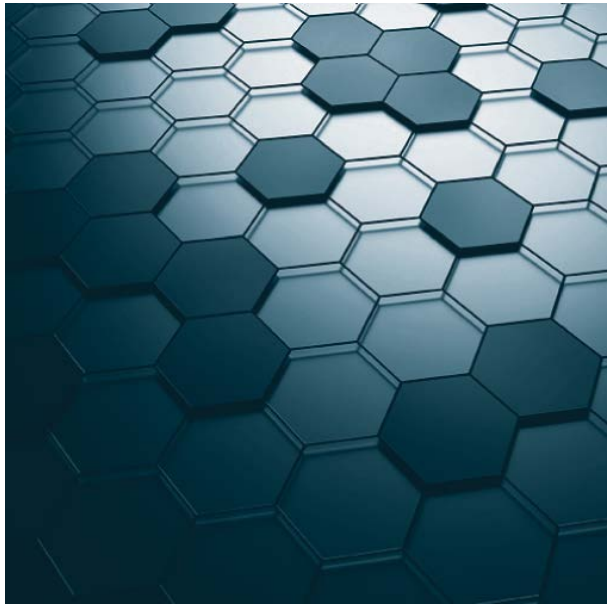
Public Safety Canada | Sécurité publique Canada

BUILDING A **SAFE** AND **RESILIENT CANADA**



Supply chain risk management and critical infrastructure inter-dependency in Canada

Ryan Schwartz
Manager, Critical Infrastructure Policy Development
Public Safety Canada

Joint OECD-JRC Critical Infrastructure Workshop
OECD Conference Centre, Paris, France
September 24-25, 2018

Canada

Outline

- Canada's *National Strategy and Action Plan for Critical Infrastructure*
- Critical infrastructure (CI) sectors in Canada
- Supply chain risk management in CI sectors (and related issues)
  - Rationale: energy and utilities, ICT, and transportation sector examples
  - The importance of extreme weather and climate-related hazards
  - Public Safety Canada's inter-dependency modelling efforts
- Questions and discussion
- Annex
  - Overview of Public Safety Canada critical infrastructure initiatives

What guides Canada's work on CI

National Strategy and Action Plan for Critical Infrastructure

- Establishes a collaborative approach to strengthening resilience and promotes 3 strategic objectives:

1. Build trusted and sustainable partnerships
2. Advance the timely sharing and protection of information within the CI community
3. Foster an all-hazards risk management approach

The Canadian approach to CI

- In Canada, we are organized by 10 CI sectors:

Energy and utilities

Finance

Information and communications technology (ICT)

Health

Food

Government

Water

Transportation

Safety

Manufacturing

Energy and utilities sector example

- Supply chain risks from Eastern North American power blackout of August 2003; approximately 50 million people without electricity for days
  - 10 million in Canada
  - 40 million in the United States

- Cascading shutdowns, triggered by trees contacting power lines, resulting in an outage covering more than 24,000 square kilometers

- Significant economic costs in the United States and Canada
  - Estimates of total costs in the United States range between $4 billion and $10 billion USD
  - Canada's GDP declined by 0.7% in August 2003, net loss of 18.9 million work hours, and manufacturing shipments in Ontario were down $2.3 billion CDN

Source: U.S.-Canada Power System Outage Task Force, April 2004

ICT sector example

- Supply chain risks (known and emerging) for information and communications technology (ICT) infrastructure, such as the development of 5G networks
  - 5G presents significant potential for social and economic benefit

- Governments concerned foreign vendors and service providers in the 5G cyber supply chain could deploy assets in domestic telecommunications infrastructure
  - To, for example, build hardware and software backdoors into products that could access networks to disrupt systems / operations, steal private data, or spy on businesses and corporations

- Canada is conducting a national security analysis to minimize cyber threats from equipment made by foreign telecommunications companies

Source: The Globe and Mail, September 2018

Transportation sector example

- Supply chain risks from cyber threats, such as NotPetya malware (June 2017)
- Spread to some of the largest global corporations, with total damages estimated at $10 billion USD
  - Global supply chain disruption stemming from local source
- Danish shipping company Maersk experienced near-total IT failure
  - Official costs of approximately $300 million USD to the company
- Maersk's ports and shipping terminals paralyzed for days, resulting in cascading supply chain impacts (e.g., delays, loss of goods), compounded by "just-in-time" delivery model in sectors such as food and manufacturing

Source: WIRED magazine, September 2018

Extreme weather, climate-related hazards

- Numerous risks to supply chains arising from climate-related impacts
  - For example, flooding can overwhelm infrastructure causing local and broader-scale impacts by damaging transportation networks, compromising access and supply chains (food, health, energy, manufacturing, etc.)

- Failing to address possible consequences of events that disrupt supply chain efficiency can result in significant financial losses to companies

- In Canada, there is little published research about indirect impacts of climate change on industry, such as changes associated with consumer demand, **supply chains**, real estate or other assets, adaptation by other sectors, legal liability or government regulation

Source: Government of Canada, 2014

Public Safety Canada's inter-dependency mapping / modelling efforts (1 of 2)

- Supply chains are a critical infrastructure inter-dependency proxy; growing internal and inter-sectoral connectivity (in Canada and globally)
  - Cross-cutting issue; important for all CI sectors in Canada, particularly energy and utilities, food, ICT, manufacturing, transportation, and water

- Public Safety Canada has undertaken high-level inter-dependency analyses of individual CI sectors as they relate to other CI sectors in Canada
  - Internal sectoral analysis with examination of cascading impacts on or across other sectors, not a detailed sector-to-sector mapping and analysis

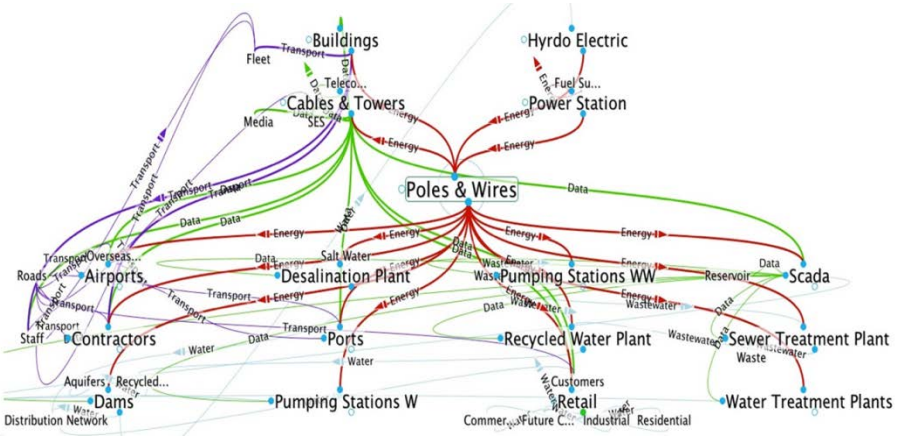
- Complex undertaking, hence Public Safety is exploring and evaluating critical infrastructure inter-dependency modelling and analysis tools
  - For example: DOMINO (Canada) and XDI (Australia)

Public Safety Canada's inter-dependency mapping / modelling efforts (2 of 2)

- Two inter-dependency models currently being evaluated by Public Safety Canada

1. **XDI platform**: captures asset engineering and design data and historical and future weather; capable of analyzing hundreds of assets in minutes
   - Buildings, roads and rail, water and wastewater systems, telecommunications
   - Flooding, coastal inundation (with sea level rise), forest fires, heat waves, wind extremes
   - Current pilot project in a British Columbia municipality

XDI CROSS DEPENDENCY INITIATIVE



2. **DOMINO model**: decision support tool designed to anticipate and model spatial and temporal effects between CI; database linked to a geographic information system
   - Consequences-based risk management approach, which aims to assess the cascading impact of critical infrastructure failure (without considering the causes that led to failure)

Discussion

- Supply chain risks to be considered in CI resilience policy:
  - *Cyber* and *climatic*; black swan potential for lengthy and costly disruptions
- Best practices for mainstreaming supply chain risk management for CI:
  - Business continuity planning / business risk management – add to existing risk spectrum
- What part of the supply chain to include (or not) in CI resilience policies:
  - Difficult to limit but localized case studies can help understand dependencies, boundaries
- Allocating risk and liability exposure along CI supply chains:
  - Risk transference, such as insurance products (e.g., overland flooding, wind, ice)
- Government and owner / operator partnerships for CI resilience:
  - Networks of networks, national strategies (e.g., Canada's new cyber security strategy)

Contact

Ryan Schwartz
Manager, Critical Infrastructure Policy Development
National and Cyber Security Branch
Public Safety Canada
Ottawa, Ontario

+1-613-949-4132
Ryan.Schwartz@canada.ca

Annex: overview of Public Safety Canada critical infrastructure initiatives

- CI Action Plan initiatives for 2018-2020
- Critical infrastructure Exercises Program
- Regional Resilience Assessment Program
- Virtual Risk Analysis Cell
- Cyber Engagement
- CI Gateway
- National Cyber Security Strategy
- Contact

CI Action Plan 2018-2020

Build Partnerships

1. Address cross-sector issues through multi-sector meetings
2. Engage with provinces and territories to strengthen critical infrastructure resilience
3. Ongoing collaboration with lead federal departments
4. Expand regional outreach of critical infrastructure programs (RRAP/VRAC/Exercises)
5. Engage with various international forums to address critical infrastructure issues

Share and Protect Information

6. Modernization and promotion of the Critical Infrastructure Gateway
7. Conduct an environmental scan on information sharing
8. Develop and distribute risk information during a steady state and during unfolding events of national significance
9. Support the acquisition of security clearances among private sector stakeholders

All Hazards Risk Management

10. Increase impact and reach of critical infrastructure site-assessments
11. Implement a risk-based approach to identify key assets/infrastructure of significance
12. Identify ways to support the critical infrastructure community in taking action to address risks
13. Conduct cross-sector exercises to strengthen preparedness and response
14. Assess the health of the ten critical infrastructure sector networks
15. Support the community in addressing risks associated with the convergence of physical and cyber critical infrastructure systems
16. Examine the National Strategy for Critical Infrastructure to determine if there is a need to update Canada's overall approach to critical infrastructure resilience
17. Develop a tracking mechanism to assess the progress of the activities in the action plan

CI Exercises Program

This team works to improve the integration of the CI community in Canada in event response and to increase the participation of CI owners and operators in exercises.

- Way forward
  - Needs assessment to determine the interests and capacity of CI owners and operators to participate in exercises
  - Identify CI-related themes and trends in After Action Reports
  - Creation of a public-private working group on CI exercises

Regional Resilience Assessment Program (RRAP)

This team conducts site assessments of CI facilities in Canada to identify and address vulnerabilities and is a service that helps CI owners and operators measure and enhance the resilience of their facilities.

This program Is:

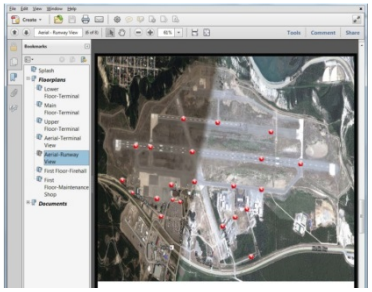
Non-regulatory

Free of cost

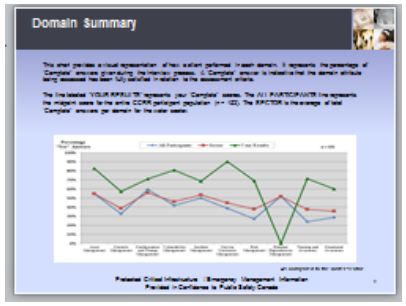
Confidential

Three **powerful** tools to measure **protection**, **resilience**, and **cyber security**:

CIRT
Critical **I**nfrastructure
Resilience **T**ool



CIMT
Critical **I**nfrastructure
Multimedia **T**ool



CCRR
Canadian **C**yber
Resilience **R**eview

RRAP (continued)

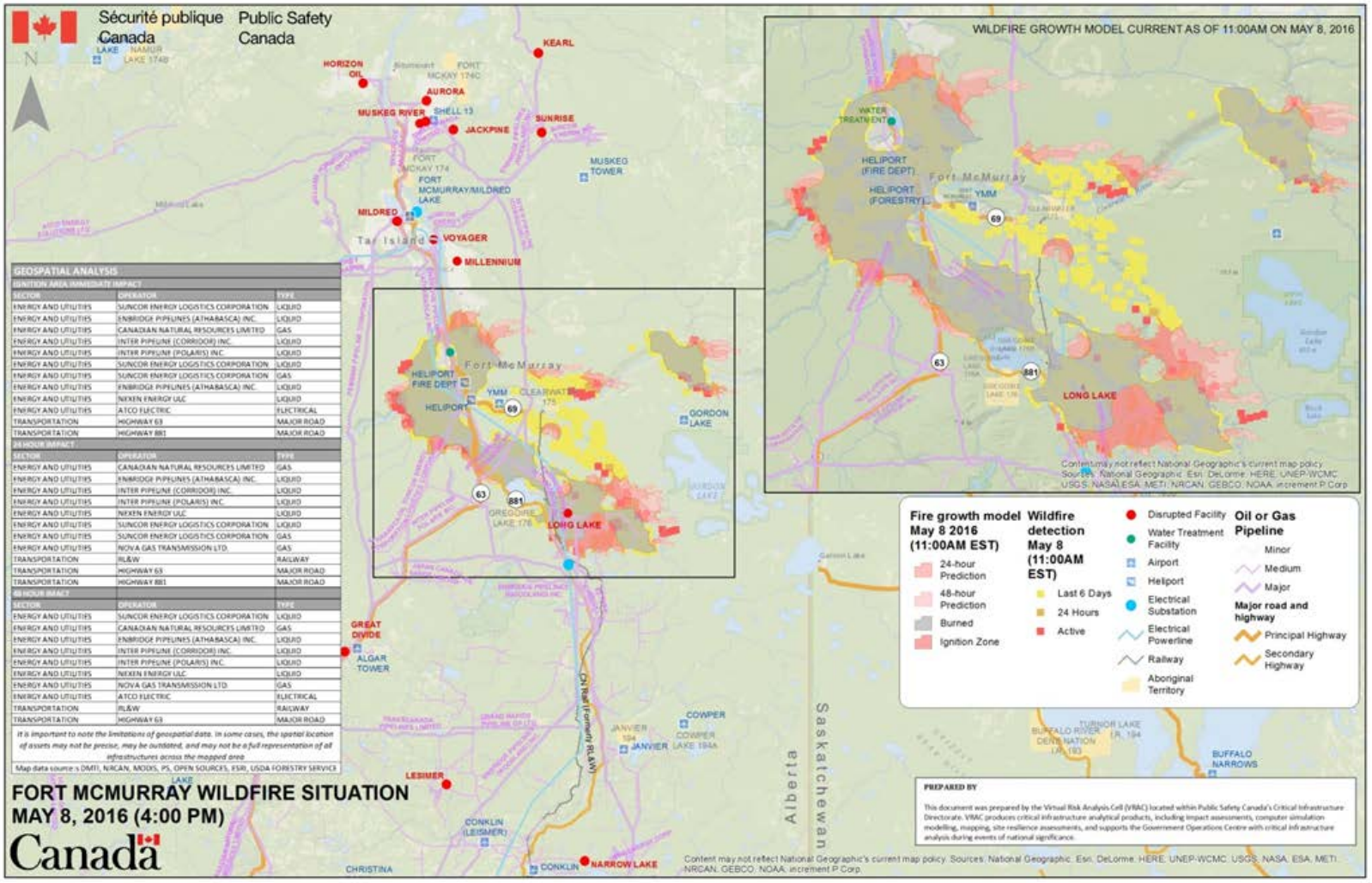
- Benefits of RRAP
  - Improve risk management and awareness
  - Make informed investment decisions
  - Establish government relationships
  - Minimal investment of time and resources
- Way forward
  - Enhancing provincial and territorial involvement in the RRAP
  - Improved assessment prioritization and information sharing
  - Complete a 3rd Cross-Border RRAP project (United States)

Virtual Risk Analysis Cell (VRAC)

This team develops and shares analytical products and produces impact assessments—including geospatial and dependency analysis—on disruptions to CI in Canada.

Steady State	***Event State***
Develops, maintains, and distributes analytical products, tools, models and simulations related to impacts and risks to CI.	Produces CI-specific impact assessments and analysis on the effect of the disruption across sectors in support of Federal, Provincial and Territorial emergency management efforts (including the Government Operations Centre).

VRAC: event state products



Cyber Engagement

This team organizes cyber engagement activities, cyber exercises, ICS symposiums, and various other projects and programs to support the cyber security needs of Canadian CI.

Industrial Control Systems (ICS) symposiums

- Brings together ICS experts from across Canada's 10 CI sectors to:
  - Provide training
  - Share tools and information
  - Better protect ICS from cyber disruptions

- Two days of presentations and lectures plus a one-day technical workshop

- Provides an opportunity to network with other CI owners and operators as well as hands-on training and awareness for CI technical operators

CI Gateway

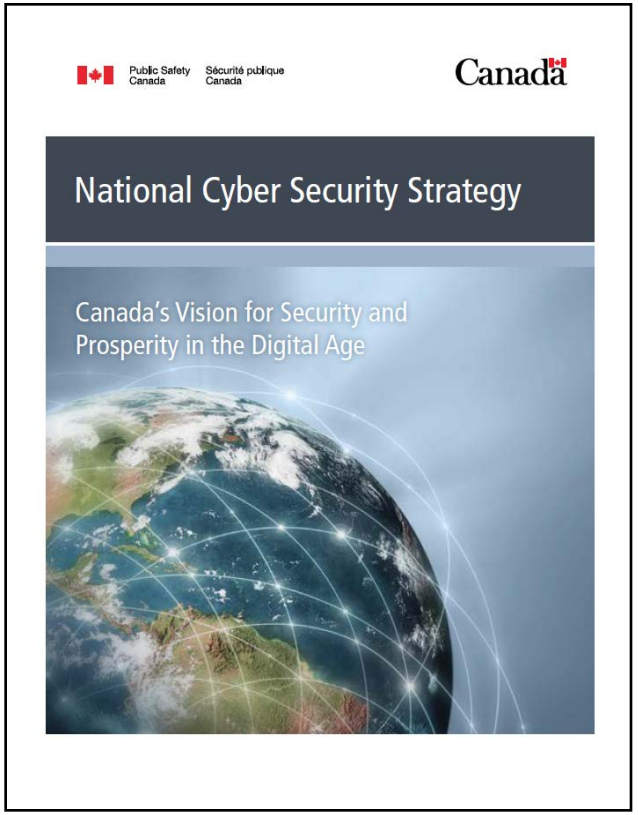
- Canada's online CI portal: encrypted and password protected platform for the sharing of unclassified information
- Information products include: risk management documents, best practices, lessons learned, meeting material, standards, and an events calendar
- Global CI Gateway: for international partners to connect virtually and share information across multiple working groups

National Cyber Security Strategy

- Announced on June 12, 2018 by federal Ministers of Public Safety and Emergency Preparedness, National Defence, and Innovation, Science, and Economic Development

- Based on 3 themes / pillars:
  - Security and resilience
  - Cyber innovation
  - Leadership and collaboration

- Federal government's 2018 Budget invested $507.7 million over five years and $108.8M per year ongoing to support the new Strategy
  - Includes a *Canadian Centre for Cyber Security* and a *National Cybercrime Coordination Unit*



Contact us

General questions: ps.ciengagements-engagementsie.sp@canada.ca

Regional Resilience Assessment Program: RRAP_PERR@ps-sp.gc.ca

Virtual Risk Analysis Cell: ps.vrac-cavr.sp@canada.ca

CI Gateway: ps.cigateway-passerelleie.sp@canada.ca