Canadian Government Intervention in Ensuring Critical Infrastructure Protection

Rahul Ravi Hulli: 40234542 Anita Archibong: 27729790 Josephine Famiyeh: 40262544

Abstract

The Government of Canada implements preventive measures to enhance national security, focusing on key sectors like government, transport, energy, utilities, and finance. Through risk assessment, including cyber-attacks, theft, terrorism, and natural disasters, it minimizes risks and increases resilience. Collaborative efforts with stakeholders are pivotal in this approach. The National Strategy and Action Plan for Critical Infrastructures addresses security issues and ensures readiness for recovery and response. Public opinion and readiness for new threats are also considered. The government prioritizes safeguarding critical pillars of society, including social well-being and national security.

Introduction

The integrity and resilience of essential infrastructure are vital for Canada's security and prosperity in an era of technological innovation and interconnection. Critical sectors like energy, transportation, telecommunications, and healthcare sustain public services and the economy. However, with growing reliance on digital networks, cyberattacks, natural disasters, and geopolitical tensions pose increasing threats. This research examines the Canadian government's approaches to ensuring the safety of vital infrastructure, including legislative programs, collaborations, and technological developments. Early action is crucial, as past events like the 1998 ice storm and recent cyberattacks have underscored the need for resilience and preparedness. The government employs a comprehensive approach, including regulatory frameworks like the Critical Infrastructure Protection Program (CIPP), sector-specific policies, and alliances with academic institutions and industry partners to enhance knowledge exchange and threat intelligence. Investments in cutting-edge technology are prioritized to strengthen defenses and minimize disruptions. However, navigating the dynamic and complex landscape of critical infrastructure security requires continuous adaptation and improvement strategies. This research aims to shed light on Canada's evolving role in protecting vital resources and contribute to understanding efforts to ensure resilience and integrity in an unpredictable environment.

Background and Motivation

The extensive protection of infrastructure in Canada is prompted by the country's vast size and interconnectedness, coupled with the importance of critical systems to its economy and citizens' well-being. Various threats, including terrorism, natural disasters, cyberattacks, and infrastructure failures, necessitate preventive measures to ensure operational integrity and resilience. The government's policies focus on safeguarding critical infrastructure to maintain stability, security, and economic growth. Continuous efforts are required to mitigate risks and address evolving threats, such as terrorism, natural disasters, cyberattacks, and infrastructure degradation. This overview highlights the government's approach to securing Canada's critical infrastructure and vital economic sectors.

Literature Review

Comprehensive national cybersecurity policies are crucial, with Canada's National Cyber Security Strategy serving as a framework for cooperation. Legislative frameworks like the Digital Privacy Act and the Security of Canada Information Sharing Act enhance threat intelligence exchange. The Critical Infrastructure Protection Program aims to bolster the resilience of vital infrastructure through risk assessments and sector-specific regulations. Canada actively participates in international cybersecurity efforts, promoting standards and capacity building. Despite advancements, challenges persist, requiring a focus on developing a cybersecurity culture and utilizing advanced technologies. Research studies evaluate the effectiveness of government interventions and suggest improvements. Industry publications offer insights and recommendations for enhancing critical infrastructure protection. International comparisons provide benchmarks and best practices for infrastructure resilience. Government speeches and media coverage shed light on goals, challenges, and actions related to critical infrastructure protection in Canada. News articles highlight cyber threats, vulnerabilities, government responses, and policy discussions, raising public awareness and fostering cooperation.

Classification of Canada’s Critical Infrastructure

In Canada, critical infrastructure sectors play a vital role in maintaining societal functions and economic stability. These include utilities and energy, transportation, government institutions, information, and communication technology (ICT), healthcare, community safety, water management, and the manufacturing industry. Each sector is integral to the country's operations and contributes to public well-being and national security. From energy transmission and financial transactions to transportation networks and emergency response systems, these sectors ensure the smooth functioning of Canada's economy and society. Moreover, they support innovation, education, and social progress, enhancing the nation's global competitiveness and resilience.

Threat Sources to Critical Infrastructure

Canada faces various threats to its critical infrastructure, from terrorism to cyberattacks, endangering public safety and economic stability. To address these challenges, a multifaceted approach involving legislation, regulation, and collaboration is necessary to enhance resilience and protect national assets, ensuring continued security and stability amidst evolving risks.

The Role of Government in Protecting Critical Infrastructure:

The Canadian government leads efforts to reduce vulnerabilities, improve threat detection, and enhance response for critical infrastructure nationwide. It oversees and manages critical infrastructure during emergencies while respecting provincial jurisdictions, providing direct assistance upon request. The primary goal is to ensure the continuous delivery of essential services.

National Strategy for Critical Infrastructure

The National Strategy encourages cooperation between vital infrastructure sectors and federal, provincial, and territorial efforts to build resilience. It prioritizes teamwork, risk mitigation, and all-hazards strategies, with shared accountability for protecting vital infrastructure. Emergency preparedness is advised for Canadians, and its implementation necessitates collaboration across many government agencies and industries. Resilient infrastructure promotes economic expansion. The Canada-United States Action Plan on Critical Infrastructure, which addresses interdependencies and global hazards, is another component of the strategy.

The Strategy

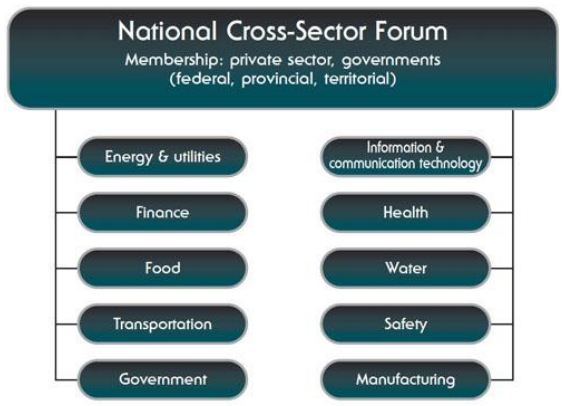

Figure 1 National Cross-Sector Forum [1]

The Strategy prioritizes partnership building for critical infrastructure stability, aligning with Canada's Emergency Management Framework. It emphasizes coordinated actions among stakeholders, with jurisdictional governments as initial points of contact during disruptions. The federal government stands ready to provide prompt assistance, relying on collaborative efforts among territorial, provincial, federal, and critical infrastructure sector partners for successful implementation. Sector networks facilitate collaboration through activities like risk assessments and mitigation plans, bolstering tailored networks with sector-specific expertise and resilience tools. A National Cross-Sector Forum promotes comprehensive resilience by encouraging information exchange. The Strategy stresses continuous, proactive, and systematic risk management. Sector-specific federal departments collaborate with provinces, territories, and infrastructure sectors to identify risks and craft all-hazard risk analyses. Enhanced information sharing, compliant with laws and policies, supports effective risk assessment and implementation. Prioritized information security necessitates amendments to access legislation and standardized protocols, with collaborative efforts aimed at enhancing Canada's information-sharing and protection practices across federal, provincial, and territorial levels.

National Strategy for Cybersecurity

Canada faces escalating cyber threats to its digital infrastructure, necessitating government-led efforts to enhance cybersecurity and shield individuals and organizations. Collaborative initiatives with global partners are crucial to combat cybercrime and bolster resilience against state actors. Focus areas include protecting Canadians from cyber incidents, fortifying critical systems, and boosting cybersecurity capabilities across federal departments. Efforts extend to supporting small and medium-sized businesses, establishing requirements for safeguarding critical infrastructure, and advancing research and innovation in cybersecurity technologies. Investments prioritize quantum computing, blockchain, digital skills development, and cyber threat research. Streamlined guidance, incident response, and enhanced information sharing with the private sector are key objectives. Public awareness campaigns and collaboration forums aim to strengthen cybersecurity nationwide. A national cyber plan, developed in coordination with provinces, territories, and the private sector, will reinforce cybersecurity measures. International collaboration is essential to combatting global cyber threats. Budget 2018 allocated significant funds to support cybersecurity initiatives, including the establishment of the Canadian Centre for Cyber Security in October 2018.

Securing Operational Technology Awareness Series (Itsap.00.051)

The Canadian Centre for Cyber Security (CCCS) initiated an awareness series in July 2022 on the risks of Operational Technology (OT) and ways to mitigate cyber threats, considering its growing connection to IT networks and the internet.

Risks	***Descriptions***
Malfunctioning Equipment and Process Disruption	Unauthorized access to operational technology disrupts processes, causing equipment malfunctions and delays.
Compromise of Intellectual Property and Sensitive Information	Operational Technology (OT) breaches risk economic losses through data exposure.
Revenue Loss from Disruptions	OT disruptions risk revenue loss from halted processes, repairs, or ransom payments.

Damage to Organizational Credibility	Operational technology breaches damage credibility and stakeholder relationships.
Compromised Security Measures, Including Emergency Services	Operational technology breaches risk public safety by compromising security measures, including those for emergency services.
Potential for Major Accidents and Disasters	OT failures can lead to accidents or disasters, risking injury or loss of life.

Operational technology failures risk safety and critical service loss, targeted by threat actors for destruction.

Current Solutions to Canada's Critical Infrastructure

Canada faces diverse threats to critical infrastructure, addressing them through collaborative emergency management with federal, provincial, and territorial governments. The Disaster Financial Assistance Arrangements help address financial needs after natural disasters, with added aid from federal, provincial, and territorial governments for affected sectors.

Phase	**Activities**
Prevention and Mitigation	Tailored measures by collaborative efforts with FPT governments. Floodway creation and land-use management for interventions.
Preparedness	Risk-based response strategy planning and emergency management training programs.
Response	Local crisis management with provincial or territorial intervention coordinated federal assistance during national crises.
Recovery	Encouragement of recovery-mitigation connections, management exercises for strategy validation, and post-event evaluations. National Public Alerting System (NPAS) for swift alerts on life-threatening situations.

Addressing Cyberattacks on Canada's Critical Infrastructure

Canada's National Cyber Security Action Plan safeguards innovation and prosperity by coordinating efforts among stakeholders. It bolsters critical infrastructure resilience through cybersecurity audits and training. Additional strategies include:

Canadian Centre for Cybersecurity	Serves as a centralized resource for operational cybersecurity assistance, enhancing threat assessment and strengthening relationships with vital infrastructure owners.
National Cybercrime Coordination Unit (NC3 Unit)	Coordinates efforts to combat cybercrime, manage Canadian cyber activities, and enhance detection.
Student Work Placement Program (SWP) for cybersecurity	Funds partnerships to align educational skills with employers' requirements.
Cybersecurity assessments and certifications for SMEs.	Aims to raise awareness and promote international standardization.
Capacity for Strategic Policy in Cybersecurity and Cybercrime:	Ensures coordination of policy concerns, supporting the Cyber Security Cooperation Program.
Cyber Security Cooperation Program	Supports projects enhancing cyber systems' security, benefiting various stakeholders.
Enhanced cooperation with the U.S.	Fosters closer collaborations in cybersecurity strategy implementation.
Enhanced collaboration with energy sector stakeholders	Aims to strengthen collaboration with the U.S., enhancing the security of the North American electricity grid and cross-border pipelines.

Comparing critical infrastructure protection mechanisms in the US and Canada.

Critical Infrastructure Protection (CIP) safeguards vital systems and assets crucial for societal, economic, or national functioning, including physical and cyberinfrastructure. It targets threats like natural disasters, cyberattacks, and terrorism, with key components like risk assessment and incident response. Governments enact laws and regulations to promote security, evolving CIP to address emerging threats and technological advancements.

US Initiatives: Protection Mechanisms of Critical Infrastructure in the US

Public-Private Partnerships (PPPs) emerged in the late 1970s for public sector efficiency, extending to various sectors including Critical Infrastructure Protection (CIP). However, their effectiveness, especially in information sharing, is limited. The National Infrastructure Protection Plan suggests the network governance approach, emphasizing collaboration and comprehensive risk management for better security and resilience.

Canada Initiatives: Protection Mechanisms of Critical Infrastructure in Canada

The Emergency Management Framework for Canada ensures a collaborative approach to safeguarding public safety. The Strategy for enhancing critical infrastructure resilience emphasizes collective risk management and interdependencies. It aims to unravel the Strategy's role in securing foundational societal elements.

Aspect	Description
Objective	Aims to fortify resilience against natural, intentional, and accidental hazards through collaboration and framework.
Fostering Collaborative Resilience	Emphasizes collaboration among governments and critical infrastructure sectors, prioritizing partnership and risk management.
Build Partnerships	Aligned with the Emergency Management Framework, optimizes resource utilization across prevention, mitigation, and recovery.
National Cross-Sector Forum	Facilitates collaboration between the private sector and governments, ensuring diverse perspectives for resilience.
Implement All-Hazards Risk Management	Focuses on applying risk management and business continuity planning to understand and manage risks comprehensively.
Share and Protect Information	Aims to enhance resilience through timely information sharing and protection, promoting coherency of action.
Information Protection	Develops exemptions and protocols to safeguard critical infrastructure information.

CISA - Critical Infrastructure Sectors

Sector	Description
Chemical Sector	DHS - Chemical Sector Risk Management Agency (SRMA): business security collaboration.
Commercial Facilities Sector	Enhances security across eight subsectors to safeguard public areas from attacks.
Communications Sector	Safeguards the communication network, including wireless and satellite technologies.
Critical Manufacturing Sector	Protects critical manufacturing sectors from disasters through assessment and safeguarding.
Dams Sector	Safeguard dams from technological and natural threats to ensure water control.
Defense Industrial Base Sector	Procures for global U.S. military operations with over 100,000 businesses.
Emergency Services Sector	Supports emergency services, environmental protection, and disaster recovery efforts.
Energy Sector	Safeguards complex network of energy assets for reliable supply and national well-being.
Financial Services Sector	Shields financial assets and access from major outages, disasters, and cyberattacks.
Food and Agriculture Sector	Collaborates to protect food-related businesses, providing resources and guidance.
Government Facilities Sector	Aids government facilities in risk assessment and defense implementation.
Healthcare and Public Health Sector	Prioritizes population health and offers response and recovery measures following incidents like disasters and disease.
Information Technology Sector	Detects and defends against cyber threats due to increasing reliance on technology.
Nuclear Reactors, Materials, and Waste Sector	Manages vast civilian nuclear infrastructure, from power reactors to medicinal isotopes.
Transportation Systems Sector	Ensures safe and efficient transportation amid the daily movement of people and goods.
Water and Wastewater Systems	Safeguarding water supply systems is essential for the stability and health of the country.

ISAO Formation and Standards Development

Information Sharing and Analysis Organizations (ISAOs) collect and disseminate cyber threat intelligence independently from sector-based ISACs. Led by the University of Texas at San Antonio (UTSA), the ISAO Standards Organization, with support from R-CISC and LMI, fosters adaptable information sharing among diverse business sectors. Current efforts aim to establish best practices for effective ISAOs, accommodating both non-sector-based and recently formed sector-based organizations.

Protection Mechanisms Of Critical Infrastructure of Critical Infrastructure in the US in Comparison to Canada

Both the US and Canada recognize critical infrastructure as essential for public well-being and acknowledge the potential impact of threats, including terrorism. They prioritize resilience-building efforts and have developed national strategies, such as the National Infrastructure Protection Plan (NIPP) in the US and the National Strategy and Action Plan for Critical Infrastructure in Canada. Both strategies emphasize collaboration, information exchange, and all-hazards risk management. Collaboration between the two countries under the Canada-U.S. Action Plan aims to address cross-border critical infrastructure challenges effectively.

Aspect	Description
Objective	Canada-US Action Plan enhances cross-border infrastructure resilience.
Interconnected Nature of Critical Infrastructure	A coordinated approach is essential due to the interdependencies of critical infrastructure between the two countries.
Strong Private Sector Collaboration	Collaboration across borders is vital for effective private sector engagement in critical infrastructure resilience efforts.
Avoiding Wasteful Duplication	Coordinated efforts prevent redundant activities and promote efficient use of resources through sharing best practices.

Coordinated Communication	Timely and accurate communication with stakeholders ensures effective responses to critical infrastructure disruptions.
Foundation & Pillars	Partnership, information sharing, and risk management drive infrastructure resilience.
Key Initiatives	EMCG, Sector Networks, Risk Analysis Cell, Information Exchange, Enhanced Security, Analytical Products, Efficient Sharing, Risk Measurement
Joint Efforts for Resilience	Partnership Development, Enhanced Information Sharing, Risk Management, Alliance Establishment and Information Sharing

Comprehensive Approaches for Government to boost the security of Critical Infrastructure

The OECD High-Level Risk Forum (HLRF) developed the OECD Policy Toolkit on Governance of Critical Infrastructure Resilience, fostering collaboration among government officials, specialists, and stakeholders to address emerging risks. The OECD Recommendation emphasizes the need for governments to strengthen resilience in critical infrastructure networks, with challenges identified in dividing responsibilities between companies and governments. Through cross-national studies and workshops, the OECD expands its network to enhance evidence-based policies for critical infrastructure resilience. The Policy Toolkit on Governance of Critical Infrastructure Resilience assists governments in developing resilience policies through effective collaborations with operators, emphasizing the identification of critical infrastructure and systemic approaches to address hazards. It advocates for partnerships, shared responsibilities, and a comprehensive risk management cycle.

Approaches for the Canadian Government to boost the security of critical infrastructure

The OECD Policy Toolkit on Governance of Critical Infrastructure Resilience, developed by the High-Level Risk Forum, aims to assist governments in creating and implementing national policies for resilience. It emphasizes collaborative partnerships, identification of critical infrastructure, and systemic approaches to address risks, promoting multi-sectoral coordination and public-private cooperation. Future collaboration with the OECD will focus on implementing the Toolkit and tracking advancements in infrastructure fortification.

Improving Policies

Critical Infrastructure Resilience Policy Steps	
Multi-Sector Governance	Adopt a whole-of-government approach. Coordinate at the Center of Government
Interdependencies Understanding	Map dependencies and vulnerabilities. Conduct stress tests
Trust and Information-Sharing	Establish secure information-sharing platforms. Ensure trust and confidentiality
Partnerships and Objectives	Partner with public and private sectors. Agree on common objectives
Policy Mix for Resilience	Implement a mix of voluntary and regulatory tools. Conduct cost-benefit analysis
Accountability and Monitoring	Monitor implementation and evaluate progress. Establish accountability frameworks
Transboundary Cooperation	Coordinate with neighboring countries. Set up international information-sharing

Improving Cyber Security

Cybersecurity for cyber-physical systems (CPS) is crucial due to increasing digitalization and potential vulnerabilities. Recent cyberattacks on critical infrastructure highlight the urgent need for robust security measures. Implementing cybersecurity best practices, such as assessing risks, incorporating security from the planning stage, and providing staff training, is essential. Continuous network monitoring helps in early threat detection and prevention. Neglecting CPS security can lead to severe disruptions, financial losses, and even loss of life, emphasizing the importance of maintaining CPS security. Collaboration and frameworks like ISA/IEC 62443 and NIST Cybersecurity Framework aid in managing CPS cybersecurity risks effectively.

Protection of Cyber-Physical Infrastructure

Protecting cyber-physical infrastructure is paramount due to increasing cyber threats, which can cause devastating consequences including service disruptions and loss of life. Addressing these risks requires a multifaceted approach involving technological, organizational, and regulatory measures, along with collaboration between public and private stakeholders. Safeguarding cyber-physical infrastructure is both a technical challenge and a moral imperative, demanding collective efforts to strengthen defenses and promote cybersecurity awareness.

Aspect	**Description**
Protection Challenges	Safeguarding cyber-physical infrastructure amid increasing cyber threats is crucial.
Technological Measures	Utilize firewalls, IDS, encryption, endpoint protection, and regular assessments for defense.
Organizational Measures	Implement training, incident response protocols, risk management, and a culture of awareness.
Regulatory Frameworks	Enact laws, reporting requirements, and mandates for adopting industry standards.
Collaboration Strategies	Foster information sharing, public-private partnerships, and coordination with government.