Canadian Government Intervention in Ensuring Critical Infrastructure Protection

Rahul Ravi Hulli
Information Systems Security
Concordia University
Montreal, Quebec, Canada
rahulravi.hulli@gmail.com

Anita Archibong
Information Systems Security
Concordia University
Montreal, Quebec, Canada
anitaarchibong2@gmail.com

Josephine Famiyeh
Information Systems Security
Concordia University
Montreal, Quebec, Canada
famiyeh21@gmail.com

***Abstract*— The Government of Canada is following a set of preventive measures to keep the country safe, whereby these assets are great institutions both in terms of social cohesion and national security. The model is a two-phase classification approach that is efficient in dealing with core sectors of infrastructure, which include government, transport, energy, utilities, and the finance sector. The risk assessment, which includes all cyber-attacks, theft, terrorism, and natural calamity identification, is of major significance. The government makes use of its instruments, including lawmaking, enacting, and uniting forces through collaboration with stakeholders, to minimize risks and increase resilience. The National Strategy and Action Plan for Critical Infrastructures provides a solution by having a significant effect on security issues like recovery, response, and readiness plans. The problem of public opinion is also to be solved, along with those related to people's readiness for new dangerous situations and the rules, which in some cases may hamper survival. The Canadian government is as alarmed about dismantling the critical pillars of their society as the major players in this game, such as social well-being and national security.**

Keywords— Canadian government, intervention, critical infrastructure, protection, legislation, regulations, risk assessment, threat mitigation, emergency response, National Strategy, Action Plan, Public Safety Canada, resilience strategy, partnerships, information sharing, technology, national security, resilience.

I. INTRODUCTION (*HEADING 1*)

The integrity and resilience of a country's essential infrastructure are crucial to its security and prosperity in an era characterized by technological innovation and interconnection [1]. Critical infrastructure sectors including energy, transportation, telecommunications, and healthcare sustain public services, the economy, and the daily lives of Canadians. They constitute the backbone of society. However, the Canadian government now views protecting these essential assets as a major priority due to the country's growing reliance on digital networks and the growing threats posed by cyberattacks, natural disasters, and geopolitical tensions. This research offers a thorough analysis of the various approaches used by the Canadian government to guarantee the resilience and safety of vital infrastructure. Through an examination of the legislative programs, collaborations, and technological developments led by federal, state, and local government agencies, this study seeks to clarify the complex web of governance that surrounds critical infrastructure security. Canada has faced several difficulties throughout its history, which have highlighted the significance of early action in securing vital infrastructure. From the destructive ice storm of 1998 to the more recent cyberattacks that targeted important industries, these events have acted as wake-up calls, driving politicians to implement measures meant to improve resilience, preparedness, and response capabilities.

In Understanding the interconnectedness of threats and vulnerabilities, the Canadian government has taken a comprehensive approach to protecting critical infrastructure in recent years [1]. There have been attempts to identify, evaluate, and reduce risks to critical assets through the development of regulatory frameworks like the Critical Infrastructure Protection Program (CIPP) and the application of sector-specific policies [1]. In addition, alliances with academic institutions, global partners, and industry players have been established to improve knowledge exchange, promotion of best practices, and cooperative threat intelligence [1]. Adopting cutting-edge technologies has become a pillar of Canada's critical infrastructure protection plan in the face of changing threats [2]. To strengthen defenses and lessen possible interruptions, investments in cutting-edge technology have been given top priority, ranging from sophisticated cybersecurity solutions to resilient infrastructure design. The environment around the protection of critical infrastructure is nonetheless dynamic and complicated despite these preventative actions. Emerging risks, fiscal limits, and rapid technical improvements provide constant problems that require constant strategy adaptation and improvement.

In navigating the complex landscape of critical infrastructure security, this research aims to shed light on how the Canadian government is changing its role in protecting the country's most important resources. It attempts to contribute to a fuller understanding of the efforts being made to ensure the resilience and integrity of Canada's vital infrastructure in an increasingly unpredictable environment by studying important policies, projects, and trends.

II. BACKGROUND AND MOTIVATION

The trigger of extensive infrastructure protection in Canada is attributed to the massive size of the country, the interconnectedness of its wide infrastructure, as well as the growth of the economy and health of its people as a result of their sustained use of critical systems. Because Canada is a developed country with well-developed cities and important industries on its soil, it faces various types of threats, for example, terrorism, natural disasters, cyberattacks, and infrastructure failures. These disasters could lead to a very noticeable disruption in operations and even endanger citizens' safety. The networking of critical infrastructure sectors stresses the need for preventive measures to address hazards and strengthen resilience, which helps keep key services running for national security and economic growth. At the center of the Government of Canada, policies are measures aimed at safeguarding the operational integrity of the critical infrastructure pieces that are important to maintain public steadiness, security, and economic growth. The government, through comprehensive strategies aimed at mitigating risks, enhancing resilience, and protecting the nation's critical infrastructure lifelines, will be obliged to continuously do so in line with the continuous evolution of threats tending to be more complex, like high terrorist activities, natural disasters, cyber-attacks, and infrastructure degradation. This introductory portion of the work is meant to give an overview of the approaches used by the government of Canada to ensure its critical infrastructure, which consists of the vital sectors of the economy, is secure.

III. Literature Review

Governments throughout the globe are now primarily concerned with cybersecurity and the preservation of vital infrastructure in an increasingly linked world. The objective of this literature analysis is to examine official government papers and publications from pertinent Canadian agencies to comprehend the methods and policies put in place to deal with these issues.

A. Government Policies and Strategies for Cybersecurity and Infrastructure Protection

Comprehensive national cybersecurity policies are frequently the first step in government initiatives. The aforementioned strategies delineate the essential vision, goals, and activities required to augment cybersecurity posture in diverse sectors [3]. In Canada, organizations like the Canadian Centre for Cyber Security and Public Safety Canada are essential to the creation and use of these tactics. To successfully minimize cyber risks, for example, the Canadian government's National Cyber Security Strategy (NCSS) offers a framework for cooperation with the corporate sector and other stakeholders [4].

Robust legislative frameworks that offer legal power and a mandate for action frequently promote effective cybersecurity strategies. The enactment of legislation like the Digital Privacy Act and the Security of Canada Information Sharing Act (SCISA), which enable government agencies to exchange threat intelligence and strengthen privacy safeguards, are examples of legislative initiatives in Canada [5]. Law enforcement and intelligence organizations may work together more successfully to counter cyber threats while protecting individual rights and privacy thanks to these legal tools.

One of the main elements of government plans is making sure that vital infrastructure is resilient to cyberattacks [6]. The Critical Infrastructure Protection (CIP) Program of Public Safety Canada collaborates with several sectors to recognize, evaluate, and reduce threats to critical infrastructure assets. The government wants to improve the security and resilience of vital infrastructure, which includes industries like electricity, telecommunications, and transportation, through risk assessments, sector-specific rules, and information-sharing channels.

Effective cybersecurity governance requires international cooperation due to the global character of cyber threats. Canada actively supports cybersecurity standards, information sharing, and capacity building in international fora like the UN, NATO, and the G7/G20. Canada's capacity to counter cyber-attacks as a group is further reinforced by alliances and bilateral agreements with important allies.

There are still several obstacles in the way of infrastructure protection and cybersecurity, despite tremendous advancements. These include the dynamic nature of cyber threats, the limitations of resources, and the requirement for constant technological advancement adaption [7]. To detect and respond to threats proactively, there will be an increasing focus on developing a cybersecurity culture, investing in workforce development, and utilizing cutting-edge technologies like artificial intelligence and machine learning.

B. Research Studies and Reports

In Canada, critical infrastructure protection (CIP) is a fundamental component of national security, especially in light of the constantly changing physical and cyber threats. This study examines scholarly research articles, reports, and studies that examine the CIP interventions and methods used by the Canadian government [8]. The need to assess the performance of laws, rules, and programs meant to protect vital infrastructure from different dangers is emphasized.

A large body of research examines government-led CIP initiatives. University, think tank, and research organization research emphasizes the creation and application of national policies, legal frameworks, and industry-specific regulations. Research, for example, examines how the National Strategy for Critical Infrastructure has improved risk management and resilience in important industries including electricity, telecommunications, and transportation [9].

Critical information on how well laws and regulations protect vital infrastructure from physical and cyber-attacks is provided by academic studies [10]. Research utilizes several approaches, such as qualitative evaluations, case studies, and quantitative analyses, to examine the advantages and disadvantages of intervention strategies. Results frequently point up opportunities for development, implementation gaps, and new difficulties like integrating new technology and dealing with the weight of regulatory compliance [11].

Determining the effectiveness of government actions in CIP requires an understanding of the dynamic cyber threat scenario. Studies look at the attack paths, threat actors, and weaknesses in critical infrastructure systems. Additionally, evaluations explore how to improve cyber resilience and lessen the impact of cyber events on critical services by utilizing threat intelligence sharing, public-private partnerships, and incident response capabilities.

Adaptive tactics and resilience-building techniques are common topics in studies on CIP in Canada [12]. Research highlights the significance of adaptability, redundancy, and continuity management in reducing the cumulative impact of interruptions to vital infrastructure. In addition, evaluations of organizational resilience capabilities highlight areas that need more funding to strengthen infrastructure resilience against a variety of threats, as well as best practices and lessons learned.

The results of research frequently lead to suggestions for improving CIP-related government initiatives and policy frameworks. Legislative changes, efforts to increase capacity, methods for collaborating across sectors, and expenditures on workforce development and cybersecurity technology are a few examples of recommendations. Furthermore, studies support a comprehensive strategy for CIP that successfully addresses complex threats by combining physical security, cybersecurity, and resilience-building techniques.

C. Industry Publications and White Papers

Critical infrastructure protection (CIP) government interventions are shaped in large part by industry groups, cybersecurity businesses, and consulting organizations [13]. These entities also provide important insights into cybersecurity practices. The purpose of this assessment is to gather opinions on government activities and suggestions for improving CIP in Canada by analyzing white papers and industry publications. It also looks at case studies, best

practices, and takeaways from actual events or cybersecurity drills concerning vital infrastructure in Canada.

A variety of viewpoints about the efficacy of governmental initiatives in CIP are provided by industry publications. White papers from consulting firms and cybersecurity companies frequently evaluate public-private partnerships, the regulatory environment, and how government policies affect industry stakeholders [14]. These sources could draw attention to issues including the difficulties in complying with regulations, the gaps in information exchange, and the necessity of more industry-government cooperation to counter growing threats.

Industry participants routinely offer suggestions, based on their knowledge and experiences, for improving government involvement in CIP. Legislative changes, financial incentives for cybersecurity investments from the corporate sector, and the creation of sector-specific resilience standards are a few examples of these suggestions [15]. Industry publications also stress the significance of threat intelligence sharing, incident response planning, and proactive risk management in protecting vital infrastructure assets.

Policymakers and industry stakeholders may both learn a great deal from real-world catastrophes and cybersecurity drills. Case studies documenting cybersecurity events or simulated exercises impacting vital infrastructure in Canada are frequently published in industry magazines [16]. These case studies shed light on the tactics used by government agencies and organizations to mitigate risks and address response difficulties. Stakeholders may prioritize areas for improvement in CIP plans and identify gaps in readiness by looking at the lessons learned from these disasters.

Industry journals often feature creative ideas and best practices for strengthening critical infrastructure's resistance to cyberattacks [17]. Case studies may demonstrate how technologies like secure communication protocols, security analytics platforms, and intrusion detection systems have been implemented successfully. Furthermore, industry viewpoints on cutting-edge topics like supply chain risk management, cloud security, and industrial control system (ICS) protection provide insightful information that may be used to shape government policies and plans.

D. International Comparisons and Benchmarks

Studies that compare Canada's approach to critical infrastructure protection (CIP) with those of other nations provide insightful information on best practices, legal frameworks, and policy frameworks for building infrastructure resilience [18]. The purpose of this research is to evaluate nations' cybersecurity capabilities and infrastructure resilience by examining literature from international organizations including the United Nations (UN), the World Bank, and the International Monetary Fund (IMF). This will serve as a foundation for cross-country comparisons [19].

International research and papers evaluate the legislative and regulatory frameworks that various nations have implemented to safeguard vital infrastructure from both physical and cyberattacks. Differences in public-private partnerships, legislative frameworks, and governance structures are brought to light through comparative analysis. Reports from the World Economic Forum (WEF), for example, contrast Canada's cybersecurity strategy with those of other developed economies, pointing out areas where policy goals and execution strategies are similar and different [20].

International organizations evaluate a nation's infrastructure resilience, particularly its capacity to resist and bounce back from disruptive events like natural disasters and cyberattacks [21]. Benchmarks for assessing the efficacy of CIP measures across various countries may be found in reports from the United Nations Office for Disaster Risk Reduction (UNDRR) and the Infrastructure Resilience Trust Fund of the World Bank. These evaluations aid in identifying deficiencies in investment priorities, capacity-building requirements, and resilience planning [22].

Comparative analyses shed light on best practices and lessons discovered in nations with strong CIP frameworks. Innovative methods of risk management, information exchange, and public-private partnership are highlighted through case studies and comparative analysis. The Organization for Economic Cooperation and Development (OECD), for instance, has published papers that highlight effective examples of cross-border collaboration and sector-specific coordination for boosting infrastructure resilience [23]. Canada and other nations can find areas for innovation and improvement in their CIP strategies by comparing their methods to global best practices.

Evaluations of nations' cybersecurity capacities offer a more comprehensive framework for comprehending their CIP strategies. Reports from global institutions including the International Monetary Fund (IMF) and the International Telecommunication Union (ITU) assess how prepared nations are to stop, identify, and address cyber threats [24]. Policymakers can identify areas of strength and areas in need of more investment, such as workforce development, research and development, and public awareness campaigns, by comparing Canada's cybersecurity posture with that of its counterparts.

E. Government Speeches and Testimonies

Speeches, testimony, and declarations from the government provide important insights into the goals, concerns, and viewpoints of Canadian officials about critical infrastructure protection (CIP) [25]. To comprehend government goals, budget allocations, legislative actions, and future directions in increasing infrastructure resilience against cyber and physical attacks, this analysis looks at speeches and testimony by government officials, politicians, and cybersecurity experts.

Government representatives' speeches and testimony provide light on the objectives and difficulties of Canada's CIP initiatives. The necessity of improved public-private cooperation, workforce development investments in cybersecurity, and the deployment of cutting-edge technology to counteract changing threats are frequently identified as key issues [26]. Government representatives may also discuss issues including resource limitations, information-sharing obstacles, and complicated regulations when it comes to protecting vital infrastructure assets.

Committee hearings and parliamentary discussions provide forums for talking about CIP-related government activities, money distributions, and cybersecurity laws [27]. These sessions' transcripts and recordings provide insights into the viewpoints of legislators, policy discussions, and

stakeholder interactions. Proposed changes to current cybersecurity legislation, funding for infrastructure resilience initiatives, and supervision of government organizations in charge of CIP are a few possible debate points.

Speeches and testimony from government representatives frequently emphasize budget allocations and legislative actions targeted at bolstering CIP in Canada [28]. New cybersecurity laws, rules, or financing initiatives to assist vital infrastructure sectors could be announced by officials. Additionally, they might give updates on how current projects—like the National Cyber Security Strategy or industry-specific CIP programs—are being implemented as well as list future funding priorities for infrastructure resilience projects.

Testimonies from industry participants and cybersecurity specialists provide insightful analysis and suggestions for improving CIP in Canada. Experts could draw attention to new risks, developments in technology, and recommended procedures for safeguarding infrastructure. Government regulations, investment choices, and policies can be influenced by their testimonies to increase the resilience of vital infrastructure assets against both physical and cyber threats.

Future goals and methods for improving CIP initiatives in Canada are frequently outlined in government speeches and testimony [29]. To address changing risks and improve infrastructure resilience, officials may lay forth strategic goals, initiatives, and collaborations. Additionally, they could stress how crucial it is for global collaboration, R&D, and capacity-building initiatives to influence CIP governance and practice in the future.

F. News Articles and Media Coverage

Real-time information and insights on cyber events, infrastructure vulnerabilities, and government actions about critical infrastructure protection (CIP) in Canada may be found in news stories, press releases, and media coverage [30]. To offer insights into the current developments, discussions, and difficulties concerning CIP in the nation, this research looks at recent media coverage.

Cyber-attacks that target important infrastructure sectors including energy, transportation, and banking are frequently included in media coverage [31]. Articles on ransomware attacks, data breaches, or interruptions of vital services can give insight into the strategies, means, and consequences of cyber threats. Furthermore, policymakers, business stakeholders, and the general public become more aware of the changing dangers to infrastructure resilience as a result of media coverage of emerging cyber threats such as supply chain assaults and zero-day vulnerabilities [32].

Articles in the news usually talk about systemic risks and weaknesses in Canada's infrastructure that affect important industries [33]. Older infrastructure, insufficient cybersecurity safeguards, or reliance on digital technology that raises the risk of cyberattacks might be the main topics of coverage. Furthermore, media disclosures may draw attention to vulnerabilities resulting from insider threats, geopolitical conflicts, or regulatory loopholes, which might lead to requests for more robust risk management and resilience measures [34].

The Canadian government's reaction and the policy discussions regarding CIP are elucidated by media coverage. Articles may discuss legislative discussions, official declarations, or legislative actions intended to increase the resilience of infrastructure [35]. Additionally, information on information-sharing agreements, sector-specific rules, and public-private collaborations provides insights into government policies for tackling physical and cyber risks to critical infrastructure.

To increase public knowledge of CIP and include stakeholders in talks, media coverage is essential. Public awareness of the value of resilient infrastructure, cybersecurity best practices, and the possible effects of cyberattacks on critical services is raised by news stories, interviews, and opinion pieces. Additionally, communication and cooperation between government, business, and civil society partners are encouraged by media coverage of cybersecurity drills, awareness campaigns, and industry efforts.

Media coverage elucidates obstacles and prospects for augmenting Canada's CIP endeavors [36]. Articles may address issues with collaboration between government agencies and stakeholders in the private sector, regulatory complexity, or resource limitations. Furthermore, sharing information on technology advancements, cooperative partnerships, or successful CIP projects highlights chances to enhance infrastructure resilience and successfully reduce cyber threats.

IV. CLASSIFICATION OF CANADA'S CRITICAL INFRASTRUCTURE

In Canada, core infrastructure components represent a group of industries that stand out in their significance, and because they are the backbone of the economy, they also assume the role of ensuring public functions in society. Every field has its importance, and the whole country's stability can be measured by the ability of the security system to appreciably respond to threats and disruptions. Among the important industries deemed essential infrastructure are the following: Utilities and Energy: Oil and gas piping is a crucial element of this portion of the system, as are utilities and energy delivery to household, industrial, or commercial clients in the whole country [37]. As such, the building block of the infrastructure of Canada is none other than the transmission of power and fuel through the wires or pipes, which are a manifestation of the ingenuity in this country. Apart from its roots, energy today is a generator, creating limitations for productivity and being vital for Canadian industries. It is one important gear that makes the wheel of the state nation roll and gives life not only to economic activity but also to numerous jobs, sometimes of a strategic nature, for the whole country. The Canadian financial sector is exemplary in this range of possibilities, from its function as a transaction to its meaning of boosting investor confidence, enhancing economic growth, and the two institutions being stable.

The food industry consists of three sectors, which include the production of foodstuffs, processing, and distribution, and finally the retailing of food products. Implementing food security is a major issue for the health of people and the prevention of any kind of social disorder. The Canadian food industry includes a set of different activities, such as agricultural production, food processing, transportation, and retail, that altogether ensure country food safety, assist national outlook uplifting and improve people's well-being, [38] This set of sectors consists of air, land, and maritime

transportation systems, which include airports, railways, highways, ports, and transit systems, which cannot be disregarded as they are the only means of goods and people's movement.

The transportation sector in Canada acts as the backbone both for domestic and international trade, allowing for the relaying of goods and the performance of economic transactions alongside support for tourism, and should therefore be seen as a fundamental element of the nation's economy and national unity. Governments' institutions and structures, including the national courts, parliament, civil service offices, and emergency response centers, are critical for the rule of law and the delivery of public goods and services [39]. Governmental infrastructure in Canada forms the basis of the democratic framework, of governance as a whole, and of emergency management, thus ensuring that the government functions properly and that these services are there whenever the citizens need them in everyday administration and case of an emergency.

Modern information and communication technology (ICT), which is not limited to telephone networks but includes internet services and data centers, is critically important for the entire country's communications, business, and access. ICT infrastructure explains the ways or channels of communication and commerce and is hence taken to be a fundamental gear of innovation, education, and social progress, hence being highly considered the main factor in the development of Canada's digital economy and the intervention in the country's global competitiveness [40]. The health sector involves various avenues where emergency care, public health, hospitals, clinics, diagnostic laboratories, and pharmaceutical supply chains offer services. The medical system of the health sector, in which the activities of ill prevention, scientific studies, health facilitation, and public health backing may affect the safety and well-being of all Canadians, also makes effective health services available in time and of high quality.

The main function of the community safety infrastructure is that it is the base that creates the system of a fast emergency response, allowing to delivery of help to disasters and other unexpected events to the places possible with a minimum delay via fast and coordinated assistance. The whole water cycle, from public wastewater treatment plants to the water distribution and sanitation network, is a critical part of hygiene, public health, and environmental safeguards [41]. The manufacturing industry is considered an essential part of the economic system that makes everything turn. These include the production of massive vehicles, aircraft, and defense industry products, among other products that account for as much as 80 percent of the gross domestic product for the country and also fulfill the needs of the nation for security.

V. Threat Sources to Critical Infrastructure

Critical infrastructure is exposed to a multitude of dangers that can seriously affect their operations, wreck economic indicators, and pose a huge risk to public safety. Ranging from the calculated strategies of terrorists, such as bombing, whose main objective is to create fear and cause chaos, to the devastating forces of nature like floods and wildfires, these destroy the basic infrastructure [42]. There are criminal activities and thefts, for instance, leading to a worsening of risk, and vulnerability decay, lack of investment, and neglect throughout time are among the issues that cause a gradual degradation of the resilience of infrastructure. The act of being imperfect and unkempt can also reveal the respective vulnerabilities, which may have left the infrastructure prone to exposure to numerous external stressors. The bleak overhang of cyber threats, whether hacking or coordinated cyberattacks, that can seriously impact the integrity and properness of information and communication technology systems used in critical infrastructure is a dangerous threat. While maintaining national security and order is the core mission of public authorities, impacting the lifelines of modern society, ascertaining the multi-dimensional security risks is the paramount responsibility. There are many intangible risks of terrorism, natural disasters, theft, and degradation that critical infrastructure has, and emerging challenges emanating from climate change, geopolitical tensions, and technological advancements [43]. Spatial conflicts and cyber spying are added to the complexity dimension that can disrupt certain supply chains and leakage of critical data for infrastructure maintenance.

Critical infrastructure faces dangers in various forms that can affect its functions, economic stability, and the safety of the public. These threats may include intentional terrorism, which can include cyberattacks, and floods and wildfires that result from nature. They aim at creating fear and uncertainty that break the peace of the public. Nature disasters happen because of the sheer destruction they can lead to, and they can even take out critical infrastructure and hinder the efforts leading to recovery. Online threats such as cyber-attacks and cyber-warfare, encompassing systems that are integrated with critical infrastructure components, are the main hazardous components in the information and communication technology sub-fields. In line with the ongoing evolution of technology, cyber threats get more complicated and striking every day, which makes cybersecurity defense against sophisticated information resources and related facilities a priority. The Canadian government can enhance the resilience of the country's critical infrastructure by dealing with multifaceted threats using legislation and regulation and working together with all the major stakeholders. The funding for infrastructure protection and cybersecurity measures comes down to safeguarding national assets and maintaining a strong position in the country as a land that is necessarily resilient and secure in the face of changing threats. As vital infrastructure systems face both intentional and natural hazards, their operability is undermined, and public safety is threatened. These dangers, which are spelled out as terrorism, cyberattacks, and natural disasters like floods and wildfires, pose great risks to critical infrastructure systems. The crimes of theft and vandalism have a cumulative effect on vulnerability and infrastructure, posing a greater threat to resilience. The very changing scenario of cyber threats poses a particularly difficult problem because adversaries aim at information and communication technology systems that are part of the critical infrastructure. Understanding that the interconnectivity of those threats and their outcomes are integral, the Canadian government will need to place more focus on comprehensive strategies that combine regulatory, legislative, and collaborative efforts to increase the resilience of vital infrastructure and ensure security, economic growth, and stability will continue.

VI. The Role of Government in Ensuring the Protection of Critical Infrastructure

For optimal outcomes, the government must assume national leadership in reducing vulnerabilities, enhancing threat and risk detection, and refining response and recovery efforts and timelines. The Government of Canada primarily assumes a management and leadership role in safeguarding and overseeing critical infrastructure during emergencies. This role is carried out with due respect to provincial jurisdictions and legislation, and the federal government provides direct assistance if requested by a province during an emergency. The Government of Canada's primary focus is refining protective measures to ensure the uninterrupted delivery of essential services and amenities to the Canadian population. To offer the necessary protection and assurance, the Government of Canada aims to enhance "information collection, assessment, and sharing, as well as risk management" [45]. The Canadian government has proposed two strategies for safeguarding its critical national infrastructures.

A. National Strategy for Critical Infrastructure

The primary objective of the National Strategy for Critical Infrastructure (CI) is to enhance the resilience of Canada's critical infrastructure. This is achieved by delineating a course of action to enhance the resilience of critical infrastructure against existing and emerging threats. The National Strategy encourages more coherent and collaborative efforts among federal, provincial, and territorial initiatives and the ten critical infrastructure sectors [46]. The foundational concepts and principles outlined in this National Strategy are derived from the Emergency Management Framework for Canada, which establishes a streamlined approach for territorial, provincial, and federal emergency management initiatives [46]. The Framework articulates cooperation principles (such as responsibility, comprehensiveness, partnerships, coherence of action, risk-based, all-hazards, resilience, continuous improvement, and clear communication) [46]. It recognizes that emergency management comprises interdependent, risk-based functions, including prevention, mitigation, preparedness, response, and recovery [46]. Drawing inspiration from this Framework and acknowledging the interconnected nature of critical infrastructure, the National Strategy advocates for forming partnerships among territorial, provincial, and federal governments, and CI sectors. It advances an all-hazards risk management approach and outlines measures to enhance information sharing and protection. Critical infrastructure may function independently or be interconnected and interdependent across territories, provinces, and national borders. The National Strategy supports the notion that roles and activities related to Canada's Critical Infrastructure (CI) should be undertaken responsibly at all levels of society. In Canada, federal, provincial, and territorial governments, local governments, and critical infrastructure owners and operators—bearing primary responsibility for safeguarding their assets and services—jointly share the responsibility for critical infrastructure. Individual Canadians are also urged to be prepared for disruptions and ensure they and their families are equipped to handle emergencies for at least the initial 72 hours [46].

The practical implementation of the National Strategy necessitates collaborative partnerships with all levels of government and critical infrastructure sectors. Owners and operators of critical infrastructure possess the expertise and information essential for governments to formulate comprehensive emergency management plans. Governments, in reciprocation, will share pertinent information promptly while adhering to prevailing federal, provincial, and territorial legislation and policies, aiding owners and operators in risk assessment and identifying best practices. This collaborative approach acknowledges that resilient critical infrastructure fosters economic growth and attracts and retains businesses, generating job opportunities. Governments enhance this partnership by furnishing owners and operators with timely, accurate, and valuable information on risks and threats, ensuring industry involvement in the early stages of creating risk management activities and emergency management plans, and collaborating with the industry to formulate and prioritize critical activities for each sector. The National Strategy establishes a collaborative framework where governments, owners, and operators can work together to impede, mitigate, prepare for, respond to, and recover from disruptions to critical infrastructure [46].

In 2011, the Canada-United States Action Plan on Critical Infrastructure was established, signifying the interconnectedness of critical infrastructure (CI) between Canada and the United States. This acknowledgment stemmed from recognizing that numerous threats on Canadian territory are directed toward the United States, establishing mutual dependencies. The action plan emphasized enhanced cooperation and communication [47]. Canada commits to collaborating with the United States and other global governments and organizations to foster a collective approach to fortifying the resilience of critical infrastructure. The strategy also considers the existing cooperative emergency management arrangements at the regional level among provinces, territories, and neighboring American states. Federal, provincial, and territorial governments and critical infrastructure sectors will collaborate to identify and address international dependencies and risks [46].

B. The Strategy

Build partnerships: Strengthening the resilience of critical infrastructure, in line with the Emergency Management Framework for Canada, demands coordinated and complementary actions from all stakeholders to optimize resource utilization and activity implementation. The adoption of complementary approaches across all levels to enhance critical infrastructure resilience facilitates coordinated endeavors for the effective execution of preventive, mitigative, preparative, responsive, and corrective measures to address disruptions promptly and efficiently. In the event of a critical infrastructure disruption, the government of the respective jurisdiction serves as the primary point of contact. The federal government stands ready to provide swift assistance if a provincial or territorial government requires additional resources during an emergency or disruption. The plan acknowledges that each responsible jurisdiction, department, agency, and critical infrastructure owner and operator will fulfil their duties to fortify Canada's critical infrastructure resilience as they deem appropriate. However, successful implementation of this strategy necessitates collaborative efforts from territorial, provincial, federal, and critical infrastructure sector partners and the establishment of mechanisms to enhance this collaborative framework [46].

The sector networks present a collaborative model enabling governments and critical infrastructure sectors to engage in sector-specific activities (e.g., risk assessments, risk mitigation plans, and exercises). Each federal department and agency dedicated to a specific sector will work with critical infrastructure partners to enhance sector networks tailored to meet stakeholders' unique needs. The Strategy outlines the functions of sector networks, emphasizing timely information sharing, addressing national, regional, or sectoral concerns, leveraging sector-specific expertise to tackle current and future challenges, and developing tools and best practices for fortifying critical infrastructure resilience across prevention, mitigation, preparedness, response, and recovery efforts. Sector networks will include relevant federal departments and agencies, provinces and territories, national associations, and key representatives from critical infrastructure sectors. Participation in these networks is voluntary, and partners will collaborate on establishing a protocol to safeguard shared information. Creating a National Cross-Sector Forum will facilitate information exchange across sector networks, addressing cross-jurisdictional and cross-sectoral interdependencies to uphold a comprehensive Canadian approach to enhancing critical infrastructure resilience. The National Cross-Sector Forum will consist of members from the ten sector networks, representing various sponsors, operators, associations, and federal, provincial, and territorial governments, serving as the cornerstone for implementing the national Strategy on critical infrastructure resilience [46].

Figure 1 National Cross-Sector Forum [44]

1. Implementation of an All-Hazard Risk Management Approach

Risk management is the continuous, proactive, and systematic process that involves comprehending, overseeing, and communicating vulnerabilities, risks, threats, and interdependencies within the critical infrastructure environment. The initial step in establishing a robust risk management process is to develop a thorough situational awareness of the risks and interdependencies faced by critical infrastructure in Canada. Sector-specific federal departments and agencies are tasked with collaborating with provinces, territories, and critical infrastructure sectors to better understand these risks and interdependencies, forming the basis for emergency management plans and programs. In advancing this comprehensive risk management process, federal, provincial, and territorial governments will engage with their critical infrastructure partners to create all-hazard risk analyses encompassing accidental, intentional, and natural hazards. While governments work towards a unified approach to enhance critical infrastructure resilience and share tools, lessons learned, and best practices, stakeholders are ultimately responsible for implementing a risk management approach suitable for their specific circumstances [46].

Share and protect information**:** Improved information sharing, per existing provincial, federal, and territorial laws, and policies, will facilitate the

Enhanced information sharing by existing provincial, federal, and territorial laws and policies will streamline the prompt exchange of actionable risk information and data concerning the overall status of critical assets. This will empower owners, operators, governments, and other stakeholders to assess risks and implement appropriate measures. Facilitating the swift sharing of information across governments and critical infrastructure sectors is crucial for effective risk management and addressing critical infrastructure interdependencies. The information-sharing improvements encompass a broader array of information products, including risk assessments, incident reports, standard practices, lessons learned, and assessment tools. The mechanisms for delivering this information will be enhanced, and measures will be implemented to protect shared information from unauthorized disclosure.

Additionally, the production of all-hazards risk information products will be tailored to the requests of critical

infrastructure stakeholders. Throughout all stages of an emergency or disruption—before, during, and after—the continuous exchange of information plays a pivotal role in fostering a unified operating picture across all levels of government and critical infrastructure sectors. This coherence of action facilitates a more comprehensive approach to prevention, mitigation, preparedness, response, and recovery [46].

Information Security, given the intricate interdependencies within Canadian critical infrastructure, the inappropriate disclosure of sensitive information that poses a risk to a province or local authority often translates into a risk for Canada as a whole. Exemptions from disclosure are feasible under territorial, provincial, and federal access to and freedom of information legislation, particularly for national security and public safety reasons. At the federal level, the Emergency Management Act of the Government of Canada, enacted in 2007, underscores the necessity of amending the Access to Information Act to provide unequivocal protection for sensitive information furnished by critical infrastructure sectors. A collaborative approach will be employed to formulate a standardized information-sharing protocol that facilitates the exchange of confidential information. Furthermore, the federal, provincial, and territorial governments are urged to collaborate in sharing best practices for information security. These collective endeavors aim to foster a more cohesive approach to information sharing and protection in Canada [46].

C. National Cybersecurity Strategy

Most of Canada's digital systems are owned by individuals and organizations outside the federal government. From individuals with minimal technology use to businesses deeply entrenched in the online world, many are unaware of the potential cyber threats they face. This lack of awareness emphasizes the need for enhanced security measures to safeguard against cyber incidents. Even those who recognize the importance of data security may need help finding affordable and adequate safeguards. To address this, the Government of Canada is taking a leadership role in cybersecurity, aiming to raise awareness and protect organizations and individuals. Additionally, international collaboration is sought to mitigate threats from cybercriminals and state actors operating beyond Canada's borders. These malicious actors exploit security gaps, low awareness, and technological advancements to compromise cyber systems, steal financial and personal information and intellectual property, and disrupt critical infrastructure.

Between 2010 and 2018, the government played a crucial role in establishing a robust cyber defense framework. Two national cybersecurity strategies were implemented, and significant investments were made in cyber defense. Creating the National Cybercrime Coordination Unit (NC3) within the RCMP and the Canadian Centre for Cyber Security marked a substantial change in the government's organizational structure. These agencies are tasked with securing and defending government information systems and responding to cyber incidents that impact critical infrastructure.

D. Canada's First Cyber Security Initiative

The Canadian government unveiled the Cyber Security Strategy for Canada in October 2010 to safeguard Canadians, businesses, and the economy from cyber threats [48]. The foundation of the Strategy rested on three key pillars:

1. *Enhancing the Security of Government Systems*
   Efforts were directed toward improving the government's capacity to detect, respond to, and recover from cyber-attacks. Data breaches have consistently declined despite the increased frequency and sophistication of cyber incidents against government networks since 2010 [49].
2. *Collaborative Protection of Crucial Cyber Systems Beyond Federal Control*
   To ensure the robust security of cyber systems, strategic partnerships were forged with critical infrastructure owners and operators, the private sector, and provincial and territorial governments [49].
3. *Empowering Canadians for Online Security*
   The Government of Canada proactively promoted cyber security awareness through outreach initiatives, including implementing the Get Cyber Safe campaign and developing targeted resources. The 2010 Strategy also saw increased investments to enhance the RCMP's and other law enforcement agencies' capabilities in combating cybercrime, encompassing intelligence, investigations, and training [49].

Over five years, the Strategy received funding exceeding $244 million, with an additional annual allocation of $60 million. Cyber defense's primary focus was securing government systems, yielding significant outcomes such as reinforcing the Communications Security Establishment's cyber defense program, establishing Shared Services Canada, and implementing improved governance and policies [48].

E. The New Cyber Security Strategy

The government unveiled its updated National Cyber Security Strategy in June 2018, a response to a comprehensive evaluation of the 2010 strategy across the entire government [48]. This fresh Cyber Security Strategy reflects insights from the Cyber Review, acknowledging cyber threats' escalating sophistication and prevalence. Simultaneously, it underscores the significant opportunity for Canadian digital innovation and cyber security expertise. Designed to be adaptable in the face of a constantly evolving cyber landscape, the new strategy acknowledges the indispensable role of digital technologies in our daily lives. Embracing this nascent cyber security strategy enables us to navigate the challenges of our digital age confidently. In this context, cyber security emerges as a companion to innovation and a guardian of prosperity. The Cyber Review highlighted three notable trends:

1. Broad support exists for law enforcement endeavours to combat cybercrime while safeguarding online privacy.
2. There is a widespread need for enhanced cybersecurity knowledge and skills.
3. Calls have been made for the Canadian government to take a more active leadership role in cyber security.

In light of evolving threats, emerging opportunities, and the imperative for collaborative initiatives, our National Cyber Security Strategy sets forth three primary objectives, namely:

F. Security and Resilience

The Canadian government is committed to protecting Canadians from cybercrime, addressing emerging threats, and securing critical systems in both the private and government sectors. Through collaborative efforts with partners and enhanced cybersecurity capabilities, the government aims to preserve and enhance cybersecurity across all federal departments and agencies. This commitment extends to safeguarding the privacy of Canadians' information handled by the federal government and ensuring the confidentiality, integrity, and availability of critical services for Canadians. Additionally, the government will bolster law enforcement capacity to combat cybercrime, fostering coordination among law enforcement agencies at various levels and collaborating with federal, provincial, territorial, and international partners. The government will enhance its investigative capabilities in cybercrime and streamline the reporting process for Canadians. Recognizing the challenges faced by small and medium-sized businesses in implementing robust cybersecurity measures, the Canadian government will assist to ensure they gain a competitive edge. Given the critical nature of cyber systems, such as power grids, communications networks, and financial institutions, any disruption could have severe implications for public safety and national security. Therefore, the federal government will work in collaboration with provinces, territories, and the private sector to establish requirements for safeguarding this digital infrastructure and deterring foreign cyber threat actors [46].

G. Cyber Innovation

The federal government is dedicated to positioning Canada as a global leader in cybersecurity by allocating funds for advanced research, fostering digital innovation, and enhancing cyber skills and knowledge. Collaborating with partners, the Government of Canada aims to increase investments in cyber research and development, prioritizing areas where Canada has distinct capabilities, such as quantum computing and blockchain technologies. Noteworthy progress has already been made, with Budget 2017 introducing the Pan-Canadian Artificial Intelligence Strategy for talent and research. The government is exploring innovative approaches to enhance cybersecurity for businesses and all Canadians, irrespective of their background. Previous commitments include investments in digital skills development, such as coding education for children. Recognizing the importance of collaboration between governments, academia, and the private sector, the federal government is addressing the cyber skills gap. Taking proactive measures now will build a future workforce that supports Canadian cybersecurity and contributes to the country's long-term prosperity. The quality of information available plays a crucial role in understanding cyber trends, prompting the federal government to fund Canadian researchers and statisticians to enhance our collective knowledge of cyber threats and opportunities [46].

H. Leadership and Collaboration

The federal government is set to play a leading role in advancing cybersecurity in Canada, closely collaborating with provinces, territories, and the private sector. To enhance operations and collaboration, the Government of Canada will streamline its efforts by establishing a single point of contact for authoritative advice, guidance, and cyber incident response. This streamlined approach aims to improve information sharing and provide necessary assistance to the private sector. Renewed efforts in public awareness and engagement, along with the creation of new collaboration forums, are part of the strategy. Collaboration with a diverse range of Canadian stakeholders will be prioritized to collectively enhance cybersecurity in the country. Furthermore, the federal government will take the lead in developing a national plan for preventing, controlling, and responding to cyber activities, ensuring efficient coordination with provinces, territories, and the private sector. International collaboration will also be emphasized, advocating for a free, open, and secure internet, and strengthening global efforts to combat cybercrime.

The 2018 strategy's core goals and initiatives were reflected in Budget 2018 investments in cybersecurity, amounting to $508 million over five years and $109 million annually thereafter. Notably, the Communications Security Establishment received $155 million over five years and $45 million annually to establish a new cybersecurity center. This led to the establishment of the Canadian Centre for Cyber Security (CCCS) in October 2018, consolidating the roles of various federal cyber organizations and enhancing cybersecurity capabilities in Canada [46].

I. Securing Operational Technology Awareness Series (Itsap.00.051)

The Canadian Centre for Cyber Security (CCCS), established in 2018 as part of the New Cyber Security Strategy, introduced an awareness series in July 2022. This series is designed to educate operators of critical infrastructures, industries, and the public about the risks associated with Operational Technology (OT) and the security measures that can be implemented to mitigate cyber threats. Operational Technology, utilized to manage and automate industrial processes across various critical infrastructure sectors, is increasingly interconnected with IT networks and, potentially, the internet, heightening the vulnerability to cybersecurity attacks [46].

Operational Technology may take the form of a Cyber-physical system (CPS), an advanced system that utilizes computer-based algorithms to control and monitor physical systems, or an Industrial Control System (ICS), a specialized system for monitoring and controlling industrial processes [46].

J. The Risks to Operational Technology (OT)

Compromising operational technology poses a range of risks, including:

Risks	***Descriptions***
Malfunctioning Equipment and Process Disruption	Unauthorized access to operational technology can lead to equipment malfunctions, disrupt industrial processes, and affect the timely delivery of products and services.
Compromise of Intellectual	Breaches in operational technology may compromise valuable

Property and Sensitive Information	intellectual property and sensitive information, such as financial and customer data, exposing organizations to potential economic losses.
Revenue Loss from Disruptions	Disruptions in operational technology can lead to revenue loss due to halted processes, costly repairs, or potentially requiring ransom payments to mitigate the impact.
Damage to Organizational Credibility	Breaches in operational technology can damage an organization's credibility, impacting its reputation and relationships with stakeholders.
Compromised Security Measures, Including Emergency Services	Operational technology breaches may compromise security measures, including those related to emergency services, posing a significant risk to public safety.
Potential for Major Accidents and Disasters	Failure of operational technology can result in major accidents or disasters, potentially causing injury or loss of life.

The impact extends beyond individual components; it encompasses entire industrial processes and poses risks to the safety of employees or operators if operational technology equipment fails. Threat actors actively seek opportunities to exploit vulnerabilities in high-value systems, processes, and infrastructure, aiming for destruction and the loss of critical services [46].

Operational Technology (OT) faces various threats and vulnerabilities that organizations must address for effective protection. Here is a breakdown of these threats, vulnerabilities, and recommended protective measures:

Threats to Operational Technology

- *Remote Access: Unauthorized access to OT systems remotely.*
- *Ransomware: Malicious software that encrypts data, demanding payment for its release.*
- *Malware: Malicious software intended to harm or exploit OT systems.*
- *Insider Threat: Threats originating from individuals within the organization with privileged access.*
- *Denial of Service (DoS) Attacks: Attempts to disrupt or limit access to OT systems.*

Consider the following vulnerabilities that an organization can manage:

Vulnerabilities (Organization-Controlled)

- *End-of-Life and Outdated Systems:* Systems that are no longer supported or updated.
- *Unpatched Software and Firmware:* Failure to apply necessary updates and patches to software and firmware.
- *Peripherals:* Vulnerabilities associated with connected peripheral devices.

Protective Measures for Operational Technology

- *Manually Test Systems:* Ensure OT systems can function adequately without internet connectivity.
- *Monitoring and Logging:* Establish robust monitoring and logging practices to detect unusual activities.
- *Updating and Patching:* Regularly update and patch software and firmware to address vulnerabilities.
- *Isolating System Processes:* Implement network segmentation to isolate critical processes.
- *Implementing the Principle of Least Privilege:* Restrict user privileges to the minimum necessary for job functions.

Remediating Compromised Operational Technology

- *Evaluate Impact and Disconnect:* Assess the impact on equipment and disconnect from the internet if necessary.
- *Use Audit Logs:* Utilize audit logs to identify the attack and compromised systems or accounts.
- *Keep Impacted Entities Isolated:* Keep affected accounts, OT, and systems disconnected or isolated.
- *Repair Damaged Equipment:* Engage IT teams to repair damaged equipment and scan for remaining threats.
- *Update and Patch Impacted OT:* Ensure impacted OT is updated and patched with the latest software version.
- *Report to Authorities:* Report incidents to the Canadian Centre for Cyber Security (CCCS) and the Royal Canadian Mounted Police (RCMP), especially for severe incidents.

Implementing these protective measures can significantly enhance the resilience of operational technology against potential threats and vulnerabilities.

VII. Current Solutions to Canada's Critical Infrastructure

Canada faces various threats to its critical infrastructure, including natural hazards such as floods, storms, earthquakes, fires and human-induced hazards like theft, vandalism, and terrorist attacks. In addressing these challenges, the Ministry of Public Safety has established an emergency management framework in collaboration with the Federal, Provincial, and Territorial governments (FPT). This framework outlines the FPT government's response to threats, employing an all-hazards approach to protect lives, the environment, and property [52]. Canada adopts four main approaches to address threats to its infrastructure. The primary goal of emergency management is to safeguard lives, preserve the environment, and protect property and the economy, with the utmost priority given to protecting life. In its broadest scope, emergency management enhances the comprehension of risks and fosters a safer, prosperous, sustainable, and disaster-resilient society in Canada. Emergency management consists of four interconnected components, outlined as follows:

Figure 2 Emergency Management Framework [59]

A. *Prevention and mitigation*

To ensure the protection of people, property, the environment, and the economy, the primary objective of this phase is to eliminate or significantly minimize the risks associated with hazards [52]. Given the often-localized nature of threats, Federal, Provincial, and Territorial (FPT) governments collaborate with their respective emergency management partners, aligning with their distinct roles and responsibilities. This collaboration aims to tailor efforts and ensure that prevention and mitigation measures are tailored to the community and its specific needs. Interventions may encompass both structural mitigation, such as the creation of floodways and dykes, and non-structural mitigation, including the enforcement of building regulations, land-use management, and the provision of insurance incentives [52].

For instance, a significant storm in August 2005 led to extensive flooding in Markham, Ontario, resulting in millions of dollars in property damage, including flooded basements. In response to residents' concerns about the ongoing construction of reverse slope driveways, the city considered amending the existing by-law in 2011. After extensive discussions and research, it was determined that reverse slope driveways contributed to urban floods by creating additional entry points for water. Consequently, in April 2012, a by-law change prohibiting the construction of reverse slope driveways was adopted [53].

B. *Preparedness*

To enhance the nation's defense against threats, Public Safety Canada collaborates with various federal agencies and provincial and territorial governments. The following measures are implemented to ensure the nation's readiness for potential threats:

- *Planning:* Planning activities aim to establish an effective and well-coordinated strategy for managing an active threat. Government entities are primarily responsible for conducting operational planning based on risk assessments and identified capability shortfalls, resulting in the creation of contingency or response plans.
- *Support for training:* Emergency management training is provided by community colleges, universities, private sector groups, and provincial, territorial, and municipal governments.
- *Management Exercises:* The National Exercise Program, designed by the government Operation Centre (GOC), aims to validate reaction strategies and training, and identify areas for improvement. This program involves government officials from all levels, first responders, non-governmental organizations, and military personnel in designing and conducting drills simulating emergencies.
- *Capability Improvement Process:* This federal strategy provides a standardized approach to gathering, storing, and communicating observations and recommendations, including best practices, among different federal organizations. The Canadian government can track and implement insights from drills and incidents.
- *All-hazard risk assessment:* This assessment identifies, evaluates, and ranks all potential dangers. It considers ways to reduce risks while addressing vulnerabilities associated with specific threats, potential outcomes if a threat materializes, and consequences.
- *National Public Alerting System (NPAS):* A collaborative project of federal, provincial, and territorial governments, NPAS empowers emergency management organizations to alert the public about impending or developing life-threatening situations swiftly. Public notifications are disseminated through radio, cable, satellite television, and compatible wireless devices.
- *Support for public safety employees:* Given the nature of their work, public safety professionals are regularly exposed to stressful situations. Recognizing the potential negative impact of traumatic exposures on the mental health of these personnel, the 2018 budget includes significant investments in post-traumatic stress injury research and treatment.
- *Emergency Management Public Awareness Contribution Program:* Established to enhance disaster preparedness among vulnerable populations [54].

C. *Response*

At the local level in Canada, which encompasses entities such as hospitals, fire departments, police, and municipalities, crises are initially addressed [46]. The responsibility to manage a threat shift to the province or territory if it cannot be controlled locally. In cases where an emergency surpasses the capacity of provincial or territorial authorities, they can seek assistance from the federal government.

- During national crises, the Government Operation Center (GOC) coordinates and aids critical government stakeholders. Its mandate involves overseeing the integrated federal response to all hazard events of national importance on behalf of the Canadian government, including supporting preparedness. As the scope of an event expands, the GOC collaborates with federal ministries, agencies, provinces, and territories. Activation of a formal incident response team by the GOC is guided by specific reporting criteria, including emergencies affecting multiple jurisdictions, federal assets, services, employees, or those requiring a coordinated response beyond routine operations. When a province or territory requests federal support due to an emergency impacting the national interest or when confidence in government is affected, the GOC becomes

involved. When provincial or territorial governments cannot eliminate a threat, they submit a formal Request for Federal Assistance (RFA) detailing the help needed from the federal government. The GOC manages RFAs through an established procedure involving cooperation and consultation among departments. Examples of requests for federal assistance include transport or logistics aid, support for civic law and order, incorporation of a mobile health unit, and using the Canadian Armed Forces as a backup force in extreme cases [55].

- The Search and Rescue Policy and Program, facilitated by the National Search and Rescue Secretariat, provides policy recommendations and assistance to support Canada's search and rescue activities. The Secretariat contributes significantly to prevention through outreach programs promoting cooperation, interoperability, and communication within the search and rescue (SAR) community. Key priorities for the Secretariat include improving Canada's Heavy Urban Search and Rescue Program, enhancing coordination of SAR prevention measures, updating the Canadian national SAR policy framework, improving SAR governance in Canada, and maintaining coordination of the Canadian government's involvement in the worldwide COSPAS-SARSAT program. The Secretariat is an oversight body and promotes treaty discussions [56].

D. Recovery

- Collaborating with their respective emergency management (EM) partners and other societal sectors, federal, provincial, and territorial (FPT) governments work to identify pre- and post-disaster vulnerabilities and highlight opportunities to enhance the accessibility of post-disaster assistance.
- FPT governments actively encourage their respective partners to establish connections between recovery and mitigation efforts, emphasizing the development of procedures prioritizing innovation and establishing more resilient communities.
- Through thorough post-event evaluations, FPT governments analyse best practices and draw insights from previous experiences. They then share these insights with their respective EM partners to integrate the findings into comprehensive EM plans [53].

The Disaster Financial Assistance Arrangements [57] are the primary tools the Canadian government uses to address the financial needs of provinces and territories after significant natural disasters. Additionally, federal, provincial, and territorial governments may offer supplementary aid tailored to specific needs to support social and economic sectors adversely affected by a disaster.

E. Solutions to Cyberattacks on Canada's Critical Infrastructure

To safeguard innovation and prosperity in Canada, which heavily relies on cybersecurity, the Canadian government has instituted the National Cyber Security Action Plan. This plan delineates the coordinated efforts of all stakeholders to ensure the attainment of cybersecurity objectives, contributing to Canada's security and prosperity in the digital age. To bolster the resilience of critical infrastructure (CI) against cyberattacks, the Department of Public Safety and Emergency Preparedness will institute a comprehensive risk management methodology. This approach will empower CI owners and operators to shield their information and systems proficiently [58]. The strategies encompass:

- Conducting cybersecurity audits to pinpoint and address vulnerabilities in cyber systems.
- Providing sector partners with information on the latest threats and trends compromising the security of industrial control systems (ICS) and training to mitigate risks and enhance ICS robustness.
- Organizing and executing cyber-based training exercises for the CI community to evaluate and enhance collective capabilities to respond to and recover from cyberattacks.

F. Additional strategies outlined in the National Cyber Security Action Plan include:

1. *Canadian Centre for Cybersecurity:* Established by the Canadian government, the Canadian Centre for Cybersecurity alleviates confusion regarding the roles and responsibilities of managing cybersecurity. It serves as a centralized resource for assistance on operational cybersecurity issues for the federal government, CI owners, operators, the private industry, and the public. Key duties include:
   - Enhanced integrated threat assessment: The Centre for Cybersecurity will contextualize attacks and generate comprehensive analyses to enhance the understanding of complex and evolving cybersecurity threats.
   - Strengthening relationships with vital infrastructure owners in the banking and energy sectors, facilitating the exchange of proprietary cybersecurity information to combat sophisticated threats.
2. *National Cybercrime Coordination Unit (NC3 Unit):* Created by the Royal Canadian Mounted Police (RCMP), the NC3 Unit coordinates efforts to combat cybercrime. Responsibilities include:
   - Managing Canadian cybercrime activities and engaging with international partners.
   - Guiding and assisting Canadian law enforcement in digital investigations.
   - Establishing a national public reporting platform for reporting cybercrime and fraud.
   - Enhancing the detection of cybercrime-related activity.
   - Strengthening the capacity of federal investigative teams for combined investigations with key international law enforcement partners.
   - Identifying and addressing threats to the safety and security of Canadians and Canadian interests.
3. *Student Work Placement Program (SWP) related to cybersecurity:* This initiative, part of the SWP, aims to fund partnerships between employers and educational institutions. The goal is to align educational skills development with the skills requirements of employers in key sectors of the Canadian economy.

4. *Providing Cyber Security Assessments and Certifications for Small and Medium-sized Businesses:* This initiative seeks to enhance cybersecurity awareness among Canadian Small and Medium-sized Enterprises, boost consumer confidence in the digital economy, and promote international standardization for better global competitiveness.
5. *Capacity for Strategic Policy in Cybersecurity and Cybercrime:* This project ensures proper coordination of strategic cybersecurity and cybercrime policy concerns among internal and external stakeholders. It supports the expanded Cyber Security Cooperation Program and initiates preliminary work on addressing cybersecurity and cybercrime data gaps.
6. *Cyber Security Cooperation Program:* As the only Government of Canada program supporting projects to enhance the security of Canada's cyber systems through grants and contributions, this program benefits various stakeholders, including academic institutions and small and medium businesses, focusing on innovation and research.
7. *Enhanced cooperation between Canada and the U.S.:* Facilitated by Global Affairs Canada's International Strategic Framework for Cyberspace, this initiative involves deploying personnel in Washington to foster closer collaborations, further implementing the cyber security strategy.
8. *Enhanced collaboration with energy sector stakeholders:* Natural Resources Canada's bilateral cybersecurity and energy collaboration will focus on strengthening collaboration with the U.S. This aims to enhance the security and resilience of the integrated North American electricity grid and cross-border pipelines, contributing to the preventive, preparedness, response, and recovery pillars, fortifying, and stabilizing the energy sector [58].

VIII. Evaluating protection mechanisms of critical infrastructure in the US in comparison with that of Canada.

Critical Infrastructure Protection (CIP) refers to a concept and set of practices aimed at safeguarding essential systems and assets that are vital for the functioning of a society, economy, or nation-state [60]. These infrastructures include physical and cyber systems and assets necessary for the operation of governments, businesses, and other organizations.

CIP efforts typically focus on identifying, prioritizing, and protecting critical infrastructure from various threats, such as natural disasters, cyberattacks, terrorism, and other hazards. This protection is essential because the disruption or destruction of critical infrastructure could have severe consequences, including economic disruption, loss of life, and national security risks.

Key components of CIP may include risk assessment, threat analysis, vulnerability management, resilience planning, incident response, and coordination among government agencies, private sector organizations, and international partners [61]. Governments often play a central role in CIP through the enactment of laws, regulations, and policies to promote the security and resilience of critical infrastructure.

CIP efforts are continually evolving to address emerging threats, technological advancements, and changes in the global landscape, such as the increasing interconnectedness of critical infrastructure systems and the growing sophistication of cyber threats.

A. US Initiatives: Protection Mechanisms of Critical Infrastructure in the US

The concept of Public-Private Partnerships (PPPs) [62] gained popularity during a period of de-bureaucratization in the late 1970s. As neoliberal critics addressed a crisis in the state and administration amidst a global economic downturn, they advocated for public bureaucracies to delegate tasks to private entities. This often-involved privatization or collaboration with private businesses, seen as a means to enhance the efficiency of public administration. Initially applied to urban construction, PPPs later extended to various domains, including technology, ecology, education, health services, and the prison industry. Over time, PPP has evolved into a broad and heterogeneous concept, criticized for becoming a catch-all label for various forms of collaboration between the public sector and private businesses [63].

The fundamental nature of PPP involves exploiting synergies through joint innovative resource use and management knowledge application. The goal is to achieve optimal outcomes for all parties involved by leveraging complementary goals and pre-existing interdependence. Collaboration is typically formalized through contracts, and success is contingent on conditions such as mutual trust, clear and documented goals and strategies, risk distribution, separation of responsibility and authority, and market-oriented thinking. Considering these conditions, the applicability of PPP to Critical Infrastructure Protection (CIP) is examined, exploring how information-sharing arrangements have become a preferred solution in the CIP field. The chapter also delves into the limitations of this approach.

In the context of Critical Infrastructure Protection (CIP), the Public-Private Partnership (PPP) model, particularly in information sharing, faces limitations, prompting the exploration of alternative solutions [64]. To address this, an expanded governance model for CIP is proposed, moving beyond direct partnerships, and incorporating various forms of interaction between the state and the private sector. This approach draws on governance theory, acknowledging the fragmented nature of political power.

B. The National Infrastructure Protection Plan

Governance theory differentiates itself from traditional government models, recognizing that political power is fragmented across different entities. This fragmentation occurs through decentralization (localization, supranationalization, privatization) and functional differentiation within the government itself. Two main strands within governance theory are neoliberal governance and the network governance approach.

Neoliberal governance advocates for "less government and more governance," seeking efficiency gains by transferring authority from government bureaucracies to the private sector. However, as the primary goal of CIP is to

enhance security rather than efficiency, the neoliberal approach has limited relevance as a theoretical foundation for CIP policy. In response, the network governance approach is explored as an alternative model.

Network governance emphasizes collaboration and is founded on a different understanding of public-private partnerships. This model forms the basis for defining the government's new role [65]. The theoretical considerations are then applied to CIP, addressing issues raised earlier. The proposed road map for CIP meta-governance outlines a strategic plan for effective implementation.

The network approach in governance theory differs significantly from the neoliberal understanding, particularly in its view of introducing governance structures. Unlike neoliberalism, the network approach doesn't consider governance structures as a means to enhance the efficiency of public administration but rather as a consequence of progressive specialization in modern societies.

Modern societies, marked by increasing division of labor, necessitate highly specific expert knowledge for task performance. This specialization blurs the lines between the public and private sectors, with many tasks now handled by specialized companies. The challenge arises when societal problems touch upon essential functions, and the state lacks the necessary capacities to fulfill tasks due to increasing specialization.

In contrast to neoliberal approaches that rely on precise definitions and contractual stipulations of tasks, the network approach recognizes that governments lack the specialized knowledge required for appropriate control over outsourced functionalities and services. This is particularly evident in Critical Infrastructure Protection (CIP), where governments struggle to assess the quality of protective measures across diverse critical infrastructures.

The network approach asserts that modern societies demand new forms of public administration. Governments can no longer simply issue instructions and monitor implementation; instead, they must create conditions for smooth cooperation without constant oversight. Public administration, under this approach, becomes collaborative, emphasizing persuasion, negotiations, and mutual trust over control and regulation [66].

To facilitate such cooperation, small and relatively homogenous networks are needed, involving all actors who can contribute to fulfilling a public service. These actors, from both public and private sectors, organize themselves quasi-autonomously, setting rules, determining responsibilities, and monitoring compliance within the network. In this model, public services are provided by independent, self-regulating, and self-organizing networks, where government agencies play a representative but not authoritative role. The concept of "governance without government" highlights the independence of these networks from direct government control.

The cooperation of stakeholders from the public and private sectors is essential to the country's efforts to strengthen the security and resilience of critical infrastructure. Under the limitations of scarce resources, they must make well-informed decisions. Risk management is important to the National Plan and is implemented at the federal, state, local, and regional levels. These levels require the development of cross-sectoral, long-term collaborations [85]. Different business plans, available resources, and regulatory environments lead to a wide range of risk tolerances, even while particular entities manage risks based on their promises, customer welfare, and governance structures. To effectively drive joint priorities, it is imperative to comprehend the many views on security investment and risk tolerance, considering government and business practices, as well as the resources and incentives that are accessible. Ultimately, the security and resilience of critical infrastructure depend on implementing robust risk management practices, combined with collaborative efforts and strategic resource allocation.

The National Plan highlights seven fundamental principles that are essential for improving the security and resilience of critical infrastructure at all levels, with a focus on strategic alliances, risk management, and cooperation:

1. **Comprehensive Risk Management**: Methods for threat disruption, vulnerability mitigation, and consequence reduction can only be developed and implemented with the support of coordinated risk identification and management, which also facilitates efficient resource allocation.
2. **Cross-Sector Dependencies**: To improve security and resilience, it is essential to recognize and manage the risks arising from interdependencies within infrastructure sectors, which calls for an all-encompassing approach to risk management.
3. **Information Sharing**: Thanks to enabling technology, trusted relationships, and legal safeguards, the critical infrastructure community must share full information about infrastructure risks and interdependencies.
4. **Partnership Approach**: Using a range of viewpoints, skills, and capacities to tackle problems as a team, the public and private sectors work together to preserve the security and resilience of vital infrastructure.
5. **Regional and SLTT Partnerships**: By combining locally based initiatives and viewpoints with national efforts, regional partnerships are crucial for identifying gaps and taking action to improve security and resilience.
6. **Cross-Border Collaboration**: Because critical infrastructure is global in scope, agreements about mutual aid and cross-border collaboration are essential. This calls for coordinated worldwide security measures as well as assessments of supply chain risk.
7. **Design Considerations**: Effective threat deterrence, detection, disruption, vulnerability mitigation, and consequence minimization strategies should be incorporated from the outset, and security and resilience should be integral considerations during the design of assets, systems, and networks.

C. Canada Initiatives: Protection Mechanisms of Critical Infrastructure in the Canada

In an era marked by increasing complexities and potential threats, the Emergency Management Framework for Canada stands as a cornerstone, defining a collaborative and interdependent approach to safeguarding the public safety of Canadians [67]. Embodying principles such as responsibility, comprehensiveness, and partnerships, the Framework outlines a comprehensive strategy encompassing prevention, mitigation, preparedness, response, and recovery.

Building upon these principles, this paper delves into a specific facet: the Strategy for enhancing the resiliency of critical infrastructure in Canada. Aligned with the Framework, this Strategy seeks to fortify critical infrastructure resilience through a collaborative effort among federal, provincial, and territorial entities. Recognizing critical infrastructure as the lifeblood of the nation's health, safety, security, and economic well-being, the Strategy navigates the intricate landscape of interconnected systems and services across jurisdictions. It acknowledges the relative nature of defining 'acceptable levels' and 'criticality,' emphasizing a collective approach to managing risks and interdependencies.

Furthermore, the Strategy underscores the multifaceted nature of enhancing resilience, blending security measures, business continuity practices, and emergency management planning into a cohesive and adaptive framework. As we embark on this exploration, the paper aims to unravel the intricacies of the Strategy and its pivotal role in securing the foundational elements of our society.

1) Objective

In a world characterized by an escalating array of risks, the critical infrastructure of Canada finds itself at the nexus of natural, intentional, and accidental hazards. The historical backdrop, punctuated by events like the Saguenay and Red River floods, the Ice Storm, and the seismic shifts following the terrorist attacks of September 2001, underscores the urgency of safeguarding essential services [68]. As our society becomes increasingly reliant on information technologies, the intricacies of interdependencies among critical infrastructure elevate the risks to unprecedented levels. Recent natural disasters and man-made incidents, such as Hurricane Katrina and the 2003 Severe Acute Respiratory Syndrome outbreak, emphasize the pressing need for a proactive and collaborative approach to protect against potential disruptions.

Recognizing the cross-cutting nature of these risks, the National Strategy for Critical Infrastructure emerges as a beacon of resilience, offering a comprehensive, collaborative, and cross-jurisdictional framework [69]. By bringing together federal, provincial, and territorial entities, the Strategy aims to fortify the resilience of critical infrastructure, facilitating a collective response to risks and strategically allocating resources to the most vulnerable sectors. Moreover, the Strategy acknowledges the global dimension of critical infrastructure resilience, engaging with international partners and recognizing regional cooperative arrangements.

As we delve into the motivations behind the development of this National Strategy, the imperative becomes clear: to navigate the intricate landscape of risks, vulnerabilities, and interdependencies, fostering a resilient foundation for the future of Canada's critical infrastructure.

2) Fostering Collaborative Resilience

Within the framework of the Strategy for Strengthening Critical Infrastructure Resilience in Canada, a foundational methodology revolves around fostering collaboration among federal, provincial, and territorial governments, along with critical infrastructure sectors. Recognizing the paramount importance of partnerships, the Strategy emphasizes the development of collaborative efforts that respect jurisdictional boundaries while building upon existing mandates and responsibilities. To facilitate this collaboration, the Strategy delineates mechanisms for enhanced information sharing and protection, underpinned by a risk management approach that forms the bedrock of efforts to bolster the resilience of critical infrastructure across the nation.

Central to the methodology is the acknowledgment that the primary responsibility for enhancing resilience rests with the owners and operators of critical infrastructure. Simultaneously, federal, provincial, and territorial levels of government actively engage in protective measures for their critical infrastructure, aligning efforts to support owners and operators in addressing this multifaceted challenge. [70] The methodology recognizes the need for a nuanced combination of security measures, business continuity practices, and emergency management planning to comprehensively address intentional and accidental incidents, disruptions, and unforeseen disruptions, ensuring the uninterrupted provision of essential services.

Crucially, the Strategy acknowledges the diversity of approaches across jurisdictions and sectors, understanding that each province and territory structures its critical infrastructure program in alignment with its unique context. At the national level, the Strategy organizes critical infrastructure into ten distinct sectors, ranging from Energy and Utilities to Manufacturing. This sectoral classification not only informs the overarching methodology but also allows for targeted and sector-specific strategies to fortify critical infrastructure resilience at both regional and national scales.

3) Build Partnerships: Forging a Collaborative Resilience Framework

In pursuit of the strategic objective of building partnerships supporting and enhancing critical infrastructure resiliency, the Strategy aligns its approach with the principles outlined in the Emergency Management Framework for Canada. Recognizing the need for coordinated action, the Strategy emphasizes complementary and coherent efforts among federal, provincial, territorial, and critical infrastructure sector partners. This concerted approach aims to optimize resource utilization and execution of activities across prevention, mitigation, preparedness, response, and recovery measures to effectively address disruptions. In the event of emergencies or disruptions, the government of jurisdiction serves as the initial point of contact, with the federal government swiftly responding to requests for assistance beyond provincial or territorial capabilities.

While acknowledging the discretion of each jurisdiction, department, agency, and critical infrastructure owner/operator in determining appropriate responsibilities, the Strategy underscores the indispensability of collaboration for effective implementation [71]. It asserts the necessity of establishing mechanisms to facilitate this collaboration, emphasizing the role of federal, provincial, territorial, and critical infrastructure sector partners.

A pivotal element of the collaborative framework is the proposal to establish sector networks at the national level for each critical infrastructure sector. Unlike prescribing a uniform structure, the Strategy envisions sector networks tailored to the unique characteristics of each sector. These

networks, comprising federal departments, agencies, provinces, territories, national associations, and sector stakeholders, will focus on information sharing, identifying issues of concern, leveraging sector expertise, and developing tools and best practices. Participation in sector networks is voluntary, with partners collaborating on a protocol to safeguard shared information

To ensure a cohesive national approach, the Strategy introduces a National Cross-Sector Forum, integrating perspectives across the ten sector networks [72]. Comprising representatives from owners and operators, associations, and government bodies, this forum promotes information exchange, addresses cross-jurisdictional and cross-sectoral interdependencies, and forms the foundation for implementing the national critical infrastructure resiliency approach. The emphasis on collaboration at both sector and national levels underscores the Strategy's commitment to forging a comprehensive and cooperative framework for enhancing critical infrastructure resilience in Canada.

4) National Cross-Sector Forum: An Inclusive Collaborative Hub

The National Cross-Sector Forum emerges as a central platform within the Critical Infrastructure Resilience Strategy, fostering collaboration between the private sector and governments at all levels—federal, provincial, and territorial. Designed to transcend sectoral boundaries, this forum brings together representatives from key sectors, including Energy and Utilities, Finance, Food, Transportation, Government, Information and Communication Technology, Health, Water, Safety, and Manufacturing. The inclusive composition ensures a diverse range of perspectives and expertise, reflecting the complex interdependencies crucial to Canada's overall resilience.

5) Implement an All-Hazards Risk Management Approach: Navigating Resilience Through Comprehensive Risk Strategies

The strategic objective of implementing an all-hazards approach to risk management lies at the core of the Critical Infrastructure Resilience Strategy. Emphasizing the application of risk management and robust business continuity planning, the Strategy defines risk management as a continuous, proactive, and systematic process that comprehensively understands, manages, and communicates risks, threats, vulnerabilities, and interdependencies across the critical infrastructure community.

Central to this approach is the cultivation of strong situational awareness regarding the myriad risks and interdependencies that confront critical infrastructure in Canada [73]. The development of emergency management plans and programs involves sector-specific federal departments, agencies, provinces, territories, and critical infrastructure sectors working collaboratively to enhance their understanding of these risks and interdependencies.

Moving forward, federal, provincial, and territorial governments will engage in collaboration with critical infrastructure partners to develop all-hazard risk analyses encompassing accidental, intentional, and natural hazards. While governments promote a common approach to strengthening critical infrastructure resilience and share tools, lessons learned, and best practices, stakeholders bear the ultimate responsibility for implementing a risk management approach tailored to their specific context.

6) Share and Protect Information: Fostering Collaborative Resilience Through Informed Decision-Making

The strategic objective of advancing the timely sharing and protection of information underscores the significance of a robust foundation for collaborative efforts to enhance the resiliency of critical infrastructure. Information sharing and protection, regarded as complementary elements, form the bedrock of effective risk management and the understanding of critical infrastructure interdependencies.

Improved information sharing, conducted in full compliance with existing federal, provincial, and territorial legislation and policies, facilitates the timely exchange of actionable information on risks and the overall status of critical assets. This exchange empowers owners and operators, governments, and other stakeholders to assess risks and take appropriate actions proactively [74].

Timely information sharing across governments and critical infrastructure sectors is crucial for effective risk management and addressing interdependencies. Responding to the requests of critical infrastructure stakeholders, enhancements in information sharing encompass a broader range of information products (e.g., risk assessments, incident reports, best practices, lessons learned, assessment tools), improved delivery mechanisms (e.g., web-based critical infrastructure information), enhanced protection of shared information from unauthorized disclosure, and expanded production of all-hazards risk information products.

Aligned with the principles of the Emergency Management Framework for Canada, federal, provincial, and territorial governments committed to openness about their work in emergency management, security, and business continuity planning [75]. Information exchange, constituting a continuous process, fosters a common operating picture among all levels of government and critical infrastructure sectors, promoting coherency of action and a comprehensive approach across prevention, mitigation, preparedness, response, and recovery.

To enhance the quality and utility of information products, sector network members will identify emerging concerns and prioritize areas for information products. These products are anticipated to be instrumental for critical infrastructure partners, empowering them to improve the resiliency of their key assets and services.

7) Information Protection: Safeguarding Critical Infrastructure in Canada

Given the intricate web of interdependencies within Canadian critical infrastructure, the release of sensitive information holds the potential to pose risks not only to a province or local authority but also to the nation as a whole. Recognizing this, exemptions from disclosure already exist under federal, provincial, and territorial access to and freedom of information legislation for reasons of national security and public safety. The 2007 enactment of the Government of Canada's Emergency Management Act

further fortified this protection by amending the Access to Information Act, explicitly safeguarding sensitive information provided by critical infrastructure sectors [76].

Governments at all levels are committed to establishing an appropriate level of protection for emergency management and critical infrastructure information, guided by considerations of sensitivity. To facilitate this, a collaborative approach involving all levels of government will be undertaken to develop a common information-sharing protocol, supporting the sharing of information provided in confidence. This collaborative effort seeks to enhance the coherence of information-sharing and protection practices across the nation.

Encouragingly, federal, provincial, and territorial governments are urged to engage in collaborative initiatives to share best practices about information protection. By pooling collective expertise and experiences, these collaborative endeavors aim to foster the development of a unified and coherent approach to information sharing and protection in Canada. Ultimately, these efforts underscore a commitment to balance transparency with the imperative of safeguarding critical infrastructure information, ensuring a resilient and secure foundation for Canada's essential services.

8) CISA - Critical Infrastructure Sectors

16 sectors of the nation's infrastructure—physical or virtual—have assets, systems, and networks that are deemed so essential to the country that their incapacitation or destruction would severely impair national security, public health or safety, or any combination of these [82].

- **Chemical Sector:** Presidential Policy Directive (PPD) 21 designated DHS as the Chemical Sector Risk Management Agency (SRMA). On behalf of DHS, CISA handles the Chemical Sector SRMA duties. In charge of the public-private partnership for the chemical sector, CISA collaborates with businesses to create resources and technologies that improve the security and resilience of the industry.
- **Commercial Facilities Sector:** Public areas are safeguarded from coordinated attacks by the Commercial Facilities Sector. CISA provides eight subsectors with strategic direction to enhance security and resilience in these areas.
- **Communications Sector:** The communications business has developed into a multifaceted, intricate network of wireless, satellite, and terrestrial technologies. To safeguard every facet of the communication industry, CISA collaborates with stakeholders in the private sector to execute the risk management framework.
- **Critical Manufacturing Sector:** To stop and lessen the effects of natural or man-made disasters, CISA finds, evaluates, ranks, and safeguards manufacturing sectors of national importance.
- **Dams Sector:** The United States has around 90,000 dams, which provide vital services for controlling and retaining water. CISA collaborates with industry partners to safeguard assets from events caused by technology, human error, and natural calamities.
- **Defense Industrial Base Sector:** For the U.S. military, over 100,000 businesses and subcontractors provide facilities, services, and supplies. These military actions are carried out globally with assistance from the Defense Industrial Base Sector.
- **Emergency Services Sector:** The Emergency Services Sector provides physical and cyber resources to support millions of skilled workers, protects the environment and property, and aids in the recovery process following catastrophes and disasters.
- **Energy Sector:** The energy industry safeguards a complex network of resources and assets related to electricity, oil, and natural gas in order to keep up reliable energy supply and guarantee the general health and well-being of the country.
- **Financial Services Sector:** The Financial Services Sector shields your financial assets and your ability to access and use them from major power outages, natural disasters, and cyberattacks, safeguarding financial institutions of all sizes.
- **Food and Agriculture Sector:** Almost all businesses in the food and agricultural sector—farmers, eateries, and facilities for producing, processing, and storing food—are privately held. In order to guard against a variety of dangers, CISA collaborates, offers resources, and offers advice with interdependent sectors.
- **Government Facilities Sector:** The goals and limitations regarding accessibility vary throughout federal, state, municipal, and tribunal government buildings and areas. The Government Facilities Sector assists these establishments in determining their particular risk considerations and provides defenses against possible intrusions or problems.
- **Healthcare and Public Health Sector:** The public health and healthcare sectors prioritize population health and offer the necessary response and recuperation measures following major incidents like natural disasters, infectious diseases, and terrorism.
- **Information Technology Sector:** The goal of the information technology sector in the twenty-first century is to detect and defend against cyber threats and vulnerabilities, which has become increasingly complex and significant due to the country's increasing reliance on technology.
- **Nuclear Reactors, Materials, and Waste Sector:** America has a vast civilian nuclear infrastructure, ranging from the power reactors that supply millions of people with electricity to the medicinal isotopes used in cancer treatments.
- **Transportation Systems Sector:** The transportation systems industry faces several hazards and challenges due to the daily movement of millions of people and goods across the nation. CISA strives to keep these systems safe and make sure that they keep running.
- **Water and Wastewater Systems:** All human activity requires access to clean, healthy water. The goal of the Water and Wastewater Systems Sector is to safeguard the water supply systems, which are essential to the stability and health of the country.

IX. Protecting Critical Infrastructure

Information about cyber threats is gathered, analyzed, and shared by an (Information Sharing and Analysis Organization) ISAO. Presidential Policy Directive 21 states that, in contrast to ISACs, ISAOs are not directly associated with critical infrastructure sectors. ISAOs provide a more adaptable method for self-organized information sharing activities among communities of interest, including small businesses from several industries, such as accountancy, legal, and consulting firms that serve clients from different industries. The ISAO Standards Organization will be the University of Texas at San Antonio (UTSA), with assistance from the Retail Cyber Intelligence Sharing Center (R-CISC) and the Logistics Management Institute (LMI) [83].

There isn't a clear model that describes the ideal procedures for creating and running ISAOs at the moment. Many businesses have voiced a need for best practices that would enable them to build an effective non-sector-based ISAO, including recently founded sector-based ISACs. The Standards Organization will assist in fostering an open discussion with industry participants who want to support the creation of information sharing models that are not limited to a particular industry and can be tailored to a range of business requirements.

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

The term "critical infrastructure" describes the resources, networks, and systems that are necessary for maintaining public health and safety, security, economic viability, and quality of life for citizens. Terrorist attacks are one of the many natural, man-made, and technical threats that can threaten critical infrastructure. Disruptions to key infrastructure can have disastrous consequences, including death tolls, destruction of property, negative economic repercussions, harm to public trust and morale, and effects on missions that are vital to the country. The intricate web of interdependencies among vital infrastructure adds to the dangers since it can have cascading consequences that extend well beyond the sector and geographical location of the occurrence that first caused problems.

On both sides of the US-Canada border, businesses and communities may be directly impacted by critical infrastructure interruptions. Impacts from interruptions can and do extend beyond international borders because of the close proximity of refineries, nuclear facilities, big manufacturing activities, and other infrastructure to the border, as well as the cross-border networks for energy, essential supplies, and transportation [77]. Redundancies (where they exist) in the intricate critical infrastructure networks, as well as the readiness of individuals and institutions, all affect our resilience, or our capacity to react to and recover from a disruption. It also depends on our numerous alliances, particularly with other governmental branches, stakeholders in the commercial sector, and foreign friends. To guarantee things like clean food, safe transportation, and functional power, we must work together to improve the safety and economic stability of our communities and fortify the resilience of our vital infrastructure.

Understanding the value of critical infrastructure, the US and Canada have both created plans to increase the critical infrastructure's resilience in their own nations. Key stakeholders come together to create a cogent action plan to address significant critical infrastructure protection gaps under Canada's *National Strategy and Action Plan for Critical Infrastructure* (National Strategy and Action Plan), which was developed in partnership with Provincial and Territorial partners and in consultation with the private sector [78].

A public-private sector cooperation is established under the United States' *National Infrastructure Protection Plan (NIPP)* to safeguard and maintain the resilience of critical infrastructure and key resources (CIKR). An integrated network of federal ministries and agencies, state and local government agencies, businesses in the private sector, and an increasing number of regional consortia are responsible for implementing the NIPP.

Numerous significant components are shared by the NIPP and the National Strategy and Action Plan. The three goals listed below form the foundation of both strategies:

- Establishing reliable alliances;
- Increasing information exchange;
- Putting an all-hazards risk management strategy into practice.

The essential infrastructure strategies in both the United States and Canada will be implemented with assistance from the Canada-U.S. Action Plan. It will also enable collaboration between the US and Canada to identify interdependencies, share best practices and information, and carry out joint exercises in order to handle a variety of cross-border critical infrastructure challenges more successfully.

1) Objective

The goal of the Canada-US Action Plan is to create a comprehensive cross-border strategy for critical infrastructure resilience, with the ultimate goal of strengthening safety, security, and resilience in both countries. There is growing pressure to act and develop an integrated strategy for vital infrastructure.

- The interconnected nature of critical infrastructure requires a coordinated Canada-U.S. approach;
- Regional approaches to cross-border collaboration need to be guided by an overarching Canada-U.S. framework for critical infrastructure;
- Strong private sector collaboration across the border needs to be supported with an integrated Canada-U.S. approach;
- Uncoordinated efforts increase the likelihood of wasteful duplication of efforts that can be managed through collaborative development and sharing of best practices; and
- Communications with critical infrastructure stakeholders (both domestic and cross border) need to be coordinated, accurate and timely.

The foundation of the Canada-U.S. Action Plan is the idea that cooperation between the two countries will improve critical infrastructure disruption prevention, response, and recovery. It will build on previous work and cooperative efforts while concentrating on areas of shared interest. The Action Plan between the United States and Canada will

specify specific deliverables to bolster shared critical infrastructure goals and improve cooperation. It will make it possible for both the US and Canada to better control hazards and increase the resilience of their vital infrastructure. Additionally, by raising awareness of shared critical infrastructure challenges and fostering collaboration between State, Provincial, and Territorial authorities, the Canada-U.S. Action Plan will improve regional cross-border relations.
The three pillars of the Canada-U.S. Action Plan - partnership development, enhanced information sharing, and risk management- will enable both countries to increase our combined preparedness for major disruptions to infrastructure.

2) Collaborating for the Resilience of Critical Infrastructure

The Canada-U.S. Action Plan must be implemented through partnerships and organizational structures dedicated to risk management, information sharing, and protection due to the intricate and interrelated nature of the essential infrastructure between the two countries [79].

3) Group for Consultation on Emergency Management (EMCG)

On October 20, 2009, in Ottawa, the Emergency Management Consultative Group (EMCG), which was created by the *Canada-U.S. Agreement on Emergency Management Cooperation (2008)* to offer central oversight in support of cooperative emergency management, held its inaugural meeting. The EMCG will facilitate communication between US and Canadian stakeholders and offer a forum for the advancement of fresh, cooperative emergency management projects. The co-chairs of the meeting on October 20, 2009, endorsed the work plans of the four working groups—one of which was focused on vital infrastructure—that had been formed in accordance with the Agreement. The cross-border approach to critical infrastructure under the Canada-U.S. Action Plan will be supported by this working group, which will offer guidance and continuity.

4) Partnerships Particular to Sectors

The main organizational structure used by the US to coordinate CIKR initiatives and operations is a partnership model. The Sector Specific Agency (SSA), a recognized Federal department or agency, and sector-specific coordinating bodies oversee each sector. Members of the owners' and operators' (usually private sector) representatives make up Sector Coordinating Councils (SCCs). Representatives from the SSAs, other Federal ministries and agencies, and State, local, and territorial governments make up Government Coordinating Councils (GCCs). These councils establish a framework that enables representative organizations from the public and private sectors to cooperate, exchange current methods for CIKR protection, and develop capacities.

The platforms for dialogue and information sharing between industry and government stakeholders that are particular to a given sector are Canada's sector networks. The sector networks are an example of a partnership model that will allow governments and the key infrastructure sectors to work together on a variety of sector-specific activities (including risk assessments, risk-reduction plans, and exercises). To facilitate sector-specific Canada-U.S. collaboration, efforts will be made to enhance cross-border representation and engagement by Canada's sector networks and the US coordinating councils. What do we do in such cases? Establish channels and opportunities for cooperation between the Canadian sector networks and the U.S. Sector and Government Coordinating Councils to enhance cross-border sector-specific collaboration.

5) Critical Infrastructure Hazard Assessment Unit

It is planned to create a virtual Critical Infrastructure Risk Analysis Cell between the United States and Canada to exchange vulnerability assessments, prioritization techniques, procedures, and best practices related to infrastructure risk. Additionally, collaborative analytical products with cross-border applicability will be developed and produced. What do we do in this case? Create a virtual Infrastructure Risk Analysis Cell between the United States and Canada to produce and exchange information and tools for risk management.

6) Exchange of Information

The willingness of the American and Canadian governments, as well as businesses, to engage in multidirectional information exchange, is the foundation for the effectiveness of the Canada-U.S. Action Plan. Better information exchange will increase the ability of governments, operators, and other stakeholders to evaluate risks and take appropriate action to safeguard vital infrastructure and increase its resilience—all while adhering to current laws and policies. Better information sharing will be supported by the Canada-US Framework.

7) Enhanced Security of Information

Before, during, and after an emergency, key infrastructure stakeholders must effectively communicate in both directions. Ensuring that information is properly protected requires action to enable trusted information sharing. As a result, the US and Canada will collaborate to create strategies that are compatible with shielding confidential information about essential infrastructure from public view. What do we do in such cases? To preserve and exchange sensitive critical infrastructure information, the US and Canada will collaborate to create appropriate channels and protocols.

8) Enhanced Information Items

Governments and the private sector, which owns and manages most of the essential infrastructure in the US and Canada, share responsibilities for strengthening the resilience of this infrastructure. Working with the public and private sectors to identify priorities and areas of development concern is a crucial part of this Action Plan, since it enables the development of focused analytical products. Critical infrastructure partners can then use these analytical tools to safeguard and enhance the resilience of important assets and services. As part of the Canada-U.S. Action Plan, the two countries will collaborate to enhance their comprehension of the information and decision-making needs of the public and private sectors in order to facilitate the creation of customized

analytical products. What do we do in such cases? In order to facilitate the creation of useful analytical products, the United States and Canada will collaborate to determine the information requirements for the public and private sectors.

9) Scheduled Distribution of Information

In an emergency, essential points of contact from several critical infrastructure sectors must promptly exchange information. On both sides of the Canada–US border, communities and infrastructure are frequently impacted by disasters. Information regarding current and/or possible hazards and dangers is shared between the governments of the United States and Canada to support efforts to avoid, prepare for, respond to, and recover from all sorts of catastrophes. Compliant protocols for providing cross-border partners with critical infrastructure information (such as alerts, warnings, and risk products) will be implemented under the Canada-U.S. Action Plan. What do we do in such cases? In the event of an incident impacting essential infrastructure, the United States and Canada will work together to guarantee efficient information sharing.

10) Measurement of Risk

The Canada-U.S. Action Plan addresses key infrastructure risks and interdependencies by taking an all-hazards strategy. Setting protection and resiliency goals, identifying crucial infrastructure and important dependencies, evaluating, and prioritizing risks, creating, and carrying out plans and programs to address the identified risks and dependencies, and gauging the success of the plans and programs are all part of this risk management approach, which is grounded in the philosophy of continuous improvement. With this strategy, which has a constant feedback loop, the US and Canada can collaborate to monitor advancements and carry out initiatives aimed at enhancing the long-term resilience of vital infrastructure. What do we do in such cases? Together, the US and Canada will identify priority regions, evaluate hazards, and create measures to resolve them. Sub-actions will be determined after a careful examination of the risk-informed priorities in each nation and the identification of shared interests.

Establishing alliances and enhancing information sharing are two further components of the Canada-U.S. Action Plan that must be implemented for these risk management initiatives to succeed. In addition to providing a shared awareness of the risk and interdependencies facing critical infrastructure in Canada and the United States, the risk management initiatives will expand on ongoing programs and operations in both nations. Establishing a thorough risk management approach between Canada and the United States begins with developing a shared situational awareness.

B. 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. Government officials get together through the HLRF to discover and exchange best practices for improving knowledge of emerging and complex risks as well as for exchanging best practices for governance and management [80]. It brings together specialists from academia, think tanks, civil society, and the commercial sector to pinpoint weaknesses in risk management and discuss potential solutions for upcoming and present issues. Adopted by the OECD Council in 2014, the HLRF's recommended best practice, the OECD Recommendation on the Governance of Critical Risks, shows the inclusive approach to policy analysis that the organization uses.

The OECD Recommendation emphasizes how important it is for governments to strengthen resilience and security in critical infrastructure networks because of the significant financial costs and social losses that interruptions to critical infrastructure cause. In order to assess how adherents were implementing the OECD Recommendation, the OECD carried out a survey in 2016. According to the survey results, dividing up the duty between companies and governments to safeguard vital infrastructure assets and guarantee a prompt return of service is a significant barrier to putting the recommendation into practice.

This was tasked by the High-Level Risk Forum with researching and producing a good practice paper on how businesses and governments can work together to build more secure and resilient critical infrastructure in order to address this challenge. In response to this request, the OECD carried out a cross-national study on the resilience of essential infrastructure, hosted topic workshops, carried out regional research projects and pilot country case studies, and participated in pertinent OECD multidisciplinary initiatives. The OECD network of policymakers responsible for critical infrastructure, along with regulators, operators from the public and private sectors, and researchers working on this topic, was expanded by these activities, which also contributed to strengthening the evidence base on critical infrastructure resilience presented in this report.

The report based on a stocktaking report that started the process and was discussed in the 2017 High-Level Risk Forum decided that in collaboration with the Joint Research Centre of the European Commission, the OECD would host a special workshop on "System-thinking for Critical Infrastructure Resilience and Security". The workshop, which was held on September 23–24, 2018, focused on the methods, instruments, and data needed to evaluate the resilience of the system as well as the policy tools that governments can use to support the resilience of critical infrastructure. Based on the workshop discussions and OECD analysis, participants proposed that the OECD High-Level Risk Forum create a "Policy Toolkit on Governance of Critical Infrastructure Resilience."

1) Objectives

The Policy Toolkit on Governance of Critical Infrastructure Resilience aims to assist governments in creating and implementing their own national policies for critical infrastructure resilience through productive collaborations with operators.

It suggests useful guidelines that governments might apply, backed by national best practices and suggestive benchmark indicators, to:

- Identify critical infrastructure, map out (inter-)dependencies and prioritize the critical services and functions, systems, and assets, where investments in resilience and security are the most required.
- Forge effective partnerships with critical infrastructure operators to build mutual trust, share information on

risks and vulnerabilities and agree on a common vision and policy objectives.
- Share responsibilities to protect critical infrastructure assets and ensure quick restoration of service.

In order to ensure critical infrastructure resilience, the Policy Toolkit suggests that governments take a systemic approach [81]. This means that their policies should target measures throughout the risk management cycle, address all hazards and threats, guarantee multi-sectoral coordination and public-private cooperation, integrate planning for the entire infrastructure life-cycle, and promote transboundary cooperation.

In the future, the OECD will collaborate with the High-Level Risk Forum to assist nations in putting this Policy Toolkit into practice and to track their advancements in fortifying vital infrastructure.

X. Approaches for Canadian 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, which is presented in this chapter. Government officials get together through the HLRF to discover and exchange best practices for improving knowledge of emerging and complex risks as well as for exchanging best practices for governance and management. It brings together specialists from academia, think tanks, civil society, and the commercial sector to pinpoint weaknesses in risk management and discuss potential solutions for upcoming and present issues. Adopted by the OECD Council in 2014, the HLRF's recommended best practice, the OECD Recommendation on the Governance of Critical Risks, shows the inclusive approach to policy analysis that the organization uses.

It emphasizes how important it is for governments to strengthen resilience and security in critical infrastructure networks because of the significant financial costs and social losses that interruptions to critical infrastructure cause. In order to assess how adherents were implementing the OECD Recommendation, the OECD carried out a survey in 2016. According to the survey results, dividing up the duty between companies and governments to safeguard vital infrastructure assets and guarantee a prompt return of service is a significant barrier to putting the recommendation into practice.

The OECD was tasked by the High-Level Risk Forum with researching and producing a good practice paper on how businesses and governments can work together to build more secure and resilient critical infrastructure in order to address this challenge. In response to this request, the OECD carried out a cross-national study on the resilience of essential infrastructure, hosted topic workshops, carried out regional research projects and pilot country case studies, and participated in pertinent OECD multidisciplinary initiatives. The OECD network of policymakers responsible for critical infrastructure, along with regulators, operators from the public and private sectors, and researchers working on this topic, was expanded by these activities, which also contributed to strengthening the evidence base on critical infrastructure resilience presented in this report.

Let’s look at the stocktaking report that started the process and was discussed in the 2017 High-Level Risk Forum. The Forum decided that in collaboration with the Joint Research Centre of the European Commission, the OECD would host a special workshop on "System-thinking for Critical Infrastructure Resilience and Security”. The workshop, which was held on September 23–24, 2018, focused on the methods, instruments, and data needed to evaluate the resilience of the system as well as the policy tools that governments can use to support the resilience of critical infrastructure. Based on the workshop discussions and OECD analysis, participants proposed that the OECD High-Level Risk Forum create a "Policy Toolkit on Governance of Critical Infrastructure Resilience.”

1) Objectives

The Policy Toolkit on Governance of Critical Infrastructure Resilience aims to assist governments in creating and implementing their own national policies for critical infrastructure resilience through productive collaborations with operators.

It suggests useful guidelines that governments might apply, backed by national best practices and suggestive benchmark indicators, to:

- Identify critical infrastructure, map out (inter-)dependencies and prioritize the critical services and functions, systems, and assets, where investments in resilience and security are the most required.
- Forge effective partnerships with critical infrastructure operators to build mutual trust, share information on risks and vulnerabilities and agree on a common vision and policy objectives.
- Share responsibilities to protect critical infrastructure assets and ensure quick restoration of service.

To ensure critical infrastructure resilience, the Policy Toolkit suggests that governments take a systemic approach. This means that their policies should target measures throughout the risk management cycle, address all hazards and threats, guarantee multi-sectoral coordination and public-private cooperation, integrate planning for the entire infrastructure life-cycle, and promote transboundary cooperation.

In the future, the OECD will collaborate with the High-Level Risk Forum to assist nations in putting this Policy Toolkit into practice and to track their advancements in fortifying vital infrastructure.

B. Improving Policies

1) Seven steps for critical infrastructure resilience policies

To strengthen critical infrastructure resilience, a comprehensive policy framework should address the following seven interrelated governance challenges:

1. Setting up a multi-sector governance structure for critical infrastructure resilience
2. Understanding complex interdependencies and vulnerabilities across infrastructure systems to prioritize resilience efforts
3. Establishing trust between government and operators by securing risk-related information-sharing
4. Building partnerships to agree on a common vision and achievable resilience objectives
5. Defining the policy mix to prioritize cost-effective resilience measures across the life-cycle

6. Ensuring accountability and monitoring implementation of critical infrastructure resilience policies
7. Addressing the transboundary dimension of infrastructure systems

C. Setting up a multi-sector governance structure for critical infrastructure resilience

Governments should adopt a whole-of-government approach to critical infrastructure resilience. Ideally, such governance would involve the sectoral ministries and agencies overseeing infrastructure delivery and regulation in the multiple critical sectors, as well as those in charge of resilience to all-hazards and threats. Coordination at the Center-of-Government would allow to manage the interests of all stakeholders and make the relevant trade-offs for effective resilience policies.

Why is this important?

Governments have a key role to play in critical infrastructure resilience. They have a responsibility to provide security and safety to citizens and are often infrastructure regulators. Governments, at central or sub-national level, can also be owners and operators of critical infrastructure, either directly or through publicly owned companies. Furthermore, investments in major infrastructure are often dependent upon major public funds. Finally, governments are also an important user or client of critical infrastructure, with expectations on their reliability for the continuity of government activities.

This presents governments with multiple and complex roles, across critical infrastructure sectors and for multiple hazards and threats. Risk managers and officials in charge of the governance of critical risks have to coordinate across several functions in government and ensure that, on behalf of the general interest, policy objectives can be achieved from a resilience perspective while balancing the relevant trade-offs.

Key policy questions:

- Is there a national strategy or policy document for critical infrastructure resilience?
- Is there a definition for critical infrastructure?
- Is a pre-defined list of critical infrastructure sectors in place?
- Is there a whole-of-government approach to the development of critical infrastructure resilience?
- Are all relevant hazards and threats considered in the critical infrastructure resilience policy?
- Is there a dedicated coordination entity responsible for designing, monitoring, and adjusting the national critical infrastructure resilience policy?

Benchmark indicators

- National policy on critical infrastructure resilience
- Inter-departmental / ministerial committee/platform to design CI resilience policies
- Coordination entity at the Center of Government

Examples of good practices

- In the United States, the Presidential Policy Directive on Critical Infrastructure Security and Resilience tasks the Department of Homeland Security to coordinate CI policies at the Federal level with sector agencies across 16 CI sectors.
- In France, the General Secretariat for Defense and National Security under the Prime Minister coordinates the CI resilience policy across 8-line Ministries for 12 infrastructure sectors and with a multi-hazard approach.

D. Understanding complex (inter-)dependencies and vulnerabilities across critical infrastructure systems to prioritise resilience efforts

Governments should adopt methodologies and metrics to identify the critical functions, systems and assets that should be prioritized for investments in building resilience. This requires a good understanding of how disruptions can affect infrastructure assets and where dependencies and interdependencies are found that could amplify their impacts. Once priority nodes and hubs are identified across interdependent systems, there is a need to assess their resilience with relevant indicators and to compare actual and expected results to see where the gaps are.

Why is this important?

Defining methodologies for risk assessment that critical infrastructure stakeholders from government and operators can use in practice and clarifying the related data requirements are fundamental steps to prioritize investments in resilience. Understanding risks and vulnerabilities of critical infrastructures is a complex task, given the underlying interdependencies and requires a systemic view. A diverse set of tools exists to identify critical assets, understand their vulnerabilities to shocking events and model the potential cascading impacts through interconnected networks. Recent research has focused on system complexity, risk modelling, and interdependency mapping, which provides rich analytical materials.

Nevertheless, governments and critical infrastructure operators are grappling with the need to choose the right tools for the identification of the most critical hubs and nodes of infrastructure systems and the assessment of their level of resilience. In practice, such analysis follows a three-tier approach, for which methodologies and tools need to be standardized. First, mapping the interdependencies (physical, digital, geographic, logical) between critical infrastructure assets and systems is key to estimating the full impact of service loss in case of disruption. Second, conducting a criticality assessment allows to classify systems, networks, and asset that are truly critical, based on the impact of their disruption on a range of pre-established criteria. Third, resilience analysis and stress-tests help identify weak points where potential failures are more likely to happen. Developing relevant indicators for infrastructure assets and systems enables the best comparison of their level of resilience.

Key policy questions:

- Is there a mapping of dependencies and interdependencies across the different critical infrastructure sectors?
- Are there defined criteria to assess the criticality of infrastructures?

- Are there multi-hazards stress tests conducted to identify weak points among critical infrastructure?

Benchmark indicators

- Identification of critical assets
- Existence of resilience indicators

Examples of good practices

- In the Netherlands, the National Coordinator for Security and Counterterrorism (NCTV) developed a 3-step methodology to first identify critical infrastructure and categorize them according to their criticality (A or B), second assess their vulnerabilities to multiple risks and third set priorities for resilience investments.
- Public Safety Canada (PSC) has undertaken high-level inter-dependency analyses of individual CI sectors with examination of cascading impacts. PSC is evaluating critical infrastructure inter-dependency modelling tools developed by the research community.

E. Establishing trust between governments and operators and securing information-sharing on risks and vulnerabilities

Governments should establish information-sharing platforms with operators of critical infrastructure so that all relevant infrastructure stakeholders obtain a comprehensive and shared understanding of risks and vulnerabilities to conduct resilience analysis. It is crucial to ensure that the design of these platforms assures security and confidentiality of information shared with clear rules of access to allow a trusted sharing of sensitive information.

Why is this important?

Information exchange is fundamental for governments to gain a comprehensive understanding of critical infrastructure vulnerabilities. It also helps operators to understand their own vulnerabilities, their dependencies on other infrastructures, and how disruptions to their services could affect other infrastructures or even themselves.

The challenge to fostering information-sharing is to build trust between parties, such that the security and proprietary of information shared voluntarily will not be publicly disclosed. Operators are not inclined to share sensitive information about their vulnerabilities, their critical dependencies, and any disruptive incidents outside of safe circles, as disclosure of certain information may lead to liability, be important for competitiveness in the market or do damage to a firm's reputation. On the government side, information-sharing may involve classified information when it relates to national security. Risks of cyber threats are another concern, as they can also increase reluctance to share information on joint platforms, if guarantees on their security are not properly assured.

In some cases, disclosure of risk information can strengthen operators' accountability and reinforce resilience measures, for climate-related risks for instance. In a world characterized by interconnected systems, the resilience of interdependent infrastructures is as strong as its weakest link. Therefore, information sharing significantly contributes to bringing infrastructure operators up to a similar understanding of what is required to reach an acceptable level of security and resilience.

Key questions:

- Are there mandatory or voluntary legislation, regulations, and policies for information sharing about risks and vulnerabilities?
- Are there information-sharing platforms for governments and critical infrastructure operators?
- Are there incentives for infrastructure operators to share qualitative information about their dependencies and vulnerabilities with the policy community?
- Are there safeguards in place to secure the confidentiality of shared information?

Benchmark indicators

- Presence of a secured information sharing mechanism
- Frequency, quantity, and quality of shared information from infrastructure operators
- Utilization/satisfaction of the information sharing *platform*

Examples of good practices

- The United Kingdom Data and Analytics Facility for National Infrastructure (DAFNI) provides a platform of data, models, and technical tools for complex infrastructure analysis to analyze system performance and make wise investments.
- Australia Trusted Information Sharing Network (TISN) for Critical Infrastructure provides national level forums for critical infrastructure operators to share vital information on risks and mitigation strategies with in a secure, non-competitive environment, and to develop collective solutions to shared problems.

F. Building partnerships to agree on a common vision and achievable resilience objectives

Governments should partner with critical infrastructure operators from the public and the private sectors to agree on a common resilience vision for critical infrastructure nationwide and on shared and achievable resilience objectives. Developing an understanding of public expectations to potential loss of infrastructure service can be a useful way to initiate dialogue.

Why is this important?

Beyond information-sharing on risks and vulnerabilities, critical infrastructure resilience depends upon governments partnering with infrastructure operators from the public and private sectors in resilience efforts. While operators and governments agree on the need to protect critical assets and maintain their services, views can differ on the level of resilience required, the means to achieve it, and on the regulatory requirements that should apply. These measures have financial implications and raise questions about who will take on additional costs to invest in resilience.

Establishing partnerships between governments and operators (public and private) to encourage dialogue on these issues is a useful approach to develop a common vision towards resilience in critical infrastructure and define shared objectives. Policy issues to be addressed include deciding on

the acceptable duration of 'down time', maintaining a level-playing field between operators, and circumventing situations of free-riding in competitive sectors. Ensuring stakeholders' engagement, including with the public, in regular meetings, institutionalized dialogues, and joint exercises can foster consensus.

Key policy questions:

- Are there institutionalized dialogues in place to engage critical infrastructure operators in resilience policy design?
- Are there processes in place to understand public expectations for critical infrastructure resilience?
- Is there a common vision of critical infrastructure resilience defined through multi-sector dialogue?
- Are there resilience objectives established to support the vision's implementation?

Benchmark indicators

- Existence *of critical infrastructure stakeholders' consultation fora*
- *Frequency of consultation fora and level of operator's participation*
- *Quality of the participatory* process

Examples of good practices

- In Switzerland, the national CIP strategy coordinated by the Federal Office for Civil Protection is based on partnerships and various platforms with CI operators, federal and subnational authorities. Beyond risk analysis and information sharing, the CI Guideline is developed jointly and allows setting resilience objectives for CI operators.
- *In Germany, the UP KRITIS is a National initiative between the state and carriers of Critical* Infrastructures for the protection of critical information infrastructures. The UP KRITIS consists of more than 450 associates.

G. Defining the policy mix to prioritise cost-effective resilience measures across the life-cycle

Governments should define a mix of policy tools to incentivize operators' investments in resilience and achieve shared resilience objectives. Such measures should address the entire infrastructure life-cycle from planning to operations, maintenance and renewal or retrofitting. Government prioritization of resilience measures should be informed by cost-benefit analysis considering repercussions on the cost of service.

Why is this important?

Governments have a range of policy tools to promote resilience objectives, including voluntary frameworks, incentives, and regulatory measures. Operators prioritize resilience to safeguard services and reputation, yet upfront costs pose challenges. Balancing public policy instruments is crucial to incentivize investment while managing financial impacts on customers and businesses.

Regulatory measures, like setting reliability requirements or mandating business continuity plans, provide clear obligations but can be costly and lag behind technological advancements. Compensation schemes for disrupted services incentivize resilience investments, allowing operators flexibility in implementation. Voluntary frameworks, such as resilience guidelines and awareness activities, promote stakeholder engagement but come with uncertainties.

Effective policymaking requires balancing public support and private investment through cost-benefit analysis to prioritize resilience measures. This ensures collective efforts toward shared resilience objectives while mitigating financial burdens on stakeholders.

Key policy questions:

- Are there resilience measures defined to increase the level of protection, robustness, redundancy, or adaptability across critical infrastructure life cycle?
- Are there minimum-security standards in place to ensure operators invest in resilience?
- Are sectoral regulators playing a role in incentivizing critical infrastructure resilience?
- Is cost-benefit analysis used to prioritize resilience measures, evaluate their impact on costs of services, and find cost-sharing arrangements?

Benchmark indicators

- Implementation plans on critical infrastructure resilience
- Infrastructure regulations provisions on resilience
- Assessments of cost-benefits of resilience measures

Examples of good practices

- In Finland, the Energy Authority sets the requirements for business continuity and reliability standards in the electricity sector, and the National Emergency Supply Agency provides tools, guidance, and methods for operators to comply with these regulations.
- In France, the State, CI operators and local authorities have agreed on measures to increase CI resilience for the risk of a major flood in Paris. This includes information-sharing, emergency preparedness and vulnerability reduction for existing and future infrastructure.

H. Ensuring accountability and monitoring implementation of critical infrastructure resilience policies

Government should monitor implementation and evaluate progress in attaining resilience objectives and define an accountability framework for critical infrastructure operators. Reviewing the effectiveness of the resilience policy tools should allow adjustments to a dynamic risk landscape and infrastructure innovations while taking into consideration the need for predictable and stable regulatory frameworks conducive to infrastructure investments.

Why is this important?

A comprehensive policy framework is a first step towards enhancing critical infrastructure resilience. Whether critical infrastructure will actually be resilient hinges on the implementation of the objectives and requirements put forward in these policies. Accountability mechanisms need to be set-up to ensure that operators carry out the stipulated resilience measures, such as criticality and vulnerability assessments, business continuity plans, back-up operating systems, exercises and stress tests, mutual aid agreements, retrofitting of assets, or risk financing mechanisms.

Monitoring implementation can take diverse forms including regular reporting, inspections and performance assessments or peer reviews. To strengthen accountability, fines for non-compliance, recognition/awards for the implementation of good practices and peer pressure through the use of open access evaluations/rankings are other available incentives that may motivate operators to prioritize investments in resilience measures. Regular evaluations are also useful to assess the effectiveness of policy instruments to strengthen critical infrastructure resilience and adapt them to keep up with the pace of innovations and emerging risk patterns.

Key policy questions:

- Is there regular monitoring of the implementation of resilience measures by critical infrastructure operators?
- Are there accountability frameworks in place to ensure that resilience measures are implemented?
- Are there reviews of the effectiveness of resilience policy instruments planned to adjust to a dynamic risk landscape?
- Are there joint exercises to test crisis and continuity management mechanisms?

Benchmark indicators

- Accountability frameworks for critical infrastructure stakeholders
- Revisions of critical infrastructure policies

Examples of good practices

- In Korea, the Ministry of Interior and Safety evaluates disaster response capacities of critical infrastructure operators every year, with a ranking that goes public. Peer pressure creates important incentives for operators to keep up their public image.
- 10 years after its adoption, the European Commission is evaluating its Directive on European Critical Infrastructures to assess whether it remains relevant and effective.

I. Addressing the transboundary dimension of infrastructure systems

Government should coordinate national critical infrastructure resilience policies with neighboring countries and beyond, to address transboundary dependencies. International information-sharing mechanisms should be set up to assess risks and vulnerabilities across borders as well as to develop common approaches for critical infrastructure resilience.

Why is it important?

Interconnected and interdependent infrastructures cross borders bringing an important international dimension to resilience. Hazards and threats do not stop at national borders and integrated supply chains can propagate their consequences. In some cases, critical infrastructure provides services in multiple countries and different jurisdictions. This makes it more compelling to integrate international cooperation in critical infrastructure resilience policies. Sharing information and good practices, adopting common approaches, and developing joint standards in critical infrastructure resilience are among the policy options that can foster international and transboundary cooperation in this area.

Key questions:

- Are there international forums to foster exchange of good practices and to build common approaches for critical infrastructure resilience policies?
- Is there international information sharing platforms on risks and vulnerability for interdependent critical infrastructure?
- Are there cooperation mechanisms in place to define joint standards for critical infrastructure resilience with neighboring countries?

Benchmark indicators

- International policy frameworks for critical infrastructure resilience
- Joint critical infrastructure resilience plans

Examples of good practices

- The Canada – United States Action Plan for Critical Infrastructure promotes an integrated approach to critical infrastructure protection and resilience by enhancing coordination of activities and facilitating continuous dialogue among cross-border stakeholders.
- The European Program for Critical Infrastructure Protection (EPCIP) is a long-term program that encompasses various instruments for the protection of critical infrastructure in the EU, including regular meetings of national CIP Points of Contact. Its external dimension includes regular meetings with strategic partners and was recently widened to include cooperation with neighboring countries.

1) Improving Cybersecurity

Cyber-physical systems have undergone amazing advancements and changes along their fascinating journey. The mechanization of weaving looms in 1784 and the electrification of factories in 1870 marked the beginning of these systems' rapid evolution toward more diversity and broader scope [84]. But the evolution didn't stop there. The advent of automation in 1969 was a crucial turning point in the development of cyber-physical systems. We have now entered a new phase of digitalization, where the strength of digital technology has allowed these systems to become even more advanced and integrated.

Advanced systems with integrated sensors, processors, and actuators are known as hyperphysical systems, or CPS. These systems have the ability to perceive and communicate with the physical world, including human users. They can ensure real-time performance and are specifically made to work in applications where safety is a top priority.

Integrated with vital infrastructures are CPS systems. By gathering information from multiple sources, this integration enables safe remote system monitoring and control. This allows operators to see possible problems before they turn into major mishaps. CPS is present in all spheres of society, including industrial production lines and healthcare facilities. However, as CPS is playing a bigger and bigger role in our lives and economies, bad actors have started to target it.

Given that the majority of CPS networks are connected to operational technology (OT), which manages tangible assets like buildings, machinery, and other infrastructure, this is especially worrisome. In order to guarantee secure and dependable operations in our increasingly digital environment, security of these systems and the networks they depend on must be given top importance.

Since many of these systems are outdated and susceptible to cyberattacks, the demand for stronger security measures is increasing. It is critical to outfit these systems with the most recent security patches as we consider the future of CPS. This involves making investments in digital transformation, which is essential to guaranteeing the dependability and security of OT and CPS networks.

Vulnerabilities and Risks

Cyber-physical systems (CPS) are vulnerable to various threats stemming from software defects, design flaws, and human error, providing opportunities for cybercriminals to launch harmful operations such as malware penetration and denial of service attacks. Incidents like hackers breaking into smart grids showcase the potential for severe consequences, including electricity cutoffs, property damage, and economic disruption. Moreover, vulnerabilities in medical equipment or internet-connected cars could lead to fatalities, highlighting the critical importance of cybersecurity precautions.

Insider attacks also pose significant risks to cyber-physical systems, as demonstrated by incidents like the Mariachi Shire Council's sewage release due to a disgruntled contractor's actions using SCADA radio commands. Similarly, the malware-induced attack on the Ukrainian power grid in 2017, affecting its SCADA system, underscores the vulnerability of these environments. Organizations must take proactive steps to safeguard their systems and protect people who rely on them, especially as activities increasingly shift online.

Recent cyberattacks, such as the ransomware attack on Colonial Pipeline in 2021 and the breach of a Florida water treatment plant's computers, highlight the urgent need for robust security measures. These incidents emphasize the vital necessity of safeguarding critical systems amidst the ongoing rise in cyber threats. Concepts of physical and cyber security are essential for protecting CPS, but unforeseen weaknesses arising from intricate interdependencies pose additional challenges. Thus, CPS must implement policies that safeguard both their physical and digital environments to protect vital infrastructure effectively.

2) There is a critical need to improve the cyber security of cyber-physical systems.

First and foremost, understanding the vulnerability of cyber-physical systems (CPS) to cyber-attacks is crucial. Cybercriminals often target the system's operational technology (OT), which controls and supervises physical actions within CPS. If cybercriminals gain control over the OT, they can influence and sabotage systems, posing significant risks to communities and economies. Therefore, cybersecurity is paramount for businesses utilizing CPS to protect against such threats.

Secondly, evaluating the existing security infrastructure within CPS is essential for enhancing cybersecurity. Technical assessments should analyze current risks, vulnerabilities, and threats, allowing security experts to develop and implement appropriate security policies and procedures. Regular testing and updates of security protocols are necessary to prevent breaches effectively.

Thirdly, integrating cybersecurity best practices from the planning to the implementation stages is vital for CPS development. Every element, from software to hardware, should incorporate security measures to ensure system security from the outset. This approach enables security experts to continuously monitor for threats and vulnerabilities, maintaining the integrity of CPS systems.

Consequences of Failure

The proliferation of cyberthreats presents dire implications for CPS's operations. There could be serious disruptions to the physical systems if these systems are not secured. For example, the 2010 Stuxnet incident successfully disrupted Iranian nuclear centrifuge operations, resulting in significant physical harm. A disruption to the water supply, banking system, or public transportation might result in significant financial losses, anger among the populace, and societal instability. Moreover, deaths could occur from medical device malfunctions. For this reason, maintaining the security of CPS is essential to both corporate operations and human lives.

Best Practices

CPS's cybersecurity needs constant work, cooperation, and development. To identify, evaluate, and manage risks, cybersecurity professionals can make use of frameworks like the ISA/IEC 62443 Standards and the NIST Cybersecurity Framework. By using these frameworks, enterprises can enhance the overall security of their CPS and apply risk-based cybersecurity solutions. Software vulnerabilities must be prevented by giving regular vulnerability scanning, penetration testing, and patch management top priority. Collaboration also facilitates the exchange of knowledge about new risks and effective countermeasures.

3) Protection of Cyber-Physical Infrastructure

Protecting cyber-physical infrastructure is paramount due to the rising frequency and sophistication of cyber threats, posing significant risks like service disruptions and economic upheaval. Addressing these threats requires a multifaceted approach, including robust cybersecurity protocols, resilience measures, and collaboration between public and private sectors.

Technological measures, such as implementing robust cybersecurity protocols, form the backbone of efforts to safeguard cyber-physical infrastructure. This involves defending against cyber threats like malware, phishing attacks, and unauthorized access to prevent potential devastating consequences.

Enhancing resilience through measures like regular risk assessments and incident response planning is essential for organizations to mitigate cyber threats effectively. Moreover, collaboration between public and private stakeholders is crucial for sharing threat intelligence, coordinating response efforts, and establishing industry-wide best practices.

Policymakers play a vital role in establishing regulatory frameworks to promote cybersecurity and resilience across

critical infrastructure sectors. This includes incentivizing investment in cybersecurity measures, establishing reporting requirements for cyber incidents, and facilitating information sharing among stakeholders. By prioritizing cybersecurity and resilience, organizations and governments can mitigate risks and ensure the continued reliability and security of critical infrastructure systems.

1. *Firewalls, Intrusion Detection Systems (IDS), and Encryption Protocols:*
    - **Firewalls**: These are essential network security devices that monitor, and control incoming and outgoing network traffic based on predetermined security rules. Firewalls act as a barrier between trusted internal networks and untrusted external networks, filtering out potentially malicious traffic.
    - **Intrusion Detection Systems (IDS)**: IDS are software or hardware solutions designed to monitor network or system activities for malicious activities or policy violations. They analyze network traffic or system logs to identify suspicious behavior or known attack patterns. IDS can provide real-time alerts to security personnel, enabling timely responses to potential threats.
    - **Encryption Protocols**: Encryption is the process of converting plaintext data into ciphertext, making it unreadable to unauthorized users. Encryption protocols, such as Secure Sockets Layer (SSL) or Transport Layer Security (TLS), are used to secure communication channels between devices or systems. By encrypting data both at rest and in transit, organizations can protect sensitive information from unauthorized access or interception by adversaries.
2. *Endpoint Protection Software:*
    - Endpoint protection software, also known as endpoint security or antivirus software, is designed to protect individual devices, such as computers, smartphones, and tablets, from cyber threats. These solutions include features like antivirus scanning, firewall protection, intrusion prevention, and behavior monitoring to detect and mitigate various types of malwares, including viruses, ransomware, and Trojans.
    - Endpoint protection software often incorporates advanced threat detection capabilities, such as machine learning algorithms and behavioral analysis, to identify and respond to emerging threats in real-time. By deploying endpoint protection software across their network, organizations can establish a comprehensive defense-in-depth strategy to safeguard their endpoints from cyberattacks.
3. *Regular Vulnerability Assessments and Penetration Testing:*
    - Vulnerability assessments involve systematically identifying, quantifying, and prioritizing security vulnerabilities in a system, network, or application. These assessments may involve automated scanning tools, manual inspection, or a combination of both techniques. By conducting regular vulnerability assessments, organizations can proactively identify and remediate security weaknesses before they can be exploited by attackers.
    - Penetration testing, also known as ethical hacking, involves simulating real-world cyberattacks to evaluate the security posture of an organization's systems and infrastructure. Penetration testers attempt to exploit identified vulnerabilities in a controlled environment to assess the effectiveness of existing security controls and identify areas for improvement. By conducting penetration testing regularly, organizations can validate the efficacy of their security measures and strengthen their defenses against potential cyber threats.

Organizational measures play a crucial role in bolstering cybersecurity defenses by focusing on human factors and organizational processes. Here's an elaboration on each aspect:

4. *Providing Regular Cybersecurity Training and Awareness Programs for Employees:*
    - Regular cybersecurity training equips employees with the knowledge and skills necessary to recognize and respond to cyber threats effectively. Training programs cover various topics, including identifying phishing attempts, practicing safe browsing habits, creating strong passwords, and securely handling sensitive information.
    - By raising awareness about common cyber threats and best practices, organizations empower employees to become proactive participants in the defense against cyberattacks. Training sessions may include interactive workshops, online courses, simulated phishing exercises, and cybersecurity awareness campaigns to engage employees and reinforce key concepts.
    - Continuous education is essential as cyber threats evolve rapidly, and new attack vectors emerge. By providing ongoing cybersecurity training, organizations ensure that employees remain vigilant and informed about the latest cybersecurity trends and techniques.
5. *Establishing Clear Policies and Procedures for Incident Response and Risk Management:*
    - Incident response policies and procedures outline the steps to be taken in the event of a cybersecurity incident, such as a data breach, malware infection, or network intrusion. These documents define roles and responsibilities, escalation paths, communication protocols, and mitigation strategies to facilitate a coordinated and effective response.
    - Risk management policies guide organizations in identifying, assessing, and mitigating cybersecurity risks to their operations, assets, and stakeholders. These policies establish risk assessment methodologies, risk tolerance thresholds, risk mitigation strategies, and risk monitoring mechanisms to proactively manage cybersecurity risks.

- Clear and well-documented policies and procedures provide guidance to employees and stakeholders on how to respond to cybersecurity incidents and manage risks effectively. They promote consistency, accountability, and efficiency in addressing cybersecurity challenges and minimize the potential impact of incidents on the organization.

6. *Fostering a Culture of Cybersecurity Awareness Within the Organization:*

- Building a culture of cybersecurity awareness involves instilling a shared commitment to cybersecurity among employees at all levels of the organization. It emphasizes the importance of cybersecurity as a collective responsibility and integral part of everyday operations.
- Leadership support and engagement are critical in fostering a cybersecurity-aware culture. Senior executives and managers should demonstrate a strong commitment to cybersecurity by prioritizing investments in security initiatives, setting clear expectations for cybersecurity compliance, and leading by example in practicing secure behaviors.
- Communication and collaboration are essential for fostering a cybersecurity-aware culture. Organizations should promote open dialogue about cybersecurity risks, encourage employees to report security incidents or concerns promptly, and celebrate achievements and milestones in cybersecurity awareness and compliance.
- Recognition and rewards can reinforce positive cybersecurity behaviors and incentivize employees to actively participate in cybersecurity initiatives. By promoting a culture of cybersecurity awareness, organizations create a resilient and security-conscious workforce capable of defending against evolving cyber threats effectively.

Regulatory frameworks play a critical role in shaping cybersecurity practices and ensuring that organizations prioritize the protection of their cyber-physical infrastructure. Here's an elaboration on each aspect:

1. *Enacting Laws and Regulations Mandating Specific Cybersecurity Measures:*

- Governments around the world have been enacting laws and regulations that require organizations to implement specific cybersecurity measures to protect their systems and data adequately. These measures may include requirements for implementing cybersecurity controls, such as firewalls, encryption, access controls, and multi-factor authentication.
- Regulatory mandates often specify minimum standards for cybersecurity preparedness and resilience across various sectors, such as finance, healthcare, energy, and critical infrastructure. Compliance with these regulations may be mandatory for organizations operating in regulated industries, with non-compliance resulting in penalties, fines, or other legal consequences.
- By mandating specific cybersecurity measures, regulators aim to raise the overall level of cybersecurity across industries, mitigate cyber risks, and protect critical infrastructure from cyber threats. These regulations provide organizations with clear guidelines on cybersecurity requirements and encourage them to invest in robust security measures to safeguard their systems and data.

2. *Requiring Organizations to Report Cyber Incidents Promptly:*

- Many regulatory frameworks require organizations to report cybersecurity incidents promptly to regulatory authorities, government agencies, or other relevant stakeholders. Prompt reporting enables timely response and mitigation efforts, facilitates information sharing and coordination among stakeholders, and helps prevent further harm or damage from cyberattacks.
- Reporting requirements may vary depending on the nature and severity of the cyber incident, with some regulations specifying specific timeframes for reporting and others requiring organizations to provide detailed incident reports and impact assessments. Failure to report cybersecurity incidents promptly may result in regulatory sanctions, reputational damage, and loss of trust from customers and stakeholders.
- By mandating prompt reporting of cyber incidents, regulators aim to enhance transparency, accountability, and situational awareness in cybersecurity matters. Timely reporting enables regulators to assess the scope and severity of cyber threats, identify emerging trends and patterns, and develop effective strategies for mitigating cyber risks and strengthening cyber resilience.

3. *Mandating the Adoption of Industry Standards and Best Practices for Cybersecurity:*

- Regulatory frameworks often mandate the adoption of industry standards and best practices for cybersecurity to help organizations establish a baseline level of security and compliance. These standards may include internationally recognized frameworks, such as the NIST Cybersecurity Framework, ISO/IEC 27001, or the Payment Card Industry Data Security Standard (PCI DSS).
- Compliance with industry standards and best practices helps organizations identify and address cybersecurity risks systematically, implement effective security controls and safeguards, and demonstrate adherence to recognized cybersecurity principles and guidelines.
- Regulatory mandates for adopting industry standards and best practices promote consistency, interoperability, and compatibility in cybersecurity practices across industries and sectors. They provide organizations with a common framework for assessing their cybersecurity posture, benchmarking against industry peers, and continuously improving their security posture over time.

Collaboration is essential in the realm of cybersecurity to effectively combat the ever-evolving landscape of cyber threats. Here's an elaboration on each aspect of collaboration:

1. *Facilitating Information Sharing Initiatives Between Organizations:*
    - Information sharing initiatives involve the exchange of threat intelligence, cybersecurity best practices, and incident data among organizations within and across industries. These initiatives aim to enhance situational awareness, enable early detection and response to cyber threats, and improve overall cybersecurity posture.
    - Information sharing can take various forms, including formal partnerships, industry consortia, information sharing and analysis centers (ISACs), and government-led initiatives. Participants share data on emerging threats, attack patterns, vulnerabilities, and mitigation strategies to collectively address common cybersecurity challenges.
    - By sharing timely and relevant threat intelligence, organizations can better understand the tactics, techniques, and procedures (TTPs) employed by cyber adversaries, anticipate potential threats, and implement proactive security measures to protect their networks, systems, and data.
2. *Encouraging Public-Private Partnerships to Coordinate Cybersecurity Efforts:*
    - Public-private partnerships bring together government agencies, private sector organizations, academic institutions, and other stakeholders to collaborate on cybersecurity initiatives, share resources, and address shared cybersecurity challenges.
    - These partnerships foster collaboration, coordination, and information sharing between the public and private sectors, leveraging the strengths and expertise of each stakeholder to enhance cybersecurity resilience and response capabilities.
    - Public-private partnerships may involve joint cybersecurity exercises, threat intelligence sharing programs, cybersecurity education and training initiatives, and collaborative research and development projects. By working together, stakeholders can more effectively identify and mitigate cyber threats, protect critical infrastructure, and promote national cybersecurity priorities.
3. *Coordinating with Government Agencies and Industry Partners to Enhance Collective Defense Against Cyber Threats:*
    - Government agencies play a crucial role in cybersecurity by providing leadership, expertise, and resources to address cybersecurity challenges at the national and international levels. Government agencies collaborate with industry partners, critical infrastructure operators, and cybersecurity organizations to enhance collective defense against cyber threats.
    - Collaboration with government agencies may involve sharing threat intelligence, participating in joint cybersecurity exercises and simulations, engaging in public-private information-sharing partnerships, and collaborating on policy development and advocacy initiatives.
    - By coordinating with government agencies and industry partners, organizations can access valuable resources, expertise, and support to strengthen their cybersecurity defenses, respond effectively to cyber incidents, and contribute to broader cybersecurity initiatives aimed at protecting national security, economic stability, and public safety.

XI. Conclusion

Pprotecting critical infrastructure is a top priority for both the US and Canada, with comprehensive strategies in place to enhance resilience against various hazards. Both countries emphasize collaboration, information exchange, and all-hazards risk management to achieve this goal. Through initiatives like the National Infrastructure Protection Plan in the US and the National Strategy for Critical Infrastructure in Canada, governments lead efforts to reduce vulnerabilities, improve threat detection, and enhance response capabilities nationwide. Collaboration across government agencies and industries is essential for effective emergency preparedness and response.

Furthermore, both the US and Canada recognize the importance of information sharing and analysis in enhancing cybersecurity resilience. While the US emphasizes sector-specific Information Sharing and Analysis Centers (ISACs), Canada focuses on Information Sharing and Analysis Organizations (ISAOs) to disseminate cyber threat intelligence effectively. The collaboration between the two countries under the Canada-U.S. Action Plan further enhances cross-border infrastructure resilience, acknowledging the interconnected nature of critical infrastructure and the necessity for a coordinated approach.

In addition to information sharing, strong private sector collaboration is vital in both countries, with efforts focused on avoiding wasteful duplication and promoting efficient resource utilization through sharing best practices. Effective communication with stakeholders is crucial for ensuring timely and accurate responses to critical infrastructure disruptions. The foundation of partnership, information sharing, and risk management drives infrastructure resilience efforts in both nations, with key initiatives facilitating joint efforts for resilience development.

Comprehensive approaches are crucial for governments to enhance the security of critical infrastructure effectively. Leveraging frameworks like the OECD Policy Toolkit on Governance of Critical Infrastructure Resilience provides valuable guidance, emphasizing collaboration among government officials, specialists, and stakeholders. By fostering partnerships and shared responsibilities, governments can strengthen critical infrastructure networks and address emerging risks more effectively. Through cross-national studies and workshops, the OECD facilitates the development of evidence-based policies, further enhancing the resilience of critical infrastructure worldwide.

Overall, protecting critical infrastructure requires a coordinated and multifaceted approach, with collaboration,

information sharing, and risk management at its core. By prioritizing these measures and leveraging international frameworks and partnerships, governments can effectively mitigate risks and ensure the safety, security, and continuity of essential services for society.

REFERENCES

[1] P.S. Canada, "Critical Infrastructure Resources," www.publicsafety.gc.ca, Dec. 21, 2018.

[2] C. S. Establishment, "Communications Security Establishment Annual Report 2022-2023," Communications Security Establishment, Jun. 29, 2023. I. S. Jacobs and C. P. Bean, "Fine particles, thin films and exchange anisotropy," in Magnetism, vol. III, G. T. Rado and H. Suhl, Eds. New York: Academic, 1963, pp. 271–350.

[3] Public Safety Canada. National Cyber Security Strategy.

[4] Canadian Centre for Cyber Security. Cyber Security in Canada.

[5] Government of Canada. Security of Canada Information Sharing Act.

[6] Government of Canada. Digital Privacy Act.

[7] Public Safety Canada. Critical Infrastructure Protection Program.

[8] University of Ottawa Centre for International Policy Studies. Assessing Canada's Critical Infrastructure Protection Policy.

[9] Canadian Global Affairs Institute. Cyber Security and Critical Infrastructure Protection in Canada.

[10] Conference Board of Canada. Enhancing Critical Infrastructure Resilience: A National Security Priority.

[11] Institute for Research on Public Policy. Strengthening Cybersecurity Governance in Canada: Lessons from Critical Infrastructure Protection.

[12] Canadian Security Intelligence Service. Cyber Threats to Canada's Critical Infrastructure.

[13] Canadian Cybersecurity Innovation Summit. Industry Perspectives on Critical Infrastructure Protection.

[14] Deloitte Canada. Strengthening Cybersecurity Resilience in Critical Infrastructure: Lessons Learned from Recent Incidents.

[15] Canadian Advanced Technology Alliance (CATA). Enhancing Public-Private Collaboration in Critical Infrastructure Protection.

[16] IBM Canada. Best Practices for Securing Industrial Control Systems in Critical Infrastructure.

[17] Cybersecurity and Infrastructure Security Agency (CISA). Cybersecurity Exercises and Incident Response: Lessons Learned from Canadian Critical Infrastructure Operators.

[18] World Economic Forum. Global Risks Report.

[19] World Bank Group. Infrastructure Resilience Trust Fund.

[20] United Nations Office for Disaster Risk Reduction. Global Assessment Report on Disaster Risk Reduction.

[21] Organization for Economic Cooperation and Development. OECD Reviews of Risk Management Policies.

[22] International Telecommunication Union. Global Cybersecurity Index.

[23] International Monetary Fund. Cybersecurity and Financial Stability: Lessons from Across Countries.

[24] United Nations International Strategy for Disaster Reduction. Making Cities Resilient: My City is Getting Ready.

[25] House of Commons Debates. Parliament of Canada.

[26] Standing Committee on Public Safety and National Security Hearings. Parliament of Canada.

[27] Speeches and Statements by Government Officials. Government of Canada.

[28] Testimonies and Expert Panels on Critical Infrastructure Protection. Canadian Centre for Cyber Security.

[29] Reports and Recommendations from Parliamentary Committees on Cybersecurity and Infrastructure Resilience. Government of Canada.

[30] CBC News. "Major Cyberattack Hits Canadian Infrastructure Sector."

[31] The Globe and Mail. "Report Warns of Vulnerabilities in Canada's Energy Infrastructure."

[32] Government of Canada News Release. "New Cybersecurity Regulations to Protect Critical Infrastructure."

[33] CTV News. "Experts Warn of Growing Cyber Threats to Canadian Financial Sector."

[34] The Toronto Star. "Public-Private Collaboration Key to Strengthening Infrastructure Resilience."

[35] National Post. "Cybersecurity Exercise Highlights Challenges in Protecting Critical Infrastructure."

[36] Global News. "Rising Cyber Threats Prompt Calls for Enhanced Infrastructure Resilience Measures."

[37] F. Chien, A. Anwar, C.-C. Hsu, A. Sharif, A. Razzaq, and A. Sinha, "The role of information and communication technology in encountering environmental degradation: Proposing an SDG framework for the BRICS countries," Technology in Society, vol. 65, p. 101587, May 2021.

[38] R. R. Das, M. Martiskainen, L. M. Bertrand, and J. L. MacArthur, "A review and analysis of initiatives addressing energy poverty and vulnerability in Ontario, Canada," Renewable and Sustainable Energy Reviews, vol. 165, p. 112617, Sep. 2022.

[39] F. J. Egloff and M. Smeets, "Publicly attributing cyberattacks: a framework," Journal of Strategic Studies, pp. 1–32, Mar. 2021.

[40] European Observatory on Health Systems and Policies, G. P. Marchildon, S. Allin, and S. Merkur, "Canada: Health system review," Health Systems in Transition, vol. 22, no. 3, 2020.

[41] M. B. Johnson and M. Mehrvar, "Winery wastewater management and treatment in the Niagara Region of Ontario, Canada: A review and analysis of current regional practices and treatment performance," The Canadian Journal of Chemical Engineering, vol. 98, no. 1, pp. 5–24, Nov. 2019.

[42] W. Liu and Z. Song, "Review of studies on the resilience of urban critical infrastructure networks," Reliability Engineering & System Safety, vol. 193, p. 106617, Jan. 2020.

[43] M. Nesbitt, "Violent crime, hate speech or terrorism? How Canada views and prosecutes far-right extremism (2001–2019)," Common Law World Review, vol. 50, no. 1, p. 147377952199155, Feb. 2021.

[44] A. S. Wilner, H. Luce, E. Ouellet, O. Williams, and N. Costa, "From public health to cyber hygiene: Cybersecurity and Canada's healthcare sector," International Journal: Canada's Journal of Global Policy Analysis, vol. 76, no. 4, p.100, Feb. 2022.

[45] M. J. Roper, "Protecting Canada's Critical Infrastructure One Byte At A Time," Canadian Forces College, 2014.

[46] g. o. Canada, "Public Safety Canada," 21 07 2022. [Online]. Available: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/srtg-crtcl-nfrstrctr/index-en.aspx.

[47] A. Graham, Canada's Critical Infrastructure: When is Safe Enough Safe Enough?, Ottawa: Macdonald-Laurier Institute, 2012.

[48] N. S. A. I. C. O. Parliamentarians, " Special Report on the Government of Canada's Framework and Activities to Defend its Systems and Networks from Cyber Attack," National Security and Intelligence Committee of Parliamentarians, Ottawa, 2022.

[49] G. o. Canada, "Canada's Cyber Security Strategy (For a stronger and more prosperous Canada)," Government of Canada, Canada, 2010.

[50] An Emergency Management Framework for Canada-Third Edition. Available: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2017-mrgnc-mngmnt-frmwrk/index-en.aspx

[51] Emergency Management for Canada: Toward a Resilient 2030. Available: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/mrgncy-mngmnt-strtgy/index-en.aspx

[52] Emergency Preparedness. Available: https://www.publicsafety.gc.ca/cnt/mrgnc-mngmnt/rspndng-mrgnc-vnts/gvrnmnt-prtns-cntr/prprdnss-en.aspx

[53] Government Operation Center. Available: https://www.publicsafety.gc.ca/cnt/mrgnc-mngmnt/rspndng-mrgncvnts/gvrnmnt-prtns-cntr/index-en.aspx

[54] Search and Rescue Policies and Program. Available: https://www.publicsafety.gc.ca/cnt/mrgnc-mngmnt/rspndng-mrgnc-vnts/nss/index-en.aspx

[55] Disaster Assistance Program. Available: https://www.publicsafety.gc.ca/cnt/mrgnc-mngmnt/rcvr-dsstrs/dsstrssstnc-prgrms/index-en.aspx

[56] National Cyber Security Action Plan. Available: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrtstrtg-2019/index-en.aspx#a03

[57] Emergency Management Framework Ontario https://www.ontario.ca/document/emergency-management-framework-ontario/components-emergencymanagement

[58] Public-Private Partnerships are No Silver Bullet: An Expanded Governance Model for Critical Infrastructure Protection, Myriam Dunn Cavelty, Manuel Suter

[59] Cybersecurity and Critical Infrastructure Protection, James A. Lewis

[60] Public-Private Partnerships (PPPs): Definition, How They Work, and Examples, The Investopedia Team

[61] Support of public–private partnerships in health promotion and conflicts of interest, Ildefonso Hernandez-Aguado and G A Zaragoza

[62] Public-private partnerships in national cyber-security strategies, Madeline Carr

[63] Network governance and collaborative governance: a thematic analysis on their similarities, differences, and entanglements, Huanming Wang, Bing Ran

[64] Smooth Operators, Predictable Glitches: The Interface Governance of Benefits and Borders, Jennifer Raso

[65] National Strategy for Critical Infrastructure, Public Safety Canada

[66] Threats to Canada's Critical Infrastructure, Public Safety Canada

[67] Renewing Canada's Approach to Critical Infrastructure Resilience, Public Safety Canada

[68] Protecting Canada's Critical Infrastructure on byte at a time, Major J.A. Roper

[69] Critical Infrastructure Partners, Public Safety Canada

[70] National Cross Sector Forum 2021-2023 Action Plan for Critical Infrastructure, Public Safety Canada

[71] Enhancing Critical Infrastructure Resiliency, Public Safety Canada

[72] ction Plan for Critical Infrastructure, Public Safety Canada

[73] Emergency Management Strategy for Canada: Toward a Resilient 2030, Public Safety Canada

[74] Information Sharing and Protection under the Emergency Management Act, Public Safety Canada

[75] Canada-United States Action Plan for Critical Infrastructure, Public Safety Canada

[76] New Canadian Action Plan for CIs, European Union

[77] Filipe Dinis: Collaboration is key to mature the resilience of Canada's critical infrastructure, Filipe Dinis, Published Jul 18, 2022

[78] Good Governance for Critical Infrastructure Resilience, OECD, Published on April 17, 2019

[79] The Toolkit for Risk Governance, OECD

[80] Protecting Critical Infrastructure, CISA

[81] Critical Infrastructure Sectors, CISA

[82] The Critical Need to Improve Cyber Security of Cyber-Physical Systems (CPSs), Cetark Corp, April 4, 2023

[83] National Infrastructure Protection Plan, Homeland Security