# STRATEGIC RISK ANALYSIS FOR THE SEAMLESS BORDERS ENVIRONMENT:

*LITERATURE SCAN REPORT*

Ian Bayne
CAE Inc.

Prepared By:
CAE Inc.
1135 Innovation Drive
Ottawa, Ont. K2K 3G7
Contractor's Document Number: 113129-006 Version 03
Contract Project Manager: Damon Gamble
PWGSC Contract Number: W7714-135838
Technical Authority: Shaye Friesen, Risk Analyst



Contract Report
DRDC-RDDC-2017-C170
July 2017

CAE Inc.

1135 Innovation Drive
Ottawa, Ont., K2K 3G7 Canada
Tel: 613-247-0342
Fax: 613-271-0963

# STRATEGIC RISK ANALYSIS FOR THE SEAMLESS BORDERS ENVIRONMENT: LITERATURE SCAN REPORT

**CONTRACT #: W7714-135838-b**

***FOR***

**SHAYE FRIESEN**

Risk Analyst, DKTTI
Defence Research and Development Canada
Centre for Security Science
222 Nepean Street
Ottawa, Ontario
Canada K1A 0K2

26 July 2017

Document No. 113129-006 Version 03

# APPROVAL SHEET

*Document No.* 113129-006 Version 03

*Document Name*: Strategic Risk Analysis
for the Seamless Borders Environment:
Literature Scan Report

**Primary Author**

**Name** **Ian Bayne**
**Position** Senior Risk Analyst

**Approval**

**Name** **Damon Gamble**
**Position** Project Manager, Defence & Security, CAE Canada

# REVISION HISTORY

| Revision | Reason for Change | Origin Date |
|---|---|---|
| Version 01 | Initial document issued. | 31 March 2017 |
| Version 02 | Revised report | 15 June 2017 |
| Version 03 | Revised report | 26 July 2017 |

# TABLE OF CONTENTS

# LIST OF FIGURES



# LIST OF TABLES

# LIST OF ACRONYMS AND DEFINITIONS

| | |
|---|---|
| ALARA | As Low As Reasonably Achievable |
| ALARP | As Low As Reasonably Practicable |
| AS | Australia |
| BIIP | Border Infrastructure Investment Plan |
| BTB | Beyond The Border |
| BTS | Border and Transportation Security |
| CA | Canada |
| CAP | Cross-Agency Priorities (DHS) |
| CBP | Customs and Border Protection (DHS) |
| CIP | Critical Infrastructure Protection |
| CIPABS | Critical Infrastructure Protection and Border Security (CA-US) |
| CPS | Cyber-Physical Systems |
| CSSP | Canadian Safety and Security Program |
| CRS | Congressional Research Service |
| CSS | Centre for Security Science |
| C-TPAT | Customs-Trade Partnership Against Terrorism |
| DHS | Department of Homeland Security (US) |
| DND | Department of National Defence (CA) |
| DRDC | Defence Research and Development Canada |
| DRM | Disaster Risk Management |
| FEMA | Federal Emergency Management Agency (DHS) |
| FFAC | Federally-Funded Academic Centers (DHS) |
| FIOP | Federal Inter-Agency Operational Plan (US) |
| GC | Government of Canada |
| GFDRR | Global Facility for Disaster Response and Recovery (UN) |
| GPS | Global Positioning System |
| HP | Health Portfolio (CA) |
| ICE | Immigration and Customs Enforcement (DHS) |
| ICT | Information and Communications Technology |
| IMA | Integrated Mission Analysis (DHS) |
| IoT | Internet of Things |
| ISAC | Information Sharing And Analysis Center (DHS) |
| ISEF | Integrated System Engineering Framework (DHS) |
| ITS | Intelligent Transportation Systems |
| MCDM | Multi-Criteria Decision Making |

| | |
|---|---|
| M/S | Modeling and Simulation |
| MDA | Maritime Domain Awareness |
| NBAF | National Bio and Agro-Defense Facility |
| NBRA | National Border Risk Assessment (CBSA) |
| NIPP | National Infrastructure Protection Program |
| NRA | National Risk Assessment (Finance Canada) |
| NSTS | National Strategy for Transportation Security |
| NTAT | Non-Traditional Aviation Technology |
| OR | Operations Research |
| PS | Public Safety Canada (CA) |
| QHSR | Quadrennial Homeland Security Review |
| RAF | Risk Assessment Framework (CSS) |
| RRAP | Regional Resilience Assessment Program (US and CA) |
| SII | Surveillance, Intelligence & Interdiction |
| S&I | Security and Intelligence |
| S&T | Science and Technology |
| SPG | Strategic Planning Guidance (CSS) |
| SRA | Strategic Risk Assessment (CSS) |
| TBWG | Transportation Border Working Group |
| THIRA | Threat and Hazard Identification And Risk Assessment |
| TISN | Trusted Information Sharing Network (AS) |
| TRA | Threat and Risk Assessment |
| TRL | Technology Readiness Levels |
| TS SSP | Transportation Systems Sector-Specific Plan |
| TSSRA | Transportation Sector Security Risk Assessment |
| UNISDR | UN Office on Disaster Risk Reduction |
| UNODC | UN Office on Drugs and Crime |
| USCG | US Coast Guard |
| WDR | World Drug Report (UN) |
| WEF | World Economic Forum |

# 1 INTRODUCTION

The purpose of this report is to summarize findings from a scan of literature related to the application of risk assessment techniques as an integral part of risk-informed decision making related to the Canadian Safety and Security Program (CSSP) and the Seamless Borders Focus Area. The primary audience includes the following Portfolios or Communities of Practice: Border and Transportation Security (BTS); Critical Infrastructure Protection (CIP); Surveillance, Intelligence & Interdiction (SII); CBRNE[1]; Police and Law Enforcement; and Community Resilience.

## 1.1 Background

The focus of the literature scan is on understanding the operational risk environment, and how risk assessments influence strategic planning and the prioritization of S&T investments. The report builds on previous work on a risk assessment framework that is inclusive of two types of risk assessment practices - general (one or two factors, usually likelihood, probability or frequency, and impact; or impact only) and specific (multi-factor assessments based on an aggregation of multiple variables such as: threat / hazard; vulnerability; consequence; criticality; resiliency; uncertainty; and likelihood). The study considers strategic risk analysis as an integral part of decision making on multiple levels. It is noted that in Canada (CA) there are multiple strategies and plans that relate to borders with different sets of objectives and priorities. By comparison, the US, at least on paper, has unifying approaches and coordinating functions to align cross-agency priorities with top-down direction, policies and missions. This situation presents challenges and opportunities for the Government of Canada (GC) and the Centre for Security Science (CSS) and its partners to use risk information in a systematic manner, as one input to evidence-based decision making, and to participate in risk assessment with US counterparts.

> Risk assessment provides decision-makers and responsible parties with an improved understanding of risks that could affect achievement of objectives, and the adequacy and effectiveness of controls already in place. This provides a basis for decisions about the most appropriate approach to be used to treat the risks. The output of risk assessment is an input to the decision-making processes of the organization. (CAN/CSA 30010, 2010, p.11)

A CSS brief on Maritime Domain Awareness (MDA) highlights the potential to leverage investments in national security and sovereignty (2013). The paper identifies four criteria for selecting S&T projects. It states the aim is to “avoid incremental investment in S&T programs that already receive significant funding from other government departments and instead leverage the outputs of these programs for Public Safety stakeholders”; and fund S&T projects that achieve the following objectives:

- Transition essential and affordable components of existing defence technology to the public safety domain;

[1] Chemical, biological, radiological, nuclear and explosives. In CSS, three Communities of Practice address these areas of interest (CB, RN and E).

- Produce practical, lightweight, industry-supported, high Technology Readiness Levels (TRL)[2] solutions that link awareness to response;
- Are horizontal initiatives that enable departments to work together; and
- Identify operational gaps and pilot programs that provide hard data to drive future investment (2013).

The CSS Strategic Planning Guidance SPG (2016/17) describes the Seamless Borders priority as, "De-risk the introduction of data-analytics, geospatial tools, and other information and surveillance technologies to improve efficiency and security of flows of people and goods at Canada's ports of entry, and ensure the integrity of Canada's borders and northern landmass" (2016, p.10).

While there is no comparison between CA and US S&T capabilities from a resource perspective, it is noted that the DHS S&T Directorate shares some common interests including "priority-setting mechanisms."[3] A Congressional Research Service (CRS) report states that the S&T Directorate "…must prioritize and balance its R&D activities and expenditures across all potential threats and among a diverse customer base" (2013, p.7). DHS priority setting is based on analysis of mission areas[4]. Steps that the directorate has taken (within a short time span, during significant organizational and security environment changes[5]) include: "*strategic planning*, *a portfolio review process* (still being refined as of September 2016, according to representatives at the bi-national working group discussions at CSS), and *partnerships with DHS operational components*[6] *to identify high-priority activities"* (ibid, p.7).

The Seamless Borders Focus Area Narrative (2016) defines the problem space using four "key priority areas": efficient cross-border flow; border-free response; border strategies and information exchange; and border perimeter integrity. For the purposes of this study, the analysis focuses on two of the four areas - border perimeter integrity and border-free response, in that order of priority. These outcomes align with the BTS portfolio and the CSSP decision factors. This limitation is consistent with the majority of investments to date, which are summarized in the Seamless Borders Focus Area Narrative statement:

> Previous and future investments have and will have the same goal: to enhance preparedness and generate evidence for decisions on adoption of technology or policies, whether they be to improve efficiency and security of flows of people and goods at

[2] NASA conceived the Technology Readiness Levels in 1974. The US formally defined the levels in 1989. Seven (7) levels are used (https://en.wikipedia.org/wiki/Technology_readiness_level#Brief_history; 04 March 2017).
[3] Selected Issues for Congress (*CRS Report*, 2013, p.7).
[4] The National Preparedness System outlines an organized process for the whole community to achieve the National Preparedness Goal. The National Preparedness System integrates efforts across the five preparedness mission areas – Prevention, Protection, Mitigation, Response, and Recovery – in order to achieve the goal of a secure and resilient Nation. (Overview of FIOP. DHS. 2016: ii).
[5] Author's opinion based on participating in a meeting with DHS RA SMEs at CSS (September 2016).
[6] The CA equivalent of 'operating components' would be the agencies that report directly to Public Safety Canada (PS), which is only part of the border management stakeholder picture in CA.

Canada's ports of entry, or ensure the integrity of Canada's borders and northern landmass, or others (2016, p.2).

## 1.2 Context and Scan Concept

There continues to be significant progress and investment based on the Beyond the Border (BTB) initiative, which complements GC departments' own investments. The annual implementation reports are available from Public Safety (PS) and the Department of Homeland Security (DHS) web sites. They summarize the evolving priorities and investments, which can be compared to the CSS (MDA) criteria above. In the absence of a CSSP risk taxonomy, this SRA literature scan takes a step back, and defines the Focus Area risk landscape in order to contain the literature search, and to highlight concepts for future consideration (e.g., using high-level risk scenarios to inform discussions across Focus Area, portfolio, jurisdictional, organizational and other boundaries).

CSS provided two DHS documents as inputs to this study: Critical Infrastructure 2025: A Strategic Risk Assessment (2016); and The Future of Smart Cities: Cyber-Physical Infrastructure Risk (2015). They are reviewed below (Refer to 3.2.2 and 3.3.3)

This study considers some United Nations (UN) information resources that are relevant to Seamless Borders, with a focus on drugs, crime, and travel and tourism. The study also mentions a few specific CA stakeholder RAs in support of characterizing the risk landscape, and identifying concepts for overcoming known challenges (e.g., governance, information sharing and collaborative risk management).

The study considers references from two perspectives: thematically and by highlighting specific references that are relevant to a Seamless Borders SRA process and information baseline.

## 1.3 Strategic Objective

The strategic objective of this report is to enhance Defence Research and Development Canada (DRDC) CSS knowledge of border management risk analysis approaches by reviewing selected Government of Canada (GC) and international information. It is assumed that components of such a system could include strategic risk analysis, based on a set of complex risk scenarios, a common impact assessment framework and other enablers.

# 2 METHODOLOGY

The literature scan was conducted during the July 2016 to February 2017 timeframe. The work builds on previous work on risk assessment frameworks. While CSS provided some material, most of the resources were identified by reviewing CA and US government web sites, and other open source literature. Some references that were identified in the Risk Assessment Framework (RAF) *Comprehensive Scan* (2015) were also considered (e.g., use of complex or multi-risk scenarios and simplified RA techniques). The author provided a short list of references to CSS in December 2016, which identified partners' references (Appendix B, updated in March 2017). However, this material was not available for the scan, which would have facilitated identification of a preliminary set of risk priorities by consolidating federal partners' perspectives. This constraint, and not having direct access to partners, resulted in the scan focusing mainly on US literature including identification of US approaches to program structure, strategic planning, and strategic and national risk assessments.

To manage the broad array of material, the scan focused on multiple dimensions of risk-informed decision making including: strategy formulation and identifying forward-focused priorities; and documentation that describes how other nations use risk information to support investment decisions. The scan considers references that pertain to key GC federal stakeholders as defined in the *Narrative* (2016, p.3). The study excludes Department of National Defence (DND) because CSS is familiar with projects and emerging capabilities that are relevant to Seamless Borders. The study points out that the Standing Senate Committee on National Security and Defence published a series of Canadian Security Guide Books that describe "security problems in search of solutions". However, these resources are not analyzed for their potential value to CSS (2007).[7]

Two areas that receive limited attention are the Arctic and the environment. Although the BTS Narrative (2013) mentions both of these as areas of interest; the study did not find evidence that there is a strategy to prioritize risks or to evaluate opportunities to leverage others' S&T/R&D investments in these domains. This SRA captures risks to the Arctic (and other oceans) indirectly, by considering them as effects in two areas: health security; and animal, food and agriculture security (See Appendix C for representative risk and resilience scenarios). One reference that is identified for further analysis is the *Arctic Resilience Report* (2016). It is included because of the multi-national decision making context, and the application of risk-informed decision making in multiple timeframes.

Recognizing that there are environmental implications for safety and security infrastructure and capabilities in general, the SRA limits consideration of the environment to the transportation security domain. Three risk areas are included in Appendix C: transportation of dangerous goods or hazardous materials; cross border pipeline security; and spill response. The study notes that a new federal Disaster Mitigation and Adaptation Fund provides $2 billion over ten years to support infrastructure required to deal with the effects of a changing climate. However, the study does not indicate if safety and security, and/or border infrastructure and management risks are part of the investment decision making process.

[7] Examples in this series include *Seaports, Coasts and Border Crossings* (2007).

While this report characterizes the risk environment and presents a framework to consider and prioritize risk and resilience scenarios, there was insufficient time and information to perform an actual assessment in collaboration with CSS and/or with selected partners. The streamlined methodology consists of the following steps (Refer to Figure 2-1):

- Context - Survey CA and US strategic plans (e.g., border, security, critical infrastructure[8], Arctic);
- Stakeholder Analysis - Review CSS Narratives and identify core stakeholders. Compare to DHS and other structures;
- Risk Taxonomy - Define risk categories that are directly or indirectly affected by border management. Characterize the risk domains and adjust stakeholders short list;
- Literature Scan - Focus on DHS and some international references that relate to the risk domains, identify lessons from SRA and risk scenario approaches and adjust the taxonomy;
- Complex Scenarios - Identify examples of complex (multi-risk) scenarios that describe the risk domains; and
- Strategic Risk Analysis – Provide a preliminary analysis and risk scenario framework, and highlight opportunities (e.g., CSSP and/or Focus Area risk taxonomy; set of significant risk and resilience scenarios of interest to stakeholders[9]; unifying impact assessment framework; consolidated picture of strengths and weaknesses of partners' existing RA practices). (Assumption: The approach for one focus area should be adaptable for other focus areas, and to support decision making at the program and portfolio levels, internally, and preferably, in collaboration with partners and stakeholders).

[8] Some nations identify border management as a discrete CI sector. The CA framework does not. It identifies transportation, but border and security (law enforcement) are implicit in the Government Sector, which is not reflective a whole of society concept. The CA ten CI sector definitions have not changed since 2009.

[9] Various CSS activities have identified specific threat and hazard scenarios, which support capability gap analysis and near-term planning, but these are not synonymous with higher level (strategic / operational environment) general risk scenarios

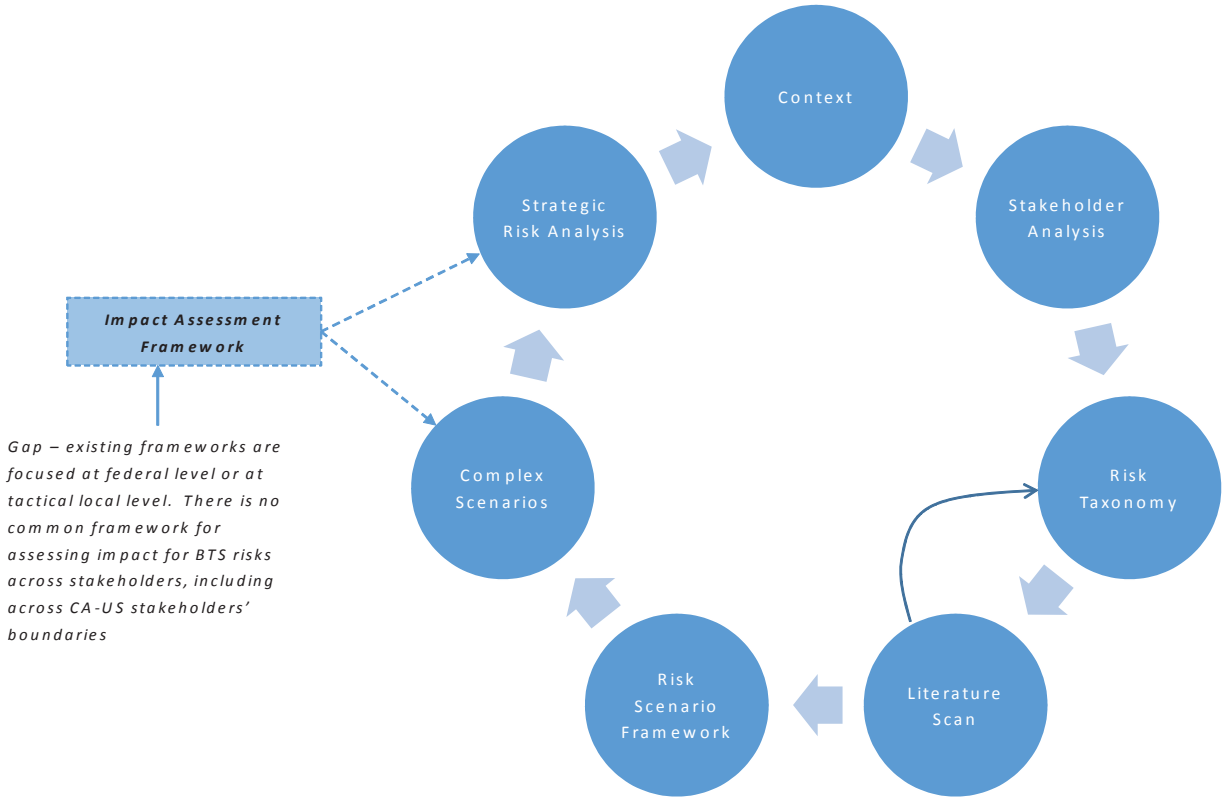



**Figure 2-1: Strategic Risk Assessment Literature Scan Methodology**

# 3 FINDINGS

The study groups findings below as follows: a thematic review based on the literature scan; a summary of key references; a preliminary characterization of the operational risk environment; a representative, multi-risk scenario management framework; study limitations; and an influence diagram of the SRA concept. This analytical framework considers the potential value of maintaining a set of complex risk scenarios and a continuous SRA process that can be incorporated into existing processes and structures with minimal disruption to the existing workflow regardless of the scope and number of resources involved in the SRA..

## 3.1 Thematic Discussion

The following five (5) themes highlight the decision making environment and implications for the SRA concept and scan: strategic forces; management concepts; pressures; challenges; and trends.

### 3.1.1 Strategic Forces

On a March 10, 2017 visit to Canada, the Homeland Security Secretary John Kelly stated that the Trump Whitehouse "wants as thin a border as we can create" and that he was "very comfortable with the level of security on the border"[10]. The precise application of S&T is one enabler to achieve this aim, which likely reinforces the CSS objective to be able to demonstrate that program investment decisions are evidence-based. If S&T is one answer to achieve thinner border objectives, technology has diverse lifecycles, and interoperability varies across solutions, then risk is surely an important input to multi-criteria decision making (MCDM) to employ the most advanced technology at the highest risk and highest value control points.

Three examples of proactive, action-oriented initiatives that directly or indirectly affect Canada's capability to manage its borders and related critical infrastructure sectors are Customs-Trade Partnership Against Terrorism (C-TPAT); Critical Infrastructure Protection and Border Security (CIPABS) initiative; and Regional Resilience Assessment Program (RRAP). Annual CIPABS implementation reports provide updates on plans and priorities. The increasing visibility of border security reinforces the CSSP goal to be able to provide evidence that CSSP investments are meeting or exceeding expectations. In risk management terms, this means being able to illustrate that S&T investments are contributing to reducing risk to a level that is As Low as Reasonably Practicable (ALARP)[11] or that investments support the taking of reasonable risks to implement innovative solutions to hard problems. The literature scan confirms that there are several limiting forces including: the difficulty to describe the impact and cascading effects of risks, should they materialize, before and after investments; the ability to consolidate and synchronize risk views from multiple perspectives; the time and effort to maintain a dynamic risk assessment process; and the lack of feedback mechanisms that describe how RA outputs

[10] Quoted in the Canadian Security Newsletter, 6 April 2017.
[11] The ALARP term originated in UK legislation related to safety management (1974). Another term used interchangeably in the US is, As Low as Reasonably Achievable (ALARA).

influence the selection of risk treatment options, investment decisions and operational performance over time.

Open source intelligence and publically-available information contains a wealth of information on border protection and critical infrastructure surety. A systematic approach to reviewing the documentation, and monitoring trends and risk indicators would support development of risk scenarios and other tools for an SRA process. While ongoing specialist evaluations of security and safety threats / hazards, vulnerabilities and consequences are essential for decision support, they are only snapshots of the dynamic threat environment, which tend to be fragmented, based on experience with recent events, and focused on near-term problem-solving.

The international literature indicates that many nations are experimenting with risk scenarios and innovative approaches that are expected to have benefits such as: broader stakeholder engagement; improved alignment of investments; better prioritization of limited intelligence and risk analysis assets; and potentially, the ability to support dashboards that indicate the risk trends before, during and after shocks to the system, and the outcomes of risk treatment decisions (e.g., S&T investments). For example, the Denmark National Risk Assessment methodologists suggest that,

> "… a useful risk scenario results from a thematic in-depth study, and it covers the following elements: (1) a relevant socioeconomic and/or physical-infrastructural context; (2) a lead-up and triggering action or event; (3) an actual serious incident; (4) a national impact of the incident including societal responses and control measures, as well as the ultimate longer-term effects on vital national infrastructure, whereby: it must be ensured that the scenario devised offers sufficient leads to be able to carry out the risk assessment in the next stage" (Vlek, 2013, p.3; as cited in *Comprehensive Scan*, CSS, 2016, p.20).

The emerging emphasis on transcontinental safety and security management systems, and strategic approaches to risk and resilience management suggest that CSS's ability to demonstrate value for money will be increasingly important.

**Strategic Forces**

US Administration focus on making the northern border "thinner"
Appetite for innovative approaches to risk and resilience management
Convergence of cyber and physical infrastructure security
Opportunities to leverage smart technologies to optimize capabilities & performance

### 3.1.2 Management Concepts

Two concepts that characterize the interdependency between government, industry and society are whole-of-government and whole-of-society approaches. Both these expressions are relevant to borders in that they highlight the need to establish common frameworks to dynamically assess risk and align risk treatment investments to ensure compatibility of control environments. The concepts also reinforce the need to share information with national security and defence stakeholders in the areas of technology, intelligence analysis, and emerging command and control concepts[12] to be able to coordinate resources that belong to multiple organizations. These holistic concepts also provide an environment where specialists and generalists improve awareness of the diversity of risk perceptions depending on: proximity to the risks: the availability of national assets and reserves before, during and after risk events; the alignment of resilience and continuity plans; and other factors.

The government-industry relationship is the cornerstone for critical infrastructure including border and transportation (security) management systems. The societal reference is relevant for other dimensions of border management including the ability to provide mutual assistance across borders for security operations, major events and disaster response (and disaster risk reduction), which implies at least minimum levels of standardization and interoperability.

> A Deloitte paper on Smart Borders states, "*Our borders have been transformed from a static line on a map to an ecosystem for shared decision making and real-time collaboration that empower government and industry to work together to create safer, more standard and cost effective perimeters*" (2014: 6)

Border community resilience is relevant to vulnerable areas (e.g., areas in between manned, patrolled or monitored border control points; Native or private lands that straddle borders; the Arctic, and remote and coastal areas; the Great Lakes and major waterways).

[12] Alberts and Hayes describe six concepts: cyclic; interventionist; problem solving; problem bounding; selective control; control free; and self-synchronization (2005, p.20-27).

Border management and transportation security will continue to compete with other societal concerns such as, health, disaster risk reduction and emergency management that can appear more threatening from the perspective of specific regions[13] or communities that are known to be vulnerable. Furthermore, in most of these cases, the impact is quantifiable, which is not always the case with many safety and security risks, and identification of proactive treatment strategies, such as crime prevention, and avoidance of terrorist attacks or extremist incidents. There is significant documentation on transcontinental organized crime, gangs, countering violent extremism, drug smuggling, human trafficking and money laundering that all have significant border management implications. The SRA discussed in this paper is inclusive of complex risk scenarios including those that are not currently a CSS area of interest for a portfolio. This (risk) management concept is central to the definition of a border and transportation security risk taxonomy.

> "*Organizational silos are common and often serve an efficiency purpose, but they also inhibit the development of deep expertise needed to build next generation capabilities. No single silo can master the new skills and disciplines, or afford to acquire them on their own.*
>
> *Despite the benefits of specialization and focus, a silo organization limits the sort of cross-functional dialogue and lateral learning crucial for better risk management and innovation*" (Schoemaker, 2015, p.5-6).

Australia (AS) reorganized its federal departments in 2015, putting border security and immigration in one organization. It will be interesting to see how this restructuring evolves. AS is a rich resource for risk information, the scale is closer to CA, and their reports are readily available in user-friendly formats. DHS includes Customs and Border Protection (CBP), Immigration and Customs Enforcement (ICE), the Federal Emergency Management Agency (FEMA), US Coast Guard (USCG) and cybersecurity within a single management construct.[14] DHS also has mature public-private partnerships whose objectives are linked to missions and national priorities (QHSR 2014, p.58). DHS web sites have significant information to help shape strategic risk scenarios and an SRA process for Seamless Borders. DHS maintains an inventory of its programs that provides insight into federal strategic missions and goals. The US also defines Cross-Agency Priorities (CAP).

Pipeline security and spill response (e.g., sources - tankers, offshore oil rigs and exploration in the Arctic) capabilities are increasing in importance. While environmental risk is not considered to be in scope for this study, cross-border pipeline security, and the free movement of emergency and security response capabilities are relevant management concepts.

The *Arctic Resilience Report* (ARR, 2016) presents a useful baseline document for future work [e.g., Arctic risk profile; multi-criteria decision making and/or a (regional) strategic risk assessment process]. A potential limitation is that this multinational report emphasizes resilience, but there is no mention of risk information being used as

> "*The resilience of local communities is thus a function of decisions made at many levels, including the international, national, sub-national and local level. These decisions may be made by individual actors or in collective governance processes*" (2016:138).

[13] CA is signatory of the Sendai Framework that focuses on natu ge.
[14] DHS has defined five mission areas: Prevent Terrorism and E Borders; Enhance and Administer our Immigration Laws; Safegu en National Preparedness and Resilience. (QHSR, 2014, p.6-7).

a decision factor (e.g., to help to prioritize investments in risk treatment and resilience). This omission is potentially a missed opportunity to make risk an integral part of strategic decision making. Chapter 5: *Shared decision making in a changing political landscape*, is relevant to BTS. Extracts of key messages in this report include:

- "Arctic policy is part of a dynamic global policy landscape, where decisions and norms from outside the Arctic increasingly shape Arctic policy;
- Negotiation, shared decision-making and policy development – often referred to as governance – play a central role in shaping change in social-ecological systems by shaping how people access, use and modify parts of the Arctic; and
- The Arctic Council faces three major challenges in a crowded and increasingly globalized Arctic policy landscape: to define its specific place and role; to strengthen its capacity to effectively engage with a multitude of other relevant policy processes; and to navigate the questions of how decision-making authority is allocated among different potential policy processes" (2016, p.128).

Chapter 5 discusses the concepts of resource, environment and multi-level governance, which are relevant to public-private stewardship of CA's three oceans and the Arctic landmass. Other areas of potential interest to CSS include: Table 5.1 - Interactions across scales and space, and related tools for policy influence (2016, p.140-141); and the discussion of case studies and cross-scale dynamics, with matrices to compare multiple variables (4.3-4.4).

A Deloitte benchmark study states that, "*In order to standardize data effectively, governments should first begin to utilize a shared risk model across its security agencies, to promote information sharing within its own borders*" (2014: 14). An observation is that, by extension, governance and management concepts must also consider safety dimensions of borders, which are equally challenging to achieve coordinated plans and investments that mitigate societal and economic risks.

The World Bank report of Disaster Risk Management (DRM) in the Transport Sector (2015) states that there is an emerging "shift from an "asset-based" approach, which sees transport as a set of discrete assets, to a "systems-based" approach, which looks at the interactions between the technical, social, economic, and organizational components of a transport system" (2015: 5). Historically, asset-based approaches are common in the physical and cyber security domains. The SRA concept and complex scenario-based approaches promoted in this paper are consistent with this shift in thinking and/or a dual approach that engages the broad stakeholder community.

**Management Concepts**

Maturing whole-of-government & whole-of-society concepts
Recognition of complexity of critical infrastructure risk environment
Greater appreciation of diversity and influence of risk perception
Agile governance including regulation, enforcement, risk and resilience management
Shift in thinking from asset-based approach to system of systems thinking

### 3.1.3 Pressures

There are significant pressures on CA, GC partners and CSS itself to demonstrate value for investment. International commitments, and societal and economic pressures on all levels of government and industry could easily consume limited policy, strategic and operational planning, intelligence, law enforcement and risk management expertise. The impact of a skill shortage would be felt by all border stakeholders including those focused on public safety, law enforcement, human health, and animal, food and agriculture security. This could happen at the same time that the international regulatory community and the US are looking for evidence that CA and trading partners are strengthening border, immigration and transportation security capabilities.

Given past CSS successes, it is likely that the GC partner's demand for CSS analysis and advice on future border management and S&T challenges will increase. Where there is already a significant investment in technology, there may be opportunities to apply and expand other science and analytical capabilities, and to refine processes that help to synchronize the efforts industry, academia and non-government resources. Examples of coordinating capabilities that could reasonably be expected to reduce pressure on border management systems, and that should be the subject of gap analyses include:

- Lifecycle management of safety and security S&T investments;
- Surveillance and patrolling the border;[15]
- Surveillance, monitoring, detection and response in support of oceans and waterways;
- Crime prevention, law enforcement and intelligence analysis;
- Enforcement of appropriate regulations and standards; and
- Audits, inspections and investigations.

Cybersecurity and privacy assurance pressures are likely to increase, and while these areas are being addressed by other portfolios, BTS risk scenarios should identify specific risks for the physical and virtual border environment (e.g., multiple GC departments, and public and private organizations storing private citizen and competition-sensitive business information; border control systems that are vulnerable to cyber attack for criminal or financial gain). The 2013 BTS Narrative states "in many border contexts cyber implications are unknown. This applies to vulnerabilities of integrated, digital automation in the supply chain, and to networks that link sensors at points of entry for cargo and travellers and at remote locations for illegal entry" (2013, p.9).

**Pressures**

Competition for qualified, knowledgeable and creative resources
Demand for personal and business information, which affects individual rights and freedoms
Vulnerability of personally identifiable and propriety business information
Vulnerability of information on security capabilities including technology-based solutions

[15] The US applies an Integrated Mission Analysis (IMA) concept (Border Patrol Strategic Plan 2012-201 (CBP, 2012, p.12).

### 3.1.4 Challenges (Opportunities)

Complicating factors for implementing an SRA process and maintaining a set of high-level risk scenarios and other tools are CA's geopolitical and public-private organizational structures. A Deloitte study compares international approaches to organizational design including CA and its Five Eyes partners. It points out that many nations have moved beyond collaborative border management to actually consolidating functions. For example, in 2003 the US established the Customs and Border Protection (CBP) agency as a centralized capability within DHS. While the policy creates a "force multiplier", the study points out that "consolidation also has its challenges", in that "once agencies and departments are combined, the overall mission can become very large and unwieldy" (2014: 17). By contrast, the UK created three distinct but closely connected functions out of the UK Border Agency (UKBA) in an effort to "balance the benefits of integration with the retention of a clear focus and mission" (Ibid)[16].

While there are some examples of 'strategic' RAs, the literature review could find no evidence that the assessments are linked to specific national or transnational strategic objectives or outcomes. This disconnect limits the usefulness of the assessments, and the ability to transition from an understanding of inherent risk that influences decisions on independent actions, to an understanding of common residual risks that supports more unifying and collaborative approaches. Many strategic or national RAs are one-off assessments, and it is not clear that they are part of a systematic and sustainable process. The general lack of performance data also limits the ability to propose, test and implement innovative approaches.

Although some CA and US assessments are labelled "strategic" or "national", these descriptors should not be taken at face value. For example, the CBSA *National Border Risk Assessment* (NBRA, 2013) is focused on vulnerabilities, and it is limited to CBSA's mandate related to border infractions. Therefore, it may be 'national' from CBSA's perspective because it deals with all border crossings and regional offices were engaged, but it is not 'national' in the sense that external stakeholders were engaged in the process. It could not be determined how the assessment is used or if it is part of a strategic management process.

Trying to compare discrete security and safety risk assessments is difficult given the diversity of cultures, approaches and environments, and the potential for information gaps and overlapping investments is significant. DHS structures its programs around mission areas (e.g., Protection Mission, supported by a Protection Federal Interagency Operational Plan (FIOP); a Transportation Systems Sector-Specific Plan (TS SSP), that are supported by common tools (e.g., DHS risk lexicon; NIPP risk assessment and other frameworks).

There are other challenges associated with comparing CA and US approaches. US programs are directed, top-down (e.g., Executive Orders, Presidential Directives) and action-oriented, as opposed to the CA voluntary and information sharing approaches. Multiple DHS programs incentivize stakeholder engagement and innovation. For example, DHS has a university,

[16] Since the 2014 Deloitte study, Australia (AS) reorganized its federal departments in 2015, putting border security and immigration in one organization.

Federally-Funded Academic Centres (FFAC) and other national assets to support its strategy. Examples include: a separate program for Countering Violent Extremism (CVE); and an emerging capability called the National Bio and Agro-defense Facility (NBAF), which is funded by the DHS S&T Division. (CRS, 2013, p.6).

The CSS investigation of a holistic Risk Assessment Framework (RAF) illustrates that the planning and scoping phase of any RA is critical. If the RA is intended to improve understanding of threats and hazards, then that represents one level of commitment. However, if the intent is to influence multi-organizational decision making and/or individual partners' programs, plans and priorities, then that poses different challenges, including the governance, and the need for mechanisms to facilitate feedback loops and manage common approaches to performance measurement. Without this level of capability and commitment, it is virtually impossible for CSS and GC partners to provide evidence that RAs made a difference, and contribute to achieving individual, collective and strategic outcomes.

The CA-US CIPABS initiative indicates that there are opportunities for CSS and the DHS S&T Division to share information, specifically in the areas of program / portfolio evaluation, and possibly, the emerging DHS Integrated System Engineering Framework (ISEF).[17] DHS is in its second iteration of its Portfolio Analysis Review (PAR) methodology, which aims to facilitate tracing investment decisions to department priorities and risks.

CSS has several years of experience with its oversight and strategic planning processes. CSS also has unique knowledge from its work on the Consolidated Risk Assessment (CBRNE portfolio, primarily in the counter-terrorism domain), which includes a rich set of seventy-two (72) threat scenarios. The CSS supported the interdepartmental working group that developed a set of twenty-six (26) all hazards scenarios that cover a broad set of threats, hazards and risks. The Health Portfolio (HP) developed an HP emergency risk assessment that includes a tailored risk taxonomy (Figure 3, 2011, p.8) and sixty-four (64) "risk vignettes" (ibid, p.10). The challenge here for PS and partners is managing and building on these diverse scenario baselines to support future work with a limited administration overhead. Most assessments have not captured this level of detail on the effort to plan, conduct and exploit assessments, which is a missed opportunity for double-loop learning and changing the thinking.

> For example, to complete the HP assessment, it took over sixty (60) specialists from multiple departments, seventeen (17) sessions over a three-month period to rank the identified health threat / hazard vignettes and four (4) additional AHRA scenarios. Using an SRA and/or high-level scenarios should improve productivity for such labour-intensive assessments by providing a framework to facilitate the grouping and prioritization of the threat / hazard vignettes based on a collective strategic view of the risk universe. Leveraging mature crowdsourcing tools should also mitigate management risks.

A 2014 Deloitte study on Smart Borders includes a comparison of CA and its Five Eyes partners' border security capabilities, such as mobile Non-Intrusive Inspection (NII), "Green

[17] CIPABS MOU and Risk / Threat Assessment Panel planning meeting at CSS (Ottawa, 21 September 2016).

Lanes[18]" and trusted traveller programs, which are described as (operational) RA tools. The report makes the point that, "…risk assessments can only be effective if they are supported by ample information sharing between agencies and governments, particularly as it relates to travelers' biographic information, good content information and risk profiles" (2014: 12).

The Global Facility for Disaster Reduction and Recovery (GFDRR) report discusses promising innovations in RA, and it highlights several 'remaining challenges' that can be extrapolated to the border security environment including:

- Harnessing risk data at an appropriate scale[19];
- Adding the complexity of secondary hazards can increase the resource and data requirements, and may significantly broaden participation in a risk assessment;
- Different techniques for rapid and slow onset disasters (probabilistic and deterministic respectively);
- Uncertainties and associated limitations in risk assessments must be communicated to the end-users; and
- The availability of loss data, which in the case of border security would include records (evidence) of direct, indirect and intangible effects of actual safety and/or security incidents (based on Chapter 2. 2014: 55-73).

A 2015 DHS paper on the convergence of cyber and physical infrastructures related to smart cities has lessons for smart technologies for border and transportation security. The paper states:

> "*Increasing the challenge for security research is the rapid evolution of key technologies underpinning Smart Cities and the wide variability in the pace and scale of technology adoption and implementation by Federal, State, and local municipalities. The confluence of rapid technology evolution and the unknown trajectory of its adoption create even greater future uncertainty for those responsible for security and risk management at all levels of government and the private sector"* (2015: 7).

This area of technical uncertainty warrants further analysis, which could be part of an SRA or CSS and/or PS environmental scanning process. Historical methods of managing the technology and the data pose a significant challenge for a system of systems approach to border management. It is the author's opinion that border stakeholders can manage discrete technology solutions relatively easily compared to other leadership and management challenges including collaboration, dynamic risk environment, big data and reliance on automation, people and knowledge. These potential sources of systemic and interdependency risk influence the effectiveness of future S&T investments that address not only specific threats, hazards and/or consequences, but also the overall capability and capacity.

[18] The 'green lanes' concept refers to the acceleration of the flow of legitimate goods and trusted travellers that are partly achieved by the use of tactical RA solutions.

[19] International natural hazards risk analysis combines hazard, exposure and vulnerability data [R=f (H,E,V)],

**Challenges**

Balancing the benefits of closer integration with a clear focus and mission
Sharing, exploiting and protecting sensitive data and information
Simplifying process to achieve a common understanding of risk in multiple timeframes
Managing a diverse operational decision making ecosystem including the exploitation of S&T
Harnessing data and techniques that are appropriate and build confidence in the outputs

### 3.1.5 Trends

The Beyond the Border (BTB) initiative (Act, 2011[20]) is fostering significant CA-US cooperation based on building a shared understanding of threats, hazards and risks, which is leading to collaborative efforts to prioritize investments based on consistent, if not common, approaches. CIPABS and RRAP are indicative of a trend that shifts the focus from policy, regulation and dialogue to action. This shift also means that outcomes should be traceable back to decisions and possibly, nation/region- and scenario-specific decision criteria. An example is the financial sector, which depends on public and private cooperation. This trend also highlights the need for flexible thinking, better data collection, willingness to take reasonable risks, and simpler ways to communicate changes in patterns, lead and lag indicators, and strategic risk trends.

In May 2016, a conference, "*The Role of Public/Private Partnerships in Tackling Financial Crime*," hosted more than eighty (80) representatives from the banking and legal professions, and government agencies in the UK and North America. The aim was simply stated as:

> "…to move beyond the talk and generate proposals for new mechanisms that could put into action genuine information sharing and partnership, thereby, transforming the financial crime system from one that is built on 'complying' to one that is dedicated to identifying and disrupting financial crime" (RUSI, 2016, Foreword).

In the conference report, Tom Keatinge, the Director, Centre for Financial Crime and Security Studies, states that:

> "Those involved in tackling financial crime from both the public and private sectors must be willing to take risks, develop new ideas and establish pilot projects that promote and test them. More innovative and flexible thinking is required. Just as finance is global and criminal funds flow unhindered across borders, so too must be our responses and efforts to identify and disrupt these criminal funds" (Ibid).

Private sector thinking on risk is informative because industry is a key stakeholder in border security risk management.

[20] On December 12, 2001, CA and the US signed the Smart Border Declaration and its companion 30-point Action Plan. The Action Plan has four pillars: the secure flow of people, the secure flow of goods, secure infrastructure, and information sharing and coordination in the enforcement of these objectives. In September 2002, expanded to cover new areas of cooperation, such as biosecurity and science and technology**.** (Smart Border Action Plan: Status Report. December 17, 2004).

> "The foundation for this habituation [of exploiting risk information] is a monitoring framework that can provide early warning of exogenous changes to the risks of highest concern. It can be helpful to think about the issues and data requirements over different time horizons…Using this output [for multiple timeframes], risk reports for senior management and the board should not only present the current risk profile of the company but also take a view on the future risk profile. Sometimes the future view can be represented effectively enough by arrows that indicate expected improvement or deterioration against key metrics. However, where potential risk trajectories are more complex, such an approach may create lock-in to a singular perspective. A segment in the reporting template dedicated to the company's future risk profile can provide a better space for discussing the implications of external indicators as well as highlighting the outcome and implications of any stress tests. Some company templates have a 'hot topics' section" (Wittenberg, 2015, p.4-5).

Trends in thinking about the problem and risk space are consistent with the CSSP concept of reframing the discussion by using Focus Areas (and enablers), and implementing complementary environmental scanning, performance measurement and other practices to support portfolio managers and sustain knowledge. The trends are also consistent with the Seamless Borders concept of developing a holistic risk assessment framework and "high-level risk scenarios" that would augment the bottom-up, capability-based planning, and threat and hazard evaluation processes.

The GFDRR report on disaster risk management (DRM) best practices highlights a number of important trends that can be adapted for a borders SRA geographic information system (GIS)-based SRA platform including: promising innovations in risk assessment in the past decade; the availability of software tools (over 100 freely available risk models for the range of natural hazards were investigated); the rise of open models and open source data; and increasing opportunities for collaboration (2014: 37-38).

**Trends**

Action-oriented collaboration (willingness to accept more organizational risk)
Openness to trying new and innovative solutions including for risk assessment
Strategic management concepts that improve governance and traceability of decisions
Open models, open source data and crowdsourcing tools to support strategic analysis

## 3.2 Review of Selected References

This section highlights some key US, international and Canadian information resources, and presents some deductions related to using a systematic SRA process. General references that are relevant to this report are at Appendix A. A short list of references focused on GC partners' RA practices to which CSS and/or partners should have access is at Appendix B. Further investigation of these references would improve understanding of partners' risk perception, existing coordinating mechanisms and the availability of shared data sets.

### 3.2.1 Availability of Information Sharing Standards

Governance and information management are known challenges for border stakeholders and resource managers. The US employs the Information Sharing and Analysis Center (ISAC) concept to facilitate communications on cybersecurity threats. In 2015, DHS established the Information and Analysis Sharing Organization (ISAO) to develop standards that will be relevant for CA-US collaboration, and potentially for GC and CSSP.

AS established the Trusted Information Sharing Network (TISN) to support Critical Infrastructure Resilience stakeholders in 2003[21]. TISN provides publications in multiple formats using TISN (i.e., Word, PDF and Zip files). It was not determined whether AS has a standards-based approach, and it uses an SRA or other processes to complement the sector-specific threat assessments. While there is a Transport Sector Group within TISN, there is no separate group for border management.

### 3.2.2 US-CA Critical Infrastructure 2025: A Strategic Risk Assessment (2016)

DHS conducted research in the May 2015 to February 2016 timeframe. The goal of the assessment is to inform private and public stakeholders of current and future trends so they can mitigate the effects on critical infrastructure. The expectation is to "inspire a deeper analytical discussion of these trends…" (2016: iv).

The assessment considers six emerging trends (and their potential consequences) that are deemed likely "to have the most profound effect on US critical infrastructure by 2025" (2016, p.iv). Recognizing the challenges to understanding the cascading impacts of these trends, the report states that, "The failure of stakeholders and senior policy makers to anticipate and mitigate the consequences of these trends is likely to result in disruption of US critical infrastructure" (Ibid, iii). The assessment uses the following terms to differentiate the trends and their components: likely, highly likely, most likely and almost certain. The report describes contributing factors (e.g., sources; risk drivers; risk and failure indicators; mitigating circumstances) for each trend and provides unclassified evidence to substantiate the assessment.

The assessment goes further and identifies key factors for each trend that can be analyzed further. For example, it states that, "…the following key information and communication technology (ICT) will have a profound effect on US critical infrastructure during the next 10 years: cyber-physical systems (CPS); global positioning systems (GPS); "Smart Cities"; Internet of Things (IoT); and 'cloud' technology" (2016: 2). The assessment cites many valuable public and private sector resources including intelligence assessments and industry studies to explain the trends and interdependencies.

[21] The sector groups of the TISN include banking and finance, communications, energy, food and grocery, health, transport and water services. In addition, there are specialist forums (Cross-sectoral interest groups), which assist in the temporary exploration of cross-cutting issues, and a resilience expert advisory group which has a strong focus on organisational resilience (CI Resilience Strategy Plan. AS. 2015: 2)

The discussion on indicators of infrastructure failure is informative when one were to consider the border as critical infrastructure. The assessment states that, "…each sector, subsector and asset type has different indicators, but some general indicators support risk assessments for most infrastructure types" (2016: 12). A limitation of this analysis is that it uses a security paradigm. The report identifies attributes that are physical and/or transactional. It does not consider the border from a system of systems or service management perspectives. It is also curious that the report does not mention cross-border transportation (and border) management infrastructure.

For the next pandemic, the report highlights some impacts on the transportation sector, namely the movement of freight by rail and the vulnerability of truck drivers. The latter vulnerability can be extrapolated to the availability of other qualified specialists across the border management spectrum (e.g., intelligence analysts; planners; incident managers; asset controllers; regulators; inspectors; equipment operators; IT and other functional specialists). This situation has implications for cross training and continuity planning (e.g., minimize border services in lower value and/or lower risk locations).

The report identifies a number of barriers to mitigating aging and failing infrastructure including: externalities (e.g., materials); new legislation and regulations; repair and replacement versus maintenance and mitigation; replacement duration and service interruption; short-term funding plans; and upfront costs (2016: 22). What the analysis does not mention are: situational awareness of the state of the infrastructure from a security, safety or other risk management perspective; and designing in security, risk mitigation and resilience during the requirements identification and project planning phases.

All six trends are directly or indirectly relevant to CSSP and Seamless Borders. To tailor and extend this report to a similar level of detail in the CA Seamless Borders or broader CA critical infrastructure context would require more time, and access to CSS partners and their assessments. Table 3-1 provides a theoretical snapshot of the relevance of the trends to Seamless Borders as a potential start point for stimulating dialogue internally in CSS and/or with federal partners.

Finally, although the assessment is not by definition a risk assessment, it is a useful example of how to identify trends that influence the risk of critical infrastructure, as one input to defining risk scenarios and doing an actual risk assessment. It was not confirmed whether DHS is maintaining this assessment process or whether CA (PS) is considering a similar trend analysis to "inspire deeper analytical discussion" within the federal government and/or with the broader CI public-private stakeholder community.

| Trend | Seamless Borders Considerations (Examples) |
|---|---|
| Growing convergence of cyber and physical domains | • Information sharing and collaborative risk treatment strategies including S&T investment<br>• Investment in, and whole-of-lifecycle management of border and security infrastructure<br>• Effectiveness of insider threat controls and countermeasures |
| Aerial threats (non-traditional | • Effectiveness of controls at ports of entry and transportation / |

| Trend | Seamless Borders Considerations (Examples) |
|---|---|
| aviation technology - NTAT) | commercial hubs<br>• Enforcement of regulations for NTAT[22]<br>• Surveillance and response capabilities including interoperability |
| Evolving terrorist threat | • Intelligence sharing including collaboration with non-traditional S&I sources (e.g., financial, border, environment)<br>• Mutual assistance and preparedness<br>• Effectiveness of insider threat controls and countermeasures |
| State of US infrastructure | • CA-US cross-border infrastructure, airspace and waterways (e.g., design-in security and resiliency; interoperability of smart borders and transportation systems) |
| Extreme weather | • Warning systems<br>• Contingency plans and preparedness |
| Next pandemic emergence and outbreak | • Border perimeter capabilities (impact on manned systems)<br>• Transportation systems (availability of qualified resources; vulnerability of truck drivers)<br>• Increased use of rail (subsector) to move freight |

**Table 3-1: Trends and Seamless Borders Considerations**

### 3.2.3 The Future of Smart Cities: Cyber-Physical Infrastructure Risk (2015)

The interconnected physical and cyber infrastructures for smart cities and intelligent transportation systems directly or indirectly affects the border environment. Furthermore, as the report points out, “greater connectivity also expands the potential attack surface for malicious actors. In addition to physical incidents creating physical consequences, exploited cyber vulnerabilities can result in physical consequences, as well” (2015: 2). Similarly, advances in this area have implications for data management and border intelligence.

> DHS describes its role as being able to “contribute to the stakeholder community to help it anticipate and plan for potential risk, and to influence the overall security environment in which these technologies will exist” (2015: 4).

The report covers three sectors - transportation, electricity, and water and waste water systems (in cities). DHS report considers cyber-physical technologies and pathways within each sector. The focus is on cyber-physical vulnerabilities that could have a significant impact on the economy, public health and safety, and/or national security.

The report identifies vulnerabilities and uses three crosscutting themes to highlight security considerations that come with integrating cyber-physical systems. Table 3-2, gives some examples of implications adapted from the report’s thematic perspective.

[22] DHS uses the generic term slow speed aerial vehicles including small Unmanned Aircraft Systems (sUAS), ultralights and gyrocopters. (2016: 6).

| Theme | Implications |
|---|---|
| Changing seams | • Seams between components become more permeable as systems become networked and accessed remotely |
| Inconsistent adoption | • Inevitable inconsistency introduces new security challenges |
| Increased automation | • Limits on human interaction with systems introduces new security challenges |

**Table 3-2: Crosscutting Themes and Implications**

The SRA implicitly considers intelligence transportation systems (ITS)[23]. The report presents a pathway (i.e., ITS disruption) and defines a sample vectors (scenarios). Examples of vectors that influence the chance of disruption include: multiple entry points; shared commercial networks with low security standards, visibility and control; familiarity of hackers with commercial networks; ITS communications nodes could be vulnerable to natural or human-caused disasters; direct attack on, or manipulation of, control or sensor data; delays in detection and countermeasures; and the large number of authorized users introduces complexity for the system security control environment. The report then provides thematic lenses for changing seams and inconsistent adoption for the vectors mentioned, which would support a broader discussion of threats and vulnerabilities.

This report could serve as a model for a similar analysis of smart borders that would support strategic, operational and technology risk analysis, and decision making processes for partners and possibly, CSS.

### 3.2.4 National Infrastructure Protection Program (NIPP, 2013)

The purpose of NIPP 2013, referred to as the National Plan, is to "guide the national efforts to manage risk to the Nation's critical infrastructure" (2013, p.3). The concept is based on an integrated and collaborative approach to address threats and hazards, vulnerabilities and consequences. The report characterizes public health and safety risks from a security perspective, and it is a very useful framework for Seamless Borders (and the border, as critical infrastructure). The Call to Action, where all actions are mapped to national goals, includes the following actions related to **Innovation in Risk Management**, which are applicable to a Seamless Borders strategic management concept (Section 6, 2013: 23):

- (5) "*Enable Risk-Informed Decision Making through Enhanced Situational Awareness;*
- *(6) Analyze Infrastructure Dependencies, Interdependencies, and Associated Cascading Effects;*
- *(7) Identify, Assess, and Respond to Unanticipated Infrastructure Cascading Effects During and Following Incidents;*

[23] An Intelligent Transportation System (ITS) is a system in which real-time data is gathered and used to inform automated decisions regarding the function of traffic-related infrastructure and hardware (2015: 16).

- *(8) Promote Infrastructure, Community, and Regional Recovery Following Incidents;*
- *(9) Strengthen Coordinated Development and Delivery of Technical Assistance, Training, and Education; and*
- *(10) Improve Critical Infrastructure Security and Resilience by Advancing Research and Development Solutions*".

Call to Action # 10 further directs that the National CI Security and Resilience R&D Plan (updated every four years) will focus on the following:

- "*Promoting R&D to enable the secure and resilient design and construction of critical infrastructure and more secure accompanying cyber technology;*
- *Enhancing modeling capabilities to determine potential impacts on critical infrastructure of an incident or threat scenario, as well as cascading effects on other sectors;*
- *Facilitating initiatives to incentivize cybersecurity investments and the adoption of critical infrastructure design features that strengthen all-hazards security and resilience; and*
- *Prioritizing efforts to support the strategic guidance issued by DHS"* (2013: 25).

While this level of coordination is likely beyond a CA federal capability, the concepts highlight the value of the strategic approach as envisaged by CSS's introduction of Focus Areas to support the prioritization, execution and transition of S&T investments into the operational environment.

### 3.2.5 CA-US Border Infrastructure Investment Plan (BIIP, 2016)

The Transportation Border Working Group (TBWG) BIIP focuses on capacity and reducing Border Wait Times. This effort relates directly to the Seamless Borders priority area of Efficient Cross-Border Flow. A review of this five-year plan suggests that risk, resilience and improvements in security (flow) are not an integral part of the design and investment decision making processes. The plan does not describe whether the partner agencies are consulting with security and/or risk specialists individually or collectively, as part of the planning process. Risk is not mentioned in the plan. From management and security perspectives, this could be a missed opportunity to use risk information to help to prioritize investments, and to design-in security, risk and resilience management, and performance measurement, throughout the planning process.

### 3.2.6 US-CA Joint Border Threat and Risk Assessment (JBTRA, 2010)

The 2010 JBTRA provides a strategic overview of significant threats and hazards facing CA-US border security stakeholders from the respective federal governments' perspectives using five categories of risk - national security; criminal enterprises; migration; agriculture; and health

(2011, p.1). The focus is threat along the physical border. The CA participants were CBSA, CFIA, CSIS, PHAC, PS, RCMP and TC.

While the report provides a useful environmental scan of border security risks, it has several limitations including: the report is focused on risk identification; it is not supported by a RA framework or methodology; there is no attempt to combine or compare threat and hazards; it does not consider the more serious impacts and cascading effects; there is no attempt to prioritize threats or hazards within or across categories; and the document does not present conclusions, next steps. The SRA study could not confirm the status of the methodology that produced this consolidated snapshot of the specific threats and hazards. This study could also not confirm if S&T stakeholders participated, and whether the team captured lessons during this process. As a one-off assessment, the process was undoubtedly useful at the time. While there is evidence that CA-US information sharing continues to improve, it is not clear that there is an ongoing joint SRA process or that the cost/benefit/risk of the process is documented.

### 3.2.7 US Strategic National Risk Assessment (SNRA, 2011)

The intent of the SNRA was to establish a new homeland security risk baseline. This unclassified version includes a description of the limitations of this initial effort. The assessment focused on known threats and hazards that were "grouped into a series of national-level events with the potential to test the Nation's preparedness" (2011, p.1). Events were grouped into three categories: natural hazards; technological/accidental hazards; and adversarial, human-caused threats/hazards (ibid). Federal stakeholders performed the assessment. There are some notable exclusions that limit the assessment's usefulness as a model for CA (author's opinion):

- "Only events that have a distinct beginning and end, and those with an explicit nexus to homeland security missions were included";
- The SNRA did not "explicitly assess persistent, steady-state risks like border violations, illegal immigration, drug trafficking, and intellectual property violations, which are important considerations for DHS and the homeland security enterprise"; and
- Furthermore, "the SNRA methodology does not explicitly model the dynamic nature of some of the included hazards" (2011, p.6).

It could not be determined if DHS plans to repeat this process and/or to overcome the limitations.

### 3.2.8 Supplemental Tool: Executing a Critical Infrastructure Risk Management Approach (NIPP, 2013)

The critical infrastructure (CI) risk management approach espoused in the National Infrastructure Protection Program (NIPP) supplement is inclusive in that it: "complements and supports the Threat and Hazard Identification and Risk Assessment (THIRA) process conducted

by regional, State, and urban area jurisdictions" (2013, p.1).[24] The methodology uses terms defined in the DHS Risk Lexicon (2010). The document states that a Strategic National Risk Assessment supports the local assessments, but there is no specific reference and it is not clear how DHS aligns the processes. The Supplement states that:

> "The critical infrastructure risk management approach can be tailored toward and applied on an asset, system, network, or functional basis, depending on the fundamental characteristics of the decisions it is intended to support and the nature of the related infrastructure" (2013, p.2).

This description indicates that the approach is similar to traditional CA physical security Threat and Risk Assessment (TRA) approaches that are normally based on intelligence judgements, historical evidence, experience, events and facts (i.e., partly, to minimize the effects of subjectivity and uncertainty). The NIPP engages a broad cross-section of stakeholders. The plan is supported by top-down direction, and significant funding and other resources. The framework is also based on analytical principles that help to ensure that assessments are documented, reproducible and defensible (2013, p.7).

DHS defines the CI RA approach to using scenarios as:

> "Homeland Security risk assessments generally should use scenarios to divide the identified risks into separate pieces that can be assessed and analyzed individually. A scenario is a hypothetical situation consisting of an identified threat or hazard, an entity impacted by that hazard, and associated conditions including consequences, when appropriate" (2013, p.8).

By comparison, an expected benefit of using a holistic RAF and complex risk scenarios is to have the flexibility to help decision makers to prioritize the lower level assessments, and plug them in by engaging the right participants, at the right time (e.g., as specific threat / hazard vignettes/mini-scenarios). That is, the SRA concept is to bring the "separate pieces" together, as opposed to 'dividing them' and assessing them in isolation, frequently with no reference to stakeholders' strategic plans and risk perception. It was not verified whether US States are required to include cross-border CI considerations in their assessments and to engage bordering provinces and territories in the assessments. It is understood that the RRAP considers cross-border dependencies and criticality in its resilience assessments, but it was not confirmed how the RRAP process considers risk.

### 3.2.9 Transportation Systems Sector-Specific Plan (TS SSP, 2015)

The plan has a section on Sector Risks that is focused on security threats. The plan is based on a Transportation Sector Security Risk Assessment (TSSRA), which is an "annually-updated, scenario-driven evaluation of risks that compares the aviation, mass transit, freight rail, highway

[24] In CA, provinces/territories have their own threat and hazard assessment processes. For example, ON uses the term Hazard Identification and Risk Analysis (HIRA). BC's process is Hazard, Vulnerability and Risk Assessment (HVRA). In the US, DHS program conditions require applicants for Grant money to use a standardized approach.

and motor carrier, and pipeline modes. For example, the TSSRA 4.0 concludes that the aviation mode has the highest risk of a terrorist attack compared to other modes" (2015, p.6).[25]

The plan goes on to state that, "the US Coast Guard (USCG) uses the Maritime Security Risk Analysis Model (MSRAM) as a terrorism risk management tool. At the national level, MSRAM supports the USCG's strategic planning efforts. The outputs of this analysis inform "a variety of port and waterway security risk decisions." The risk analysis considers the USCG-defined risk space, which explicitly includes: aging infrastructure; natural disasters; global climate change; and extreme weather events.

The TS-SSP states that, "the Sector engages its partners through a collaborative process to determine Sector goals, priorities, and risk methodologies as they relate to the physical, human, and cyber elements of critical transportation infrastructure" (2015, p.7). The engagement process and common decision criteria could provide valuable lessons. For example, security threats can often dominate investigation of people and operational safety issues (e.g., availability of certified seafarers, air traffic controllers or other specialists).

Informative sections of the "plan"[26] include: identification of cross-sector issues (3.3); an R&D framework (3.3.3); sector goals and priorities (4); sector interdependencies (5.1.1); R&D (5.1.3)[27]; alignment with the five National Preparedness Framework (NPF) mission areas (5.2); measuring effectiveness (6) and alignment of sector priorities with Joint National Priorities and NIPP goals (Appendix B). Curiously, there is no mention in the plan of Mexico or Canada, or how regional interests factor into the RAs.

### 3.2.10 National Protection Framework (NPF, 2016)

The US has multiple high-level frameworks. The National Protection Framework (NPF):

> "… describes the core capabilities, roles and responsibilities, and network of coordinating structures that facilitate the protection of individuals, communities, and the Nation. It is focused on actions to protect against the Nation's greatest risks in a manner that allows American interests, aspirations, and way of life to thrive" (2016, p.i).

The framework defines eleven (11) national core capabilities for the Protection mission, which is the mission that is closest to Seamless Borders' span of influence, recognizing that CSSP and the Focus Area cross all missions. Core capabilities that are unique to the Protection mission include:

[25] It is likely that this risk perception is still highly influenced by 9/11 (author's opinion). The TSSRA and MSRAM were not available to analyze how the processes consider cross-border and transient transportation risks, such as transnational organized crime and drug smuggling. These two RAs are included on the Seamless Borders short list of references (Appendix B).
[26] The plan is not a plan per se. It describes the why and the what. It does not describe the how-to's, with specific actions and indicators, which would presumably be in other documents or left up to individual stakeholders to develop.
[27] This section refers to a Critical Infrastructure Security and Resilience National R&D Plan (CISR R&D Plan).

- Access Control and Identity Verification;
- Cybersecurity;
- Physical Protective Measures;
- Risk Management for Protection Programs and Activities; and
- Supply Chain Integrity and Security (2016, p.17).

The CI (security) risk management approach uses the terms threat and risk interchangeably. The process is based on identifying and assessing known threats (hazards) and vulnerabilities, and a range of probable consequences associated with specific event scenarios.

A key feature of the NPF, is that it "relies on existing coordinating structures to promote integration, synchronization, and resilience across various jurisdictions and areas of responsibility" (ibid). The range of "*coordinating structures*" includes: operations centres; law enforcement task forces; critical infrastructure sector, government, and cross-sector coordinating councils; governance boards; regional consortiums; information-sharing mechanisms, such as state and major urban area fusion centres; health surveillance networks; and public-private partnership organizations at all levels.

> "Multiple core capabilities under the protection mission area rely upon sound, science-based vulnerability assessments, risk-informed standards, and advanced tools to detect and identify potential threats" (2016, p.34).

The framework defines a steady-state Protection Process that clearly identifies 'assess and analyze risk' as an integral step in a continuous process. Figure 3-1 depicts the process. The NPF includes a "protection escalation decision process" to deal with potential changes to the steady-state (2016, p.27). There is a Protection Federal Inter-Agency Operational Plan (FIOP), which indicates a significant level of engagement and collaboration.

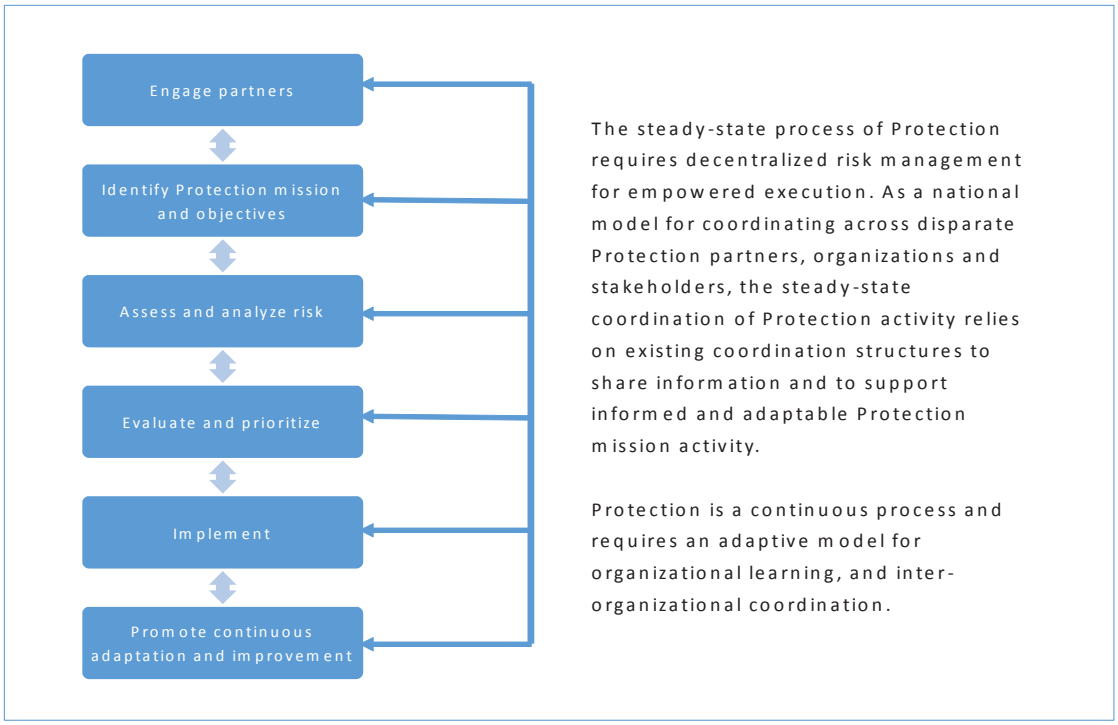



Figure 2: Steady-State Protection Process. NPF. 2016: 25

**Figure 3-1: Steady-State Protection Management Process**

While this process is logical, it is top-down and focuses on security, which means that other societal (and safety) risks could be missed or under-represented. Strengths include: it is a national model; it emphasizes engagement as a discrete sub-process; it recognizes the need for an escalation supporting mechanisms; and it explicitly mentions the need for continuous improvement and adaptability. The author is not aware of a CA-equivalent model for security or other GC/PS programs. The process should be adapted to consider safety and security components of the risk space, and hybrid threats like the cyber-physical infrastructure.

## 3.3 Characterizing the Risk Landscape

The CSSP Focus Areas are intended to facilitate a strategic view of areas of interest to support the prioritization of investments in safety and security. S&T challenges are defined in the Strategic Planning Guidance (SPG), which is part of the annual planning cycle. Priorities are defined by portfolios and communities based on partners' inputs, which are consolidated in Focus Area Narratives and updated annually.

To constrain the literature scan and to support an SRA-informed approach, this project defined seven (7) priority risk domains for Seamless Borders (Appendix C, Table C-1). The framework considers the following areas to be mostly out of scope: environment and natural disasters, with the exception of the border's role in facilitating cross-border mutual assistance – that is, the

coordinated response to and support for major events, and natural or human-caused disasters; and physical infrastructure (e.g., international bridges, rail, roads and waterways); and some cross-border assets (e.g., pipelines).

### 3.3.1 Risk Management Framework

Figure 3-2 below identifies the Seamless Borders risk domains through a security lens. The framework also streamlines the literature scan. The framework supports the identification of multi-risk scenarios to highlight interdependency and systemic risks, and cascading effects. The European Union applies these concepts in its national risk assessments (Refer to the Comprehensive Scan, CSS). Examples of risks for the seven (7) risk domains are in Appendix C.

Where CA or other documents use non-standard terms, the DHS terminology is adopted to improve consistency with US DHS language (e.g., animal, food and agriculture security). To capture common risks and to avoid repetition of specific risk scenarios, the framework allocates risks to one domain using best judgement. This approach also strives to achieve some balance among domains. For example, the capability to maintain situational awareness (SA) of cyber-physical systems and the data infrastructure is included in the border (operations) security domain. Its inclusion illustrates that whereas bottom-up systems approach would focus on interoperability and data fusion of disparate systems. A holistic approach would also focus on the broader issues namely, visibility of the total cost of ownership and lifecycle management issues; for example, to ensure that the most advanced technology is deployed, and resources are optimized, for the highest risk and highest value border infrastructure locations. Such an approach would also promote alignment of performance standards, data collection, pre-disaster agreements, and design principles to build security, risk treatment and resilience thinking into management systems and infrastructure decisions.

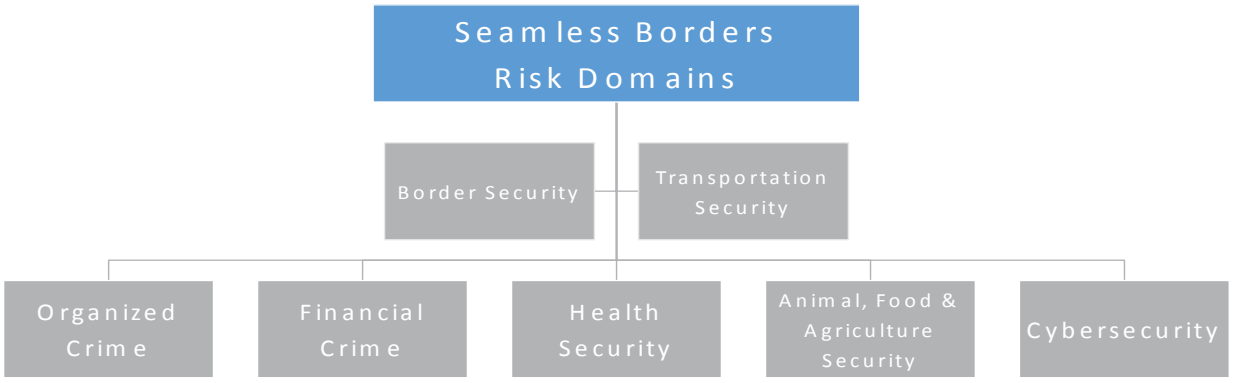



**Figure 3-2: Seamless Borders Risk Domains**

To address the limitations of not having access to CSS partners or relevant RA documentation, the author extends the framework to include an indication of the risk at the domain level. Appendix C also highlights some key indicators to demonstrate how such a characterization could help to stimulate and focus discussion.

### 3.3.2 Multi-Risk Scenario Planning Framework and Next Steps

Building on the framework above and the characterization of risk domains in Appendix C, the report includes a scenario management framework in Appendix D. It illustrates the potential to leverage a graphical representation of complex risk scenarios to isolate scenarios of interest and to highlight interdependencies and cascading effects. The concept is also that the scenario planning process itself would add value in other ways. It would guide the performance data collection to provide evidence that the assessments:

- Support risk treatment decisions over multiple timeframes;
- Contribute to bridging risk communications and process gaps across jurisdictional, organizational, functional and other boundaries;
- Support capability management decisions throughout the total lifecycle of the S&T investments, including being able to map the as-built and planned technology and data infrastructure to the multi-faceted risk environment;
- Aid in prioritizing specific threat, hazard and vulnerability assessments and other controls;
- Enable unifying impact analysis processes to compare, consolidate and/or prioritize diverse risk snapshots; and
- Contribute to improving supported (e.g., strategic planning) and supporting mechanisms including environmental scanning, data collection and performance measurement.

The concept is that the prioritization of risk scenarios is implemented progressively as part of the CSS and/or stakeholders' normal workflow with the following coordinated strategy:

- Phase 1 - validate the risk domains; refine the examples for the domains and select the most relevant high-level scenarios (example framework at Appendix C); develop a unifying impact assessment framework; prioritize the scenarios in each risk domain based solely on impact; refine impact descriptions, adding quantitative thresholds where practicable; compare the priorities across domains; develop a list of the top 'n' scenarios; and do a data gap analysis and develop a coordinated data collection and standardization strategy;
- Phase 2 - engage external stakeholders, preferably leveraging existing relationships and information sharing agreements, modern crowdsourcing technology, and common productivity tools to validate and refine the scenarios; prioritize the scenarios by domain and possibly, for the overall focus area, preferably with border management as a discrete critical infrastructure 'sector'; and then, refine tools, guide data collection and performance measurement to support a system of systems approach; and
- Phase 3 - provide the toolkit to federal partners, and regional and local stakeholders for further validation and enrichment including criteria to differentiate risk scenarios for specific regions based on real life experience; and implement a progressive and repeatable process, with knowledge management, continuous process improvement, coordinated academic and non-government funded research, and adaptability as guiding principles.

Some logical next steps to this literature review include: confirm the status of the initiatives captured in Appendix B, and emerging PS priorities, programs and initiatives; identify the as-is information sharing environment; and identify opportunities to sustain and improve the environment (e.g., use of modern technology, such as crowdsourcing and cloud security). CSS could play a lead, support role or facilitation role depending on its future direction for exploiting the focus areas concept, and implementing a holistic risk assessment framework.

### 3.3.3 Limitations

A strategic objective of this project originally was to provide some tools to support the Seamless Borders Focus Area and its CSS portfolio stakeholders. However, because of time and other constraints, CSS shifted the focus to a literature scan. To retain at least some of the concepts that build on previous CSS work on RAF, this report strives to achieve the following goals:

- Highlight relevant references at the partner and strategic level with a focus on emerging CA-US initiatives;
- Demonstrate a methodology for structuring a streamlined literature review and monitoring process by using a common definition of risk domains that can be refined over time; and
- Presenting some concepts and frameworks based on the literature review and preceding work that could form part of a CSS risk toolkit that would overcome the constraints of fragmented threat, hazard and vulnerability snapshots, and improve situational awareness of the operational risk environment without adding an administrative burden on to portfolio managers.

### 3.3.4 Iterative SRA Concept

A preliminary influence diagram is included at Appendix E to illustrate the iterative nature of a risk assessment framework and a dynamic process that is tailorable and that engages stakeholders in a participative process. Four balancing loops are depicted (B1-4) to close the gap in the performance of risk (capability and resilience) assessment processes, and to improve the value of risk information to decision making and mission success.

The author's hypothesis is that much of the effort in public and private organizations is currently focused on B1 (the assessment, with controls assessments and treatment selection being the responsibility of others). This approach tends to constrain assessments to focus on closing near-term gaps based on specific threat/hazard snapshots (and in some cases, supported by capability gap analysis and real events or near misses – known knowns and known unknowns). Examples of other self-imposed constraints are processes that only consider risks perceived to be under an organization's or jurisdictions "control" or for which there is potential liability. Some intelligence-based assessments focus on real events within a specific geographic area or timeframe. While this approach is still valuable and it contains the level of effort and cost, it can also limit the thinking and value of more dynamic processes that engage diverse stakeholders.

Conceptually, other feedback loops (B2-4) represent a strategic approach that broadens the dialogue and supports a multi-level risk-informed decision making concept that helps stakeholders to focus on the right risks, at the right time.

Such an SRA framework can be implemented internally (CSS or GC partners), and/or it could be implemented collaboratively, assuming that the process leverages modern technology and provides adequate centralized administrative support, without adding excessive administrative overhead and cost.

# 4 CONCLUSIONS AND RECOMMENDATIONS

Given the global risk environment[28] and the CA-US (and Arctic Nations) relationships, it is likely that attention on all dimensions of border and transportation security will remain constant and probably increase. The first phase of any risk assessment is the 'context'[29], which in this case involves having an understanding of the national and diverse stakeholders' operating and decision making environments, strategic plans and priorities. The changing risk perception of the borders environment could increase pressure on GC, CSS partners and private sector stakeholders to demonstrate that their plans, including risk management plans, and strategic investment decisions are meeting strategic objectives, and reducing risk (e.g., ALARP), and/or that stakeholders are taking reasonable risks. This trend could put more emphasis on collaborative approaches to decision making, strategic planning, risk and resilience management, performance measurement and other coordinating processes. An emphasis on BTS could also present opportunities for CSS to contribute in discrete areas of resource optimization and decision support systems (e.g., OR; decision support; M/S).

Although DHS has significantly more resources and levers than Public Safety and its partners, it is clear from early discussions in the CIPABS Risk / Threat Assessment Panel that there are opportunities for sharing information and collaboration, where even small successes could have big impacts for both parties. The potential value of using an SRA process and complex risk scenarios is that they would complement existing intelligence and evidence-based threat assessments. They could also be used to prioritize specific assessments, and to engage the right resources, to focus on the right risks, at the right time. The challenge for CA would be to incorporate novel approaches that complement existing specific constructs, so that they are mutually-supporting and manageable.

The US has significant levers to incentivise its stakeholders including: top-down direction; action-oriented planning processes; and multiple Grants programs. Even so, given the scale and complexity of the federal government, the literature shows that the US faces similar challenges when it comes to implementing SRA, demonstrating that S&T investment decisions are evidence-based, and verifying that cross-agency priorities are achieving the desired national goals and strategic outcomes.

This SRA study confirms that there is a significant amount of user-friendly open source literature, especially on US programs, strategies and prioritization approaches (reinforced by frequent newsletters, conferences and other learning opportunities). The next Quadrennial Homeland Security Review (QHSR) in 2018 will be of particular interest as it will likely touch on many topics of mutual interest including: architecture; decision making; S&T challenges; threat / hazard trend analysis; and performance measurement. Analysis of international trends

[28] There are multiple snapshots of global risks from diverse perspectives including the World Economic Forum's annual Global Risk Report, and Organization of Economic Cooperation and Development (OECD) High-Level Risk Forum, and focused assessments on themes including: organized crime; drug threats; human trafficking; money-laundering and terrorist financing; and other border-related safety and security management systems issues.

[29] CAN/CSA-IEC/ISO 31010: 10, Risk assessment techniques.

indicates that there should also be useful information from other nations' sources including Europe, Australia / New Zealand and elsewhere, where borders, immigration and refugee management, and organized and financial crime are high international, societal and whole-of-government priorities.

A preliminary list of partners' references was developed (e.g., Appendix B). Also included is an indication of the risk at the domain level and highlights some key indicators to demonstrate how such a characterization could help to stimulate and focus discussion.

This report included analysis that builds on previous CSS work including the Seamless Borders RA Framework pilot project. This study considered several themes that were modelled on the US 2025 study report. This report also summarized some key literature that directly or indirectly relates to ongoing CIPABS collaboration and emerging PS initiatives.

To shape the literature review and to support future work, the report characterizes the risk landscape by defining domains and representative risk scenarios (Appendix C). Although, there is no CSSP portfolio related to financial crime, it was retained as a discrete risk domain to highlight the links between: border security; illegal immigration; smuggling of bulk cash and trade-based money laundering[30], organized crime and gangs, and terrorist financing; situational awareness; and potentially, "follow the money" capabilities. The financial sector is also the community with experience in big data and analytics, quantitative risk analysis and risk tolerance, which are of interest for an SRA process that goes across single focus areas.

The focus of this report is on security in general. Health security, the Arctic, cybersecurity, smart technologies and the environment would warrant their own studies and interaction with GC SMEs. However, this report does identify a few references that relate directly to multi-organization decision making, which were useful to validate the risk domains and assess the level of maturity of selected partner's collaborative RA and planning capabilities [e.g., HP Emergency Risk Assessment Report (2011) and the Arctic Resilience Report (2016)]. The first describes an assessment of threat and hazards from an HP perspective. The second is highlighted for what it does not describe. There is no mention of risk as an input to governance, comparison of case studies or prioritization of resilience initiatives. Either this work is contained in other documents, or it is an example of a systemic gap that could result in missed opportunities to initiate cooperative risk treatment strategies. These observations are intended as a case study to illustrate that a systematic SRA process would expose systemic gaps; such as, the CA-US Border Infrastructure Investment Plan (BIIP) does not mention risk in the prioritization of investments or operational risk management contexts. An effective SRA treatment strategy would influence decision makers to design-in security throughout the project lifecycle, and to focus on operational risks (not just project risks) early in the planning and investment allocation phase, not after solutions are deployed.

A representative multi-risk scenario management framework that is adapted from national risk assessment work sponsored by the European Union is at Appendix D. It is intended to illustrate how graphics and high-level risk scenarios can be adapted for multiple purposes including: to

[30] CBSA did not consider a number of known risks in the *National Border Risk Assessment* (2013) due to self-imposed constraints.

expand the thinking about risk assessments to include multiple timeframes and the operational environment, and to identify opportunities to exploit SRAs to highlight interdependency and systemic risks that cross safety and security boundaries; and influence and/or help to prioritize specific, lower level, capability-specific risk assessments.

In addition to monitoring CA-US initiatives (e.g., CIPABS; RRAP; BIIP) and developments in the US, future literature scans and targeted research studies could provide clarity on strategic risks by considering the following resources: the arctic (e.g., ARR); smart technology for the border and transportation infrastructure; the key role of border security and intelligence in the war on drugs and crime, and the prevention and mitigation of health, and food, animal and agriculture security risks; borders as a discrete critical infrastructure sector; application of OR and other decision support techniques to border system of systems issues including the total lifecycle management of the border physical and cyber technology infrastructure; not-for-profit organizations and think tanks [e.g., Australian Security Research Centre (ASRC)]; and global analysis such as, travel and tourism competitiveness (WEF); global assessment report (UNISDR), world drug report (UNODC), and disaster response and recovery (GFDRR) and government to government risk assessment capacity building (AS).

# APPENDIX A REFERENCES

The list below contains references related to this report.

Alberts, D.S. & Hayes, R.E. (2005). *Power to the Edge: Command and Control in the Information Age (2005)*. Third Printing. Information Age Transformation Series. Command and Control Research Program (CCRP). Department of Defense (DoD). [International Command and Control Institute. (2017). www.dodccrp-test.org]

Arctic Council. (2016). *Arctic Resilience Report*. M. Carson and G. Peterson (eds). Stockholm Environment Institute and Stockholm Resilience Centre. Stockholm: Norway. http://www.arctic-council.org/arr.

Border Infrastructure Investment Plan (BIIP) 3.0. Canada-United States (CA-US) Transport Canada. August 2016.

Canada Border Services Agency. Risk Management & Foresight Division. (May 2013). *National Border Risk* Assessment *2013-2015 (NBRA)*.

Canadian Standards Association. (December 2010). *Risk management – Risk assessment techniques*. CAN/CSA-IEC/ISO 31010-10.

Centre for Security Science. (2016). *Comprehensive scan for the Canadian Safety and Security Program (CSSP) risk assessment framework: establishing a method and process for assessing the distribution of investments*. CAE Document No. 113129-006.

Centre for Security Science. (2014). *Risk scan: a review of risk assessment capability and maturity within the Canadian Safety and Security Program (Part 1 – Review of Risk Capability and Maturity; Part 2 – Supporting Material)*. Tech. No. DRDC-RDDC-2014-R36.

Centre for Security Science. (January 2017). *Risk Assessment Framework: Seamless Borders Pilot Project*. Reference Document. DRDC-RDDC-2017-R081.

Centre for Security Science. (2016). *Seamless Borders Focus Area Narrative*.

Centre for Security Science. (2016). *Strategic Planning Guidance (SPG) for 2017-2018*. CSSP.

Congressional Research Service (CRS). (14 April 2014). *The DHS S&T Directorate: Selected Issues for Congress (2014)*. R43064.

Defence Research and Development Canada. (10 December 2013). *Maritime Domain Awareness in the Canadian Safety and Security Program (CSSP)*. Scientific Brief. DRDC CSS LR 2013-042.

Department of Homeland Security. (February 2017). *2012-2016 Progress Report: BTB Action Plan*.

Department of Homeland Security. (2015). *BTB Implementation Report to Leaders (annual reports)*. US.

Department of Homeland Security. Office of Community Partnerships and Federal Emergency Management Agency (FEMA). (July 2016). *Countering Violent Extremism (CVE) Grant Program*.

Department of Homeland Security. (2014). *Federal Emergency Management Agency (FEMA) Strategic Plan 2014-2018*.

Department of Homeland Security. (August 2015). *The Future of Smart Cities: Cyber-Physical Infrastructure Risk.* Office of Cyber and Infrastructure Analysis. National Protection and Programs Directorate.

Department of Homeland Security. (2013). *National Infrastructure Protection Plan (NIPP) 2013: Partnering for Critical Infrastructure Security and Resilience*. US.

Department of Homeland Security. (June 2016). *National Protection Framework (NPF)*. Second Edition.

Department of Homeland Security. (June 2012). *Northern Border Strategy*.

Department of Homeland Security. (August 2016). Overview of the Federal Interagency Operational Plans.

Department of Homeland Security. (February 2017). *Program Inventory*. Retrieved from: https://www.dhs.gov/publication/federal-program-inventory

Department of Homeland Security. (18 June 2014). *The Quadrennial Homeland Security Review (QHSR)*.

Department of Homeland Security. (2011). *Risk management fundamentals*. Homeland Security Risk Management Doctrine.

Department of Homeland Security. (December 2011). *The Strategic National Risk Assessment (SNRA) in Support of PPD 8: A Comprehensive Risk-Based Approach toward a Secure and Resilient Nation*. US.

Department of Homeland Security. (2013). *Supplemental Tool: Executing a Critical Infrastructure Risk Management Approach*. NIPP 2013.

Department of Homeland Security. Department of Transportation. (2015). *Transportation Systems Sector-Specific Plan*.

Department of Homeland Security. (April 2016). *US-CA Critical Infrastructure 2025: A Strategic Risk Assessment*.

European Community. (2013). *Scenarios for cascade events; New Methodologies for Multi-Hazard and Multi-Risk Assessment Methods for Europe,* MATRIX Project, Deliverable D3.3. European Community's 7th Framework Program.

European Community Research & Development Information Service (CORDIS). (2016). *New Multi-HAzard and MulTi-RIsK Assessment MethodS for Europe.* Retrieved from the European Commission website: http://cordis.europa.eu/project/rcn/96701_en.html.

Financial Transactions and Reports Analysis Centre of Canada. (2015). *Combating Money Laundering and Terrorist Financing*. Fintrac Annual Report. Immigrations and Customs Enforcement (ICE). *Strategic Plan 2016-2020*.

Global Affairs Canada. (2011). *Perimeter Security and Economic Competitiveness*.

Global Facility for Disaster Response and Recovery (GFDRR). *Understanding risk in an evolving world: emerging best practices in natural disaster risk assessment*. World Bank. 2014.

Hay, A., Philips, J. et al. (2016). *Smart City Connectivity to Support Municipal and Community Resilience.* Southern Harbour. 2016.

International Organization for Standardization (ISO). (2009). *Risk management – risk assessment techniques.* CAN/CSA-ISO/IEC 31010:2009. Geneva.

Organization for Economic Cooperation and Development (OECD). (2015). *National Risk Assessment (NRA):* profiles of selected OECD countries, High Level Risk Forum (HLRF). Public Governance and Territorial Development Directorate. Public Governance Committee. GOV/PGC/HLRF(2015)8/ANN1.

Organization for Economic Cooperation and Development (OECD). (2015). *National Risk Assessment:* profiles of selected OECD countries, High Level Risk Forum (HLRF). Public Governance and Territorial Development Directorate. Public Governance Committee. GOV/PGC/HLRF(2015)8/ANN1.

Public Health Agency of Canada. (November 2011). *Health Portfolio (HP) Public Health Emergency Risk Assessment Report*. Risk Assessment Sub-Committee. Joint Emergency Preparedness Committee (JEPC).

Public Safety Canada (PS). (2010). *Joint Border Threat and Risk Assessment (JBTRA).*

Public Safety Canada (PS). (2014). *Beyond the Border (BTB) Forward Plan*. Annex to BTB Implementation Report.

Royal Canadian Mounted Police. (March 2016). *Strategic priorities*. Retrieved from: http://www.rcmp-grc.gc.ca/prior/index-eng.htm

Royal United Services Institute (RUSI) for Defence and Security Studies. (October 2016). *Building Trust and Taking Risks in the Global Effort to Tackle Financial Crime*. Occasional Paper. UK.

Schoemaker, P. (2015). *Strategic Approaches to Managing Uncertainty*. Decision Strategies & Wharton. Wharton Risk Management and Decision Processes Center. 19 October 2015. (Research summary; not published at time of downloading, November 2016).

*Smart Borders Increasing security without sacrificing mobility*. Global Public Sector. Deloitte. 2014.

*The Future of Smart Cities: Cyber-Physical Infrastructure Risk*. Office of Cyber and Infrastructure Analysis. National Protection & Programs Directorate. DHS. August 2015.

The World Bank. *Disaster Risk Management in the Transport Sector: A review of concepts and international case studies*. 98202. June 2015.

The World Bank. Global Facility for Disaster Reduction and Recovery (GFDRR). *Understanding risk in an evolving world: emerging best practices in natural disaster risk assessment*. 2014.

United Nations Office for Disaster Risk Reduction (UNISDR). Global Assessment Report on Disaster Risk Reduction (GAR). *Making development sustainable: the future of disaster risk management*. 2015.

United Nations Office on Drugs and Crime (UNODC). World Drug Report. 2016.

*United States-Canada Agreement for Cooperation in Science and Technology for Critical Infrastructure Protection and Border Security (CIPABS*). (June 2004).

United States Customs and Border Protection (CBP). (2012-2016). *Border Patrol Strategic Plan: The Mission Protect America*.

United States Customs and Border Protection (CBP), Canada Border Services Agency (CBSA), and Royal Canadian Mounted Police (RCMP). (July 2010). US-CA Joint Border Threat and Risk Assessment (JBTRA). Published 2011.

United States Department of Justice & Drug Enforcement Agency. (October 2015). *National Drug Threat Assessment (NDTA) Summary (2015)*. DEA-DCT-DIR-008-16.

Vlek, C. (2013). *How Solid Is the Dutch (and the British) National Risk Assessment? Overview and Decision-Theoretic Evaluation*. DOI: 10.1111/risa.1205. Society for Risk Analysis. US.

Wittenberg, A., & Smith-Bingham, R. (2015). *Anticipating emerging risks – a blend of creativity and pragmatism*. Global Risk Center. Marsh & McLennan Companies. Downloaded from Wharton Risk Management and Decision Processes Center, October 2016.

# APPENDIX B PARTNERS' RESOURCES

This following list has been updated from the Risk Assessment Framework (RAF) Project Reference Report (January 2017). It includes resources that directly or indirectly affect situational awareness of security, safety, risk and resilience assessments being conducted in the Seamless Borders space. In most cases, CSS or its partners should have, or be able to get, this information, which would provide insight into how partners are using risk assessments in their internal and collaborative S&T investment prioritization processes.

The availability of individual threat / hazard "snapshot" assessments, which are dynamic, is less important than the evidence of documented processes and coordinating mechanisms that are systematic, repeatable and sustainable. This information would constitute part of the evidence that partners' and CSSP priorities consider risk from strategic, operational and program perspectives.

## CBSA

- Status of National Border Risk Assessment (NBRA). 2013.31 (CBSA. Secret, held by CSS).
- Status CA-US Integrated Border Enforcement Teams (IBET) threat assessments. (Last one in 2009.) (CBSA, RCMP, others.)
- Status of US-CA Joint Border Threat and Risk Assessment (last one in 2010).
- Status of CBP Container Security Initiative (CSI). CBP examines "high-risk cargo" in foreign marine ports.

## Transport Canada

- Maritime Domain Awareness (MDA) and the Interdepartmental Maritime Sub-Working Group (IMSWG), threat or risk assessments (TC - lead, DND, DFO/CCG, RCMP, others).[32]
- Strategic Risk Assessment Methodology.
- Multi-modal risk assessments.
- Lessons from (Aviation) Security Operations Risk Assessment Model (SORAM) – regional inspection planning tool (outputs are classified Secret).
- Any unclassified risk scenarios or assessments for specific border crossings or ports of entry.
- Risk Assessment Matrix (RAM) Methodology Guide (Draft, copy held by CSS).
- CA-US Transportation Border Working Group (TBWG) and action plan (2015-17).
- CA-US Border Infrastructure Investment Plan (BIIP). V3.0. August 2016 (TBWG).
- CA-US Integrated Cargo Security Strategy (ICSS) Program (pilot project reports).

[31] Apparently, the last NBRA is 2014. It was not determined whether CBSA provided the results to CSS.
[32] National security and sovereignty focus.

- Security Operations Risk Assessment Model (SORAM). 2008.

## Public Safety

- Regional Resilience Assessment Program (RRAP) and Virtual Risk Analysis Centre (VRAC):
  - Site criticality, resiliency, capability and/or risk assessment methodologies.
  - Examples of risk scenarios related to border security or specific points of entry.
  - Reports from RRAP pilot projects.
- Canadian National Risk Profile (NRP) project – risk assessment methodology.
- Canadian CI Sector Risk Profiles - Transportation (and treatment of borders and law enforcement).
- Strategic National Risk Assessment (SNRA), DHS - last one 2011: DHS web site).
- After-Action Review, PanAm Games (2015) and other major events (accreditation of athletes; cross-border emergency response; integrated risk assessment processes).
- All Hazards Risk Assessment (AHRA) methodology - final report, workshop reports and computer-based decision support tool.

## RCMP

- Domain Awareness WG (CBP and RCMP) reports on pilot projects (or specific risk products).
- Border security risk scenarios or assessments (preferably, unclassified).
- Risk assessment methodology or assessments in support of Serious and Organized Crime Strategy (RCMP, 2013, on web site).
- CA-US Cross-Border Crime Forum (prioritization process / criteria; engagement strategy).

## Health Canada / PHAC / PS

- Health Portfolio Public Health Emergency Risk Assessment Report. Risk Assessment Sub-Committee. Joint Emergency Preparedness Committee (JEPC). Health Canada. November 2011.
- Health Security Working Group (CA-US Beyond the Border Action Plan initiative) – threat / hazard, impact and risk assessment processes (rationalization / convergence of local, provincial and federal approaches; collaboration between public and private stakeholders; Sector Risk Profile).
- Health Portfolio Emergency Risk Assessment. 2007.
- Canadian equivalent to US National Health Security Strategy (prioritization of countermeasures).

### CFIA / AAFC

- Canadian studies or risk scenarios related to prioritizing agro-terrorism countermeasures and capability improvements.
- Canadian equivalent of animal, plant and agriculture security plans and risk assessment processes.
- Importer Risk Assessment Model. Part of Enterprise-based Risk Assessment (ERA) Model initiative focused on food safety risks. CFIA.

### CCG / Fisheries and Oceans Canada / Natural Resources Canada

- Maritime Security Risk Analysis Model (MSRAM). USCG.
- Area Risk Assessment (ARA) Methodology (environmental). CCG.
- Integrated Business & Human Resources Plan (IBHRP). Previous version 2012. CCG website.

### Finance Canada / Financial Transactions and Reports Analysis Centre of Canada (Fintrac)

- *Assessment of Inherent Risks of Money Laundering and Terrorist Financing in Canada*. National Risk Assessment (NRA). Finance Canada. 2015.
- *Anti-money laundering and counter-terrorist financing measures Canada*. Mutual Evaluation Report (MER). Financial Action Task Force (FATF). September 2016.

# APPENDIX C SEAMLESS BORDERS RISK DOMAIN CHARACTERIZATION

Table C-1 summarizes the seven (7) risk domains for Seamless Borders. Although, there is no CSSP portfolio related to financial crime, it is included to highlight the links between: border security; illegal immigration; smuggling of bulk cash and trade-based money laundering, organized crime and gangs, and terrorist financing. Its inclusion also would contribute to situational awareness, data analytics and 'follow-the-money capabilities. Furthermore, its inclusion highlights opportunities to engage different federal partners at the appropriate time to develop or gather a set of complex risk scenarios (e.g., Financial Transactions and Reports Analysis Centre of Canada (Fintrac), Criminal Intelligence Service Canada (CISC), Canada Revenue Agency (Charities) (CRA), Natural Resources Canada (NRCan), Environment Canada, Fisheries & Oceans, Indigenous and Northern Affairs Canada). Its inclusion is consistent with the statement in the Strategic Planning Guidance (SPG, 2016):

> This [*public concerns over privacy rights in reference to Bill C-51*] reinforces the complexity of mitigating threats and hazards and the need to consider multiple factors – including factors that are not directly related to the national safety and security domain (*Threats and Hazards Mitigation Focus Area*, p.7).

To demonstrate the utility of this framework to simulate dialogue and manage scope, the author includes risk trends and indicators based on a qualitative assessment of a border perspective using best judgement and operational and risk management experience including in safety, security, and CI risk and resilience management. The risk trends are relative other domains using a border lens. Trends are also indicative of opportunities including for more analysis by stakeholders including the extended S&T/R&D/OR community and with DHS. Two factors are shown – **risk exposure** and **risk trend**. Colours indicate level of risk exposure (simple mode – low - green, medium – brown and high - red). Arrows indicate the risk trend, which may or may not influence the risk exposure depending on the control environment and other factors. [Note S&T is a key component of the management control environment (e.g., management, technology, procedures).

To more fully characterize the risks, CSS/PS should consider other tools including: definitive program-oriented risk taxonomy; SRA process; stakeholder and impact assessment frameworks; standardized scenario format; typologies, case studies or other graphical representations of operational and risk scenarios; information search criteria and streamlined process; and criteria to inform data collection, performance measurement and selection of risk treatment strategies, which can withstand the scrutiny of the external stakeholders including program auditors.

**Table C-1: Characterization of Risk Scenarios**

| Risk Domains | Characterization of Risk Scenarios<br>*(inputs to scenario development and risk prioritization)* | Risk Trend | Indicators |
|---|---|---|---|
| Border operations & security | • Lack of situational awareness of the whole of lifecycle management systems for technology and data within the border physical-cyber technology infrastructure<br>• Lack of data on cross-border prevention, protection and response capabilities (e.g., terrorism, major events and disasters)<br>• Illegal immigration and smuggling increases in between border control points and/or on Native lands<br>• Delays in information sharing for major sporting events (e.g., credentials, identity verification, handling asylum seekers)<br>• Insufficient data on volume of criminals, extremists and gang members crossing borders<br>• (US) Security controls exceed (CA) privacy assurance standards and degrade public confidence<br>• Shifting resources to border security reduces GC flexibility for other priorities including: crime prevention; cybersecurity; defence; and medical countermeasures<br>• Preclearance controls expose Canadians' data to misuse or unauthorized access |  | • Significant investment<br>• Cyber-physical systems<br>• Balance of human and automated systems<br>• Data integrity and information security<br>• Information sharing and interoperability<br>• Travel and tourism<br>• Refugees and immigration<br>• US regulations / trust<br>• Critical infrastructure<br>• Complex relationships at ports of entry (e.g., compartmented risk at airport and port authorities)<br>• Smart technologies |

| Risk Domains | Characterization of Risk Scenarios<br>*(inputs to scenario development and risk prioritization)* | Risk Trend | Indicators |
|---|---|---|---|
| | • Lack of situational awareness of controls for insider threat within border security organizations and supply chains<br>• Lack of data on inspection, investigation and enforcement efficiency and effectiveness (fit-for-purpose)<br>• Abuse of power by and a lack of accountability of border officials that violates human civil rights and/or business confidentiality protection measures<br>• Excessive delays or inefficient controls at border crossings that increase costs to trucking small business owners / operators<br>• Inefficient controls that have an adverse impact on tourism and border community businesses | | |
| Transportation security | • Exploitation of surveillance gaps in major waterways increases<br>• Exploitation of inter-modal intersections and hubs increases<br>• Lack of situational awareness of illegal activity across modes and jurisdictions<br>• Lack of situational awareness of container and cargo supply chain risks<br>• Lack of reliable data and awareness of strengths and weaknesses of critical infrastructure sector<br>• Insufficient security and response capabilities to |  | • Significant collaboration<br>• Environment (e.g., movement of crude oil, dangerous goods)<br>• Remote communities and the North<br>• Skill and knowledge (workforce)<br>• Agility (shift between modes)<br>• Aging critical infrastructure |

| Risk Domains | Characterization of Risk Scenarios<br>*(inputs to scenario development and risk prioritization)* | Risk Trend | Indicators |
|---|---|---|---|
| | minimize impact of pipeline failures on vulnerable areas<br>• Mismatches in rail security and accident response capabilities between CA and US<br>• Slow response to accident involving hazardous material at major border crossing<br>• Over regulation decreases sector competitiveness | | • SA of supply chain risks<br>• Smart technologies |
| Organized crime | • Stronger US-Mexico border controls and constant US demand for drugs shifts smuggling supply routes to US through Canada<br>• Fragmented academic research fails to address border and security issues (e.g., gangs; radicalization; crime prevention) |  | • Adaptability of OC<br>• Link between OC, gangs, drugs and ML/TF<br>• Corruption and coercion<br>• US strengthens Southern border, restricts travel |
| Financial crime[33] | • Smuggling of bulk cash and trade-based ML increases financing of criminal activity, violent extremism, radicalization and terrorism<br>• Failure to detect fraud, corruption and/or extortion at border crossings, ports of entry and/or transportation hubs |  | • Value, volume, velocity of transactions<br>• Electronic fund transfer<br>• Anonymity<br>• Complexity of business relationships<br>• Complexity of regulations |

[33] Although CSSP does not have a portfolio focused on financial crime, the border and some existing portfolios directly or indirectly interact financial crime. This domain highlights the relationships that affect the border environment: organized crime and gangs; smuggling, human trafficking and other crime; money laundering and terrorist financing. This approach could also help to identify new partners (e.g., Fintrac), sources of information, and/or unique knowledge and capabilities (e.g., risk analysis; big data; analytics). The SRA should also highlight opportunities for focusing academic research and identifying opportunities to increase capacity in CSS knowledge areas (e.g., operations research).

| Risk Domains | Characterization of Risk Scenarios<br>*(inputs to scenario development and risk prioritization)* | Risk Trend | Indicators |
|---|---|---|---|
| | | | • Extortion. Corruption, white collar crime<br>• Cybersecurity<br>• Critical infrastructure |
| Health security | • Infectious disease outbreak that exceeds medical system capacity and resilience<br>• Medical countermeasures are inadequate and US specialized resources are not available<br>• Lab and vaccine production capacity is slow to respond and/or dependency on other nations and industry<br>• Lack of actual events reduces priority for investment in preparedness, risk mitigation and resilience<br>• Lack of data on critical infrastructure preparedness and resiliency<br>• Past successes reduce priority for investment in research labs and prevention (e.g., SARS; e-coli) |  | • Opioid epidemic, addiction, mental health<br>• Next pandemic<br>• Vulnerable populations<br>• Lab capacity<br>• Standards and employability<br>• Urban density and mass transit<br>• Preparedness |
| Animal, food & agriculture security | • Lack of reliable data on, and situational awareness of, food supply chain control effectiveness<br>• Lack of situational awareness across threat vectors or pathways (e.g., smuggling, ship hulls, illegal importation) |  | • Surveillance and detection<br>• Transportation vectors<br>• Lab capacity and mutual assistance across borders |

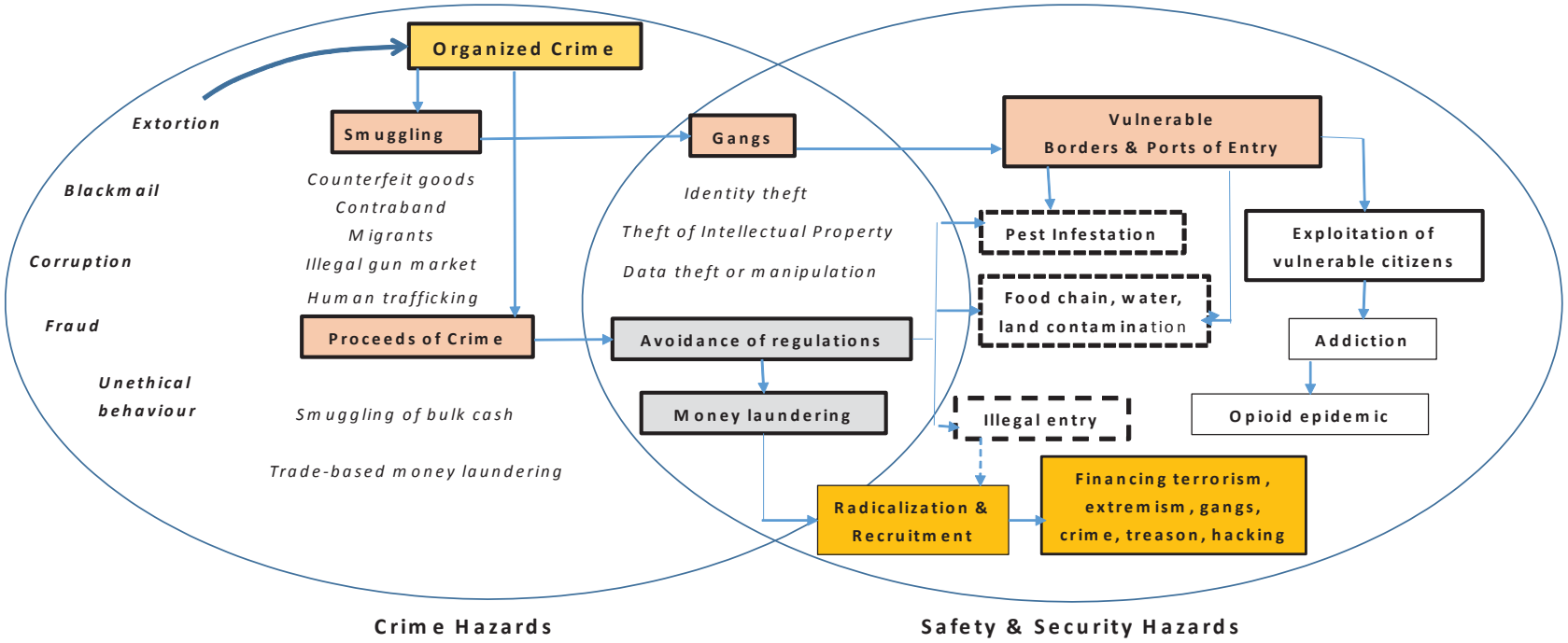
| Risk Domains | Characterization of Risk Scenarios<br>*(inputs to scenario development and risk prioritization)* | Risk Trend | Indicators |
|---|---|---|---|
| | • Public and political complacency do not sustain or reduce investment in capability improvements [e.g., zoonotic and animal disease (ZAAD) defence[34]]<br>• Lack of data on human and animal critical infrastructure preparedness, countermeasures and resiliency | | • Time between crises<br>• SA of supply chain risk<br>• Knowledge |
| Cybersecurity[35] | • Non-IT asset vulnerabilities – transportation networks; traffic management systems<br>• Targeted external or internal attacks on border or transportation systems storing personal and business sensitive information (e.g., identification, authorization, registration, licences, intellectual property; cargo, container and other security plans and risk assessments)<br>• Lack of data on communications and non-IT critical infrastructure control effectiveness, preparedness and resiliency<br>• Lack of compliance with standards and enforcement capability (e.g., voluntary compliance) |  | • Significant investment<br>• Redundancy and resiliency at points of entry<br>• Knowledge<br>• Private and sensitive business information stored in multiple systems with multiple standards and safeguards<br>• SA of vulnerability and control effectiveness across systems |

[34] DHS resources include ZADD Center of Excellence in the Homeland Security University program and the Institute for Infectious Animal Diseases at Kansas State University.

[35] The Border Transportation and Security (BTS) *Narrative* (2013) states, “In many border contexts cyber implications are unknown. This applies to vulnerabilities of integrated, digital automation in the supply chain and to networks that link sensors at points of entry for cargo and travellers and at remote locations for illegal entry” (2013, p.9).

# APPENDIX D MULTI-RISK SCENARIO PLANNING FRAMEWORK

Figure D-1 is an example of a multi-risk framework that strives to illustrate the interconnectedness of the border security risk management environment. Such a tool could be used to illustrate the value of using high-level risk scenarios to influence and/or help to prioritize special risk assessments, and to identify opportunities to engage different stakeholders on multiple levels, and to leverage existing relationships, working groups and networks to facilitate a more strategic dialogue on risk.




Adapted from: Relationships between different hazards (the arrows are orientated in the sense of triggering) (Figure from MATRIX Deliverable 6.3). European Community, 2013: figure 15. Cited in Comprehensive Scan for CSSP. CAE 5843-011. 2016.

**Figure D-1: Example of Multi-Risk Scenario Planning Framework**

# APPENDIX E STRATEGIC RISK ASSESSMENT CONCEPT

The influence diagram illustrates the iterative nature of a continuous dynamic risk assessment process that engages stakeholders in a participative process. Four balancing loops are depicted (B1-4) to close the gap in the performance of risk (capability and resilience) assessment processes, and to improve the value of risk information to decision making and mission success.

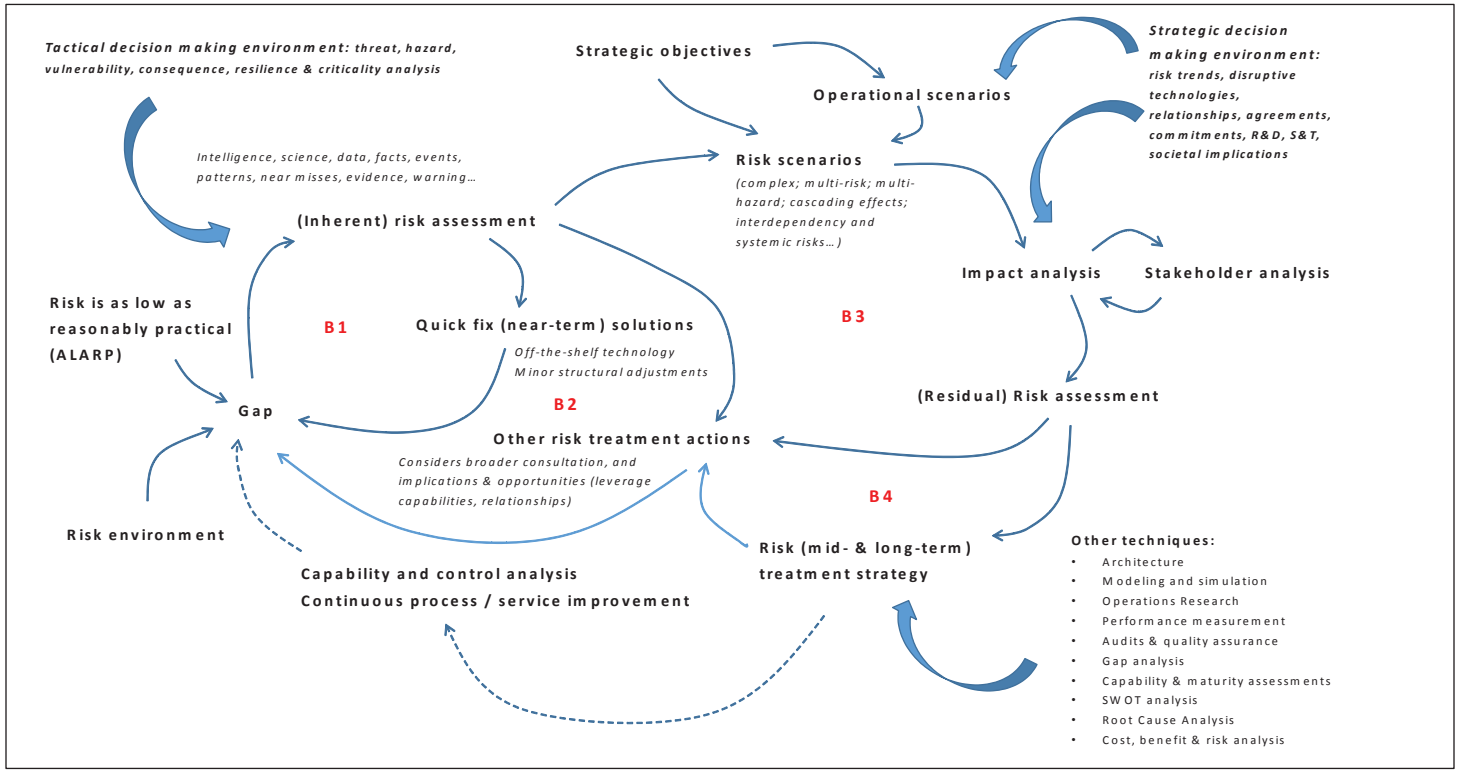



Figure E-2: Strategic Risk Assessment Concept