

Doug Hales
D Hales Consulting

Dr. Paul Chouinard
DRDC Centre for Security Science

Defence R&D Canada – Centre for Security Science
DRDC CSS TM 2011-26
December 2011

Canada

Implementing Capability Based Planning within the Public Safety and Security Sector

Lessons from the Defence Experience

Doug Hales
D Hales Consulting

Dr. Paul Chouinard
DRDC Centre for Security Science

Defence R&D Canada – CSS

Technical Memorandum
DRDC CSS TM 2011-26
December 2011

Principal Author

Original signed by Doug Hales

Doug Hales

D Hales Consulting Inc.

Approved by

Original signed by Jack Pagotto

Jack Pagotto

Section Head ESEC S&T

Approved for release by

Original signed by Mark Williamson

Mark Williamson

DRDC CSS DDG- DRP Chair

Abstract

Capability Based Planning (CBP) has been described as the “gold standard” and has now been in use in military communities for just over a decade. Use is now being extended to public safety and security. This report reviews the environmental impetus, founding principles and initial expectations, and reflects on lessons learned and best practices. It identifies both some of the inherent issues with CBP and some of the unique challenges involved in applying CBP in the public safety and security realm. It concludes by offering some thoughts on the Way Ahead.

Résumé

La planification fondée sur les capacités (PFC) a été décrite comme étant « l’étalon-or » et est utilisée par les collectivités militaires depuis un peu plus de dix ans. Son utilisation est maintenant élargie à la sécurité publique. Le présent rapport examine les mesures incitatives environnementales, les principes fondateurs et les attentes initiales. Le document offre aussi une réflexion sur les leçons retenues et les pratiques exemplaires. Il décrit également certains des problèmes inhérents à la PFC et quelques-uns des défis particuliers présents dans l’application de la PFC dans le domaine de la sécurité publique. Le document se termine en présentant quelques réflexions sur l’avenir.

Executive summary

Implementing Capability Based Planning within the Public Safety and Security Sector: Lessons from the Defence Experience

Doug Hales; Paul Chouinard; DRDC CSS TM 2011-26; Defence R&D Canada – CSS; December 2011.

Introduction: Capability Based Planning (CBP) was introduced in the 1990s to address the inherent ambiguity in the post-Cold War security setting. It offered a credible alternative to threat based planning and a means to address environmental uncertainty. CBP has subsequently been adopted by close Allies and was recently described as the 'gold standard'. Use of CBP is being extended to the public safety and security sector and application has drawn on the experience and practices from defence. While there are lessons learned and practises which can be imported it should also be noted that public safety and security face unique challenges.

Results: There is general agreement on the intent and core principles of CBP:

- Planning should start with a holistic appreciation of the problem space and acknowledge the perspectives of all key stakeholder groups;
- A common logic model should be accepted to facilitate collaborative analysis and synthesis and a co-joined taxonomy adopted to ensure definitional consistency;
- Multiple, plausible and illustrative scenarios should be used to hedge against uncertainty and to test concepts and compare options;
- Requirements and gaps, and sometimes even plans, should be descriptive not prescriptive, and framed in terms of capabilities thereby encouraging innovative problem solving; and
- Constraints should be acknowledged and provision made for prioritization.

CBP builds on previous approaches to defence Force Development planning and institutionalization in Australia, Canada, the United Kingdom and the United States has varied. Doubt persists over whether CBP can be more than an analytical approach, whether it can also serve as an organizing principle. CBP anticipates and incorporates a shift towards centralised policy direction in response to the escalating interdependencies. In promoting a holistic perspective CBP confronts complex 'wicked problems' characterized by indeterminate and changing causal relationships. This has led to recognition of the need for continuous planning and the inadequacy of traditional processes.

Application efforts have also highlighted organizational challenges which are particularly pertinent to public safety and security. Although a shared vision and integrated concept is useful a CBP planning process must also reflect and respect individual stakeholder mandates, risk profiles, planning horizons and decision cycles.

The Technical Cooperation Programme (TTCP) Joint Systems and Analysis (JSA) Technical Panel 3 has developed and published a CBP logic model.[1] It presents a simplified and prescriptive exemplar. It does provide for arbitration and apportionment as a prelude to implementation but it does identify activity elements and associated products which would allow for a number of horizontal integration points.

A capability taxonomy is required to support analysis and synthesis. The ability to decompose and explore elements and at the same time fit and fuse findings is central to CBP. While perhaps ideal, a single common partitioning scheme has proved impractical. Typically a non-prescriptive, hierarchical catalogue is used to describe and aggregate the requirements derived from mission analyses of illustrative scenarios. Capabilities can be defined in terms of activities or outcomes. There are distinct advantages to the former for public safety and security, most notably the ability to clarify roles and responsibilities. At some point these must be assigned and related to physical assets, and capability planning linked to capability management. It is people and equipment rather than abstractions which are administered and deployed operationally. An additional third framework is often used to describe the components which enable and generate latent capability. In addition to recruiting people and acquiring equipment these include doctrine and training. Capability management and generation are usually the purview of individual and independent departments and agencies. The most pressing implementation challenge lies in developing and settling on a task categorization scheme and crosswalk mapping assets to capabilities.

Scenarios are an integral part of CBP. They provide context and a vehicle to share and capture assumptions. There is general agreement that a set of illustrative scenarios is required to represent the environment and allow for uncertainty. There is less agreement on how many scenarios should be in the set and the level of fidelity. The clear preference, political sensitivities permitting, is to ground scenarios in the "real" world reducing requirements to create artificial environments and facilitating the potential to transition to standing, contingency plans. There is a wealth of recent literature relating to selecting missions, characterising scenarios and articulating concepts of operations in terms of capability requirements. In short:

- Risk – incident probability and consequence - presents a common currency allowing for comparison and prioritization;

- Morphological approaches can then be used to validate scenario sets. Practice suggests that intended use determines the fidelity necessities; and

- Increasingly architecture frameworks are serving to discipline data collection, depict relationships and integrate enterprise perspectives.

It should not be surprising that there is often a diversity of views when it comes to deciphering ambiguity and interpreting, complex casual relationships. Hence CBP is part art and part science, and relies in part on Subject Matter Expertise. CBP borrows from emergent decision support techniques and combines best practices in hard and soft analysis. Value Focused Thinking

[1] The Technical Cooperation Program (TTCP) is an international partnership/organization established to facilitate technical information exchange and scientific collaboration and program harmonization and alignment between American, Australian, British, Canadian and New Zealand defence communities.

presaged the current emphasis on outcomes, technology has facilitated the solicitation of dispersed expertise applying Delphi techniques and Multi-Attribute Utility Theory provides a methodology for comparing and rank ordering alternatives. These are intended to be transparent not deterministic; caution should be exercised in interpreting and employing results, and note taken of the advantages of hedging and dangers of sub-optimization.

The centralization of policy authority is environmentally driven and a likely to induce some resistance. For its part CBP can contribute to building trust and to establishing policy coherence and promoting integrated planning. The public safety and security environment is unique - different from defence. Adoption and adaptation of CBP will reflect stakeholder diversity and must acknowledge the differences in priorities, capacities and organizational cultures. Initially it may serve more as an organizing principle but it can be used to foster a portfolio management approach where common cause is seen to exist. Patience, tolerance and leadership will be required, as will the acceptance that:

- Implementation pace and practice will vary;
- A bottom-up approach is likely to develop first and initially dominate; and
- Information sharing is a critical pre-requisite and will invoke transactional costs

CBP incorporates business planning and management trends and; in particular, is buttressed by evolving risk management and system engineering disciplines. Such external impetuses are unlikely to wane. Risk provides a common lens with which to assess natural hazards, industrial accidents and terrorist threats and to compare mitigation alternatives. System engineering brings to the fold an enterprise perspective and architectural frameworks a means for capturing interdependencies and modelling system operation. These representations provide both a communal view of a collective undertaking and a point of departure for collaborative exploration and incremental/spiral enhancement.

Significance: While for defence CBP represents an evolution, for public safety and security it may be more akin to a revolution sparked by elemental changes in the environment - pervasive and ambiguous threats and mounting complexity and interoperability challenges. This has precipitated a requirement for collaborative planning between public safety and security stakeholders. CBP may not hold all the answers (sometimes government is fragmented for good reason and 'wicked' problems are intractable) but CBP does offers sound precepts and the means to promote innovation and integration. Although the governance challenges may differ the Allied TTCP defence community has established some 'best practices' which can be exploited.

Future plans: The paper identifies some first steps for introducing CBP to the public safety and security sector that include:

- Identifying and establishing an institutional champion, and a 'capability champion' to spearhead/initiate CBP in a particular capability area;
- Identifying and establishing a means of institutional memory;

- Establishing policy goals to outline the scope of capability based planning within the sector;

- Collective risk assessment as a starting point for the development of collective objectives; and

- Building towards collaborative planning by ensuring stakeholder buy-in at all stages ("herding" not "stampeding").

It's time to take the bull by the horns.

Sommaire

Mise en œuvre de la planification fondée sur les capacités dans le secteur de la sécurité publique : Leçons tirées de l'expérience de la Défense

Doug Hales; Paul Chouinard ; DRDC CSS TM 2011-26 ; R & D pour la défense Canada – CSS; décembre 2011.

Introduction : La planification fondée sur les capacités (PFC) a été adoptée dans les années 90 afin de s'aborder le problème de l'ambiguïté inhérente dans le contexte de la sécurité de l'après-guerre froide. Elle offrait une solution de rechange crédible à la planification fondée sur les menaces et constituait un moyen de faire face à l'incertitude environnementale. La PFC a par la suite été adoptée par de proches alliés et a été récemment décrite comme « l'étalon-or ». L'utilisation de la PFC s'étend maintenant au secteur de la sécurité publique et son application a été inspirée de l'expérience et des pratiques liées à la défense. Bien qu'il y ait des leçons retenues et des pratiques qui peuvent être importées, il faut aussi remarquer que la sécurité publique fait face à des défis particuliers.

Résultats : Il existe une certaine unanimité sur le but et les principes de base de la PFC :

- La planification doit commencer par une connaissance holistique de l'espace-problème et reconnaître les perspectives de tous les groupes d'intervenants clés;
- Un modèle logique commun doit être accepté afin de faciliter l'analyse et la synthèse collaboratives et une taxonomie conjointe doit être adoptée afin d'assurer la cohérence définitionnelle;
- Des scénarios multiples, plausibles et indicatifs devraient être utilisés afin de se prémunir contre l'incertitude, de mettre à l'essai les concepts et de comparer les options;
- Les exigences, les écarts et parfois même les plans doivent être descriptifs et non normatifs et être formulés en termes de capacités, encourageant de ce fait la résolution novatrice de problème;
- Les contraintes doivent être reconnues et des dispositions prisent pour l'établissement des priorités.

La PFC se base sur des approches antérieures en matière de planification et d'institutionnalisation du développement des forces de défense de l'Australie, du Canada, du Royaume-Uni et des États-Unis. Des doutes persistent sur le fait que la PFC peut être plus qu'une approche analytique, à savoir qu'elle pourrait également servir de principe d'organisation. La PFC prévoit et intègre un changement vers une orientation centralisée de la politique en réponse aux interdépendances croissantes. En faisant la promotion d'une perspective holistique, la PFC affronte des « problèmes pernicieux » complexes caractérisés par des relations de cause à effet changeantes et indéterminées. Cette situation a entraîné la reconnaissance de la nécessité de faire appel à la planification continue et a démontré inefficacité des processus traditionnels.

Les efforts d'utilisation ont aussi mis en relief les défis organisationnels qui se rapportent particulièrement à la sécurité publique. Bien qu'une vision commune et un concept intégré soient utiles, un processus de planification de type PFC doit aussi tenir compte et respecter les mandats respectifs des intervenants, les profils de risque, les horizons de planification et les cycles de décision.

Le Comité technique 3 du Groupe des systèmes et de l'analyse (JSA) du Programme de coopération technique (TTCP) a élaboré et publié à modèle logique du PFC.[2] Il s'agit d'un exemple simplifié et normatif. Il stipule que l'arbitrage et la répartition sont un prélude à la mise en œuvre, mais il ne précise pas les éléments d'activité et les produits associés qui permettraient de tenir compte d'un certain nombre de points d'intégration horizontale.

Une taxonomie des capacités est nécessaire afin d'appuyer l'analyse et la synthèse. L'aptitude à décomposer et à explorer les éléments tout en adaptant et en fusionnant les résultats est essentielle à la PFC. Bien qu'un mécanisme de partitionnement unique commun aurait probablement été idéal, celui-ci s'est avéré difficilement applicable. Habituellement, un catalogue hiérarchique non normatif est utilisé pour décrire et regrouper les exigences provenant des analyses de mission des scénarios indicatifs. Les capacités peuvent être définies en termes d'activités ou de résultats. Pour la sécurité publique, il y a des avantages nets pour les premiers, en particulier celui de clarifier les rôles et les responsabilités. À un certain moment, ceux-ci doivent être attribués et liés à des biens matériels et la planification des capacités doit être liée à la gestion des capacités. Ce sont des personnes et de l'équipement plutôt que des abstractions qui sont gérés et déployés opérationnellement. Un troisième cadre supplémentaire est souvent utilisé pour décrire les éléments qui habilitent et génèrent les capacités latentes. En plus de recruter des gens et d'acquérir de l'équipement, cela comprend la doctrine et l'instruction. La gestion et la production de capacités sont généralement du ressort d'agences et de services distincts et indépendants. Le défi de mise en œuvre le plus urgent est l'élaboration et le choix d'une structure de classification des tâches et l'établissement d'un tableau de concordance reliant les biens aux capacités.

Les scénarios font partie intégrante de la PFC. Ils fournissent le contexte et constituent un véhicule permettant de poser et de partager des hypothèses. Il existe un consensus sur le fait qu'un ensemble de scénarios indicatifs sont nécessaires pour représenter l'environnement et tenir compte de l'incertitude. Le consensus n'est pas aussi général sur le nombre de scénarios qui doivent constituer cet ensemble et sur le niveau de fidélité. La préférence nette, si les sensibilités politiques le permettent, est de baser les scénarios dans le monde « réel », réduisant ainsi la nécessité de créer des environnements artificiels et facilitant la possibilité d'effectuer une transition vers des plans de contingence permanents. En matière de besoins en capacités, il existe une profusion de documents récents portant sur le choix de missions, la caractérisation de scénarios et l'articulation de concepts d'opération. Pour résumer :

- Risque – possibilités d'incident et conséquence – présentation d'une monnaie commune permettant de faire des comparaisons et d'établir des priorités;

[2] Le Programme de coopération technique (TTCP) est un partenariat/une organisation internationale créée pour faciliter l'échange de renseignements techniques, la collaboration scientifique et l'harmonisation des programmes entre les communautés de défense états-uniennes, australiennes, britanniques, canadiennes et néo-zélandaises.

- Des approches morphologiques peuvent alors être utilisées pour valider les ensembles de scénarios. La pratique suggère que l'utilisation prévue détermine ce qui est nécessaire pour déterminer la fidélité;

- De plus en plus, les cadres d'architecture sont utilisés pour mettre au pas la collecte de données, illustrer les relations et intégrer les perspectives d'entreprise.

Personne ne devrait être surpris d'apprendre qu'il existe souvent plusieurs points de vue lorsqu'il est question de déchiffrer les ambiguïtés et d'interpréter les relations de cause à effet complexes. En conséquence, la PFC est à la fois un art et une science; elle repose en partie sur une expertise en la matière. La PFC emprunte aux techniques émergentes d'aide à la prise de décision et combine les pratiques exemplaires dans les analyses rigoureuses et moins rigoureuses. L'approche axée sur l'utilité annonçait l'importance accordée actuellement aux résultats; la technologie a facilité la sollicitation de l'expertise dispersée en appliquant les techniques Delphi et la Théorie de l'utilité à critères multiples offre une méthodologie permettant de comparer et de classer les différentes solutions d'ordonnancement. Tout cela devait être transparent et non déterministe; il faut faire preuve de prudence dans l'interprétation et l'utilisation des résultats et prendre note des avantages de la protection et des dangers de la sous-optimisation.

La centralisation des pouvoirs en matière de politique est guidée par les environnements et il est probable que celle-ci produise un pu de résistance. Pour sa part, la PFC peut contribuer à instaurer la confiance, à assurer une cohérence entre les politiques et à faire la promotion de la planification intégrée. L'environnement de la sécurité publique est unique; il est distinct de celui de la défense. L'adoption et l'adaptation de la PFC reflètent la diversité des intervenants et doit reconnaître les différences de priorités, de capacités et de culture organisationnelle. Au début, elle pourra servir davantage de principe organisateur, mais elle peut être utilisée pour favoriser une approche de gestion de portefeuille où une cause commune peut être perçue. La patience, la tolérance et le leadership seront nécessaires, tout comme il faudra accepter que :

- Le rythme et les pratiques de mise en œuvre vont varier;

- Une approche ascendante va probablement d'abord se développer et dominer au début;

- Le partage d'information est un préalable essentiel et mettra en œuvre des coûts transactionnels.

La PFC incorpore les tendances en matière de gestion et de planification des activités et, en particulier, elle est étayée par l'évolution de la gestion du risque et des disciplines de l'ingénierie système. Il est peu probable que de tels élans extérieurs diminuent. Le risque constitue une lentille commune avec laquelle on évalue les dangers naturels, les accidents industriels et les menaces terroristes et il permet de comparer les solutions de rechange en matière d'atténuation des risques. L'ingénierie système met de l'avant une perspective d'entreprise et des cadres architecturaux comme moyens de saisir les interdépendances et de modeler les opérations de système. Ces représentations offrent une vue communautaire d'une entreprise collective et un point de départ pour exploration collaborative et l'amélioration progressive/en spiral.

Portée : Bien que la PFC de la défense constitue une évolution, pour la sécurité publique elle tient davantage à une révolution déclenchée par des changements dans l'environnement –

Menaces omniprésentes et ambigües, complexité croissante et défis d'interopérabilité. Cette situation a accéléré le besoin de mettre en place une planification collaborative entre les intervenants de la sécurité publique. La PFC ne possède peut-être pas toutes les réponses (parfois le gouvernement est fragmenté pour de bonnes raisons et les « problèmes pernicieux » sont insolubles), mais la PFC offre véritablement des préceptes solides et les moyens de promouvoir l'innovation et l'intégration. Bien que les défis en matière de gouvernance puissent différer, la communauté de défense alliée du TTCP a établi quelques « pratiques exemplaires » qui peuvent être utilisées.

Perspective d'avenir : Le présent document répertorie les premières étapes servant à présenter la PFC au secteur de la sécurité publique qui comprennent notamment :

- L'identification et la nomination d'un champion institutionnel et d'un « champion des capacités » afin de mener/lancer la PFC dans un domaine de capacité particulier;
- Détermination et création de mémoire institutionnelle;
- Déterminer les buts des politiques afin de décrire la portée de la planification fondée sur les capacités dans le secteur;
- Évaluation du risque collectif comme point de départ pour l'élaboration d'objectifs communs;
- Construire en vue d'une planification collaborative en s'assurant de l'engagement des intervenants à toutes les étapes (rassembler et non provoquer la déroute).

Il est temps de prendre le taureau par les cornes.

Table of contents

List of figures

List of tables

Acknowledgements

This work was supported by the DRDC Centre for Security Science. The authors would like to acknowledge the sage advice and staunch support provided by Jack Pagotto.

This page intentionally left blank.

1. Introduction

CBP was introduced in the 1990s to address the inherent ambiguity in the post-Cold War security circumstances; an environment that has been characterized as volatile and uncertain. Threat-based, single point-in-time scenario solutions were inadequate if only because the pace of political and technological change was outstripping the ability of staffs to keep up. A "new" planning framework was needed: emphasis was placed on delivering "capabilities" to address a widening range of risks.

There were a number of complementary drivers, not least the blurring of Service boundaries and competing demands for public funds. Expanding weapon ranges and the increasing importance of space challenged the traditional Navy, Army, Air Forces fiefdoms. Concurrently defence departments faced calls to reduce expenditures and allow governments to reap a "peace dividend" and to address a Revolution in Military Affairs (RMA) resulting from advances in Command, Control, Communications, Computers, Information, Surveillance and Reconnaissance (C4ISR) related technologies. The RMA sought to leverage these advances led by the private sector and to borrow best management practices from industry. Enterprise planning focused on "the non-war fighting, institutional or business functions"[3] and the RMA placed increased emphasis on enabling capabilities. CBP was seen as a means to promote and manage innovation to transcend organizational stovepipes and establish an effective mediation process - "to facilitate trade decisions across capabilities, across components, and between war fighting and enterprise needs"[4], to enhance objectivity, transparency and accountability, and to link outcomes, requirements and resources.

Capability Based Planning (CBP) has been widely adopted by the Defence community led by Australia, Canada, the United States and the United Kingdom. It has been described as the "gold standard" and its use is being extended to include public safety and security. The purpose of this report is to provide a detailed baseline understanding of capability based planning (CBP) to promote a shared understanding of CBP amongst staff of the Defence Research and Development Canada (DRDC) Centre for Security Science (DRDC CSS) but may be of interest to the broader community.

1.1 Objectives

This report is unusual in the sense that it has not been commissioned and has no direct sponsor in part due to the lack of a central governing body in the Canadian public safety and security realm. It developed and expanded in scope as a result of a series of discussion over coffee[5] on the challenges applying CBP presents both in general and in the public safety and security realm in particular. Subsequent discussions confirmed that confusion exists over what CBP is and that there is a need for documentation and discussion. The objectives are to:

- Review base principles and define CBP

[3] Colonel Stephen K. Walker, Capabilities-Based Planning: How it is intended to work and challenges to its successful Implementation, US Army War College, 18 March 2005, pp. 10.
[4] Ken Krieg, Capabilities Based Planning – The View From PA&E, presentation to the Military Operations Research Society (MORS) Capability Based Planning Workshop, Washington D.C., 20 October 2004.
[5] It may be worth noting that the authors have collectively more than 25 years of experience in the development of CBP theory and its implementation.

- Reflect on lessons learned, best practices and the state of the art after more than a decade of use
- Identify distinguishing issues in applying CBP in the public safety and security realm
- Offer thoughts on the Way Ahead

The aim is to stimulate thought and provoke discussion.

1.2 Outline

The document is organized into largely self-contained sections calculated to allow busy readers the opportunity to focus on their area of interest. The outline below is intended to show the relationship between sections and to guide the reader in finding sections of interest within the document:

- Section 1 Introduction outlines the background, objectives and organization of this report
- Section 2 Capability Based Planning describes principles and inherent challenges
- Section 3 Application introduces a conceptual model and observations on how this methodology has been employed
- Section 4 Best Practices attempts to document procedures that have proven to work
- Section 5 Supporting Stanchions notes that Risk Assessment, Mission Analysis and Systems Engineering are key enabling components to CBP
- Section 6 Way Ahead offers opinions and advice on the evolving future of CBP
- Section 7 Conclusion provides a summary and final thoughts

1.3 Background

CBP originated in the defence domain and most of the thinking, lessons learned, experience and best practices still reside within this domain. Where CBP has been applied to the public safety and security domain (e.g., the United States and the Netherlands) these versions of CBP have drawn heavily on CBP practices within their respective defence departments. Not surprisingly, this paper will refer to the defence CBP experience. While some experience with defence planning issues might be useful for the reader it should not be essential for understanding the basic concepts. However, it is acknowledged that the use of defence terminology when communicating with members of the public safety and security domain can be an obstacle to understanding CBP. There is a further problem in that the public safety and security community is not homogenous and no one single document will likely suffice and prove adequate for explaining CBP to the entire community. Therefore, it is planned that a number of shorter CBP "primers", tailored for different public safety and security communities, will be developed from this baseline document. This paper attempts to explore CBP's strengths and weaknesses, implementation opportunities and issues, and identifies a possible Way Ahead for exploiting and institutionalizing CBP in the public safety and security realm.

CBP was to be concept-led and invert the traditional structural planning paradigm substituting top-down for bottom-up integration (Figure 1). Stress was placed on hypothesis development & testing and on modelling & simulation to understand and mitigate risk. Hence CBP was viewed as a means to tackle affordability issues in the initial stages of the acquisition cycle and to address

a perceived gap in explanation by linking investments and outputs to desired effects and outcomes. As the past decade unfolded defence planners were reluctantly drawn into Stability Operations and Homeland Security. Interpretations of security broadened and recognition of the increased (and increasing) interdependencies struck home. Defining events such as the 9/11 attacks, the war in Iraq and Hurricane Katrina underscored the requirement for intergovernmental and interdepartmental collaboration (Whole of Government (WoG) and Integrated Government of Canada response[6]) and for public-private partnerships. Clearly a reductionist approach was no longer adequate; a holistic approach to operations and planning was required if stakeholder efforts were to be coordinated and full advantage taken of the potential these semi-autonomous agents offered. Enterprise architecting and system engineering practices were embraced and exploited in an attempt to structure and understand organizational and procedural complexity, and to design and develop appropriate policies and practices.

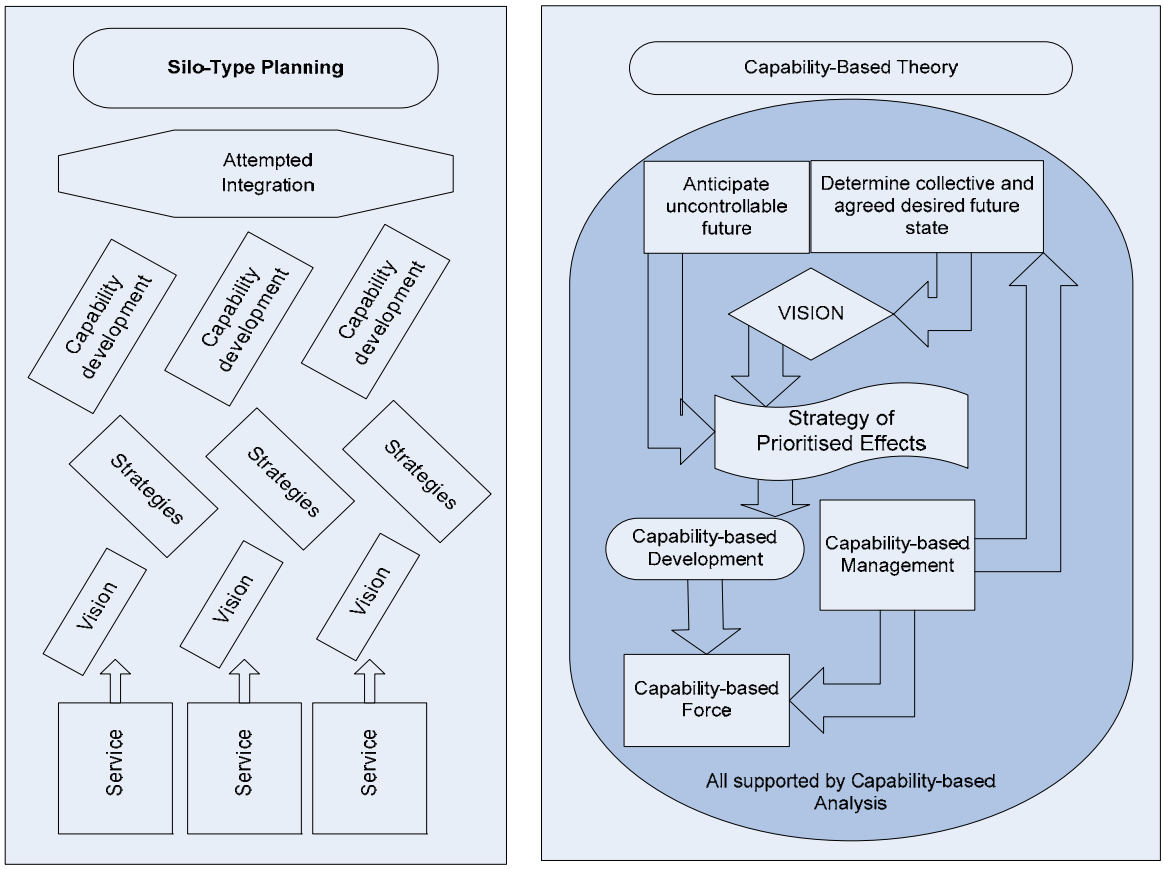

Figure 1 A New Paradigm[7]

This paradigm shift is depicted in Figure 1. In lieu of integration at the end of the cycle, often as an afterthought, concepts were to be (in the words of the US Department of Defense) "born joint"

[6] The taxonomy continues to evolve. Whole of Government is interpreted to mean all three levels of government in Canada whereas Integrated Government of Canada refers to coordination between Federal Departments and agencies.

[7] Sheryl Boxall, Defence Capability-Based Framework: The theory behind a capability-based framework that enables Defence to be led by Strategy – driven by Capabilities, Directorate of Future Force Development, New Zealand Defence Force, May 2011

and a shared collective vision used to define requirements and determine priorities. Following 911, nations and NATO have been working to implement and extend this concept beyond defence. A number of challenges and issues exist which are discussed in more detail below. These include integrating variations in organizational time horizons (i.e. positioning of the "future"), achieving an appropriate balance between competition and collaboration, agreeing on a taxonomy which is descriptive rather than prescriptive and creating an effective governance structure to conduct portfolio management across agencies. These are formidable challenges but, encouragingly, progress is being made. At this point CBP has not been fully institutionalized and some are prepared to jettison the concept to continue the search for a silver bullet. This would be short-sighted. Many of the misgivings relate to challenges involved in centralizing policy direction whether the centralizing agency is a single executive such as a Chief of Defence staff or a more collaborative national body such as the Senior Executives Responsible for Emergency Management (SOREM). Others relate to specific implementation instantiations e.g. the aim was never to lift all constraints and produce unaffordable wish lists. A less than plausible end product casts doubt and challenges the credibility of the planning process. Similarly overly prescriptive "proceduralization" will inhibit innovation. Perhaps most importantly it needs to be recognized that it is far from an established and static science; CBP continues to evolve. It been just over 10 years since CBP was introduced and it seems an appropriate to review the objectives and remark on implementation challenges, and note that there is now general consensus on what CBP is and agreement on taxonomy and principles.

1.4 Methodological Approach

The standard operational research study follows the steps of defining the decision-makers problem, developing a strategy to address the problem in a scientific manner, conducting the analysis using appropriate models and data and reporting the results back to the decision maker. Applying this standard "rationale" approach to complex issues like the implementation CBP within the public safety and security realm presents a challenge that was noted by Peter Checkland and Sue Holwell[8], pioneers in what is now called "soft" operations research. This challenge stems from the disparate public safety and security community which makes it impossible to identify THE decision maker never mind accord and articulation of the problem in a manner that makes it suitable for normal mathematical or logical analysis. Therefore the approach must be more epistemological (i.e., trying to understand the different valid perspectives of the "problem") rather than ontological (i.e., the modelling of an external reality accepted by all stakeholders). Consequently, considerable effort must be spent in the "problem formulation" stage than would normally be the case and initial goals must include development of a shared understanding of the problem amongst stakeholders followed by agreement on shared goals and action plan to achieve those goals. This paper seeks to initiate that process by provoking thought and discussion around the issue of more coherent and effective planning across the multitude of stakeholders in the public safety and security realm.

[8] Checkland, P. and and Holwell, S., " 'Classic' OR and 'Soft' OR – an Asymmetric Complementarity", in *Systems Modelling: Theory and Practice*, edited by Pidd, M., John Wiley & Sons, 2004

2 Capability Based Planning

The Kinnaird Report is illustrative of catalysts which had begun to pervade and disturb defence communities in response to post Cold War procurement review/reform initiatives.[9] It recommended sweeping changes in processes and governance and the establishment of a single focal point for a capability area – vested with both the responsibility and authority to deliver a capability to the Australian Defence Force. The analyst community was charged with developing an appropriate taxonomy and model. One of the earliest and clearest definitions of CBP was provided by Paul Davis who described it as "planning, under uncertainty, to provide capabilities suitable for a wide range of modern day challenges and circumstances, while working within an economic framework". [10] For their part capabilities have been determined to be "the ability to achieve a desired effect under specified standards and conditions through combinations of means and ways to perform a set of tasks"[11] linking CBP to outcomes and metrics.

It is also worth establishing what CBP is not. It is not 'a Copernican Revolution'. "The key idea is to start from what needs to be done and work back to an affordable force that can do it. This is fundamentally different from starting with what you have and working out how to improve it (or keep as much of it as possible if facing cuts)." [12] While CBP also reflects a recent enterprise wide, WoG strategic orientation, it builds on, and incorporates and extrapolates, elements of alternative approaches. This is most obvious in the treatment and use of a risk assessment, scenarios and mission analysis. There is considerable advantage in recognizing its legacy and situating CBP as a recent supplement to a continuum. The US Naval War College identified a number of alternative approaches to Force Development (Figure 2). As suggested, CBP borrows from each. It is intended to be top-down and concept driven, and to provide for feedback from experimentation and experience. It acknowledges network centric principles. Centralized formulation is seen as key to policy coherence and decentralized implementation as key to operationalization. A bottom-up, lessons learned process is also an integral element of CBP. Scenario sets are used to provide contextual focus and define threats/hazards; requirements are described in terms of functional requirements and risk used to establish program priorities. While perhaps not as obvious, hedging is integral. At the May 2011 Technical Panel 3 (TP3) *Analysis Support to Strategic Planning Workshop* the intent and requirement for agility was noted. It was suggested that, given environmental uncertainty, a balanced approach to investment should be adopted and over optimization/premature specialization should be avoided. This has particular consequence for public safety and security as optimization and resilience are in many ways competing demands.[13] There is an inherent tension between flexibility and efficiency. CBP aspires to satisfy both imperatives and support risk management, to be technology primed and fiscally bounded.

---

[9] Defence Procurement Review 2003, M. Kinnaird Review Chairman, prepared for Dr. Peter Shergold, Department of the Prime Minister and Cabinet and Chair of the Secretaries Task Force on Defence Procurement, Australia, http://www.defence.gov.au/dmo/publications/dpr_report.pdf

[10] Paul K. Davis, Analytical Architecture for Capabilities-Based Planning, Mission-System Analysis and Transformation, RAND, Santa Monica, 2002, pp.1

[11] Military Operations Research Society CBP Workshop, Washington, October 2004.

[12] Closing the Loop, op. cit. pp. 6

[13] The concept of resilience has been the field of materials science and is used to describe the ability of a material to recover its original state following deformation. It has been used in the public safety and security realm to express the ability of an enterprise or nation to return to "normal" following an attack or natural disaster.

Force Development: Alternative Approaches

Approaches	"Drivers"	Strengths	Pitfalls
Top-Down	Interests/Objectives/Strategies	Focus on Ends	Ignores constraints too long
Bottom-Up	Current Military Capability	Emphasizes real world	Neglects future
Scenario	Situation	Specific focus Dynamic	World unpredictable Takes on life of its own
Threat & Vulnerability	Risks Adversaries Own Weak Points	Emphasise capability Balance of Power	Too simplistic Not adaptable Retrospective
Capability Missions	Functions	Maximises Strengths Capability View	Sub-optimization tendancy May ignore higher goals
Hedging	Minimize Risk	Confront uncertainty Assure balance, flexibility	Undertates friendly strengths Worst-case analysis
Technology	Systems	Stresses knowledge Encourages Creativity	Often costly for small gain High risk
Fiscal	Budget	Foster Fiscal Discipline	Underfunding Leads to "fair sharing"

Ref: Bartlett et al. Strategy and Force Planning, 3rd Edition, 2000

Figure 2 Alternate Approaches to Force Development[14]

Similarly CBP objectives – informed and coherent decisions – represent more evolution than revolution. Derivation can be traced to such initiatives such as the US Planning, Programming and Budgeting System (PPBS) introduced in the US Department of Defense (DoD) in the McNamara era and national equivalences e.g.:

- Decisions should be based on explicit criteria
- Needs and costs should be considered simultaneously
- Major decisions should be made by choices among explicit, balanced, feasible alternatives[15]

CBP proponents argue that the fault with PPBS lay in placing the accent on programming and budgeting and neglecting the planning component. Since the 1960s reporting and audit practices have shifted with more emphasis being placed on policy objectives and outcomes rather than purely measuring inputs. Expectations of government have grown and the pace of business, private and public, has accelerated underscoring the importance of anticipation and justifying adoption of an overarching, integrative framework. Ideally, such a framework would be scalable and adaptable, capable of supporting both client diversity and different levels of abstraction. A strong case could be made on these merits alone for applauding CBP's ambition. It has historical geneses but has been tailored to cater to today's security environment. A number of base principles can be distinguished.

[14] Henry C. Barlett, G. Paul Holman Jr. and Timothy E. Somes, *The Art of Strategy and Force Planning*, Naval War College Review, Spring, 1995, pp. 114-126.
[15] Jim Bexfield MORS Workshops on CBP: The Past & the Present; MORS CBP Workshop, 3 April 2006.

2.1 Principles

The objectives cited are ambitious and CBP risks trying to be all things to all people. At its core, it provides for a functional analysis of operational requirements, i.e. it identifies and characterizes the capability demands necessary to respond to a broad range of circumstances and challenges.[16] It is an approach intended to support (not supplant) decisions and to inform the development of operational and investment plans through the apportionment of risk. A number of basic principles can be distinguished:

The departure point should be broad, include a holistic appreciation of the problem space and incorporate an inclusive and integrative approach. CBP should acknowledge the perspectives of all key stakeholder groups and recognize that capabilities are provided through a combination of people, process (policy, doctrine, SOPs) and tools (technology);

- To facilitate synthesis and collaboration analysis a common logic model should be accepted and a co-joined taxonomy adopted to ensure definitional consistency;
- Scenarios are a central component of CBP. They provide context and a means to share assumptions. Multiple plausible and illustrative scenarios should be used to hedge against uncertainty and to test concepts and compare options i.e. organizational structures, critical business processes and supporting systems;
  Requirements and gaps, and sometimes even plans, should be descriptive not prescriptive, and framed in terms of system or solution agnostic capability functions – i.e. "heavy cargo transport over 2000km" rather than stipulating a specific airframe, (thereby establishing what has been described by some as an idea marketplace and by others as a sandbox) thereby encouraging innovative problem solving; and
  Constraints should be acknowledged and provision must be made for prioritization. The aim was never to generate unaffordable "wish lists".

As the Hague Centre for Strategic Studies states "CBP has put (more broadly defined) capability, not platform) packages at the centre of a more adaptive defence planning approach that still tests capabilities against but no longer derives them one-on-one from individual point scenarios."[17]

It has been recognized for some time that the planning process is often equally if not more valuable than the product. The experience gained to date is instructive and development of CBP to date has been iterative. Implementation has been uneven and tailored to national context and primacies. As always, periodically, it is worth taking stock. A number of challenges and barriers to implementation of CBP have been identified. The challenges fall into 3 categories: conceptual, organizational and operational.

[16] Initially, within both the DND/CF and TTCP community, CBP was construed to include requirements definition, options analysis and acquisition/capability generation. More recently in Canada it has become more narrowly used to describe the front-end goal characterization. Confusion can exist because the two interpretations are often used interchangeably.
[17] Hague Centre for Strategic Studies, Closing the Loop: Towards Defence Management, pp. 7.

2.2 Conceptual Challenges

CBP has fallen out of favour with sectors within the US defense community. Perhaps the nub of the problem lies in confusion over whether CBP is intended to be more than an analytical tool and decision support lens. It has also been presented as a force structure design process and employed as an organizing principle. In short, there is a tendency to see CBP as a hammer and every problem as a nail, and this presents issues and pitfalls of which the public safety and security realm needs to be aware. There are a number of inherent challenges to any aspirant to a WoG planning process.

Planning provides a means to position our futures thinking. In today's environment this requires coming to grips with ambiguity, complexity and continuous change. Holistic planning is inherently difficult. Reflective reductionist thinking can lead to a focus on means rather than ends. To move beyond is challenging. ``Our planning forte has been short term, analysis-driven, reactive planning. We haven't done so well in long-term, synthesis-driven active planning``[18]. CBP is intended to promote coherency and continuity. Hence, there is a requirement to admit and appreciate linkages – import, relationships and relevance - and to integrate plans and programs.

One of the most obvious trends is a move towards centralized policy authority. In large part this is a reaction to the current security environment - recognition of the need to move beyond de-confliction towards aligning policies and coordinating activities, thereby avoiding creating problems downstream. This caution is a natural phenomenon and some resistance should be expected[19]. It is difficult to separate this from opposition to CBP itself; any planning system must provide for mediations. However intellectual disagreements over policy substance should not be permitted to degenerate into bureaucratic turf protection.

Orientation, ideally holistic and open-minded, is only part of the challenge. There may also be a lingering belief that there is an ultimate solution for every problem waiting to be discovered and implemented. Unfortunately "there is a whole realm of social planning problems that cannot successfully be treated with traditional, linear analytical approaches"[20]. 'Wicked problems' require both an innovative and comprehensive approach. Typically they bridge organizations and there is often disagreement over cause, priority and/or remedy. Attempts to address wicked problems may have cascading effects and lead to unintended consequences. They often also present planning staffs and decision makers a moving target. Perhaps the most to be expected of any planning system in this environment is to identify the direction rather than the destination.

Analysis and planning have become central, continuous and complementary activities. At is core analysis is the business of reducing uncertainty based on the information available and reasoning. As more information becomes available plans have to be adjusted. It has proven difficult in practice to sustain an ordained "cyclical" approach given the number of moving parts and pace of events. An orderly, linear, one-size fits-all process may provide a useful model but is likely to prove inadequate. Modularization is an emergent challenge to any strategic planning system and

[18] Wayne M. Hall, Shaping the Future: A Holistic Approach to Planning, US National War College, 1992, pp. 2

[19] In addition, there are limits to centralization within democratic, free market societies which value pluralism.

[20] Australian Government, Tackling Wicked Problems, 2007, pp. 3

poses governance issues. CBP does offer the prospect of a corporate logic model combining theory and practice.

2.3 Organizational Challenges

Strategic planning requires working across accountability structures to align policies, plans and programs. Many of the current threats are cross-jurisdictional or transnational in nature.[21] Challenges relating to governance expand exponentially in moving from the defence to the public safety and security sector. Even within the American Department of Defense (DoD), British Ministry of Defence or Canadian Department of National Defence (DND), CBP must co-exist within a larger, sometimes mandated, usually pre-existing managerial framework. Ideally capability analysis would be linked explicitly to performance measurement and accountability frameworks. Even within such large departments ownership of capability components is dispersed and decision orchestration is required. In developing the CBP model it was envisaged that specific policy goals would derive from government guidance that would bound and direct planning through patently defining interests and establishing levels of ambition. In practice "no clear mechanism exists to produce top-level 'national' guidance that is accepted and applicable across all levels of government, non-government organizations, and the private sector"[22].

The Australian public service identified three alternative strategies for dealing with 'wicked problems', the type of problems many defence and public safety and security planners face. While authoritative strategies can offer timely and efficient governance, "an essential ingredient is that other stakeholders acquiesce in the transfer of power to the anointed few and agree or are forced to abide by their decisions". [23] Alternatively competitive strategies encourage new ideas and are appropriate for programs such as the Chemical, Biological, Radiological-Nuclear and Explosives Technology Initiative (CRTI) but may not be appropriate for inculcating a WoG culture. Competitive strategies can invite conflict and stalemate and divert scarce resources. The Australian study concludes that collaborative strategies are "the most effective in dealing with wicked problems that have many stakeholders amongst whom power is dispersed". [24] Collaborative strategies will be needed if CBP is to succeed. Outcomes are often a result of a sequence/series of decisions and the commitment to a strategy more important than the agreement on every detail. The experience of the NATO approach to defining requirements (the Defence Requirements Review) illustrates that it is possible to combine the three strategies with authoritative analytical elements and a market-based fulfillment of requirements embedded within an overarching collaborative strategy.

While the centralization of direction over policy would help to ensure consistency, such an approach is both impractical and problematic. Mandates need to be respected and cultural preferences and principles (e.g. collegiality and participation) need to be acknowledged in order to realize a sense of procedural and institutional legitimacy and assure implementation. Whereas in a department a dedicated and empowered office/branch might suffice to oversee CBP, a pluralist approach and a committee may be warranted in the public safety and security realm.

---

[21] Ric Smith, Report of the Review of Homeland and Border Security, 4 December 2008. Summary & Conclusions

[22] Sharon L. Caudle, Homeland Security Capabilities-Based Planning: Lessons from the Defence Community, Homeland Security Affairs, Volume 1 Issue 2, 2005, pp.5

[23] Tackling Wicked Problems, op. cit., pp. 9

[24] Tackling Wicked Problems, op. cit., pp. 10

Developing a WoG planning capability/extending CBP to the public safety and security arena augurs for acceptance of a softer, federated approach complementing and leveraging existing, embedded departmental and agency governance structures and planning processes. Initial research into meta-organizational shared decision making sponsored by DRDC suggests that situational complexity can be viewed as a continuum ranging from Simple through Complicated to Complex and approaches along a second continuum ranging from coordination through cooperation to collaboration.[25] Underwriting collaboration and partnerships are a "win-win-win view of problem solving"[26]. This offers the prospective of more coherent and comprehensive planning but comes at a price in the form of increased transactional costs (including time) and a requirement for facilitation skills.

With their increased tempo of deployed operations since the end of the Cold War, defence departments have had difficulty finding enough personnel to staff the planning, management and analytical needs of both CBP and deployed operations. If this has been an organizational challenge for defence departments it is even more likely to be so for the public safety and security sector which has traditionally had a much lower ratio of planning to operational staff than defence.

It also appears obvious that to generate a WoG strategic planning capability organizational slack may have to be created and expectations will have to be managed prudently. Most Other Government Departments (OGDs), provincial and municipal partners and many in the business sector lack the dedicated expertise and staff capacity resident within defence departments. A strong business case would be required to support a bid for resources. This is in itself challenging as it is difficult to quantify the advantages a holistic perspective (policy coherency and program integration) offers and determine the cost/benefits of efforts to foster an innovative culture. The gains may be more long term than immediate. Familiarity with the framework, best practices and supporting tools and the reuse of information and models can ease introduction and implementation of any strategic planning process, not least CBP. The establishment of a repository of expertise and models may be warranted, and beyond reach of smaller departments and agencies. Placement and the role and best means to engage industry and academia are a very topical issue. A study has been commissioned by DND to consider options for establishing a Capability Analysis Centre. Meanwhile streamlining and tailoring the CBP process and developing the supporting tool suite should be priorities.

It is fairly easy to trace its genesis and relate how past practices informed CBP. There is also general agreement on the underlying principles although these are not often made explicit. There are conceptual and organization challenges to implementation and application has been uneven and nationally distinctive. CBP has been grafted on to complement or replace existing governance structure and analytical practices, and the immediate emphasis placed on different aspects of planning in response to local priorities. The next section examines the TTCP TP3 logic model and how different countries have approached application.

[25] Louise Lemyre et al. Research Using In Vivo Simulation of Meta-Organizational Shared Decision Making (SDM) Task 1: Synthesis of Case Studies to form a SDM Framework, draft report December 2009, pp. v

[26] Tackling Wicked Problems, op. cit., pp. 10

3 Operational Challenges

There are a series of challenges related to applying and putting CBP into practice. As noted in the previous chapter these challenges usually fall into one of three categories, which are:

1. Conceptual: CBP can be difficult to understand. In particular, since the intent of CBP is to improve planning across "stove-pipes", whether within or across organizations, CBP practitioners will need to grapple with different world views, doctrine, language, etc. used by the various "stove-piped" communities. Some conceptual challenges may be largely intractable; all that can be done is to recognize them. Education will help but effective educational material must be tailored so that it can be understood by a community with its own unique world view.

2. Organizational: CBP can be resource intensive and almost certainly will require resources from across the various "stovepipes" in order to take into account the perspectives of the various stakeholders. Organizational challenges were discussed in the previous chapter, but by and large are a fact of life and will for the most part be constraints that an effective CBP process will need to accommodate. There is no approved structural template for conducting holistic planning across government or across the public safety and security domain.

3. Operational: Operational challenges deal more with doctrine and procedural practices. The obvious start point for understanding these challenges is the CBP logic model developed by Technical Panel 3 (TP3) of the Joint Systems and Analysis (JSA) Group of The Technical Cooperation Program (TTCP) which will be the focus of the discussion in this chapter.

3.1 The TP3 Logic Model

American, Australian, British and Canadian defence scientists met in 2003 and developed a generic CBP logic model[27] shown below (Figure 3) outlining key activities. This process starts with strategic guidance and concludes with creation of an affordable capability investment plan. This is a model - a simplified abstraction useful for promoting discussion and acquiring insights, not an exact nor a prescriptive representation. It does offer a modularized approach recognizing distinct analytical exercise components. However it also needs to be understood that breaking up a process 'chain' into separate links does not do justice to the more complex linkages that will need to be considered in any specific, practical implementation of the logic model.

[27] The logic model used by the Centre for Security Science to inform its scientific programs has been derived from the TP3 model and it can be found in Annex A.

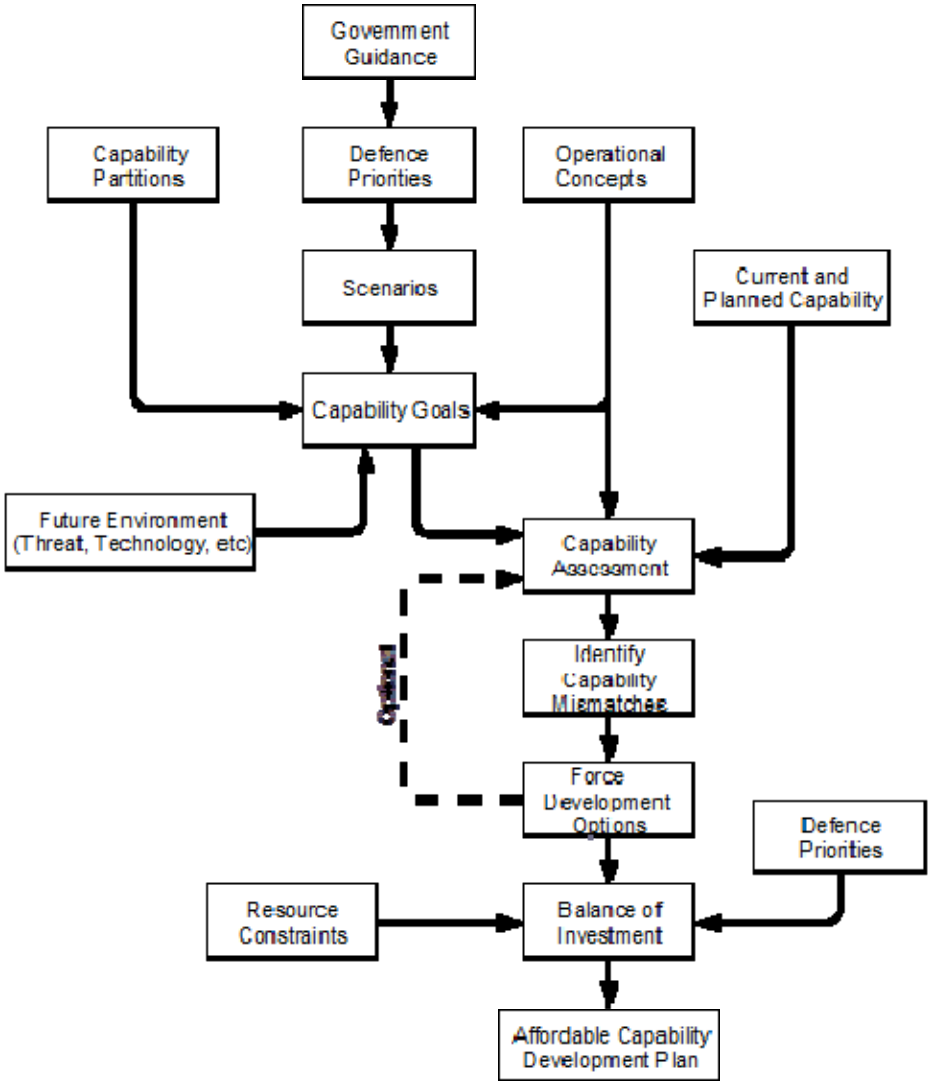

Figure 3 TP3 Capability Based Planning Model

3.2 Concepts

The TP3 process model depicts CBP as an ordered sequence of activities. The Canadian Forces (CF) CBP Handbook contends that CBP "can be described simply as 'start from what you want to achieve and work back to what you need'".[28] It is not quite that simple. In practice there are a number of decision cycles – ranging from the strategic to tactical - to accommodate. It may be more useful to view the CBP process outlined as a decision hierarchy. CBP incorporates a suite (if not a sequenced series) of decisions. At each level the decision elements – uncertainty, risk preference, time horizon and problem structure – must be identified and isolated. "Often arguments over which is the best decision arise because the participants do not realize that they

[28] Chief of Force Development, Capability Based Planning Handbook Version 6.2. National Defence, December 2010, pp. 9

are arguing on different grounds."[29] The information gathered and presented and level of detail provided should reflect decision level.

Strategic guidance is often episodic (e.g. periodic White Papers) whereas investment provisions (business plans and performance management) may follow an annual financial cycle. The pace of technological innovation will vary by field/capability domain. Even within defence CBP is not as systematic and linear as portrayed. Fortunately each activity concludes with a "product" providing input to the next activity, and an opportunity to exchange information and a chance to resynchronize. This is significant in that many departments and agencies lack the planning experience, expertise and structure which defence departments have developed over time. Dissecting CBP and highlighting the supporting analysis components does serve to highlight the requirement for, vertical and horizontal coordination. The demand for analysis is increasing and requires husbandry, witness the introduction of analytical agendas to establish analytical priorities.

The TP3 suggests that CBP is driven by a suite of Operational Concepts. These reflect organizational values and doctrinal theory, and inform the response to scenarios. Concepts describe the manner (ways) capabilities (means) can be employed to satisfy mission objectives (ends). There is a temporal dimension - as future concepts mature and the supporting elements are established in place, future concepts become today's doctrine. The original TP3 CBP focus was on long term force development. Operational Concepts play a key role here as depicted. Significantly for public safety and security, it should be realized, and has been recognized by the military community, that Operational Concepts represent a middling component of a hierarchy of concepts. The nomenclature differs within the community but typically consists of Capstone or Integrating Concepts, Operational or Operating Concepts and Concepts of Employment. The former describe in broad terms foundational philosophy, principles and guiding precepts establishing an authoritative basis for subordinate concepts. These tend to be reviewed and approved at very senior levels. Operational Concepts describe roles and responsibilities and relationships between organizations and activities. Typically these are mission-oriented e.g. Peace Support Operations and reviewed and approved by Operational authorities. Operational Concepts may be complemented in this middle tier by Functional Concepts which describing a capability domain or field of specialization. Whereas Operational Concepts provide a vertical perspective Functional Concepts provide a cross-mission horizontal perspective. CBP must recognize and integrate both perspectives. To this end the US military maintains a set of Joint Operating Concepts. Lastly, Concepts of Employment represent the lowest tier and are used to describe system or asset usage. Experience suggests that innovation occurs on all levels, arguably more often on the lower tiers when inventive approaches to employing and exploiting technologies are adopted. Two points are worth underscoring. CBP is intended to be concept-led but this is not intended to suggest down-top, big ideas should dominate. In a recent study of strategic defence management which examined practices in several nations and the World Food Organization, The Hague Centre for Security Studies concluded that:

> The real drivers for change are at the operational/tactical levels rather than at the strategic ones, and are much more bottom-up (from performance management) than top-down (from policy). Upon reflection, we consider this a cause for optimism rather than

[29] Ronald Howard, Decision Analysis, 23 September 2008, pp. 105

concern, as it promises a much more realistic anchoring of strategy (however ambitious it may be) in operational and financial realities.[30]

Concepts, as much as plans, need to be integrated. This is an important take-away for public safety and security. Secondly, and as illustrated in Figure 4, while stage-setting general direction is important and flows top-down this must be complemented and accompanied by concrete bottom-up instantiation proposals. These are usually treated organizationally as separate processes with different governance structures and these can result in divergences and/or white spaces and exasperate decision makers. To contribute to decision coherence CBP must establish a framework which integrates concepts.

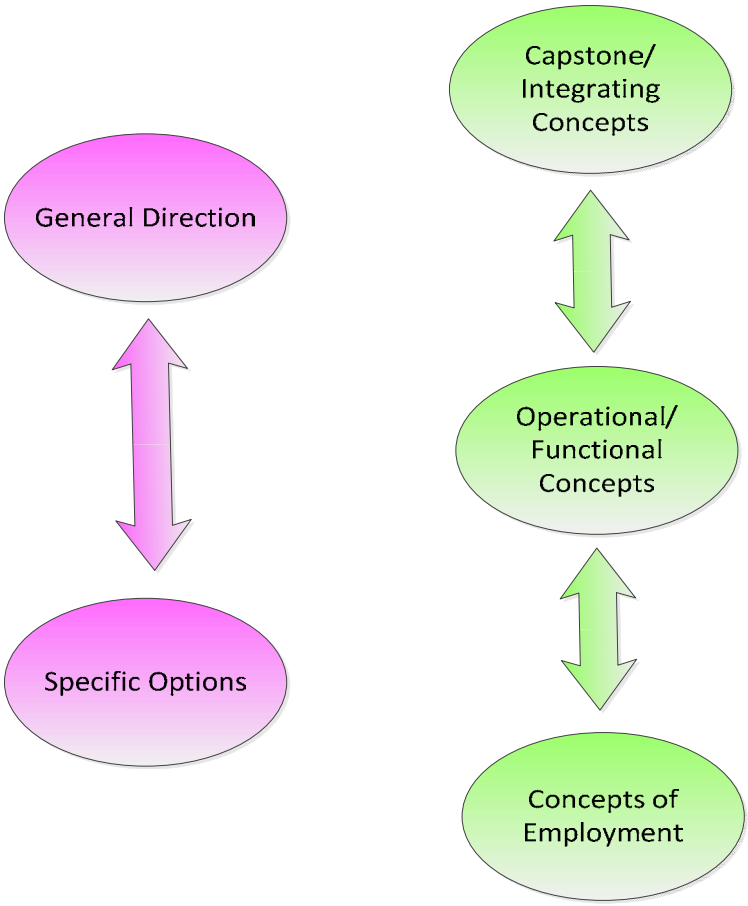

Figure 4 Concept Hierarchy

Many of the challenges the defence communities have confronted are shared with the public safety and security community. Emergency management partners face similar competing demands for increasing flexibility and simultaneously reducing margins for error; hence, it is not surprising that they look to defence for advice on how to implement CBP. The defence community now has years of experience (over a decade's worth) and a forum through The

[30] Closing the Loop, Op. cit. pp. 7

Technical Cooperation Program (TTCP) to discuss best practices and lessons learned. While TP3 model rationale has, by and large, survived transition from theory to practice, issues have arisen and challenges remain.

3.3 Guidance

Typically policy goals and strategic guidance are usually described in terms of intangible objectives. "The goals enunciated tend to be heavy on politics and weak on policy – especially on detailed policy guidance. This leaves a sizeable gap between the lofty policy goals of the high-level documents and the actual detailed [defence] planning."[31] This poses two challenges related to interpreting and rendering. The "decision engineering" process for transforming and framing opaque policy direction into well-defined plausible problems should be both well-understood and systematic. Selection and approval of appropriate, illustrative scenarios is discussed in more detail in a subsequent section. Semantic interoperability is required to support an integrative planning framework, i.e. fielding and employing a common language. This can provide a bridge between narrative and quantitative analysis. The model does not make explicit the range of supporting skills necessary to implement fully CBP.

3.4 Partitioning

There are limitations to our cognitive abilities. It is difficult, if not impossible, for most analysts and decision makers to deal with complex problems as a whole. A key to success in implementing CBP is the faculty to combine analysis and to synthesize (i.e. to decompose the problem and examine aspects in detail while retaining association to higher goals and system-of-system behaviour). Table 1 has been included to accent the distinction between analysis and synthesis. CBP aspires to integrate processes and products. It is "built upon the assumption that all capabilities can be deconstructed into a set of mutually exclusive elements and attributes that describe the tasks required to effect the capability"[32] , and the assumption that these elements can in turn be reassembled and the whole reconstructed. It should be appreciated that this is a tall order.

[31] Closing the Loop, Op. cit., pp. 10
[32] Walker, op. cit., pp. 15

	Analysis	Synthesis
Step 1	The entity to be understood is taken apart	Identify one or more larger systems of which the entity of interest is a part
Step 2	Understand the behaviour of each part of the entity taken separately	Understand the function of the larger system(s) of which the entity is a part.
Step 3	Aggregate the knowledge of the parts of the system in an effort to explain the behaviour or properties of the whole.	Disaggregate the larger containing system to identify and understand the *role* or function of the entity and the nature of its interfaces with the larger system
Focus	**Knowledge** of entity structure, how it works and delivers its *outputs*	**Design** of entity behaviour and *outcomes* in the larger system(s) it is part of
Benefit	Analysis provides knowledge to make an entity work ***efficiently*** and to repair elements of it as they stop working	Synthesis provides systemic understanding of the entity behaviour for it to work ***effectively*** as a whole in a greater system.

Table 1 Analysis & Synthesis[33]

The TP3 Panel considered this challenge and concluded that no parsing scheme is "ideal, but some are worse than others" noting "different parts of the organization will have different partitioning drivers".[34] A single, common capability partitioning scheme would be the ideal but experience to date suggests is impractical particularly when the underlying scheme is asked to underpin enterprise planning, management and employment functions. Put bluntly, no accounting unit offers universality. Two to three schemes and an accompanying "Rosetta Stone" are required. One of the underlying principles of CBP is that requirements should be defined in functional terms i.e. desired outcomes should be characterized in terms of capabilities – the ability to achieve desired effects. These are deliberately abstract. As the CF CBP Handbook puts it, "the CBP process starts with a 'pure' view of capability" achieved by employing an "activity" lens.[35] One of the goals of CBP is to remain non-prescriptive for as long as possible to avoid foreclosing options. At some subsequent point the functional requirements must be related to organizational assets. The military typically refer to these as Force Elements.[36] This distinction between needs and solutions is integral to CBP. "The reason is that the *ability* to do something will probably remain in constant demand, whereas *how* we deliver that ability changes as technology advances or affordability becomes an issue."[37]

[33] Richard Hodge, A Systems Approach to Strategy and Execution in National Security Enterprises, PhD Thesis, University of South Australia, January 2010

[34] TTCP JSA TP 3, Guide to Capability-Based Planning, 2003, pp. 7

[35] CBP Handbook, op. cit., pp. 9

[36] The original Canadian Forces Concept of Employment developed in conjunction with the introduction of CBP proposed using Tactically Self Sufficient Units as basic building blocks. This may be viewed as a bottom-up asset oriented outlook. Although the term is no longer used the concept is implicit in many examples of CBP implementation. Conversely the DND/CF now define Force Elements in terms of mission import reflecting an effects orientation e.g. a FE is "an entity… which makes a direct contribution and is essential to deliver mission effects and/or achieving the objective of an assigned mission". CBP Handbook, op. cit. pp. 13

[3737] Sheryl Boxall, Defence Capability-Based Framework, New Zealand Directorate of Future Force Development, Capability Branch, pp. 11

This distinctive is long-standing – CBP merely tries to bridge the gap - and is reflected in organizational processes, mandates and structure. For example the US Joint Capabilities Integration and Development (JCIDS) approach distinguishes between a Functional Needs Analysis and a Functional Solutions Analysis. Although the positional titles change frequently capability planning, acquisition/generation and employment roles are organizationally separate in the Canadian Department of Defence (DND). Establishing a common language and organizing principle is to a large degree a challenge that CBP inherited. However, CBP does offer an integrating theoretical concept.

The high level logic model is depicted below (Figure 5). It illustrated the underlying rationale and reflects adaption of accepted system engineering processes. Guidance determines government needs and (using scenarios) analysis is conducted to identify functional requirements. These, in turn, are used to define performance and design parameters (solutions analysis).

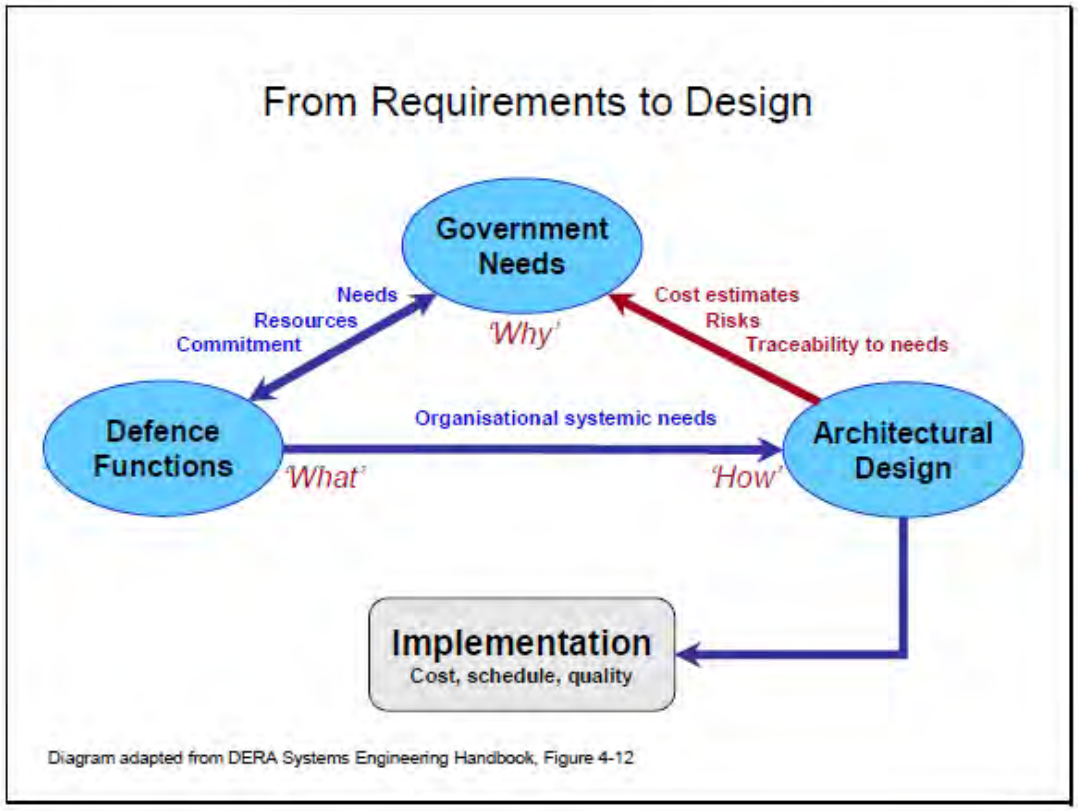

Figure 5 Requirements to Design Logic Model

This logic is also reflected in the NATO model which distinguishes three separate but coupled analytical activities used in conducting Defence Requirements Review (Figure 6). Mission Analysis is employed to determine NATO needs (*Why*), Situation Analysis to determine representative planning situations (scenarios) and Capability Analysis to define functional requirements (*What*). Synthesis integrates these complementary analytical thrusts and identifies the capability/force packages required to satisfy NATO objectives. The central role mission

analysis plays, the use of tasks to define requirements and the requirement for a synthesis function are significant.

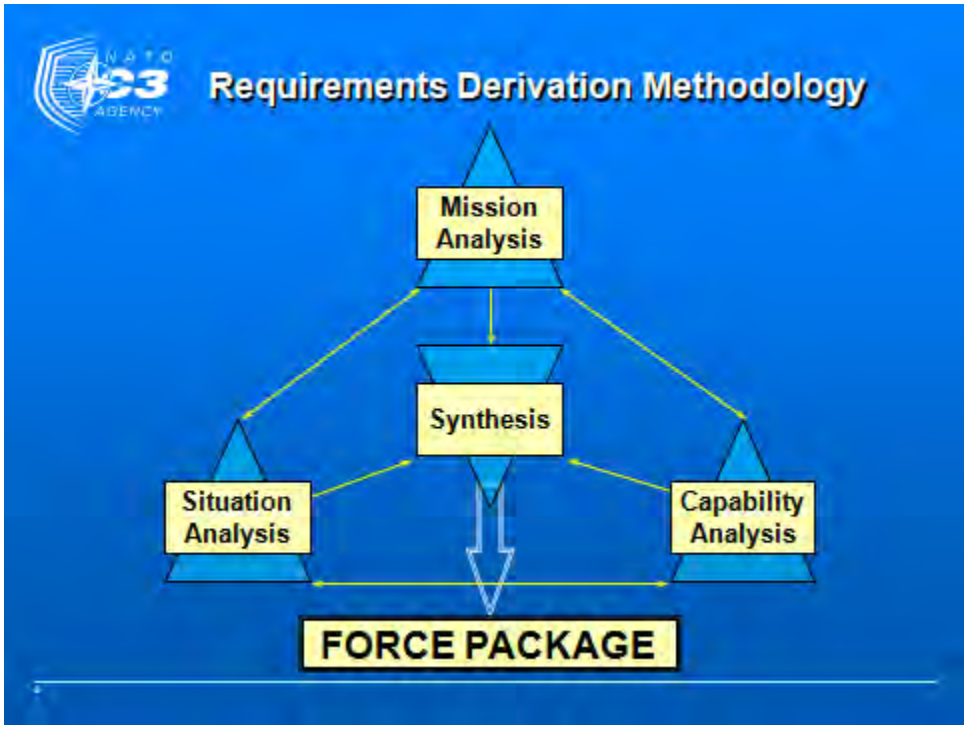

Figure 6 NATO Requirements Derivation Methodology

In implementing CBP task hierarchies have been developed to support Mission-Task analyses and provide a shared lexicon.

There are a variety of conceptual frameworks and categorization schemes. In their comparison of national strategic defence management models The Hague Centre for Strategic Studies drew a useful distinction between activity and outcome based task lists. They noted that the former offers clear advantage in clarifying roles and responsibilities while the latter may provide richer insight into the contribution of a task to accomplishment of strategy facilitating prioritization between tasks.[38] The authors' preference and recommendation for public safety and security is to adopt an activity based task list, at least initially, to ensure that organizational obligations are fully articulated and completely understood. However, synthesis or integration will eventually require outcome-based or mission-oriented task lists linked to identified, high risk threats and hazards and concepts on how to mitigate those risks.

The ability of existing and prospective organizational units/assets to fulfill tasks provides the means to gauge gaps and assess risk. While there may be a conceptual element relating to the realization of the need for separate hierarchies, the more pressing implementation challenge lies in developing and agreeing task and asset categorization schemes and establishing the "crosswalk".

[38] Closing the Loop, op. cit. pp. 146

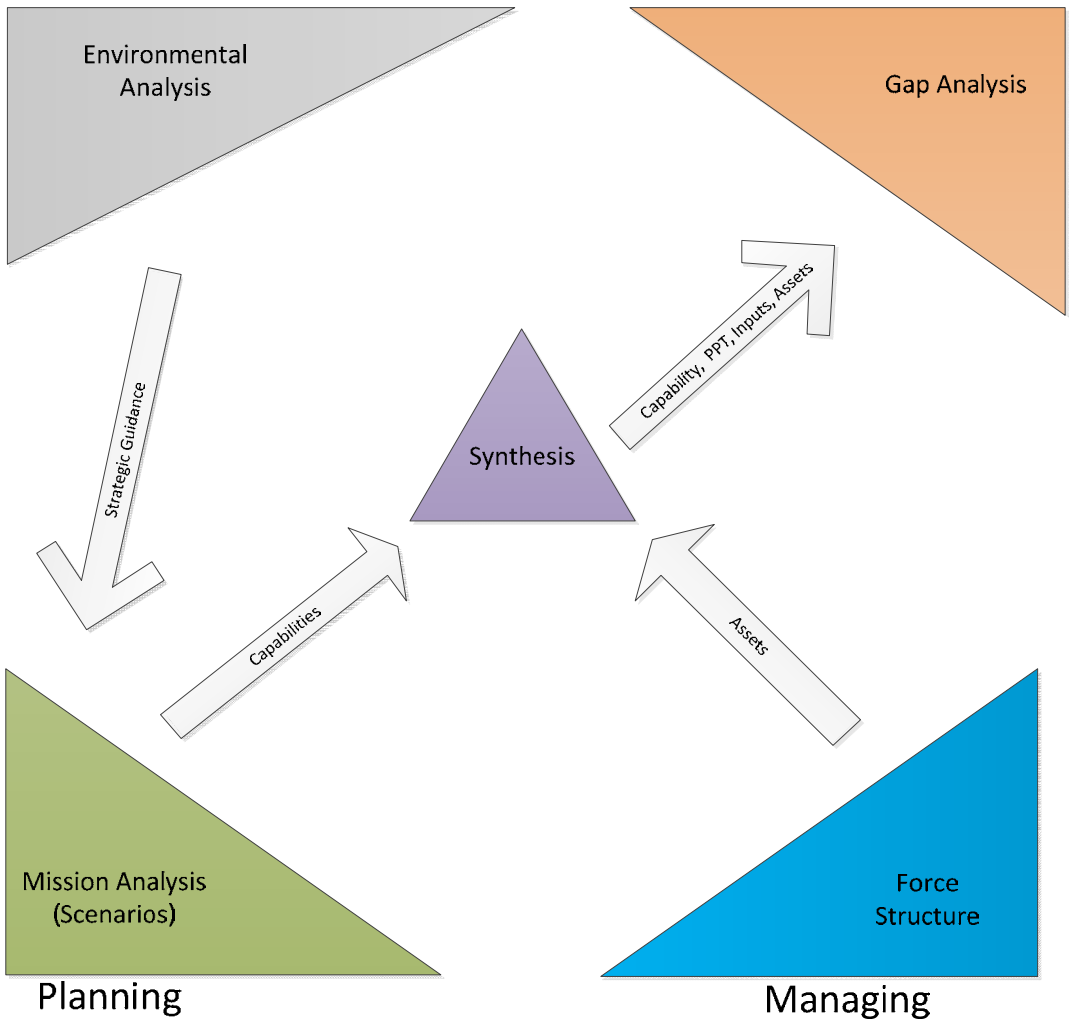

Figure 7: Cross Walking

The goal of any task list is be exclusive and exhaustive, as well as non-prescriptive and practicable. As suggested, hierarchical schemes have been employed to cater for demands for scalability. They have provided the vehicle to implement CBP as an organizing principle. The challenge is that this is but one lens and one perspective does not capture the inherent complexity adequately. The "cube" shown below (Figure 8) was an early (crude) attempt in DND/CF to depict this multidimensionality. Others have conceived it as a multidimensional lattice. The cube was considered too intricate and deleted from more often than used in DND/CF presentations on CBP but it did capture the spirit of the challenge. It does serve to illustrate key perspectives: planning, management and employment, each with their own constituent units.

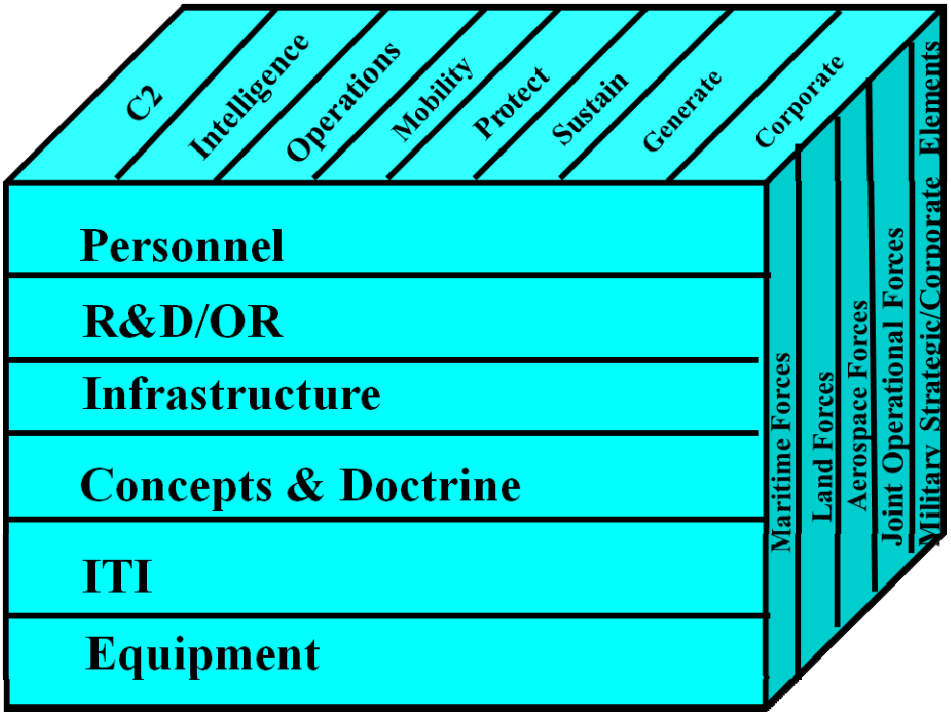

Figure 8 Multidimensionality

Introducing new or substituting capability for previous organizational (e.g. Service) silos illustrates value (i.e., outcomes defined through desired capabilities) for effort (i.e., outputs defined through the ability of service silos to generate capability). Acceptance of co-existing schemes and permeability is necessary. Two further observations can be made. It should not be surprising that a capability-based task hierarchy serves better at the strategic level than at the tactical level. The former is focused on the conceptual and the longer term. Second, on a more practical level, provision must be made for care and custodianship of task lists. New tasks may arise (e.g. cyber) and the common "book of prayer"/"dictionary" will need to be periodically reviewed and refreshed. This would appear to be easier in national militaries. Responsibility can be assigned to doctrine custodians. In the public safety and security realm periodic reviews by representatives from the user community might be considered. Annual reviews along the lines by which NATO conducts of its Crisis Response System and Crisis Response Measures may serve the Alliance. Among the most important roles these task hierarchies serve is to support analysis.

3.5 Scenarios

Mission Analysis using a suite of scenarios will provide an indication of the range of capabilities required. Quantifying requirements requires planners to make some assumptions about concurrency. These may be derived directly from Strategic Guidance or explored and risk determined for different assets inventories/force structure options. The intent of CBP is to structure not complicate the subsequent gap analysis. The analysis should be tailored and the level of fidelity fit for purposed. If detailed analysis is warranted models can be developed incorporating distribution curves reflecting demand profiles and substitution rules acknowledging

that non-specialized tasks can be carried out by a variety of units. The outputs - gaps/risk - can be expressed in several ways using different "currencies". Gaps can be structural and relate to either capability or capacity. They can also be procedural. Capability shortfalls signal an inability to achieve the desired effect to perquisite standards under prescribed conditions. Capacity deficiencies typically are expressed in terms of asset insufficiencies. In either case further deconstruction is generally required and it is necessary to define gaps and options in tangible terms.

Framing concurrency demands and risk poses their own challenges. Strategic Guidance rarely provides explicit direction on Levels of Ambition. There is an element of discretion – whether to participate and what resources to commit - involved in many operations. Within the public safety and security realm, there may be no option with regards to "response" but there is considerably more discretion when it comes to "protection", "prevention" and longer term "recovery". Assumptions need to be explicit and decision makers presented with options to discuss framed in terms of risk. Assessment and presentation of risk is an art in its own right, e.g. capability gaps over time and comparisons between arriving later on site versus asset shortages. Agreeing substitution rules and differentiating between preferred and available assets complicate the risk assessment procedure and presentation. As with risk, gaps can be characterized in a number of ways. Gaps are often presented in terms of the employment - capability requirements or unit shortfalls using the task hierarchy and asset inventory. Assets have people, equipment and readiness components and infrastructure and increasingly info structure enablers. Gaps can also be expressed in terms of capability generation. The Canadian Collaborative Capability Definition, Engineering and Maintenance (CapDEM) Technology Demonstration Project (TDP) distinguished three axes: People, Process and Material. It proposed that analysis can be conducted and capability gaps defined using these axes. The axes provide a useful construct for characterizing whether problems relate to personnel selection and training; tactics, techniques and procedures (TTPs) and/or infrastructure and equipment. Finally gaps can be expressed in terms of capability management, i.e. inputs provide another, equally valid perspective. Capabilities can also be defined indirectly in terms of personnel, doctrine, training, equipment, infrastructure, and info structure components. The Australians term these Fundamental Inputs to Capability, the British Defence Lines of Development.[39] The DND/CF, used until recently[40], Personnel, Research & Development, Infrastructure & Organization, Concepts, Doctrine & Collective Training, Information Technology, and Equipment, Supplies & Services (PRICIE) construct reflects an attempt to link capability components to departmental organization and managerial structure. Such decomposition are useful as they facilitate a comparison of options (including costing) and eventual incorporation of the option selected into organizational business plans and the association of projects with higher level goals and objectives. All of these perspectives and partitioning schemes are valuable and valid, and reflect collectively CBP's ambition and the diversity of stakeholders. Most notably it is worth drawing attention to the multiple ways gaps are communicated. "Capability" gaps may be defined in terms of functional incapacities; people, process, and/or technology shortfalls; assets or generational components. Each lens serves a purpose. Functional gaps are used to inform long term planning and acquisition programs. The CapDEM derived people, process and technology perspective to better define the problem and

[39] The DND/CF PRICIE construct (Personnel. Research & Development, Information, Concepts & Collective Training, Infrastructure and Equipment) was chosen to both capture capability components and to provide direct linkage to departmental level 1 budget holders.

[40] The current construct is the one developed by the US Department of Defence, which is Doctrine, Organization, Training, Material, Leadership, Personnel and Facilities (DOTMLPF) where the order reflects an increasing difficulty to address.

solution space. Describing gaps in terms of outputs - unit quantities and/or qualities -resonates with managers and operators. Finally, defining gaps in terms of inputs – capability components – speaks to capability generators. All these perspectives are valid, and all derive from common, corporate strategic guidance. Mission-to-task analysis provides a means to link the three and to relate each to an associated and interdependent risk perspective i.e. operational risk and programmatic risk.

3.6 Model Limitations

The TP3 model assumed a common (rational) actor – a shared worldview and unified structure.[41] Even within organizations there are multiple actors and micro-cultures. This suggests that a more pluralist approach needs to be adopted in extending CBP to the public safety and security sector. Each department and agency, and public sector partner, is unique and has its own mandate and priorities and its own planning and governance practices. The "chain of command and exercise of authority are different"[42]. Grafting rather than uprooting and reseeding is more likely to succeed. In this case, lessons learned from the NATO Force Development process may be useful. It integrates an additional apportionment activity into the CBP model. Following mission analysis and in response to identified gaps targets are reviewed and agreed and a pool of capabilities maintained which can be drawn on in a crisis. This additional mediation step is important in a federated system. A holistic enterprise wide view encourages self-synchronization. In parallel and concurrently, each partner can integrate discussion into their decision cycles, personal targets into their organizational plans and, on completion, register their intentions for the community's benefit. This notion of accommodation differs from that of consensus. "Consensus implies that all the stakeholders fully agree that the proposed changes best serve all of their needs. The concept of accommodation recognizes that this is a very rare state of affairs in most real-world situations and that most of the time individual needs can only be partially met by collective propositions".[43]

3.7 Scoring Application

Applying broad principles to particular circumstances always poses challenges. The TP3 Guide provides a theoretical model; it does not purport nor provide much direction on application. Implementation of CBP has been uneven, of necessity, catering for context and circumstances. It stands to reason that the model must be shaped to fit needs. However it is also useful to stand back. Recently Paul Davis, one of the original architects of CBP, shared his thoughts on the current status of play (Figure 9), contrasting CBP aims and achievements. His observations suggest that practitioners have been more successful bureaucratizing (reducing CBP to mechanical planning and programming processes) than realizing its objectives and exploiting its potential. He singled out the resistance to constraining planning; a preference for/reliance on complex, detailed models; and an inability to measure capability as expectations that have not

[41] Graham Allison's contribution was to challenge this view of government and present complementary models based on organizational behaviour and bureaucratic politics i.e. he suggested that government decisions are the result of many contending forces. Graham T. Allison, Essence of Decision: Explaining the Cuban Missile Crisis, Boston: Little, Brown, 1971.
[42] Caudle, pp. 18
[43] Soft systems methodology, pp. 2

been met. In the discussion following his presentation there was general agreement that linkage to concept development and experimentation (CD&E) was loose (i.e. CD&E had not been exploited to foster innovation and inform planning). This assessment was sobering but served to identify opportunities for improving application

Features

	Suggested	Implemented
Plan for uncertainty and adaptiveness	••••	••
Work within economic framework demanding choice	••••	•
Use simple, agile models, exploratory analysis, parametrics; support this with layers of deeper research and analysis as needed	••••	•
Modularize system for simple models, scenarios,…	••••	•
See "requirements" and "scenarios" as outputs of technical analysis and dialog with decision makers, only then as "drivers;" iterate	••••	••
Measure capability to actually do mission; focus initially on mission, not solutions; include innovative conops	••••	•• weak on innovation
Emphasize jointness	••••	••••
Organize, manage around fixed capability areas	No, tailor as needed	••••
Systematize, routinize, bureaucratize analysis	No! No! No!	••••

Figure 9 Paul Davis Thoughts on CBP in 201144

[44] Paul Davis, Thoughts on Capability Based Planning in 2011, presentation to the TP3 Analysis Support to Strategic Planning Workshop, Ottawa, 13 May 2011

4 Emergent Best Practices

There are a range of best practices which have emerged to support CBP. Three distinct phased processes can be distinguished: recognition, exploration and evaluation. The first involves analysis of ambitions, context and objectives, the second more detailed requirements definition and options identification and the third design and evaluation of candidate solutions (either comparatively or against a set of criteria/performance standards). Several broad areas of analytical "best practice activities, which are listed below, support these processes:

- Recognition activities:
  - Selecting missions
  - Relating risk
- Exploration activities:
  - Characterizing scenarios
  - Employing architectural frameworks
- Evaluation activities:
  - Supporting decisions
  - Applying caution

Although each area of analytical activity can be characterized as primarily supporting a given processes, they can also be seen as threads of activity which span the processes. For example, "relating risk", while primarily intended to link strategic guidance to operational objectives, must be taken into account during both options identification and the evaluation of candidate solutions. Similarly, "employing analytical architectures" is a key activity for linking the three processes from end-to-end. This is consistent with the multi-tiered approach implicit in CBP (i.e., CBP can be seen as an iterative processes which provides greater and greater detail essential for the implementation of strategic guidance but with a corresponding narrowing of the range of options). Having analytical activities that link the processes allows flexibility by providing a decision trail to facilitate back-tracking should a selected option prove infeasible.

The remainder of this chapter discusses each analytical activity area in detail.

4.1 Selecting Missions

One of the first challenges is to "operationalize" strategic guidance. Best practices suggest that this can be done through identification of a set of illustrative missions. This raises questions of how many and which scenarios should be analyzed. It is tempting to offer a glib response along the lines of "enough" and "you'll know". There is no right answer. No doubt the availability of analytical resources will limit the number of scenarios, but nonetheless the set should adequately cover the spectrum of missions anticipated and scenarios used as forcing agents to explore issues and provide insights. More is not necessarily better; use cases can be grouped into classes. Each should be unique and can be viewed "as 'compression points' in the continuum of variations and possibilities"[45]. As Paul Davis suggested at the TP3 workshop, it may be useful to distinguish between the use of scenarios to inform strategy formulation and the use of scenarios to inform strategy implementation. A multi-tiered approach is recommended. A summary may

[45] Working with scenarios, risk assessment and capabilities, October 2009, pp. 18..

suffice to illuminate options and support big "P" policy decisions, with more detail required to understand fully the implications and manage the direction outlined. At the higher level scenarios provide a tool for qualification and at the lower level a tool for quantification. A number of national models incorporate a two (or multiple) pass CBP process. In practice resource implications restrict and determine to a large degree the number of mission analyses which can be undertaken, and maintained i.e. refresh rate is a factor. The UK has a larger catalogue than many other countries and considers these on a rolling basis. Obviously the set must be representative and provide for an examination of topical issues and the support of pending decisions. One of the areas which could be improved relates to coordination of effort and exchange of information – development of a broader, pan-government "analytical agenda" and establishment of a framework for characterizing scenarios i.e. ensuring full advantage is taken of individual department and agency mission analyses. In complex systems errors are not distributed randomly; therefore, a concerted effort is needed to identify areas where a small, focused effort can avert significant risk.

Following 911 the focus of many governments was on counter-terrorism. The assumption was that preparing for terrorist events would ensure preparation for all events. This was reflected, for example, in the US Department of Homeland Security (DHS)'s initial scenario set. The logic proved contentious; it could be argued equally capabilities developed to cater for more probable all-hazard incidents could be ramped up.[46] More significantly, in practice, pre-occupation with counter-terrorism narrowed stakeholder participation and did not provide adequate balance-of-investment decision support to underwrite targeted resource allocation. As Sharon Caudle observes "stakeholders generally control the information, resources, and authority required to support CBP, and their requirement must be considered from the onset"[47]. Writing of Australia, Ric Smith a former [48]Minister of Defence invited to review Homeland and Border Security concluded "while crisis management by the Commonwealth has generally been done well 'on the day', the current hazard-specific approach and the absence of consistent national arrangement for handling significant crisis exposes the Government to several areas of vulnerability".

Hence considerable thought should be given to scenario selection and approval. Selection is important as it likely reflects and will inform investment priorities. Scenarios can serve to check excessive convention and consider the no-man's land separating stock and trade contingencies and speculation. A scenario set that is too conventional and does not adequately stress existing capabilities can mask vulnerabilities. It has been suggested that shocks embodying an interaction/intersection of trends are more likely in the future and that strategic shocks are less failures in prediction than failures in policy and planning.[49] If the scenarios are too farfetched or they are too many of them the mission analysis may be perceived as a resource consuming distraction. Hence an engagement and approval process is highly desirable. In essence, selecting scenarios involves establishing "hedges", ideally those that are robust over the largest number and most critical futures.

Scenarios serve as an instantiation of policy and a means to overcome psychological and organizational planning barriers. It is important that the key stakeholders review and endorse the

[4646] Sharon L. Caudle, Homeland Security Capability-Based Planning: Lessons from Defence, Homeland Security Affairs, Vol. 1, Issue 2, 2005, pp. 12.
[47] Ibid, pp. 6
[48] Ric Smith, op. cit. para 9
[49] Nathan Freir, Known Unknowns: Unconventional 'Strategic Shocks" in Defense Strategy Development, November 2008, http//www.StrategicStudiesInstitute.army.mil/, pp. 7

scenario set which will be used to guide implementation of their direction. Inclusion will foster acceptance of the results of the mission analysis. The scenarios must present a believable future operating environment yet stretch existing capabilities to expose inherent risks in existing capability. Credible Subject Matter Experts are needed to complement the analysts and support mission analysis. Within each scenario a number of "friendly" and "enemy" Courses of Action (COAs) may be identified and time and/or resource constraints restrict the analysis. General practice is to opt for the "most likely" rather than "worst case". The sheer number of factors may be daunting and preclude conducting a traditional (linear) sensitivity analysis. In lieu the computational power available should allow exploratory analysis to be conducted i.e. all parameters to be investigated simultaneously, the problem space defined and the "most likely" COA situated.

A Specialist Team was convened recently to review current best practice in operations analysis support to national defence planning. Surveys were completed and a workshop held. The results were not surprising: "scenario-based analysis was confirmed as a fundamental element of contemporary analytical support".[50] The majority of nations identify contingencies and develop these into specific planning situations. Significantly, "most nations have implemented an explicit link between national policy and definition of their national scenario set"[51]. This is easier to do for Defence than it is for public safety and security, e.g. CF missions are listed in the *Canada First Defence Strategy*.

4.2 Relating Risk

As the US DHS has recognized "Capabilities-Based Planning is a form of all-hazards planning. It addresses the growing uncertainty in the threat environment by using a wide range of possible scenarios to bound requirements and thereby reduces the tendency to fixate on any one threat, hazard, or set of conditions".[52] Risk provides somewhat of a common denominator. It can be used to express strategic vulnerabilities, capability deficiencies, asset shortfalls and/or operational jeopardy. If nothing else risk analysis provides a means to compare apples with apples and to foster a shared understanding of threats/hazards. The importance of establishing a common departure point should not be underestimated. It represents the first step in developing collective objectives. An All Hazards Risk Assessment (AHRA) process is a part of Public Safety Canada (PS)'s emerging practice. The methodology developed by the Dutch (Figure 10) and adapted by Defence Research and Development (DRDC)'s Centre for Security Science (CSS) reflects best practices. It starts with an assessment of threats, integrating as appropriate near term and long term threats. Scenarios are used to instantiate threats and support analysis. Mission-to-task and capability analyses follow.

[50] NATO SAS-081 Specialist Team Summary Report, Analytical Implications of the NATO Defence Planning Process, pp. 9-5
[51] Ibid pp. 9-6
[52] DHS, Capabilities-Based Planning: Overview, http://www.scd.hawaii.gov/grant_docs/Capabilities_Based_Planning_Overview_12_17.pdf, pp1

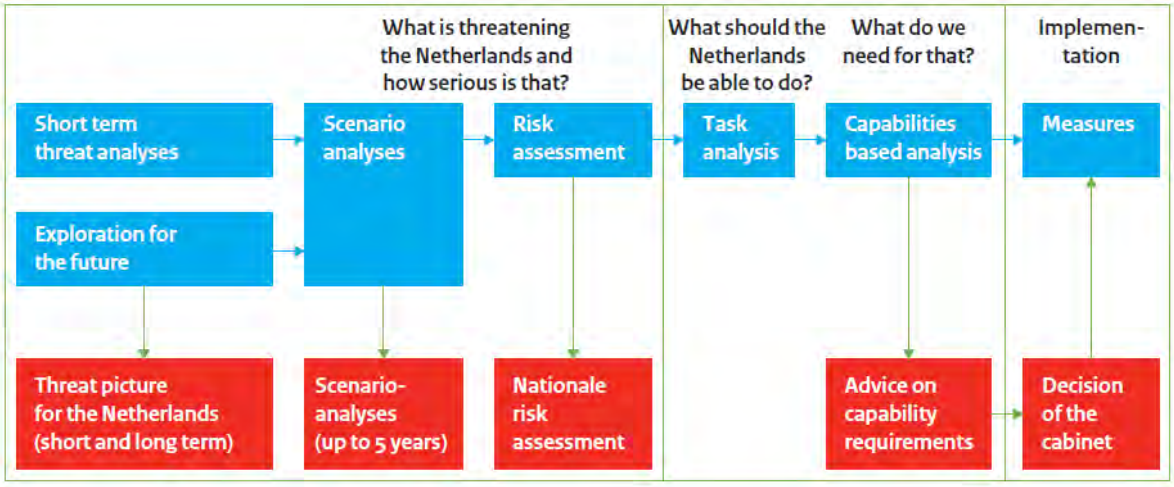

Figure 10 Dutch National Safety & Security Methodology

The risk taxonomy CSS has developed (Figure 10) categorizes events and offers a comprehensive catalogue of possible threats/hazards. Insofar as possible, determinations of likelihood and impact are decided objectively. Historical occurrence and scientific models and projections are used to establish the probability of natural hazards, and Intelligence estimates used to define the likelihood of malicious threats. Precise scenario probability estimates can suggest a misleading insight into the future and inhibit acceptance. Groves and Lempert have offered a simpler scenario threshold test to consider in selecting and prioritizing scenarios for elaboration and comprehensive analysis e. g. "How likely would this scenario have to be in order to justify a change in strategy?"[53]

Traditionally militaries have been used to project power and defend territory against foreign aggressors. In most Western states they are used only as a means of last resort in domestic theatres. Hence, White Papers and equivalent strategic guidance try to frame risk and spell out missions, directing planning and largely negating the requirement to develop homeland defence-oriented risk taxonomy. Military taxonomies reflect this direction and are encapsulated in doctrine. Most commonly defence scenarios are depicted in terms of progression along a spectrum of conflict. It should be noted that this model can present challenges as policy makers are usually understandably reluctant to define risk and prioritize between missions. For their part threat assumptions are built into the scenarios. Public safety and security threats and hazards span departmental mandates and lack established doctrine; therefore, a common taxonomy and transparent risk assessment methodology is essential. A definition of scenarios along a spectrum defined by a line parameter, like "conflict", is unlikely.

[53] David G. Groves and Robert J. Lempert, A new analytical method for finding policy-relevant scenarios, Global Environmental Change, 17, 2007, pp. 81, http://www.rand.org/pubs/reprints/RP1244.html

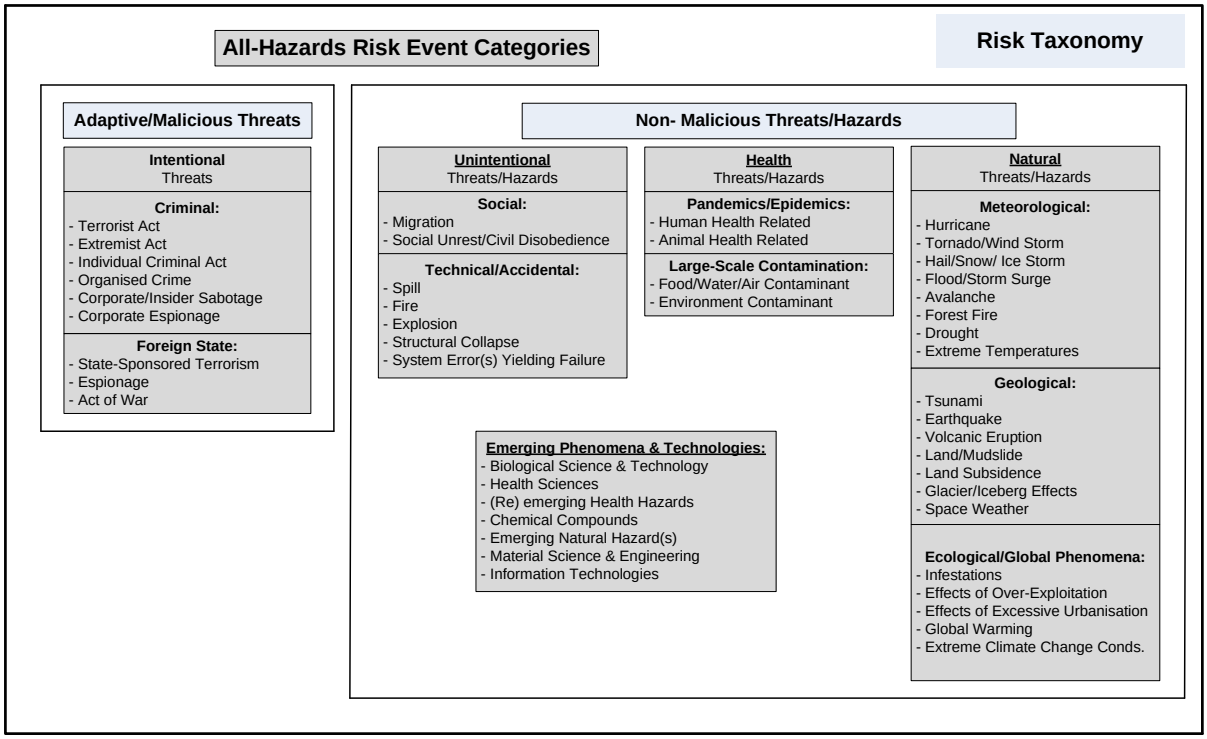

Figure 11 AHRA Risk Taxonomy

Risk assessment remains, again, part science and part art. Future risk is difficult to assess, particularly socio-technological risk because there is no underlying actuarial data available. Intangibles such as losses of trust, reputation, cohesion and goodwill are impossible to calculate precisely. "The response usually is to adopt a three level matrix of high, medium and low levels of probability, and another three level matrix of impact, which allows for some of the disciplines of risk management to be adopted". [54] The CSS has refined the matrix and provided associated word pictures. This approach serves the purpose of refining strategic intent to those scenarios of greatest interest for CBP analysis. This type of strategic-level risk assessment should not be confused with more detailed operational risk assessments required to guide development and assessment of risk mitigation options.

Following identification of risks, the AHRA process includes subsequent development of Risk Scenarios to exemplify the threats/hazards identified; they provide context to capture shared assumptions and to support consequence analysis. Impact assessments are based on a set of criteria and associated consequence ladders. The scaling itself can be linear or logarithmic. The latter may be the more valid of the two in capturing psych-social impact. An example is provided below (Table 2):

[54] Peter Sommer and Ian Brown, Reducing Systemic Cybersecurity Risk, OECD/IFP Project on "Future Global Price Shocks"
Organisation for Economic Co-operation and Development (OECD), 2011, pp. 35

Base Rating	Magnitude and Severity
Nil	No Impact
0	No specialized response, no damage or significant clean-up or restoration cost
1	Some local specialized response, no damage or significant clean-up or restoration cost
2	Some local specialized response, short term damage but no significant clean-up or restoration cost
3	Some local specialized response, short term damage and significant clean-up or restoration cost
4	Multi-jurisdictional specialized response, short term damage and significant clean-up or restoration cost
5	Multi-functional, multi-jurisdictional specialized response, medium term damage and significant clean-up or restoration cost
6	Multi-function, multi-jurisdictional specialized response, long term damage and significant clean-up or restoration cost.
7	Multi-function, multi-jurisdictional specialized response, long term localized damage with significant economic, political, health, safety consequence
8	Multi-function, multi-jurisdictional specialized response, long term large spread damage with catastrophic economic, political, health, safety consequence
9	Multi-function, multi-jurisdictional specialized response, essentially permanent damage with catastrophic economic, political, health, safety consequence

Table 2 Environmental Impact

A group of Subject Matter Experts completes the impact assessment which is then combined with the likelihood to determine risk profile and support comparative evaluation. This is a good example of disciplined "soft" analysis. This approach both encourages and relies on stakeholder participation. As always, the selection of experts is critically important. Confidence in the outcome is directly proportional to confidence in the experts contributing their judgment.

4.3 Characterizing Scenarios

Reference was made to the desirability of establishing a scenario characterization framework and relational database which would facilitate information exchange and foster collaboration. The approach developed by Peter Schwartz and exploited by Shell has been described as the scenario-axes method. Two key drivers are identified and the combinations depicted in a quadrant used to define four different story lines. This is effective for considering alterative futures, challenging mental models and providing insights. This scenario-axes approach does not work well in supporting the diversity of audiences involved in public policy debates. It has been found that "the standard scenario-axes technique failed to serve as a unifying structure for diverse

participants" not least because "the unavoidable role develops' judgments play in constructing scenarios provides ample opportunity for partisan challenges to their relevance and accuracy". [55]

A more multi-dimensional approach than that employed by the Shell approach is required. The CSS has looked into this and identified some of the key dimensions which can be used to characterize scenarios (Figure 12). The Risk Taxonomy serves as one perspective; a Scenario Time Horizon provides another important perspective. The latter was developed by CSS to encourage tactical back casting and "full spectrum" scenario analysis to ensure attention was focused on preparatory, preventative and protection measures which might have averted or minimized the consequences of an incident and, to a lesser degree, on recovery which will extend past immediate response to an incident. Typically the focus of scenarios has been on a description of the incident and immediate response. It is envisaged that the scenario framework could be used to support communities of interest, structure lessons learned, and assist in portfolio management.[56]

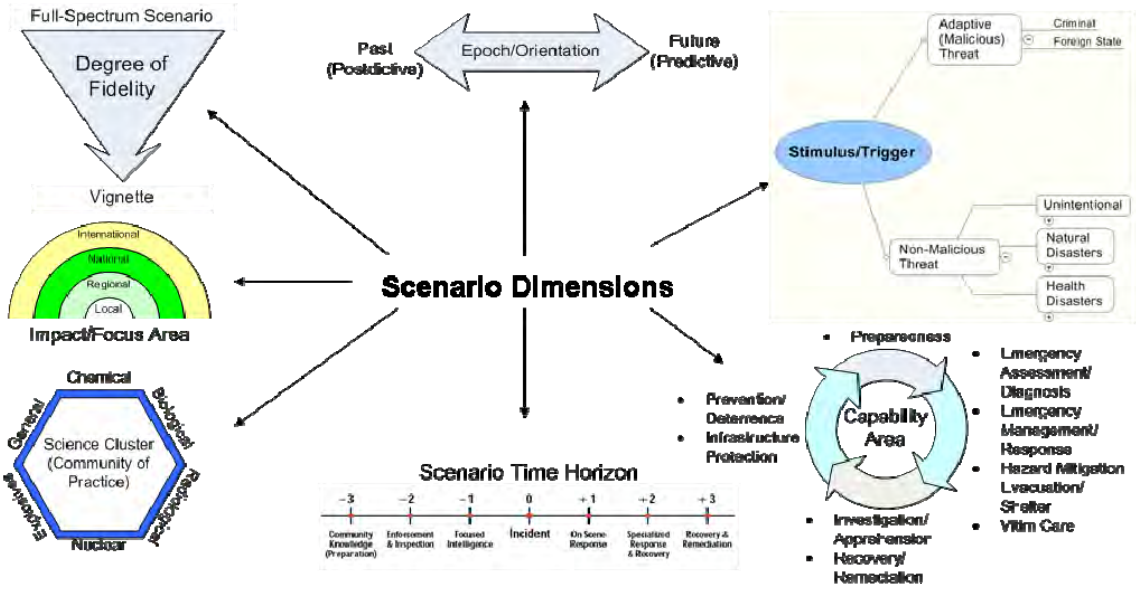

Figure 12 CSS Framework – Scenario Dimensions[57]

All these perspectives are valid but potentially problematic. "The multiplicity of combinations of a large number of uncertainties suggests hundreds to millions of potentially interesting scenarios."[58] A follow-on DRDC Centre for Operational Research (CORA) project extended research into scenario characterization and selection. A software application was developed for CORA to support morphological analysis of a scenario set. The scenario planning factors (dimensions) identified by SMEs were divided into 3 classes: drivers, descriptors and derivatives (Figure 13). Using Field Anomaly Relaxation (FAR), the set of possible scenario combinations was reduced and plausible scenarios distinguished. This embodied an attempt to link elements of

[55] Groves, op. cit. pp. 74
[56] Douglas Hales and Peter Race, Applying a Framework for Defining Emergency Management Scenarios, Journal of Emergency Management, Vol. 9 No. 1, January/February 2011. Pp.24.
[57] Hales op. cit. pp. 16
[58] Groves, op. cit. pp. 74

explicit direction and capability requirements (derivatives).[59] One of the key advantages anticipated was generation of a cross-scenario view of the requirement for a capability. The framework was also proved useful in characterizing and generating profiles past operations. FAR attempts to reduce the set of conceivable scenarios. An alternative approach is to exploit modern computer capacity and conduct what has been termed exploratory analysis i.e. perform multiple simulation runs to define the boundaries of the problem space then use statistical clustering methods to distinguish and select "relevant" illustrative scenarios for detailed analysis.

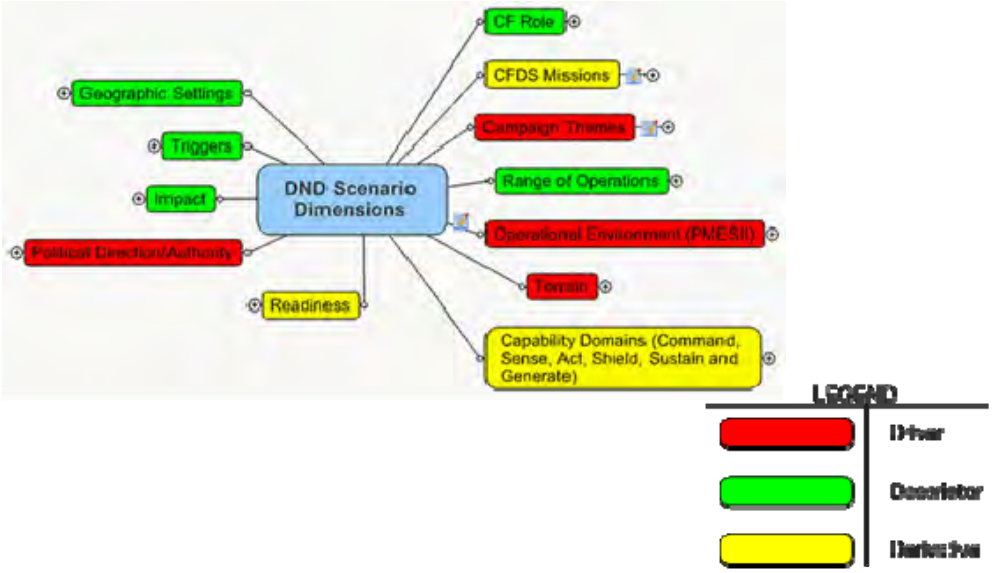

Figure 13 DND Scenario Dimensions: Drivers, Descriptors & Derivatives[60]

Scenarios can describe waypoints and convey powerful portraits. Illustrations of prospective situations are often more compelling than generalized descriptions of trends. The consensus across the NATO SAS (System Analysis and Studies) 081 group and experience to date suggests that the benefits of scenario-based analysis are maximised when real-world settings are used. This eases the "read-in" familiarization workload and alleviates any requirement to generate an artificial geographic backdrop. In addition, real world situations inherently are more complex than artificial scenarios which tend to be simpler in construct. Political sensitivities may preclude declassifying real-world scenarios but this is more of a problem for defence than for public safety and security. "Generic scenarios are likely more suitable for analysis of the longer-term future or to support consideration of emergent threats" [61] but to date public safety and security has been focused on the near to midterm.

[59] It is interesting to note in passing the indicators that the Hague Centre for Strategic Studies used to characteristic national ambitions i.e. Reach, Concurrency, Interoperability, Unilateralism, Pre-emption and Violence Spectrum. De Spiegeleire, op. cit. pp 65. This AUDEX index could also be used to characterize and select scenarios.

[60] Shaye K. Freisen, Doug Hales, Neil Chuka, Charles C. Morrisey and Peter Race. Covering the Bases: Development of a Framework for Defence Force Planning Scenarios, 15th International Command and Control Research & Technology Symposium, Paper ID 029, pp. 10

[61] NATO SAS 081 pp 9-8

4.4 Employing Architecture Frameworks

Once the scenario(s) are agreed, mission analysis can commence. "Scenario analysis cannot predict the probabilities of [major] changes but can consider consequences and help organizations develop strengths and the resilience needed to adapt to foreseeable changes."[62] The starting point is a concept of operations, describing actor roles and responsibilities. Generally speaking the CONOPs is a narrative; it captures the gist but not necessarily the detail. Architectures are being employed and increasingly accepted as best practice. They impose discipline and provide a means to structure information and articulate CONOPs i.e. a tool to describe roles and assist in modelling complex systems/systems-of-systems. Although scalable, it takes time and requires stakeholder commitment to create a useful architecture-based model; relationships may not be well understood, often business processes are not well documented and/or standard operating procedures may be largely implicit. Architectures prove a means to impose definitional consistency and to reflect, integrate and retain knowledge for reuse. The starting point is the status quo (the "as is"). In order to be able to appreciate fully functions, requirements, issues and options, the current state is described – a shared view of the "system" is developed. Alternatives for a "to-be" then can be explored and evaluated.

Architectures provide different perspectives of an enterprise or system under study derived from a common dataset. Architecture frameworks establish standard textual, graphic and tabular products ("views"), each a unique, prescribed perspective. Most architecture frameworks trace their roots back to a two dimensional matrix introduced by John Zachman (Figure 14). Each cell is created by the intersection of a perspective and a focus. Hence, it provides a formal and structured way of defining and viewing an enterprise's information system. The completed matrix provides a synoptic view describing subordinate models without specifying procedural approach or modelling language. The Zachman Framework has subsequently been extended and refined, and a number of architecture frameworks exist. Most include equivalent primary products. All have tried to avoid methodological specification and to remain tool agnostic. All have the same aim: to allow different people to draw tailored perspectives of the problem and potential solution spaces.

The benchmark and most widely used architecture framework is the US Department of Defense Architecture Framework (DoDAF). A Public Security Architecture Framework (PSAF) derivative was developed but has not been employed often. The DoDAF offers a number of advantages; to wit, it is maintained and it is supported by software vendors. For example the latest iteration includes Service Views in addition to Systems Views and incorporates Capability Views derived from the UK Ministry of Defence Architecture Framework (MODAF)[63]. Similarly in Canada a Department of Defence Architecture Framework (DNDAF) has been developed which incorporates Security Views.[64] Best practice may not be agreed but there are sound arguments for basing public safety and security modelling on the DoDAF. It offers a range of products which can be employed to depict any enterprise. An on-going UK governments study has been exploring the value of architectures in improving critical infrastructure resiliency. The UK project is not yet complete but mid-term results are promising. Applying and exploiting these frameworks has highlighted the need for an associated data model and modelling 'tool'. The United Prolife for DoDAF/MODAF (UPDM) standard proposed by the Object Management

[62] ISO 31010, pp. 40
[63] http://www.mod.uk/DefenceInternet/AboutDefence/WhatWeDo/InformationManagement/MODAF/
[64] http://www.img-ggi.forces.gc.ca/pub/af-ca/index-eng.asp

Group mat help address this challenge and is having some impact with Architecture Framework application vendors.

	DATA *What*	FUNCTION *How*	NETWORK *Where*	PEOPLE *Who*	TIME *When*	MOTIVATION *Why*
Objective/Scope (contextual) *Role: Planner*	List of things important in the business	List of Business Processes	List of Business Locations	List of important Organizations	List of Events	List of Business Goal & Strategies
Enterprise Model (conceptual) *Role: Owner*	Conceptual Data/ Object Model	Business Process Model	Business Logistics System	Work Flow Model	Master Schedule	Business Plan
System Model (logical) *Role:Designer*	Logical Data Model	System Architecture Model	Distributed Systems Architecture	Human Interface Architecture	Processing Structure	Business Rule Model
Technology Model (physical) *Role:Builder*	Physical Data/Class Model	Technology Design Model	Technology Architecture	Presentation Architecture	Control Structure	Rule Design
Detailed Representation (out of context) *Role: Programmer*	Data Definition	Program	Network Architecture	Security Architecture	Timing Definition	Rule Speculation
Functioning Enterprise *Role: User*	Usable Data	Working Function	Usable Network	Functioning Organization	Implemented Schedule	Working Strategy

Simple example of the 1992 Framework.

Figure 14 Zachman Framework

DoDAF also provides for Activities Based Methodology (ABM). Organizations and systems are mapped to activities (tasks). This is useful in coupling architectures to capabilities since capabilities typically are expressed in terms of an ability to achieve desired effects through activities. If resource consumption is also associated (and time treated as resource) with activities business process simulation can be used to consider utilization rates and track information flows. Granted this is a level of detail that may not be required but illustrates the value of architectures in transitioning from conceptual through logic to physical models and from static to dynamic system behavioural analysis. Experience to date suggests that the operational views are particular useful in representing multi-agency concepts of operation and that capability views will be useful in supporting interdepartmental campaign planning i.e. investment management in instances where interdependencies are a factor.

Model integration is a challenge which is being addressed by the Architectural Framework community. Open standards are being adopted and meta-data models introduced. At the operator's level task lists have been developed to promote a communal lexicon, define capabilities and establish standards. The DHS has published a Target Capability List (TCL) and PS a Canadian version (TCL-C). It might be premature to present use of task lists as best practice but the writing is on the wall. The stated intent of the US DHS is to further tailor the TCL and introduce a tiered hierarchy based on classes of jurisdiction. "The primary purpose of Tiers is to

account for reasonable differences in target levels of capability amongst group of jurisdictions based on characteristics such as total population, population density, and critical infrastructure".[65] The TCL and TCL-C provide a capability catalogue which is being used to support exercise evaluation and requirements definition and to provide a common descriptive language of capabilities. It isn't much of a stretch to envisage it being used to inventory capabilities and to structure lessons learned.

As observed earlier capabilities provide a common currency for planners and managers. Relational databases can be used to stimulate the necessary cross walk, and cross talk. Relating capability acquisition programs (personnel or equipment) to capabilities domains assists portfolio management; whether distributed or departmental. CBP also endeavours to integrate plans over time and a temporal view is an important risk management decision support aid. Scenarios are set in time; e.g. some may be set in near future to support event or contingency planning. More commonly, and this might even be considered best practice, scenarios are situated a little beyond one capability acquisition cycle. This might be 2-3 years for a capability enhancement, e.g. minor training, process improvement or introduction into service of commercial technology, or 5-10 years in the future if a major upgrade to capability (e.g. significant equipment acquisition) is anticipated. DoDAF 2.0 provides for both a "Capability Taxonomy" (describing the partitioning scheme) and a "Capability Phasing" view (CV3) which lays out "the planned achievement of capability at different points in time or during different specific periods of time"[66]. This CV3 lays out an investment strategy and provides a departure point for developing a more detailed implementation/campaign plan. It links capability requirements to acquisition plans and a timeline. All to say that timely identification of issues and positioning scenarios is an important component of CBP, but there are constraints. Few departments, agencies and/or partners will have sufficient resources to project and analyze scenarios and generate for comparison a series of time slices. Linking capabilities to projects is a key step but to take full advantage i.e. to ensure visibility and support federated governance this information must be shared. An equivalent of the Department of Defence (DND)'s Capability Initiative Database (CID) may be order. It characterizes projects in terms of capability functions, production inputs (PRICIE dimension), timing and outputs (assets).

4.5 Supporting Decisions

Doubtless the most challenging and contentious CBP process involves the prioritization of decisions, deciding the relative merit of requirement elements and the relative importance of projects. Consensus is easier to achieve on the tactical level when needs are apparent and the focus is often on the near future, and it should not be surprising that this is where CBP is gaining traction in public safety and security. However, dependencies – not least interoperability – need to be factored in. Typically program level decisions are more problematic and call for portfolio management. Decision makers are often presented with discrete decisions on projects. Context becomes important; to understand the relationships between projects while a strategic vision and an overarching structure is required to balance competing demands. "Framing is the most difficult part of the decision analysis process".[67] A capability-based plan offers assistance in

[65] DHS, Capabilities-Based Planning: Overview, op. cit. pp. 3
[66] DOD, DoDAF 2.0, CV3, http://cio-nii.defense.gov/sites/dodaf20/CV-3.html
[67] Ronald A. Howard, Decision Analysis: Practice and Promise, Management Science Vol. 34, No. 6, June 1988, pp. 684

situating individual projects. Even then some debate should be anticipated. Stakeholders will likely have unique perspectives reflecting their organizational and personal risk profiles and time appreciations.

Thus CBP is both art and science. Not surprisingly it lends itself to a blend of hard and soft analysis. Best practices include applying Value Focused Thinking (VFT), Soft Systems Methodology (SSM) and Multi-Criteria Decision Analysis (MCDA)/Multi-criteria Decision Making (MCDM). VFT was developed by Ralph Keeney. He argued that people often focus first on identifying and comparing options rather than on articulating and prioritizing objectives. A less than fully satisfactory and even suboptimal solution can result. In VFT "values" (rating criteria) are determined before rather than after alternatives. Value analysis is an obvious complement to CBP. It provides the means to uncover hidden objectives and expand the range of opportunities being considered. The intent is to broaden thinking and encourage innovation. "The key is to start with the objectives and determine the best option rather than the more tempting practice of starting with the familiar option."[68]

CBP aspires to treat environmental ambiguity and uncertainty. Although trends may be discerned the future remains indeterminate, and the more distant is murkier than the near future. Still a plan is better than no plan, and confronting the future through planning to gain insight is valuable. In facing "wicked" problems direction rather than point solutions should be recognized as the goal, and obviously forecasts must be revisited periodically. CBP's solution to this challenge is to rely on "collective intelligence" to shape and inform scenarios. Typically Delphi techniques are used to canvas views and these, in turn, shape and complement subsequent analysis. Structured questionnaires are prepared and completed independently and anonymously by a panel of experts. Often, as reflected in the AHRA process, a 5 or 7 point scale is used, and word pictures or language ladders employed to add description to the scale. Surveys can be conducted online and web-based use opens up the possibility not only of greater participation but also of configuring panels representing different communities and comparing results. The Delphi method also provides a tool for engaging multiple stakeholders and implementing participatory policy making. Delphi techniques always involve iterative independent polling and controlled feedback/presentation of results. A facilitator summaries the results without attributing views (cluster analysis may be employed) and the pool of experts are invited to consider, possibly revise, their initial responses. This provides an opportunity for convergence and validation. At its simplest form themes and degree of consensus can be distinguished. Unanimity may not be desirable and it may be useful to investigate outliers. One analyst suggested distinguishing between areas of consensus, divergence and wildcards. Characterization along these lines would facilitate investigation of the reasons for diverging opinions and consideration of outliers.

SSM developed in response to an attempt to use apply a systems engineering approach to "wicked" managements problems. Development commenced in the late 1960s. Like CBP it "treats the notion of system as an epistemological rather than ontological entity"[69] and, like architecture frameworks, it acknowledges the existence of different perspectives. Elements of the CATWOE criteria (Clients, Actors, Transformation, Weltanschauung (Worldview), Owner, Environment) can be found in Zachman's matrix. What SSM offers is a systemic approach aimed at assuring logic and rigor in framing problems and offering decision support. It involves

[68] US Defense Science Board Task Force on Defense Intelligence, Counterinsurgency (COIN) Intelligence, Surveillance, and Reconnaissance (ISR) Operations, Officer of the UnderSecretary of Defence, February 2011, pp. 37

[69] Soft system methodology, pp. 1

interviewing key stakeholders and constructing reference and "to be" process models as a prelude to preparing recommendations. The process is intended to be iterative and SSM accommodates the use of "hard" operational research tools (i.e. linear programming, queuing theory, statistics, simulation, etc.) should such tools prove to be useful for the specific study under consideration. A prime attraction of SSM is its purported capability to address complex, "messy" problems. These can be thought of as decision impasses in which all or some of the following apply: multiple stakeholders with different accountabilities and different perspectives, multiple (possibly imprecise or even conflicting) objectives, many variables with complex interdependencies, difficulties in objectively determining measures of effectiveness, a need to incorporate risk, a need to address uncertainty, and a desire to build consensus and "buy-in" to ensure success. CBP and the best practices described incorporate significant and substantive elements of SMM.

If, using VFT, objectives have been determined, a table can be generated with using criteria as columns and options as rows (Table 3). This decision matrix/decision table is a convenient means for presenting data to facilitate a comparison of options. It constitutes a central core element of MCDA/MCDM. The criteria can be weighted and numerical scores representing aggregate utility given to options. Multi-Attribute Utility Theory (MAUT) provides a ranked ordering of alternatives based on expected utility. Some caution is in order. Although numeric values are established, the apparent mathematic precision is deceptive. The product represents informed judgment; it is a decision engineering artefact. Over emphasis on measurement may be counterproductive. As one pundit observed "building a better scale doesn't change your weight".[70] Nonetheless MAUT has advantages. It provides an objective and transparent technique for structuring comparative analysis and capturing SME (Subject Matter Expert) judgment. Sensitivity testing and examine of the spread of opinions can be used both qualitatively and quantitatively to explore the robustness of the rank ordering. MAUT is a decision support aid. It is intended more to provide insight than a definitive solution. The initial rank ordering should be reviewed and discussed. Provision is often made for a second round, mimicking a Delphi approach and providing an opportunity to "socialize" results.

	Criteria 1	Criteria 2	Criteria 3
Option 1			
Option 2			
Option 3			

Table 3 Decision Matrix

4.6 Applying Caution

The evaluation criteria must provide for additive independence for the resultant rank ordering to be valid. Even then interpretation of the comparisons will likely require explanation. A MAUT like approach has been attempted to generate predictive risk matrixes (Figure 15) and to rank order hazards. Typically risk matrices can compare only a small fraction of pairs of hazards/threats. As mentioned previously shown in the example below, "a common approach is to divide risks into 3 bands."[71] They provide a simple effective screening and socialization tool

[70] Ronald J. Baker, Measure What Matters to Customers: Using Key Predictive Indicators, John Wiley & Sons, Hoboken, N.J., 2006, pp. 3

[71] ISO 31010 Risk management- Risk assessment techniques Final Draft 2009, pp. 16

but should be accompanied by a normative approach detailing properties and attributes. Word pictures/language ladders help to illustrate scaling and assist in reducing subjectivity but don't ensure the problem space is defined fully.

Table II. Example of a Predictive Risk Matrix for the Federal Aviation Administration

Severity / Likelihood	No Safety Effect	Minor	Major	Hazardous	Catastrophic
Frequent					
Probable					
Remote					
Extremely Remote					
Extremely Improbable					

HIGH RISK
MEDIUM RISK
LOW RISK

Source: Federal Aviation Administration, 2007 www.faa.gov/airports_airtraffic/airports/resources/advisory_circulars/media/150-5200-37/150_5200_37.doc.

Figure 15 Example of a Predictive Risk Matrix[72]

The same holds true for rank ordering. It too is useful but caution should be employed in applying the results dutifully. The International Organization for Standardization observes that:

> Risks can be complex in themselves, as, for example, in complex systems which need to have their risks assessed across the system rather than treating each component separately and ignoring interactions[73]

It should be appreciated that "a priority-setting rule that rates each uncertain hazard based on its own attributes only will, in general be unable to recommend an optimal subset of co-related risk-reducing opportunities"[74]. Tony Cox concludes that:

[72] Louis Anthony (Tony) Cox, Jr. What's Wrong with Risk Matrices? Risk Analysis, Vol.28 No. 2 2008, pp. 498
[73] ISO 31010, pp. 19

> No priority rule can recommend the best portfolio (subset) of risk-reducing opportunities when the optimal strategy requires diversifying risk-reducing investments across two or more types of opportunities or when it requires coordinating correlated risk reduction from opportunities of different types (having different priority scores).[75]

The danger bureaucratization and optimization presents in seeking a deterministic process were raised at the recent TP3 workshop. Humans are better than algorithms when it comes to hedging. Probability distributions can be used effectively in some circumstances to characterize uncertainty but are ill suited to address decision challenges relating to "deep uncertainty", situations "where decision makers do not know nor cannot agree upon the system model that relates action to consequences, the prior probabilities on inputs to the system model(s), or the value function that ranks the desirability of the consequences".[76] Simulation models also have significant limitations. The observations that Groves and Lempert note with respect to water management system models can be extended to many simulations exploring public policy options e.g. "they were too complex to be adequately understood by interested parties, imbedded too many important and contentious assumptions about how the system functioned, or were too cumbersome to evaluate the many proposed management options under a wide range of possible future conditions".[77] This harkens back to Paul Davis opinion that better use could be made of simpler, more agile models. These are particularly valuable in the problem exploration phase when options are being identified, and more detailed simulation models more effective in the evaluation and system design phase. Perhaps most importantly best practice is to exploit decision support aids but recognize their inherent weaknesses.

[74] Louis Anthony (Tony) Cox, Jr. What's Wrong with Hazard-Ranking Systems? An Expository Note, Risk Analysis, Vol. 29 No. 7, 2009, pp. 945
[75] Ibid, pp. 944
[76] Groves, op. cit. pp. 75
[77] Groves, op. cit. pp. 77

5 Public Safety and Security

Although it extended and combined elements of past practice, CBP was introduced, and welcomed, as an answer to the 21st century planning challenges. The value of CBP is in harmonizing or integrating disparate planning across multiple stakeholders. Within defence, as discussed in this document, prime drivers included changes in both technology and the operational environment that necessitated breaking down the traditional service stovepipes of the army, navy and air force. Increasingly technical innovation has come from the private sector and the Area of Operational Responsibility assigned to military commanders has become congested with non-traditional partners (e.g., joint and combined operations are now the norm). In addition to the obstacles that the Service stovepipes present to a harmonized planning process, defence departments have to worry about interoperability with other national militaries. In particular, the comparative rapid pace of development by the US military has been a challenge for all of its defence partners as they struggle to maintain a reasonable level of interoperability. Further, as mentioned, militaries have found themselves working with non-traditional partners in operations where they have found it a challenge to attain unity of purpose. The latter problem has led to initiatives such as 3D (diplomacy defence and development), WoG, and 'comprehensive approaches' to achieve better effectiveness in operations. To date there has been little if any attempt at extending capability based planning across even the most important non-defence partners; probably due to the difficulties that defence has had in implementing CBP internally. The underlying challenge is acknowledgement and management of co-evolving plans. Both an agreed framework and effective governance structure are required.

This challenge is equally applicable to public safety and security. They too, whether deployed with armed forces or in responding to domestic emergencies, are faced with a requirement for concerted action. Increasingly interdependencies are one factor. The empowerment of the individual and small groups is another, expanding and compounding probability and consequence calculations. This places a premium on pre planning and prior preparations. Adopting a 'full spectrum' approach and addressing potential emergencies in their incipient phase ('left of bang') may offer more options and improve prospects for deterrence/prevention. Collaborative planning is becoming an imperative. Some areas are particularly ripe, e.g. cyberspace. A review in the US concluded that "the central problems in the current federal organization for cyber security are lack of a strategic focus, overlapping missions, poor coordination and collaboration, and diffuse responsibility."[78] It is suspected that many similar if not all of these problems also reside north of the border.

This paper focuses primarily on the Integrated Government of Canada planning and response. The arguments for adopting a 'soft' approach to CBP and the practices advocate could justifiably be broadened. Most of Canada's critical infrastructure is privately owned auguring for adopting a collaborative approach. Further, in many cases, whether appropriate or not, when emergencies arise there is a tendency to turn to Ottawa. This predisposition parallels trends in Allied countries. It represents a significant shift in attitudes and expectations attributable to society's pervasive connectivity and increasing interdependency. "Without the immediacy of modern communications technology, a disaster in one part of the country did not make an impression on

[78] CSIS Commission on Cyberspace for the 44th Presidency, Securing Cyberspace for the 44th Presidency, Centr for Strategic and International Studies, December 2008, pp. 34

people in another part".[79] The implications are significant: more than ever the government must translate the public's level of tolerance for risk into plans and programs.

5.1 The Public Safety and Security Environment

When one considers the public safety and security domain, the diversity of stakeholders is as at least as great and very likely even greater than that in defence which presents challenges to implementing CBP, and harmonizing plans. The one advantage defence departments seemingly enjoy is a unity of purpose established through the government fiat. However, in practice, the Service elements (army, navy and air force) often find themselves in direct competition for limited budgetary resources to fund the high cost of capability sustainment and replacement. Further defence's focus on a longer time horizon allows for variance in interpreting trends and forecasting the future. The lack of an arbitration process which is perceived to be 'fair' to mitigate this competition has been one of the more significant obstacles to implementation of CBP as originally envisaged.

Turning to the public safety and security community, the problem becomes more complex. There is a greater diversity amongst stakeholders:

- Not all stakeholders have safety and security as their primary mission leading to divergence in unity of purpose;

- Some stakeholders who need to collaborate for safety and security may simultaneously be commercial competitors leading to an unwillingness to even share information let alone harmonize planning;
- Governments operate at different levels and scales, and sometimes disagree on jurisdictional boundaries;
- Planning perspectives vary across stakeholders with respect to a number of factors such as experience, time horizons and risk tolerance;
- Past experiences of stakeholders working together could result in a high degree of trust amongst the group where past experience has been positive or a high degree of mistrust where past experiences were negative;
- Different stakeholders often have a different perspective on issues and often use language which is distinctive. (As noted previously, causality is difficult to establish in dealing with "wicked problems".) This can lead to unintended misunderstandings amongst stakeholders.

There is a tendency to see partnerships as all or nothing. Everyone does not deserve or need to be involved in all decisions. Return on investment factors into partnering decisions. A more useful approach might be to view coordinating and administering relationships as a form of portfolio management. "The main components of a good relationship portfolio management program include: implementing control systems; minimizing dependency risk; measuring partner performance; rationalizing the portfolio and identifying cost reduction opportunities."[80] Successful meta-organizations have established entry hurdles and performance norms, and core

[79] Patrick S. Roberts, Our Responder in Chief, National Affairs No. 5 Fall 2010, pp.83
[80] Eggers, William D and Stephen Goldsmith, Government by Network: The New Public Management Imperative, Deloitte Research & the Ash Institute, 2004, pp. 20

management capability. Aligning goals and incentives is a starting point. An agreed and effective performance measurement system is also needed to establish whether partners are fulfilling their obligations. This is admittedly easy said than done. "Outcomes in government are often murky, hard to define, harder to measure, and may take years to realize."[81] Hence the need for VFT. As Eggers and Goldsmith suggests, the challenge isn't surmountable but dependent on getting some things right. Trust reduces transactional costs and "the easiest way to create trust is to choose network partners who share your goal"[82]. It is also important to recognize that "trust is built on personal relationships and in small groups. Large diffuse groups with a floating population are not conducive to building trust". [83]

5.2 Limitations of Collaboration

As William Olson has pointed out there are limits to collaboration/coordination and a need to temper expectations. The growth of complex environments has made implementing national strategic goals more difficult and necessitated even broader coordination efforts. Modern government faces diverse demands and this is manifested in structural differentiation which has evolved over time in a piecemeal fashion. These reflect different histories and institutional lives which predate CBP. This structure was not arrived via an agreed model or approved process and typically in Western societies reflects a deliberate separation of powers and system of checks and balances that are essential in a democratic society. Harmonized and integrated "whole of society" planning processes run counter to these key elements of democracy. It follows that what is logically sound may not be practically possible or even perceived as "logical" by all stakeholders. Equally importantly and worth noting is that collaborative planning – whether capability based or not - cannot make bad policy good. Nor can it overcome challenges posed by insufficient resources and/or inadequate authority. Institutional biases and habits can also impeded collaboration. In the mind of many stakeholders the conviction exists that this serves as a cover for control. Olsen notes that in the US "constant DoD calls for more and better coordination begin to look like demands that other agencies conform to DoD imperatives and business practices".[84] Further, defence's relative institutional weight may also be resented.

However, instances of collaboration do take place. Olson suggests that:

> *Real coordination – that called for by non-routine situations – tends to take place under the pressure of circumstance, of overwhelming need in the face of demanding situations. Real coordination is almost always ad hoc. Thinking about coordination tends to take place in the shade, in a more relaxed atmosphere. It has the time to reflect, but also lacks the sort of imperatives that make real coordination necessary and thus powerful enough to overcome the natural inertia inherent to bureaucratic engagement requiring non-routine coordination*.[85]

This explains in part why acceptance of CBP in the public safety and security realm seems to be largely bottom up. Stakeholders have different mandates, governance constructs, time horizons,

[81] Ibid, pp. 17
[82] Ibid, pp. 18
[83] CSIS Commission on Cybersecurity for the 44th Presidency, op. cit. pp. 45
[84] Willam J. Olson, Chapter 5 Interagency Coordination: The Normal Accident or the Essence of Indecision, pp. 226.
[85] Olson, op. cit, pp. 242

decision cycles and incentive structures. Unfortunately, frequently, "institutional rewards and incentives, values and sentiments are near things. Coordination is a distant virtue, fine in principle but risky in practice". [86]

So should CBP be abandoned? The answer is no. Not only because the demand is obvious and growing but also because there is light ahead. Mancur Olson has observed that small groups organize before large ones and 'minority' groups can trigger change and effect outcomes. William Olson concludes that "as a general rule, coordination works best when key individuals desire it and work to make it happen on a small scale within discrete operations, for limited purposes over defined time frames, with clear lines of authority[87]" and that "in large part, interagency coordination, while resistant to grand designs and commissariat control, often occurs because the people within organizations are dedicated to outcomes that produce coordination, sometimes against all odds"[88].

5.3 Progress to Date

To date, within the public safety and security, CBP serves (and has contributed) more an organizing principle than as a planning process. There are good reasons for this. First, and rightly so, the immediate focus is on enhancing Command & Control (C2) and first responder interoperability, enhancing existing processes and leveraging available technology. Architectures have been used to support planning for major events (e.g. 2010 Olympics) and for municipal emergencies (e.g. 2011 Gateway Exercise) but in these cases the emphasis has been on integrating assets rather than requirements definition and capability generation – and the models developed have not been maintained. The public safety and security community can take a lesson from NATO, which, post-Cold War and despite being a defence organization, shares similar challenges through identifying shared goals and translating those goals into effective action. CBP provides an organizing planning structure for NATO. Nations can map their contributions in terms of assets (Force Elements) to the capability targets identified through the Alliance's Defence Requirements Review (DRR) process. In a similar fashion for public safety and security CBP can provide a useful framework for capturing an inventory of assets and competencies and for evaluating proposals for functionally oriented programs such as PSTP (Public Security Technology Program) and CRTI. The Consolidated Risk Assessment exercise which has begun may provide a launch point for placing more emphasis on CBP for WoG concept development, strategic planning and program integration. Planning to date has been largely silo'ed (see Figure 1) and department plans have focused on optimizing the employment of current assets. Times are changing. With increased investment in an increasing integrated public security and safety environment will come increased scrutiny, increased call for analysis and an increased insistence on establishing WoG procedural legitimacy. The increased risk from cyber threats may provide an opportunity to focus on next generation people, process and technology requirements. However it is difficult to see how public safety and security can be 'concept led' without providing an organizational focal point and developing a managerial process.

[86] Olson, op. cit. pp. 242
[87] Olson, op. cit. pp 249
[88] Olson, op. cit. pp 249

6 Supporting Stanchions

Distinguishing capability planning from capability generation, capability management and capability employment may be organizationally significant but should not be allowed to obscure pre-requisite vertical couplings. At the moment it would appear that priority should be given to horizontal linkages at the top and the bottom. That is plans need to be coordinated and to co-evolve and impediments to interoperability and exploitation of available assets removed.

CBP could be depicted as sitting at the intersection between risk assessment, mission analysis and systems engineering drawing best practices from each (Figure 16). One could correctly argue that foundational elements are being put in place and one (perhaps the preferred approach) is to recognize and promote progress in all of three areas. Spiral development will likely prove more effective in the long run than rigorous sequentialism. Moreover all are essentially defence agnostic and equally valid to the public safety and security realm.

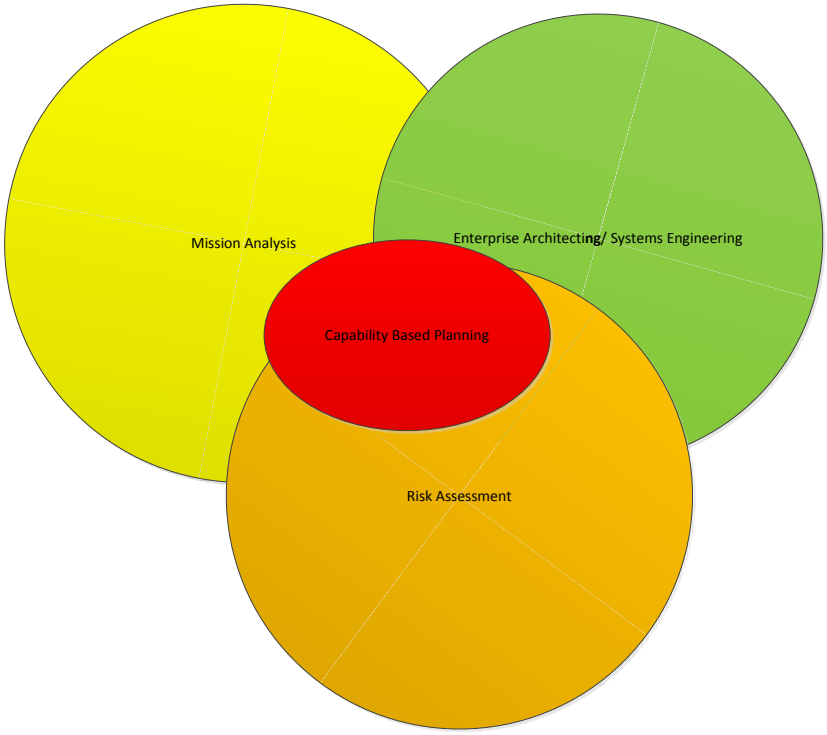

Figure 16 CBP at the Intersection

6.1 Risk Assessment

CBP aspires to integrate planning and inform prioritization, programming and budgeting. Risk management is an integral component. Risk assessment drives decision making at all levels and, equally importantly, provides a common lens across temporal spectrums i.e. from Preparation and Prevent to Recover. The institutionalization of deliberate risk assessment, reasoned judgments about threat/hazard origins and preliminary analysis of the most appropriate responses will help

routinize prudent hedging of strategy and planning.[89] It follows that CBP should follow best practices for risk management, and that introduction and adoption of the AHRA will methodology will provide a third prop to mission and systems analysis.

ISO 31000 advises that, to be effective, risk management should adhere to a set of principles. Examples of obstacles which can be anticipated in implementing CBP and managing future risks across multiple stakeholders are provided below mapped to each of the principles so that the reader can appreciate the scale of the problem. It should be noted that this list of examples is not meant to be exhaustive. A more thorough consideration should be given when implementing CBP with a given set of stakeholders.

- **Creates value.** In any multi-stakeholder environment there will be a mix of communal and individual benefits as well as varying levels of contributions from each stakeholder. Consequently it will be challenging to ensure that each stakeholder receives a return on investment commensurate with the stakeholder's level of contribution. Economics has investigated the problem of the "tragedy of the commons" where the result of individual agencies, acting rationally and in their own self-interest, will be to the detriment of long term shared values and the problem of "free riders" where by an individual agency contributes less than the benefit accrued leading to degradation or neglect of shared benefits. An example of this could include a critical infrastructure owner using security concerns around a major event as a means to use public funds to finance security measures which potentially are (or at least perceived to be) the responsibility of the owner.

- **Integral part of organizational processes.** Ideally risk management should be an integral part of each contributing partner's processes. However, in light of the issues related to communal and individual value creation, and given the diversity of stakeholders, it is unlikely that a shared risk management framework will be integral to the same degree across the community. In addition, stakeholders will often have limited visibility into the pressures and priorities and the internal structure and communication networks, both formal and informal, of other stakeholders. This makes it a challenge to appreciate to what degree the shared risk management framework is integral part of the organizational properties of external stakeholders. For example in some cases in municipalities the responsibility for mitigation versus hazards remains the responsibility of emergency management while in other cases risk management extends across all municipal functions, including, for example, land use planning.

- **Part of decision making.** Risk management that is a part of decision making will share many of the challenges of making risk management an integral part of organizational processes. However, when dealing with shared, complex problems the decision making process might need to be shared across multiple stakeholders as no one stakeholder may the complete understanding of the shared problem or of the full range of potential solutions. One characteristic of "wicked" problems is that the understanding of the

[89] Freier, op. cit. pp. 3

problem will differ by group according to their preferences to solutions (i.e., solutions become mixed into the understanding of the problem). Examples include foreign intervention in failed states where a full understanding of the challenges in stabilising a particular country requires knowledge from local citizens and authorities, intervening military, humanitarian aid organizations and diplomats; all with a tendency to view the challenge in light of the "solution" they provide (i.e., "security" for the military, "human development" for the humanitarian aid agency, etc.).

- **Explicitly addresses uncertainty.** As discussed above, full awareness of shared problems may require merging the knowledge of a number of shareholders. This implies that for any one stakeholder, there will be knowledge gaps of which they might not even be aware (unknown unknowns). In addition, the addition of more stakeholders introduces further uncertainty tied to dependencies on the degree of collaboration and relationships with other stakeholders. A shared solution to address a capability gap requires each stakeholder to rely on other stakeholders who may or may not live up to their part of the bargain. For example, consider the case of an organization that has a continuity plan to maintain operations in the event of a "300 year" flood and this plan is dependent upon another stakeholder's ability to maintain operations. If they have no knowledge of/insight into the continuity plans of that stakeholder they no longer know with certainty whether or not their continuity plans are effectual. While that stakeholder can address that uncertainty by considering alternatives the challenge of understanding dependencies two or more steps away is extremely difficult. Mutual dependence is trust based which in turn requires information sharing and understanding.

- **Systematic, structured and timely.** Operationalizing a "systematic, structured" shared risk management framework or capability based planning process will of itself likely prove a challenge. A diverse group of stakeholders will invite and often produce differing levels of resource commitments, training standards and operating procedures resulting in an overall uneven systematic and structure process. Similarly, time horizons may vary considerably. What is "timely" may have singularly different meanings to different stakeholders who operate on vastly different decision cycles. For example, an electricity company with a long term (decade plus) outlook may experience challenges working with a telecommunications company which is focused on the near term (one year "long term" time horizon) if the electricity company's capability based plans and decisions are dependent on future, unknown choices by the telecommunications company.

- **Based on the best available information.** While trust may be common reason stakeholders are reluctant to share information, there are also a number of valid and more defensible reasons why a stakeholder would not want proprietary information divulged to other stakeholders. For example, if the police divulge evidence it could jeopardize criminal investigations and prosecutions. But, in some instances, if they withhold information from other stakeholders it could increase public risk. This dilemma is often referred to as the "need to know" versus the "need to share". In a knowledge-based economy information is currency and must be managed prudently. Finally there are number of related issues e.g. timelines, accuracy, completeness, assurance that go into determining what constitutes the 'best available information'.

- **Tailored.** Without a clearly defined and agreed space problem, developing a tailored risk framework may prove impossible. Bounding is difficult particularly when faced with 'wicked problems'. A well-tailored and shared risk framework may require narrowing the scope which could mean that overall risk is not adequately addressed. Wild cards and black swans must also be accommodated. For example, airport security involves a number of stakeholders with a divergence of perspectives. Restricting a risk management framework to only few security aspects and stakeholders might seem appropriate but the exclusion of others may introduce significant gaps as analysis of events like the "shoe bomber" has shown. High reliability Organizations (HROs) operate in high risk environments and manage complex, tightly coupled systems. In assessing risk they focus on weaknesses within critical systems and on interactions between systems. All to say that appropriate tailoring is a challenge, and tied in part to culture.

- **Takes human cultural factors into account.** Understanding the culture of other stakeholders requires extensive exposure and experience and, even then, is challenging. Risk profiles may vary considerably and often reflects recent institutional history as shown by DHS focus prior to and post Katrina. For example, the military and police have extensive experience working with each other, but challenges to working together due to cultural differences are frequently observed in major event security planning. While the Olympic Maritime Operations Coordination Centre overcame these challenges for the Vancouver Olympics, it's worth noting that there were challenges despite a long shared operational history amongst maritime agencies.

- **Transparent and inclusive.** As long as information sharing remains a challenge in multiple stakeholder situations, full transparency will be unattainable. Even partial transparency will be difficult without clear agreement on when information will be or should be shared. The principle of inclusiveness introduces boundary or scoping issues. A fully inclusive approach for addressing shared risks will often mean including stakeholders who might only have a minor role related to the original risks but will bring with them additional concerns around unrelated activities. In the case of airport safety and security, if one extends airport safety and security to all agencies in the airport that may have a role in safety and security it will likely introduce the stakeholders, such as merchants at the airport, whose primary activity is not safety and security but selling goods to travellers. In addition, airport safety and security is dependent on external agencies such as first responders who, even if safety and security is their primary responsibility, have extended areas of responsibility well beyond the airport. Where the "boundary" of the problem is drawn will significantly affect both the understanding of the problem and the range of potential solutions, yet there may be a lot of unknowns that will impede the ability of a group of stakeholders to do so.

- **Dynamic, iterative and responsive to change.** Implicit in much of the above discussion is that managing a group of diverse stakeholders involves time consuming activities like negotiation. Making it through the risk management or capability based planning process once will be difficult. Doing so iteratively, as is suggested by best practice and in a dynamic and responsive manner is even more so. In particular, once stakeholders have come to an agreement after a lengthy process them may not be inclined to re-visit that process. The archetypal examples are international organizations such as the North Atlantic Treaty Organization (NATO) which use a consensus decision making processes. Frequently they are accused of being slow or even non-responsive when a

situation seemingly calls for urgency and the legitimacy and authority bestowed by a negotiated, consensus decision is under appreciated.

- **Facilitates continual improvement and enhancement of the organization.** Many individual organizations aspire to be "learning organization" but find it a challenge to do so. Becoming a "learning" multi-organization is even more difficult. Stakeholders that may internally admit to flaws may be reluctant to share this information with partner stakeholders. If something has gone wrong when there are legal or other accountability implications, acknowledging even the need for improvement may only come as a result of an external, formal inquiry. Examples in this area are plentiful and none will be mentioned out of courtesy. Finally it's worth noting that even when an operation has gone well perhaps more due to luck than the collective effectiveness of stakeholders, there's very little incentive for stakeholders to recognize flaws and hence the need for improvement even though not doing so could have major risk implications for the future.

Implicit in the ISO 31000 guidance for effective risk management across is an agreement on what is the enterprise for which risk is being evaluated. Broad statements, such as "reducing risk to the community from all hazards" are obviously open to various interpretations. Also implicit in the ISO 31000 guidance is that there is a clear overall governance structure for managing risk. The challenge to implementing an effective risk management framework is not surprising as a key aspect of multi-stakeholder collaboration is that while stakeholders work together for a common goal they also seek to maintain their autonomy which is counter to the CBP objective of harmonizing or integrating planning. The task of harmonizing multi-stakeholder planning falls into a class of problems, for which there are significant social, economic and political factors, known as "wicked problems". There are several characteristics of wicked problem, and a primary one relevant to CBP is that each stakeholder will see the problem differently and usually in terms of solutions preferred by each stakeholder, which is counter to the intent of CBP to avoid committing to decisions to early in the process. This implies that there is a significant danger when leadership for implementing CBP is dominated by a subset the stakeholders. Yet, getting all stakeholders to act together without a clear overall goal may well be impossible. Perhaps the challenge of balancing the need for leadership with the need to respect stakeholder perspectives may be the greatest challenge to implementing CBP. However, there is promise. Recent research[90] indicates that effective collaboration can be directed and can be taught as a skill provided organizations recognize the distinction between deeper collaboration to solve problems and coordination that is primarily information sharing.

6.2 Mission Analysis

We need to add very little here to the discussion in the previous chapter. Increasing use has been made of scenarios post-911 to characterize the environment and support planning and training. An increasingly number of missions that may be defence-relevant but are not defence-specific has been identified. In the public safety and security realm mission-to-task analysis using the TCL-C is being conducted to support municipal exercises. Capabilities can be used to describe

[90] Lemyre, L.; Research Using In Vivo Simulation of Meta-Organizational Shared Decision-making (SDM) - Task 4: Modeling of Communication and Decision Functions within a Shared Decision-making (SDM) Framework, DRDC CSS Contractor Report, draft.

functional requirements and can serve as an organizing principle. This avoids prematurely constraining solution providers, whether industry/academia in the case of procurement programs or OGDs in the case of contingency planning or operations; for example, some use has been made of capability catalogue/registers. Perhaps equally importantly mission analysis and architecture frameworks have been and are being used to support simulation interactive training. NATO and some of the TP3 nations are also conducting post hoc mission analysis and framing lessons learned in terms of capabilities. It is worth noting that personnel from OGDs now regularly attend and are familiar with the Canadian Forces' Operational Planning Process. However, exposure to structured mission analysis remains ad-hoc and a wider educational effort is needed.

6.3 Systems Engineering/Enterprise Architecting

Systems Engineering and Enterprise Architecting are becoming mature disciplines and recognized, established practice in government. They provide a method and tools for modelling and understanding intricate systems and systems of systems. There are now dedicated courses, recognized certification programs, and a growing pool of expertise. Many of the CBP principles reflect Systems Engineering thinking. Recognition of the need to consider life cycle costing and through life capability management has provided further impetus and solidified systems engineering as a supporting specialization.

The International Council on Systems Engineering (INCOSE) views Systems Engineering as a profession, a process, and a perspective:

- A discipline that concentrates on the design and application of a system or system of systems, taking into account all variables and relating social to technical aspect, as distinct from the parts

- An iterative process of top-down synthesis, development, and operation
- An interdisciplinary approach and horizontal orientation.

Notably these accords with a WoG approach. Systems Engineering also recognizes that decisions made early in the life cycle can have enormous implications. The challenges are similar:

- System elements operate independently
- System elements have different life cycles.
- The initial requirements are likely to be ambiguous
- Complexity is a major issue
- Management can overshadow engineering
- Fuzzy boundaries cause confusion
- Systems of Systems (SoS) engineering is never finished[91]

MITRE has observed that "engineering" mega-systems is inherently "messy". The boundaries are ambiguous, expectations are continuously changing, unanticipated opportunities emerge and the cooperation and competition mix between stakeholders and participants is prone to shifting.[92]

[91] INCOSE, Systems Engineering Handbook,(version 3.1) August 2007, pp.
[92] Al Grasso, *MITRE and Systems Engineering….Engineering Systems*, Presentation to Defence Research and Development Canada, Washington, 6 January 2006.

Enterprise Architecting is also becoming mainstream, driving interoperability standards and elevating planning to departmental and WoG levels. Enterprise architecting encourages common business practices. While the immediate focus is on Informational Technology it is not hard to imagine extending and exploiting documented architectural descriptions and reference models. Architects are valuable because they provide a means to capture and represent knowledge and a scalable reference. The problem space is dynamic and policy makers and planners have to focus on moving targets. Organizations deal with this challenge in a variety of ways, most commonly through narrowing and "locking down the problem definition"[93]. To be clear the system boundaries and architecture scope need to be defined to support analysis; the challenge and promise is that models can be integrated to support synthesis.

[93] Tackling Wicked Problems, op. cit. pp. 12

7 Way Ahead

So what's ahead for CBP and what does that augur for public safety and security?

Not surprisingly there has been 'push-back' to capability-based planning. Some of the criticism may be deserved; CBP is in danger of failing to live up to the hype. In particular, only now are the practices and tool suite maturing. However, and more disconcertingly, it appears some of the resistance stems from opposition to the centralization of policy authority and resentment of heightened expectations that implementation activities will be harmonized within government and with external partners. Those drivers aren't going away. Resourcing may be a more legitimate concern. Analysis and synthesis are required to support holistic planning and program integration. The argument is that costs savings should fund this increment. One of the most important lessons learned from defence is that allowance must be made for transaction costs and that incentives must be offered.

There is no doubt that the world has changed. Globalization and empowerment of individuals have altered the security environment significantly placing increased claims on pre-planning and analysis to support an accelerating decision cycle. Hence, increasingly planning must be holistic and future and preventive oriented. The past distinctions drawn between deliberate/contingency and immediate/operational planning have blurred. It is interesting to note in passing that, at least in the CF, Mission Analysis now mimics Operational Planning Process (OPP). At the same time it is important to distinguish between CBP modules and understand that the required skill sets will differ. 'Analysts' may be best positioned to interpret strategic guidance and identify scenario drivers and 'planners' best positioned to identify task and support mission analysis. Generally speaking 'operators', the actual actors, are well placed to conduct subsequent determination of asset requirements and the prioritization of gaps. As noted the initial challenge is to develop an effective crosswalk between communities and their respective taxonomies and associated task lists.

Interaction between the three - analysts, planners and operators - is vital to develop a shared appreciation of issues and appropriate and ensure accurate information as fidelity demands expand in moving from conceptual to physical models. The UK NITEworks has distinguished 3 types of "interventions".[94] The first being policy interventions which CBP can play a supporting role capturing the difference between policy options in terms of fairly generic capability requirements. CBP plays an even more significant role in the second, requirements interventions. It can be exploited to determine and describe functional specifications and to evaluate options. Architecture frameworks are particularly useful both here and in considering opportunistic interventions, i.e. openings, often identified bottom-up, to exploit technology, import new practices and/or leverage external programs. They provide the means to design and develop integration plans. CBP offers a structured approach to align supporting analysis, and an evolutionary and iterative approach to engage planners in requirements definition and system design.

CBP was adopted to assist in coping with environmental complexity and uncertainty. Innovation and hedging are key components. Innovation often occurs at the intersection of disciplines; cross

[94] UK Ministry of Defence, Experimental Network Integration Facility (ENIF) Scoping Study March 2003, pp. 42

pollination is a proven enabler i.e. the value of collaboration (the wisdom of crowds) should be recognized. Diversity can help overcome some 'bad habits', such as:

- Cognitive consistency: People tend to relate unfamiliar events or facts to what they already know, thus ignoring key inconsistencies that are critical to understanding the problem at hand and solutions that might work
- Evoked set: People tend to look for the familiar, the known, and overlook the new and different, thus tending to make decisions that are familiar but not necessarily situational astute
- Mirror image: People tend to see the bad in others and the good in themselves, assuming the worst in intentions in others and the best of motives in their own efforts
- Group think: People in groups tend to fall in line with the common outlook or emerging consensus, overlooking contradictory information or approaches that go against the grain
- Sufficiently Satisfying (i.e., Satisficing): People often stop with "good enough" solutions, going for what is at hand or is familiar and not examining possibilities in more depth[95]

Francis Fukuyama argues that "hedging against future risks… also requires collective action, specifically a sharing of decision authority and a pooling of resources across organizational and international boundaries"[96]. It is resourcing and governance adjustments which have lagged.

Strategy-led planning can be a challenge in a multilateral context. Implementation pace and practice will vary, and will be in some cases be event driven. The challenge lies in applying precepts to novel circumstances. There may be a tendency in debate to conflate strategic, operational and tactical/technical issues and to resist change. "Pervasive uncertainty tends to strengthen the position of the status quo".[97] CBP can serve adaptation by circumscribing autonomy by relating plans to a central vision and by breaking down organizational and intellectual barriers and offering a wider range of alternatives. Uncertainty can be mitigated to some degree by wide-ranging and objective analysis.

Effective governance and information management are key enablers. A federated approach to adoption is developing and offers the greatest prospect for success. Writ large, public safety and security can be viewed in part as a meta-organization, an association of autonomous members each of whom retains separate identify and equal standing. Typically the central authority is weak; it is a shared or common purpose enabled by connectivity which establishes the meta-organization. Decision authority overlap is characteristic and "meta-organizations often have trouble when determining whether a decision should be made at a meta-organizational level or at an organizational level"[98]. A constant flow of information is required to allow for continual assessment, alignment and adjustment. This flow both reflects and creates trust. One of Public Safety Canada's key roles is to promote and manage the exchange of information. "Contemporary conceptualizations of governance are placing more emphasis on the interdependency between government and non-government organizations with the central government role becoming more of a coordinator and manager of networks through facilitation

[95] Olson, op. cit. pp. 237
[96] Francis Fukuyama, Blindside: How to Anticipate Forcing Events and Wild Cards in Global Politics, Brookings Institute, Washington, D.C., 2006, pp. 171
[97] Carl Conetta, We Can See Clearly Now: The Limits of Foresight in the pre-World War II Revolution in Military Affairs (RMA), Project on Defense Alternatives, March 2006, pp. 12
[98] Lemyre op. cit. pp 39

and negotiation."[99] Membership is usually voluntary and there are fewer conventions and rules than lends credibility and legitimacy. Fortunately, the need for (open) standards – meta-informational storage and exchange protocols – has been recognized and specifications are being developed.

CBP has obvious advantages and attractions as means to promote policy coherence. The underlying logic model reflects tried and tested Operational Research principles now being applied to planning; it incorporates prior planning approaches and combines essential elements of art and science. It recognizes interdependencies and the need for increasing collaboration and integration offering public safety and security a maturing approach to holistic planning. Transparency and open deliberation are key elements of CBP and consistent with best business practice. Perceptions of decision legitimacy are important and need to be addressed. Transparency goes some way to recognizing the public as a partner in public safety and security. In sum, CBP has much to commend it and is likely to remain theoretically favoured for some time.

No doubt the lack of agreement on taxonomy impedes communication. "A critical feature of any worthwhile analysis is discipline in the use of language".[100] Disparate mandates and the misalignment of incentives is a more significant problem. Without a properly structured 'market', departments and agencies may opt rationally to under invest if the costs of decisions are borne by others. "In an increasingly interdependent networked economy of the developed world, 'such deviations from optimal security decisions may cascade through the whole system'". [101] CBP won't solve but may contribute to informing the problem.

CBP's ambition within the public safety and security realm should be admitted. Trying to pursue a bold agenda with a weak mandate is a high risk proposition if not a recipe for failure. Implementation will require support from leadership if challenges are to be met and CBP is to realize its potential. This is important but appears more treatment of the symptom than disease. Leaders are required to make decisions under conditions of uncertainty. Information is never complete and perfect and managers on all level accept that they must act before all the facts are in. They must consider what is known, make reasonable assumptions, weigh probabilities, gauge risk, and assess the costs and benefits of acting or not acting and of the options presented. CBP offers the *means* to provide decision support. It does not serve and will not survive if it is portrayed as an *end*.

Senior management are faced with making a series of discrete decisions and CBP needs to demonstrate value added in informing options. Capacity is not evenly distributed and challenges don't come neatly packaged. Some thought needs to go into considering when and where to apply CBP and acceptance that take-up and application will be uneven. It has the ability to enable collaboration and planning across stakeholders and can and is being used as an organizing principle to establish communities of interest. At the same time it should be recognized that there are transactional costs associated with generating and sustaining networks and meta-organizations. As Ron Howard observes the question of how much decision analysis is an economic one.[102] Gross benefits need to be reviewed and validated periodically. The intent was

[99] Ibid pp. 45
[100] Sommer, op. cit. pp. 81
[101] Sommer, op. cit. pp. 48.
[102] The rule of thumb he offers is 1% i.e. spend at least 1 percent of the resources to be allocated on the question of how they should be allocated.

never to replace existing structural stovepipes with new stovepipes based on capability domains but, rather, to introduce a unifying perspective. Target Capability Lists can be used to institute standards and serve an organizing function but in applying CBP most countries (the UK Ministry of Defence being the exception) have not forced integration nor imposed/substituted a capability based organizational structure. The TCL-C can be used to foster semantic interoperability and provides a framework for registering requirements and inventorying assets. Leadership and a commitment to a greater exchange of information is a critical enabler. Another critical enabler is providing diagnostic advice. Analytical resources are a valuable and limited resource but the informative value provided by analysis is an essential enabler. It follows that collaboration should start here. The CSS is well positioned to support CBP implementation.

8 Conclusion

A number of conclusions can be drawn and lessons learned from the CBP experience to date. As CBP extends into the public safety and security realm planners should:

- Recognize the nature of the environment
- Acknowledge the requirement for holistic planning
- Endorse the aims and underlying principles of CBP
- Accept that implementation will be uneven
- Adopt a federated governance model
- Address the requirement for supporting people, procedures and tool elements
- Learn from and leverage the defence CBP experience

The problem space itself has become integrated, and the blurring of boundaries between operational services, between departments and between public and private sectors will likely continue. Interdependency both breeds vulnerability and presents opportunity. The operating environment will be characterized by complexity and change and driven by accelerating decision cycles. Planning has become indispensable and more difficult. One of the first requirements is to develop the capability and capacity to conduct holistic planning and effect 'integrated delivery'.

A holistic planning approach is required to consider and address inter-domain, cross-cutting public safety and security issues - "wicked problems". A 2008 Australian study into Homeland and Border Security concluded, arguably the obvious, that "departments and agencies concerned must be well connected and networked, and cultural and, technical and other barriers minimized".[103] While objectives may be shared perspectives will differ. A shared taxonomy and inclusive, integrative, non-prescriptive process is required to support WoG, eventually Whole of Society (WoS), preparation and mobilization in response to natural emergencies and malicious attacks.
CBP has simple but ambitious aims. It aspires to promote innovation and support analysis, to combine inspiration and organization. Schwartz and Randall argue that "one cannot foresee strategic surprises without being imaginative, but the results will not be believed without being systematic".[104] CBP represents an attempt to recognize the reality of a complicated and complex world and apply method to madness.[105] It presents a sound logic model. Supporting elements include risk assessment, mission analysis and system engineering. CBP's willingness to explore alternate solutions is fitting. It has been suggested that complex adaptive problems require complex adaptive solutions. CBP's emphasis on concepts is intended to foster an ability to address unconventional problems. Finally the increased transparency CBP offers will assist in building trust and establishing a sense of procedural legitimacy.

The TP3 model captures key elements of the CBP process but does not articulate them in great detail. The benefit of excluding details is that the model can be applied widely, across nations and across the tactical to strategic continuum. Implementation becomes subject to interpretation

[103] Ric Smith, op. cit. para 5
[104] Peter Schwartz and Doug Randall, Ahead of the Curve (Chapter 9) in Fukuyama ed. Blindside, pp. 97-98

and modification. TP3 presents a simplified linear model. The defence experience suggests that (and this really doesn't come as a surprise) this ideal is unachievable in practice. The 'real world' keeps intruding and imposing inconvenient, out-of-sequence demands. The model doesn't portray well the interplay between serial and parallel activity and the sheer complexity of the process. Public safety and security planners, "purists" in particular, should acknowledge and accept this.

The TP3 model does identify clusters of activities which, to some degree, modularize CBP. Workshops have been held to exchange information and develop best practices for individual process elements, and some of these have been discussed in the paper. The significance for public safety and security is recognition that CBP can be introduced and institutionalized incrementally. Although the logic may be accepted implementation will likely be driven by exogenous drivers and organization demands. This uneven pace will try the patience of some and will likely result in some transactional costs but will help embed CBP. These will subside somewhat once procedures are established and decisions are 'routinized'. The first step is to establish broad policy goals.

Collaborative planning will require coordination and governance. This paper has argued that a federated model and distributed leadership with centralized policy formulation and decentralized execution, offers the best return on investment. This approach exploits the emergent business environment and network management practices. It urges herding rather than stampeding as a first step in establishing stakeholder buy-in, recognizing that organizational mandates and autonomies must be respected, self-organization and self-synchronization promoted and allowance made for socialization. As noted the TP3 model needs to provide for mediation. A portfolio approach to relationships management is recommended partner diversity and environmental dynamics. A study of meta-organizational dynamics suggests that a core group will be required to provide direction and incentives, and that processes and norms will develop over time. Time permitting, consensus confers legitimacy and authority.

Meanwhile the required supporting people, processes and tools elements can be further developed. A range of tools and techniques and skill sets is required to support CBP. There is no right (staff) answer when it comes to foretelling the future and/or evaluating intangibles. Collecting more information will not resolve uncertainty. 'Wicked problems' require analysis in multiple dimensions, not the least the "wicked problems" are primarily social science phenomena but the field of social science is highly fragmented with no common language, such as mathematics provides for the natural sciences, and is difficult to amalgamate. "Some of the social science is primarily observational, and other parts are quantitative and rigorous but narrow."[106] Reliance must be placed in facilitation/elicitation methodologies and subjective judgement. At the same time overconfidence can be placed on the results of methods, such as MAU, that are designed to generate insights not answers. Traditionally the Operations Research community which has supported planning and analysis has focused recruiting efforts on 'hard' scientists and mathematicians. The value of "people skills" and the need to complement and balance this core with 'soft' scientists have been recognized and are being readdressed. The import for public safety and security is to concede that not everyone is equal and/or best equipped to serve as a planner and analyst. There is a need to better understand the essential skill sets. Many of those Stephen Goldsmith and William Eggers identify as prerequisites for network management

[106] Davis, Paul K., Kim Cragin editors, Social Science for Counterterrorism: Putting the Pieces Together, RAND, 2009, pp. xxxix

(negotiation, contract and contact management, team building) are equally applicable to collaborative planners.[107] Analysts are specialists in their own right, the best of breed driven by intellectual curiosity and informed by knowledge and experience. It would be an exaggeration to use a 'don't try this at home' analogy but equally wrong to dismiss out of hand the contribution professional analysts bring to the table.

CBP is more a series of processes than one process. One of the lessons learned from defence is to tailor decision support – comparable to reading the question - and avoid trying to delve into detail too early. There is a penchant to overcomplicate. Tactical specifics may do little to clarify strategic choices. Timing is important; knowing when to decide is in itself significant. Ideally demand should be consumer driven and customized. It behoves us to concede that, in practice, the planning process is shaped as much if not more by planner push than policy pull. Simple, agile exemplars can be elaborated on and high fidelity models developed subsequently as required. It is also noteworthy that most nations separate policy option from capability option comparisons, and needs analysis from solution analyses. A distinction can also be made between capability options and program options, solutions and campaign planning.

Procedures and tools can also be viewed from the three supporting stanchions:

- Risk Assessment: Risk assessment provides a means to develop a shared appreciation of the environment and challenges and the departure point for development of a WoG/WoS risk management framework. Most of the theoretical legwork has been done; a common framework will facilitate aggregation. Public Safety Canada has a common taxonomy with the TCL-C, compatible with the TCL of DHS – fulfilling a key imperative to be interoperable with Canada's most significant international partner, and has initiated a trial implementation program. One of the keys to success will lie in grafting onto existing organizational structures and practices. Risk Assessment informs the selection of drivers and scenarios. Again a fairly mature methodology exists, and it is worth underscoring that this is another area where more may not translate into better.

- Mission Analysis: One of the biggest challenges on the horizon relates to developing appropriate mission-oriented task hierarchies and lattice works relating capabilities to assets and planning to management. The TCL-C needs to be expanded and to mature. This is a thorny challenge. The mission provides context and rationale, a strictly functional task description without setting and purpose may be susceptible to misinterpretation. This is an area in which the Centre for Security Science can, and arguably should, play a leading role. CSS can also advise on the mechanics required to support virtual communities and collaborative knowledge sharing across geographic and organizational divides e.g. extranets, webinars, portals, electronic rooms, modelling & simulation.

- Systems Engineering: This brings us to systems engineering. A useful distinction is often drawn between complicated and complex. Interdependence and inclusion increases the number of factors and interactions rendering a system complicated (i.e., characterized by having many moving parts). In comparison complex systems are characterized by non-predictive behavioural changes: patterns may be discernable but small differences in

[107] Goldsmith, Stephen and William D. Eggers, Governing by Network: The Shape of the Public Sector, Brookings Institute Press, 2004.

initial conditions and/or minor perturbations may produce significantly divergent outcomes.[108] Generally speaking, uncertainty cannot be eliminated at the complex systems-of-systems level. System engineering is useful for capturing assumptions and constraints, less so for establishing them. System engineering principles do provide a set of guiding principles and system engineering practices a valuable design and development methodology but CBP is more than systems engineering. Calculation must be preceded and complemented by creativity. One of the lessons drawn from CapDEM is that capability engineering can't be allowed to dominate capability planning. Another more positive conclusion was that architecture frameworks can be used to help span the gap, to discipline concept articulation and to convert logic models into physical models. A corollary is to treat conceptual determinism with caution recognizing that precision inferred does not diminish the uncertainties related to known unknowns.

There are other lessons to be learned and best practices which can be imported from both the public and private sectors. Most have been discussed; one has not. Foremost among the lessons learned is the need for adaptability. Successful business enterprises survive and succeed by anticipating trends and revising plans. CBP is a means not an end and that it will likely mutate as it matures. One of the keys to success for public safety and security is to become a learning community. Culture is the intervening variable between intent and implementation. There is considerable literature available on how to systemize organizational learning. Sullivan and Harper posit a six step cycle: targeting opportunities, collecting data, creating knowledge, sharing expertise, completing short term applications and conducting long term applications.[109] Lemyre et al have identified key learning strategies (Figure 17) – this goes some way to suggesting how to approach implementation of CBP. Establishing an institutional memory and champion are a part of the first step.

Key learning organization strategies
• Action Learning
• Cross-Functional Teams
• Work-outs
• Strategic planning
• Parallel learning structures
• Corporate Scorecard
• Benchmarking
• Groupware
• Distance conferencing

Figure 17 : Examples of Learning Organization Strategies[110]

CBP has obvious advantages and attractions as a means to promote policy and program coherence. It recognizes interdependencies and the need for increasing collaboration and

[108] Alberts and Hayes suggest complex endeavours involve multiple independent command chains, actors with differing value and perception of circumstances and indeterminate cause and effect relationships. Alberts, D .& Hayes, R. Planning Complex Endeavours, http://www.dodccrp.org/files/Alberts_Planning.pdf

[109] Gordon R Sullivan and Michael V. Harper, Hope in Not a Method: What Business Leaders can Learn from America's Army, Random House, New York, 1996, pp. 206-207. There is a good follow-on discussion of organizational learning in John A. Nagl, Counterinsurgency Lessons from Malaya and Vietnam: Learning to Eat Soup with a Knife, Praeger, Westport, Connecticut, 1966.

[110] Lemyre et al. op cit. pp. 70

integration offering public safety and security a maturing approach to holistic planning. Transparency and open deliberation are key elements of CBP and consistent with best business practice and with acceptance of the public as an essential partner. Perceptions of decision legitimacy are important. Transparency goes some way to recognizing the public as a partner in public safety and security. In short, CBP – in one guise or another - is likely to remain a preferred planning practice for some time. However, varying size of organization amongst stakeholders and authority imbalances can inhibit the required collaboration inherent in CBP. Hence implementation will require support from leadership if challenges are to be met and CBP is to realize its potential. CBPs ambition should be admitted and valued. Trying to pursue a bold agenda with a weak mandate is a high risk proposition if not a recipe for failure.

To reiterate, while for defence CBP represents an evolution, for public safety and security it may be more akin to a revolution sparked by elemental changes in the environment - pervasive and ambiguous threats and mounting complexity and interoperability challenges. This has precipitated a requirement for collaborative planning between public safety and security stakeholders. CBP may not hold all the answers (sometimes government is fragmented for good reason and 'wicked' problems are intractable) but CBP does offers sound precepts and the means to promote innovation and integration. Although the governance challenges may differ the Allied TTCP defence community has established some 'best practices' which can be exploited.

This paper has identified some first steps for introducing CBP to the public safety and security sector that include:

- Identifying and establishing an institutional champion;
- Identifying and establishing a means of institutional memory;
- Establishing policy goals to outline the scope of capability based planning within the sector;
- Collective risk assessment as a starting point for the development of collective objectives; and
- Building towards collaborative planning by ensuring stakeholder buy-in at all stages ("herding" not "stampeding").

It's time to take the bull by the horns.

References

Alberts, D.S. & Hayes, R. E. (2006). Planning Complex Endeavors. U.S. Department of Defense, Command and Control Research Program (CCRP), Washington, D.C. April 2007 http://www.dodccrp.org/files/Alberts_Planning.pdf

Australian Government, Defence Procurement Review 2003, M. Kinnaird Review Chairman, prepared for Dr. Peter Shergold, Department of the Prime Minister and Cabinet and Chair of the Secretaries Task Force on Defence Procurement, Australia, http://www.defence.gov.au/dmo/publications/dpr_report.pdf

Australian Government. Tackling Wicked Problems: A Public Policy Perspective, 2007
Caudle, Sharon L. *Homeland Security Capabilities-Based Planning: Lessons from the Defence Community*, Homeland Security Affairs, Volume 1 Issue 2, 2005

Baker, Ronald J. Measure What Matters to Customers: Using Key Predictive Indicators, John Wiley & Sons, Hoboken, New Jersey, 2006

Checkland, Peter and Holwell, Sue, " 'Classic' OR and 'Soft' OR – an Asymmetric Complementarity", in *Systems Modelling: Theory and Practice*, edited by Pidd, M., John Wiley & Sons, 2004.

Chief of Force Development. Capability Based Planning Handbook Version 6.2. National Defence, December 2010

Chim, Leung, Rick Nunes-Vaz and Robert Prandolini, *Capability-Based Planning for Australia's National Security*, Security Challenges, Vol. 6, No. 3 (spring 2010), pp. 79-96
Cox, Louis Anthony (Tony) Jr. *What's Wrong with Risk Matrices?*, Risk Analysis, Vol. 28, No. 2, 2008, pp. 497-511

CSIS Commission on Cyberspace for the 44th Presidency, Securing Cyberspace for the 44th Presidency, Centr for Strategic and International Studies, December 2008

Conetta, Carl. We Can See Clearly Now: The Limits of Foresight in the pre-World War II Revolution in Military Affairs (RMA), Project on Defense Alternatives, March 2006

Cox, Louis Anthony (Tony) Jr. *What's Wrong with Hazard-Ranking Systems? An Expository Note*, Risk Analysis, Vol. 29, No. 7, 2009, pp 940-948

Davis, Paul K., Kim Cragin editors, Social Science for Counterterrorism: Putting the Pieces Together, RAND, 2009, pp. xxxix

US Defense Science Board Task Force on Defense Intelligence, Counterinsurgency (COIN) Intelligence, Surveillance, and Reconnaissance (ISR) Operations, Officer of the UnderSecretary of Defence, February 2011

De Spiegeleire, S., P. van Hooft, C. Culpepper and R. Willems. Closing the Loop: Towards Strategic Defence Management, The Hague Centre for Strategic Studies, The Hague, The Netherlands, March 2009

DHS, Capabilities-Based Planning: Overview, http://www.scd.hawaii.gov/grant_docs/Capabilities_Based_Planning_Overview_12_17.pdf

Eggers, William D and Stephen Goldsmith, Government by Network: The New Public Management Imperative, Deloitte Research & the Ash Institute, 2004

Frier, Nathan. Known Unknowns: Unconventional 'Strategic Shocks" in Defense Strategy Development, November 2008, http//www.StrategicStudiesInstitute.army.mil/

Goldsmith, Stephen and William D. Eggers, Governing by Network: The Shape of the Public Sector, Brookings Institute Press, 2004

Grasso, Al. MITRE and Systems Engineering….Engineering Systems, Presentation to Defence Research and Development Canada, Washington, 6 January 2006

Groves, David G. and Robert J. Lempert, A new analytical method for finding policy-relevant scenarios, Global Environmental Change (17), 2007, pp. 73-85, http://www.rand.org/pubs/reprints/RP1244.html

Howard, Ronald. Decision Analysis: Applied Decision Theory, 23 September 2008

Keeney, Ralph. Value Focused Thinking: A Path to Creative Decision Making, February 1996.
Freisen, Shaye K., Doug Hales, Neil Chuka, Charles C. Morrisey and Peter Race. Covering the Bases: Development of a Framework for Defence Force Planning Scenarios, 15th International Command and Control Research & Technology Symposium, Paper ID 029

Hales, Douglas and Peter Race, *Applying a Framework for Defining Emergency Management Scenarios*, Journal of Emergency Management, Vol. 9 No. 1, January/February 2011, pp. 15-24

Hall, Wayne M. Shaping the Future: A Holistic Approach to Planning, US National War College, March 1992

Hodge, Richard. A Systems Approach to Strategy and Execution in National Security Enterprises, PhD Thesis, University of South Australia, 31 January 2010

Howard, Ronald A. *Decision Analysis: Practice and Promise*, Management Science Vol. 34, No. 6, June 1988, pp. 679-695

International Organization for Standardization, ISO/DIS 31010 Risk Management – Risk assessment techniques, Final Draft, 2009

International Organization for Standardization, ISO/DIS 31000 Risk Management – Principles and guidelines on implementation, Draft, 2008

Lemyre, L. el al, *Research Using In Vivo Simulation of Meta-Organizational Shared Decision-making (SDM) - Task 4: Modeling of Communication and Decision Functions within a Shared Decision-making (SDM) Framework*, DRDC CSS Contractor Report, draft

NATO Research and Technology Organization, Handbook on Long Term Defence Planning, RTO Technical Report 69, April 2003

Olson, William J. *Interagency Coordination: The Normal Accident or the Essence of Indecision*, Chapter 5 in The Affairs of State: The Interagency and National Security, Gabriel Marcella editor, Army War College, December 2008, http://www.StrategicStudiesInstitute.army.mil/

Rodman, Peter W. Presidential Command: Power, Leadership, and the Making of Foreign Policy from Richard Nixon to George W. Bush, Alfred A. Knopf, New York, 2009

Smith, Ric. Summary and Conclusions: Report of the Review of Homeland and Border Security, December 2008, http://www.dpmc.gov.au/media/statement_2008_12_04.cfm

Wikipedia, The Zachman Framework, http://en.wikipedia.org/wiki/Zachman_Framework

Working with scenarios, risk assessment and capabilities in the National Safety and Security Strategy of the Netherlands. October 2009
http://www.misrar.nl/UserFiles/File/BP_1_ZHZ_annex%202%20National_Riskassesment__English(1).pdf

Annex A: DRDC CSS CBP Logic Model

The CBP logic model used by the DRDC Centre for Security Science (CSS) is found below in figure 18. The DRDC CSS logic model has been derived from the TP3 model discussed in the main body of the report. It has been modified to include a more explicit reference to risk assessment. It should be noted that DRDC CSS logic model has not included an explicit reference to "Government Guidance". That has been because the strategic policy guidance for CSS is implicit in its mandate. However, it is an unfortunately omission since it can mislead some into thinking that the CBP is a bottom-up planning process. Nothing could be further from the truth. CBP has always been intended as a planning process that is informed by bottom-up operational insights but driven by top-down guidance.

Figure 18 : DRDC Centre for Security Science CBP Logic Model

List of symbols/abbreviations/acronyms/initialisms

3D	Diplomacy, Defence and Development
ABM	Activities Based Methodology
ADF	Australian Defence Force
AHRA	All Hazards Risk Assessment
C2	Command and Control
C4ISR	Command, Control, Communications, Computers, Information, Surveillance and Reconnaissance
CapDEM	Capability Definition, Engineering and Maintenance
Clients, Actors, Transformation, Weltanschauung (Worldview), Owner, Environmental constraints	
CBP Capability Based Planning	
CBRNE	Chemical, Biological, Radiological-Nuclear and Explosives
CD&E	Concept Development and Experimentation
CF	Canadian Forces
CID	Capability Initiative Database
COA	Course(s) of Action
CONOP	Concept of Operation
CORA	Centre for Operational Research (DRDC)
CRTI	CBRNE Research Technology Initiative
CSS	Centre for Security Science (DRDC)
CV	Capability View (for DoDAF)
DDR	Defence Requirements Review (NATO defence planning process)
DND	Department of Defence
DNDAF	DND Defence Architecture Framework

DoD	Department of Defense (US)
DoDAF	DoD Architectural Framework
DHS	Department of Homeland Security (US)
DRDC	Defence Research and Development Canada
DND	Department of National Defence
FAR	Field Anomaly Relaxation
HRA	High Reliability Organizations (i.e., organizations successful at avoiding catastrophes in an environment where accidents can be expected)
INCOSE	International Council on Systems Engineering
ISO	International Organization for Standardization
JSA	Joint Systems and Analysis (TTCP Group)
JCIDS	Joint Capabilities Integration Development System
MAUT	Multi-Attribute Utility Theory
MCDA	Multi-Criteria Decision Analysis
MCDM	Multi-criteria Decision Making
MoD	Ministry of Defence (UK)
MoDAF	MoD Architectural Framework
NATO	North Atlantic Treaty Organization
OGD	Other Government Departments
OPP	Operational Planning Process
PPBS	Planning, Programming and Budgeting System
PRICIE	Personnel, Research & Development, Infrastructure & Organization, Concepts, Doctrine & Collective Training, Information Technology, and Equipment, Supplies & Services
PSTP	Public Security Technology Program
RMA	Revolution in Military Affairs

SAS	System Analysis and Studies (NATO research panel)
SME	Subject Matter Expert
SOREM	Senior Executives Responsible for Emergency Management
SoS	System of Systems
SSM	Soft Systems Methodology
TCL	Target Capability List (US DHS)
TCL-C	Target Capability List – Canadian (informal Canadian version of US TCL)
TDP	Technology Demonstration Project
TP3	Technical Panel 3 (of JSA / TTCP)
TTCP	The Technical Cooperation Program
TTP	Tactics, Techniques and Procedures
UK	United Kingdom
US	United States
VFT	Value Focus Thinking
WoG	Whole of Government
WoS	Whole of Society

DOCUMENT CONTROL DATA

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

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

Centre for Security Science Defence R&D Canada
222 Nepean St. 11th Floor
Ottawa, ON Canada K1A 0K2

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.)

Implementing Capability Based Planning within the Public Safety and Security Sector: Lessons from the Defence Experience

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

Hales, D; Chouinard, P.

5. DATE OF PUBLICATION (Month and year of publication of document.)	6a. NO. OF PAGES (Total containing information, including Annexes, Appendices, etc.)	6b. NO. OF REFS (Total cited in document.)
December 2011	82	3

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.)

Centre for Security Science
Defence R&D Canada
222 Nepean St. 11th Floor
Ottawa, ON Canada K1A 0K2

9a. PROJECT OR GRANT NO. (If appropriate, the applicable research and development project or grant number under which the document was written. Please specify whether project or grant.)	9b. CONTRACT NO. (If appropriate, the applicable number under which the document was written.)
33CM01	

10a. ORIGINATOR'S DOCUMENT NUMBER (The official document number by which the document is identified by the originating activity. This number must be unique to this document.)	10b. OTHER DOCUMENT NO(s). (Any other numbers which may be assigned this document either by the originator or by the sponsor.)
DRDC CSS TM 2011-26	

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

Unlimited

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

Unlimited

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

Capability Based Planning (CBP) has been described as the "gold standard" and has now been in use in military communities for just over a decade. Use is now being extended to public safety and security. This report reviews the environmental impetus, founding principles and initial expectations, and reflects on lessons learned and best practices. It identifies both some of the inherent issues with CBP and some of the unique challenges involved in applying CBP in the public safety and security realm. It concludes by offering some thoughts on the Way Ahead.

La planification fondée sur les capacités (PFC) a été décrite comme étant « l'étalon-or » et est utilisée par les collectivités militaires depuis un peu plus de dix ans. Son utilisation est maintenant élargie à la sécurité publique. Le présent rapport examine les mesures incitatives environnementales, les principes fondateurs et les attentes initiales. Le document offre aussi une réflexion sur les leçons retenues et les pratiques exemplaires. Il décrit également certains des problèmes inhérents à la PFC et quelques-uns des défis particuliers présents dans l'application de la PFC dans le domaine de la sécurité publique. Le document se termine en présentant quelques réflexions sur l'avenir.

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.)

Planning; Public Safety; Public Security; Capability