Government of Canada | Gouvernement du Canada

Office of Critical Infrastructure Protection and Emergency Preparedness

Bureau de la protection des infrastructures essentielles et de la protection civile

THREAT ANALYSIS

Number: TA03-001
Date: 12 March 2003

Threats to Canada's Critical Infrastructure

Purpose
The purpose of this paper on *Threats to Canada's Critical Infrastructure* is to provide a taxonomy of the **natural**, **accidental** and **malicious** threats that have been identified as those most likely to impact upon Canada's national critical infrastructure. The paper will aim to provide informed forecasting for the relative probability of these threats and hazards.

Audience
This report is primarily intended to provide owners and operators of Canadian critical infrastructure (CI) with baseline information regarding potential threats to their networks and systems. Owners and operators are the acknowledged experts with regard to the vulnerabilities they confront, but many have indicated that there is a lack of credible information regarding threats.

Emergency managers in the public and private sectors could also employ this report to enhance their understanding of the variety of threats and hazards which the Government of Canada is addressing.

Finally, policy makers at all levels of government may use the paper as a jumping-off point to examine threats and vulnerabilities in CI sectors within their constituencies.

Note: For the purposes of this paper the terms "**threats**" and "**hazards**" will be used interchangeably to describe the independent variables which affect existing vulnerabilities to produce risk/disaster scenarios.

For comments on this product, or for general information, please contact OCIPEP's Communications Division at:

Phone: (613) 944-4875 or 1-800-830-3118
Fax: (613) 998-9589
Email: communications@ocipep-bpiepc.gc.ca
Web Site: www.ocipep-bpiepc.gc.ca

Notice to readers
OCIPEP publications are based on information obtained from a variety of sources. The organization makes every reasonable effort to ensure the accuracy, reliability, completeness and validity of the contents in its publications. However, it cannot guarantee the veracity of the information nor can it assume responsibility or liability for any consequences related to that information. It is recommended that OCIPEP publications be carefully considered within a proper context and in conjunction with information available from other sources, as appropriate.

Any suspected criminal activity should be reported to local law enforcement organizations. The RCMP National Operations Centre (NOC) provides a 24/7 service to receive such reports or to redirect callers to local law enforcement organizations. The NOC can be reached at (613) 993-4460. National security concerns should be reported to the Canadian Security Intelligence Service (CSIS).

EXECUTIVE SUMMARY

- Canada is growing increasingly *dependent* upon the collection of products and services that make up our domestic critical infrastructure (CI) network. Those sectors, in turn, are becoming increasingly *interdependent*, as telecommunications and cyber elements continue to underwrite them. These two factors combined make us more vulnerable to threats from **natural**, **accidental** and **malicious** threats to our CI.

- **Risk** is assessed as a combination of **threat** (expressed as the probability that a given action, attack, or incident will occur), **vulnerability** (expressed as the probability that a given attack, or vulnerability will succeed, given that the action, attack or incident occurs), and **consequence** (expressed as some measure of loss, such as dollar cost, resources loss, programmatic impact, etc.). The total risk of operating a system is assessed as a combination of the risks associated with all possible threat scenarios. Risk is reduced by *countermeasures*. However, the cost of countermeasures (relative to the potential risks) is applied when arriving at any holistic risk management strategy.

- Four factors contribute to Canada's vulnerability to the broad spectrum of threats. First, Canada's population, built environment, and wealth, are increasingly concentrated in a small number of highly vulnerable areas and many such communities are at risk from multiple hazards. Second, climate change could increase the frequency and severity of extreme weather events. Third, Canada's built environment is aging and is more susceptible to damage. Fourth, communities are increasingly more reliant on advanced technologies that are frequently disrupted during disasters.

- Traditionally, the Canadian government has viewed infrastructure protection in the context of physical security and the protection of physical assets. The basis of this activity was the Vital Points Programme (VPP), established in 1938 to identify and protect facilities and services critical to the national interest. The Government of Canada's ability to gauge threats to CI has traditionally been contingent upon an ability to evaluate the *intent* of an actor, coupled with their *capability* to carry out a deliberate action. This process was significantly easier when dealing purely in the physical realm. However, with the advent of cyber-based threats, threat agents are diffuse in nature, and the capacity to inflict significant damage is readily available and relatively easy to use by those with even a cursory knowledge of and ability with computer technologies.

- The ongoing phenomenon of climate change is altering our capacity to effectively manage the risks associated with natural disasters. Moreover, it is affecting Canada in particularly distinct ways. In the past 10 years, Canada has faced the greatest increases in average annual temperatures of any country, and a commensurate rise in severe weather-related natural disasters. Associated with these shifts has been an increased occurrence of phenomena such as severe storms, floods, droughts and forest fires.

Natural Hazards Threats to Canadian CI

- Natural disasters have accounted for 69.9 percent of all disasters in Canadian history. Flooding has been, by far, the greatest cause of disasters in Canada in the 20th century, followed by severe storms.
- Geomagnetic storms, earthquakes, forest fires, tsunamis and health-related epidemics all represent significant natural hazard threats to Canadian CI.
- In recent years, the death toll due to natural disasters in Canada has decreased, while the economic costs of the damage has increased. The trend is possibly the result of two divergent factors. The response to natural disasters has become more sophisticated and better coordinated among all the partners, while the cost of securing our domestic infrastructure has risen greatly as the Canadian CI network becomes more complex and interconnected.
- Trends in the number of annual natural hazard-related threats should continue along an upward trend.

Accidental Threats to Canadian CI

- Accidents are, by definition, unforeseen. It is, therefore, difficult to predict future trends in accidents involving the critical infrastructure.
- Accidents involving CI generally involve human-error, mechanical failures and computer programming errors.
- With the increased scrutiny in both the public and private sectors on critical infrastructure protection and business continuity planning, accidental threats to CI are less likely than ever before. CI robustness has been reinforced in virtually all sectors, and where the primary infrastructure has been deemed vulnerable, redundancies have been built in. These measures have made most CI sectors less prone to the negative impacts of accidents on CI facilities and networks.
- The negative impact resulting from accidents involving CI elements should continue along a downward trend.

Malicious Threats to Canadian CI

- Infrastructure has long been a target for malicious attack, whether for criminal, military or political purposes.
- There are a range of actors, employing a range of tools (from conventional weapons, weapons of mass destruction - including chemical, biological radiological and nuclear agents, to cyber tools) who have displayed a willingness to engage in malicious activity directed to cyber and physical CI.
- The September 11 attacks have served to heighten our awareness of the threats to, and potential vulnerabilities within, Canada's physical and cyber infrastructure (and the nexus points where the two interconnect).
- Cyber crime and the criminal and terrorist use of information technology are significant issues for law enforcement. A sophisticated information infrastructure, a large pool of potential hackers within the country and heavy reliance on computer-based CI are all factors in making computer-based crime a serious threat to Canada. However, currently there is a limited ability on the part of federal and provincial government departments and agencies to collect, collate, analyze and synthesize the modest amount of substantive qualitative information on actors, their actual and potential capabilities, intended targets, and recorded attempts to penetrate or attack assets or systems.

- The Water, transportation and oil pipeline systems make appealing targets, given their diffuse nature and the difficulty of effectively protecting them from attack.
- In spite of attempts to secure these systems, the threat of a malicious attack on CI could increase. Canadian society relies on these networks, services and systems to increasing degree, thus making them ever more attractive targets.

- Responsibility for emergency measures, including CIP, in Canada is shared among all three levels of government. The federal government provides national leadership and coordinates the overall CIP effort. Those agencies with mandates that incorporate CIP are listed in Annex A.

TABLE OF CONTENTS

INTRODUCTION

Canada's CI consists of those physical and information technology facilities, networks and assets, which if disrupted, damaged, manipulated or destroyed, would have a serious impact on the health, safety, security or economic well-being of Canadians or the effective functioning of governments in Canada. Our national CI is made up of six sectors comprising: ***energy and utilities*** (such as electrical power and, natural gas and oil transmission systems); ***communications*** (such as telecommunications and broadcasting systems); ***services*** (such as financial services, food distribution and health care); ***transportation*** (including air, rail, marine and surface); ***safety*** (such as nuclear safety, search and rescue and emergency services); and ***government services*** (including major government facilities and information networks or assets). Together, these sectors constitute a complex web of interconnected, interacting services and people that underlie every social and economic activity in the country. As Canada continues to develop as a modern, urban, technology-driven society, our dependence on this web of services will increase exponentially. Moreover, each sector is, in varying degrees, dependent on the others. As our economy and society become more sophisticated, the growing interdependence between different sectors makes us more vulnerable to threats from natural, accidental and malicious sources.

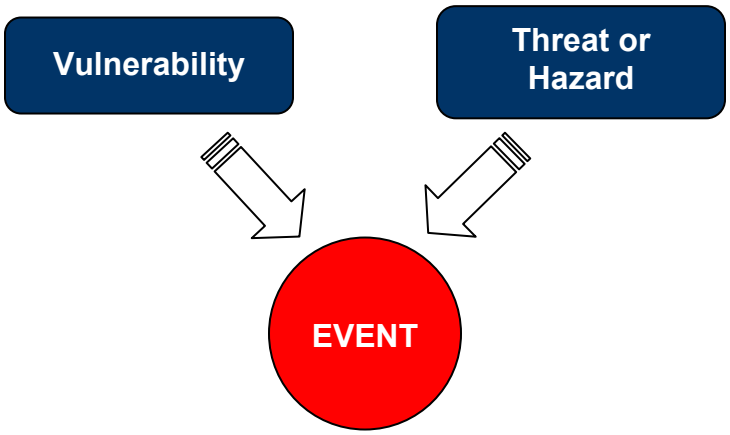
The telecommunications sector is generally regarded to be the backbone of CI in Canada underpinning in very meaningful ways the transportation, banking and finance, and electrical power sectors. Uninterrupted communication of data is essential to conduct government operations, emergency services and commerce. Canada's information dependence, combined with increasing vulnerabilities, a decreasing number of infrastructure nodes and links, and the growing capabilities and willingness of malicious actors to conduct physical and cyber attacks, has made telecommunications and information systems attractive and lucrative targets. These concepts will be developed more fully in the malicious threat portion of this paper.

Responsibility for emergency measures, including CIP, in Canada is shared among all three levels of government. The federal government provides national leadership and coordinates the overall CIP effort. Individual industries have working groups and committees examining protection of their own infrastructures, and there is close liaison with the government agencies responsible for infrastructure protection.

THREAT + VULNERABILITY + CONSEQUENCE = RISK

The terms threat, vulnerability and risk have often been used casually and interchangeably, when in fact they each have distinct and complementary definitions. Figure 1.0 below illustrates how threats and vulnerabilities interact.

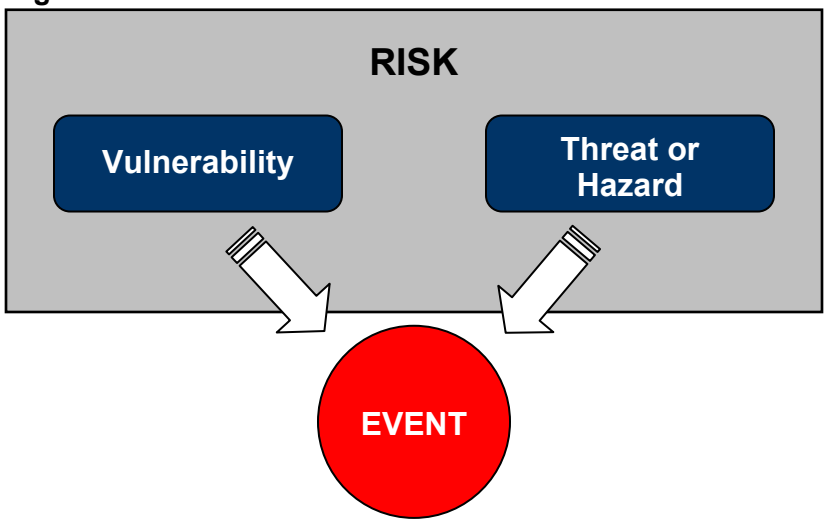
Figure 1.0



Thus, it is the coming together of a specific threat with a corresponding vulnerability that produces the potential for harm or disaster. As an example, ice storms can be a serious threat to power distribution lines, as was experienced in Ontario and Quebéc in 1998. The power grid damage occurred because the distribution towers were vulnerable to breaking from the enormous weight of built-up ice. Had the towers been sturdier, or if the cables had been buried, this vulnerability would have been removed, and the threat (the ice storm itself) would not have caused power outages. Another example would be a computer virus that attacks a specific software product. A computer might become infected with the virus (the threat), but its impact will only be fully realized if the computer is running the targeted software product (the vulnerability); if not, the virus could do nothing at all.

A vulnerability to a threat does not necessarily mean that it will cause harm/damage. For example, many homes are built in low-lying areas (the vulnerability) that would flood if a river overflowed its banks (the threat). But decades could go by without a flood ever occurring and any damage being done. Thus, the convergence of a threat with a vulnerability, combined with the knowledge or appreciation of a harmful consequence which might emanate from them, produces the potential for harm; this scenario is referred to as *risk* (see Figure 1.1).

Figure 1.1



Private and public sector organizations who employ risk management methodologies generally adopt a four-stage model:

1. **Preparedness** – This stage includes those steps taken in advance of an event to prepare for its occurrence, including the development effective policies, response plans and procedures for how best to manage an emergency; the purchasing and stockpiling of emergency supplies; and the comprehensive training and exercising by emergency responders. The steps taken in the preparedness stage should be aimed at reducing the impacts and losses from inevitable failures or disruptions in the future.

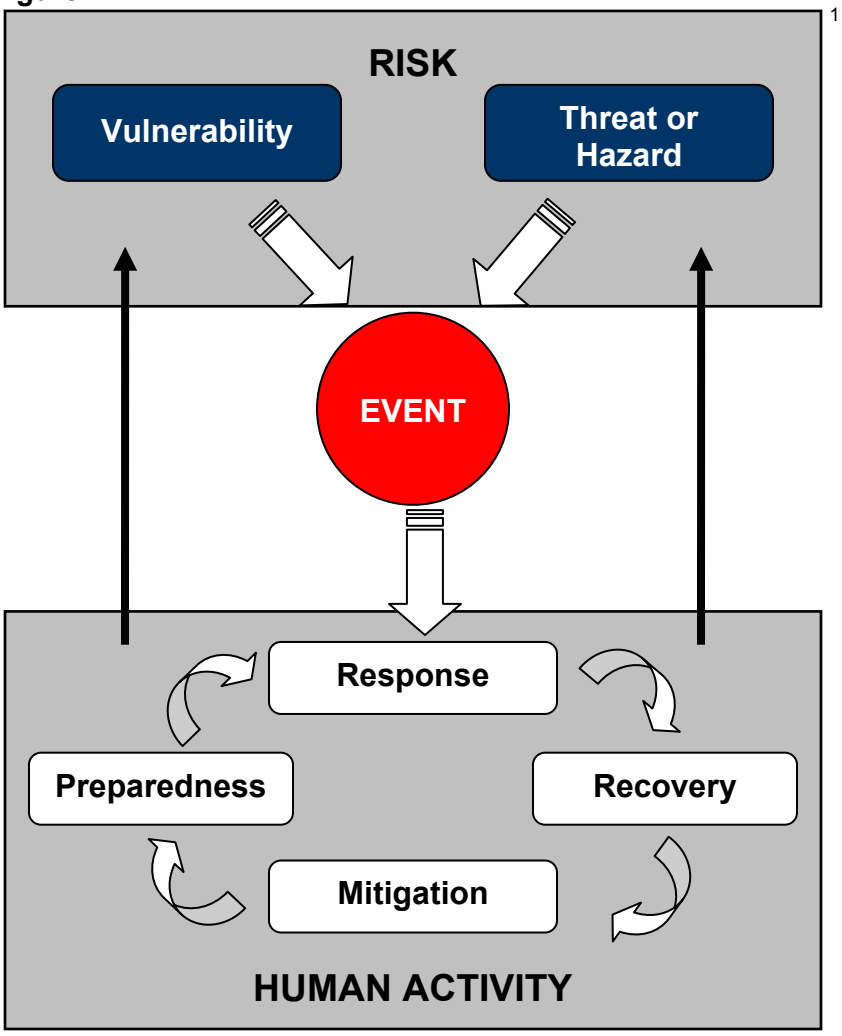
2. **Mitigation** – This stage involves applying a series of sustained actions to reduce or eliminate the long-term impacts and risks associated with natural and human-induced disasters. Mitigation plans usually specifically address a vulnerability (such as restricting homebuilding in flood plains) or a threat (actively seeking out and capturing terrorists).

3. **Response** – When an event takes place, damage and harm can be minimized by responding quickly and in a coordinated fashion. Response activities are typically handled by our first responders (fire fighters, police, ambulance services), but in serious emergencies other agencies and levels of government can also become involved.

4. **Recovery** – The recovery stage includes those efforts taken to repair and restore communities after an emergency. Once the immediate situation is stabilized, the affected community or organization needs to recover from the incident and rebuild. These activities are necessary to ensure the long-term viability of the community or organization and to prevent what in some cases can be serious long-term economic harm.

All these activities together serve to reduce the overall risk of harm. The entire process is illustrated below in Figure 1.2.

Figure 1.2



[1]

Comprehensive emergency management plans come with associated costs. These costs can include both financial and "opportunity costs", or the costs of choosing one potential option over another based on a series factors. Understanding the full ramifications of these costs is essential in arriving at a complete risk management strategy.

For example, in the wake of the 1998 Ice Storm, many commentators suggested that underground cables would have limited the storms economic impact. Ontario Hydro does in fact install underground cables in locations where an overhead routing is not possible. This means the majority of installations are within major urban areas including Ottawa, Toronto, Hamilton, London and Thunder Bay and new cables are being installed to service Windsor. Today, there are over 245 circuit kilometres of 115 and 230 kilovolt underground cable in operation. However, these installations generally cost about five to ten times more than an overhead line with a similar capacity.[2]

1 Etkin, David. "Risk transference and related trends: driving forces towards more mega-disasters." Environmental Hazards 1 (1999), pp. 69-75. Elsevier Science Ltd.

[2] Ontario Hydro ICE Report, pg. 75.

Table 1.0 – Unit Costs for Overhead Transmission lines

Voltage	Unit Cost for 2-circuit Overhead Lines per kM[1]
500 kV	$1.3 million
230 kV	$1.0 million
115 kV	$0.5 million

While the advantages of underground cables are many, (notably: increased public and personnel safety and reduced outage frequencies) there are also corresponding disadvantages. Cable faults are costly to repair and difficult to locate. As a result, underground systems have lower outage frequencies, but the duration of an outage once it occurs is typically much longer than on an equivalent overhead system. Outage times to find faults and repair them typically range from 8–48 hours or longer.[3]

Table 1.1 – Estimated Costs for Underground Transmission lines[4]

Voltage	Circuit-kM Affected	Unit Cost per kM for a two-circuit cable installation [1] (Compensation included)	Estimated replacement cost using cables (Eastern Ontario)
500 kV	360	$15 million	$ 2,700 million
230 kV	700	$5 million	$1,750 million
115 kV	400	$3 million	$600 million
		TOTAL	$ 5,050 million

Note: 1 The unit costs for the underground cable installations assume two circuits are installed simultaneously to minimize excavation and installation costs.

Prior to the 1998 Ice Storm, Hydro One (formerly Ontario Hydro) officials believed that their transmission towers had been built well above standard, in terms of their weight bearing capacity. Few emergency managers would have predicted the enormity of the weight of the ice that accumulated or the cascading effect of conductor, poles and tower collapses. Some experts have retroactively compared the stress incurred by the transmission towers as a result of the ice accumulation to the World Trade Center building collapses. At some point, the cost of prevention becomes far greater than the probability of risk or failure. The same principle applies to the burying of electrical cables. Eventually the costs of maximum prevention can, in some cases, be so onerous as to make the entire process unfeasible.[5]

THREAT IDENTIFICATION & ANALYSIS

Threat analysis is a key component in the management of CIP. Traditionally, the Canadian government has viewed infrastructure protection in the context of physical security and the protection of physical assets. The basis of this activity was the Vital Points Programme (VPP), established in 1938 to identify and protect facilities and services critical to the national interest. The nature and magnitude of physical threats

[3] Ibid.
[4] Ibid.
[5] Derived from discussions with Hydro One Networks Inc. officials, 17 January 2003.

have evolved relatively slowly over time allowing for the establishment of indicator and warning mechanisms.

However, the Government of Canada's ability to gauge threats to CI has traditionally been contingent upon an ability to evaluate the *intent* of an actor, coupled with the *capability* to carry out a deliberate action. This was significantly easier when dealing purely with securing the physical realm. However, with the advent (and growing prevalence–let alone aptitude) of cyber-based threat actors, the threats are more broad in nature, and the capacity to inflict significant damage is readily available and relatively easy to use by those with even a cursory knowledge of, and ability with, computer technologies.

The threat environment can be defined by the interaction of the infrastructure elements and the threat agents. Table 1.0 demonstrates how complex the relationship has become. The means of attack or incident can be both physical-based and cyber-based. The target can be cyber, such as the information or applications on a network, or physical, such as a telecommunications cable. In reality, it is becoming increasingly difficult to distinguish between purely physical and cyber components of the infrastructure.

Table 2.0

The CI Threat Environment

		M E A N S	
		PHYSICAL-BASED	***CYBER-BASED***
T A R G E T	***PHYSICAL***	- Bombing a hydro tower - Severing a telecommunications cable with a backhoe - An explosion at an oil refinery - Ice storm debilitating Hydro towers	- Hacking into the SCADA[6] system that controls municipal sewage and water – indirect physical impact. - Geomagnetic storms affecting CI elements
	CYBER	- Use of electromagnetic pulse and radio-frequency weapons to destabilize electronic components.	- Hacking into a critical government network - Penetrating the SS7[2] telecommunications transmission controls

Four factors contribute to Canada's vulnerability to the vast spectrum of threats. First, Canada's population, built environment and wealth, are increasingly concentrated in a small number of highly vulnerable areas, and many such communities are at risk from multiple hazards. Second, climate change could increase the frequency and severity of extreme weather events. Third, Canada's built environment is aging and is more susceptible to damage. Fourth, communities are increasingly more reliant on advanced technologies which are frequently disrupted during disasters.

[6] Supervisory Control and Data Acquisition (SCADA) and Signal System 7 (SS7) are operations control systems that are prevalent in critical infrastructure.

Using the lessons learned from the 1998 Ice Storm, the Saguenay and Red River floods, in conjunction with the preparations for the Y2K roll-over, the Government of Canada felt that CIP needed to be viewed through a new prism. The more established concepts and precepts of emergency management would be dovetailed with the CIP. The so-called "four pillars" of the emergency management continuum (mitigation, preparedness, response and recovery) effectively complement those of the critical infrastructure protection continuum (protection, detection, response, recovery). This means that almost any event that can threaten national CI, whether a flood, tornado, a terrorist bomb or hacker attack, also can pose a threat to people and property, and could potentially require an emergency response. In short, good CIP is part of good emergency management broadly conceived, and good emergency management provides an envelope of support to effective CIP. The mandate of the Office of Critical Infrastructure Protection and Emergency Preparedness (OCIPEP) addresses these dual responsibilities.

OCIPEP's "all hazards" approach goes deeper than merely the conjoining of EM and CIP philosophies. It also means that the organization reacts and responds to **natural**, **accidental** and **malicious** threats which could impact upon Canada's CI. The following sections will provide a general taxonomy of these threats. In addition to listing those threats which the organization perceives to be most likely, or those where public understanding of the threats are limited (i.e. geomagnetic storms), these sections (where available) will provide some historical trend analysis which will allow for educated inferences as to future probability of the threats.

NATURAL THREATS

HISTORY

Canada's size, varied topography and relatively severe weather patterns make it particularly susceptible to the occurrence of natural disasters. Individuals, communities, and local, provincial and federal governments, face increased risk of death, suffering, destruction, and cost from disasters, not only as a result of the potential increase in frequency of disaster events, but also increased exposure to risk.

This section will examine those natural phenomena that have the potential to result in disastrous situations in Canada. Most noteworthy are floods, severe storms (including severe winter storms such as ice storms and hail storms, hurricanes and oft-accompanying tornadoes, geomagnetic storms, earthquakes and tsunamis, fires, and epidemics (including West Nile virus, and Foot and Mouth disease).

Natural disasters can have a significant impact on CI elements in a short period of time. The primary point of impact tends to be the physical infrastructure, such as hydro lines and bridges. Damage is not always localized, often resulting in a ripple effect across a number of sectors. The ice storm in Central and Eastern Canada in 1998 is an excellent example of the degree of damage that can occur in a short time period.

According to the Canadian Disaster database, natural disasters have accounted for 69.9 percent of all disasters in Canadian history.[7] Flooding has been, by far, the greatest cause of disasters in Canada in the 20th century, followed by severe storms. Although natural disasters are necessarily prompted by a severe *natural* phenomenon, it must be iterated that human impact on the environment can play a significant role in both the prevalence and scope of certain natural disasters. The ongoing phenomenon of climate change, unless addressed by concerted human action, will inevitably, and significantly, alter our capacity to effectively manage the risks associated with natural disasters.

Canada could also be susceptible to epidemic threats to its social and economic fabric: West Nile virus and Foot and Mouth disease are currently considered to be significant threats. Currently, smallpox and anthrax are considered to be low level threats.

NATURAL THREATS TO CANADIAN CRITICAL INFRASTRUCTURE

Climate Change and its Potential Impact upon Canadian Critical Infrastructure

In recent years, the world has experienced increasingly dramatic shifts in climate. This phenomenon is affecting Canada in distinct ways. In the past 10 years, Canada has faced the greatest increases in average annual temperatures of any country,[8] and a commensurate rise in severe weather-related natural disasters. Associated with these shifts has been an increased occurrence of phenomena such as severe storms, floods, droughts and forest fires. These occurrences have led to higher maintenance, clean-up and insurance costs. "Conservative estimates indicate that Canadians currently spend in excess of $12 billion per year in coping with and adapting to weather and climate."[9] These costs are becoming increasingly exacerbated by the ongoing phenomenon of global climate change.

"Scientists predict that the warming will not be evenly distributed and that the polar regions and inland temperate zones, such as the Canadian prairies, will experience even higher temperatures and in some regions, less precipitation. Warmer temperatures will gradually cause polar ice to melt. Combined with the expansion of ocean water due to warmer water temperatures, sea levels could rise to a level that will threaten coastal areas and small island nations. As well, with more thermodynamic energy in the global system, there will likely be an increase in occurrences of extreme weather events, leading to threats to human safety and property damage. Climate change can be argued to be the most pervasive and far-reaching environmental issue ever dealt with by the international community."[10]

Climate change will affect the frequency and severity of extreme weather events in several ways. First, it is believed that the additional warming will change the distribution

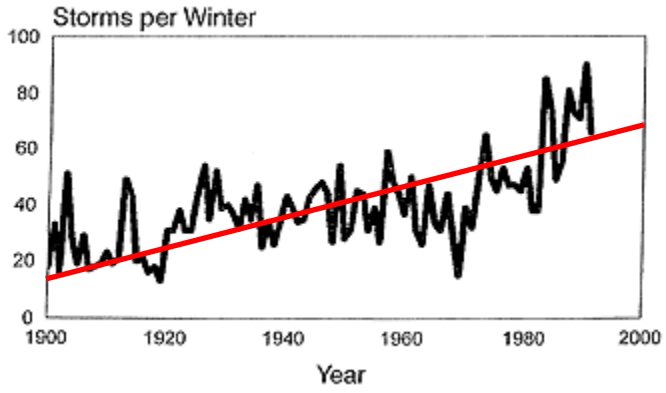
[7] http://www.ocipep.gc.ca/disaster/default.asp
[8] Environment Canada, *The Science of Climate Change*, Apr. 2001, 24. Online at www.msc.ec.gc.ca/saib/climate/Climatechange/CC_presentation_e.PDF
[9] Environment Canada. "CO2/Climate Report" Fall 2002 Issue. Pg. 4.
[10] James Bruce, Ian Burton, Mark Egener. "Disaster mitigation and preparedness in a changing climate." May 1999

of heat and thus the flow of energy through the climate system. This in turn, will alter the circulation patterns of the atmosphere and the oceans, and it will also modify the hydrological cycle by which water is circulated between the Earth's surface and the atmosphere. As a result, the position of many of the world's major storm tracks could shift significantly.[11]

Secondly, it is expected that a warmer climate would affect the physical processes that generate different types of extreme weather events. A virtually certain outcome of a rise in global temperature is a widespread increase in the amount of water that is moved through the hydrological cycle. Consequently, more moisture will be available in the atmosphere to fall as rain or snow. General circulation models indicate that a warmer atmosphere will increase the amount of moisture transported into the middle and high latitudes of the Northern Hemisphere. These models also suggest that the additional precipitation will likely occur in heavier falls rather than in more days of precipitation. Moreover, these models seem to suggest that the number and intensity of severe thunderstorms will increase in most areas in a warmer climate.[12]

Determining changes in frequency and severity of Northern Hemispheric storms is fraught with difficulty because a number of different criteria of intensity can be used (e.g.: central atmospheric pressure, strongest winds, heavy rains, etc.), each presenting problems in obtaining long-term consistent sets of data or weather maps. However, of particular interest to Canadians is a reported marked increase since the 1970s of very intense winter storms in the Northern Hemisphere (see Figure 2.0). In eastern North America, seven of the eight most intense storms that developed in the past 50 years occurred in the most recent 25-year period.

Figure 2.0 – Frequency of Intense Winter Storms in the Northern Hemisphere[13]



For tropical cyclones and hurricanes (many of which impact upon Canada's coastal region's–see 2002 super-typhoon Pogsona which hit Guam in December 2002 and resulted in hurricane force winds off the coast of B.C.), data from the World Meteorological Organisation (WMO) yields no evidence of changes in frequency and intensity on a global basis. At the same time, the frequency of North Atlantic hurricanes declined over the period 1970–1987, while those in the western Pacific increased. These changes are much more likely to be due to the relatively persistent warm El Niño

[11] Ibid.
[12] Ibid.
[13] Ibid.

Southern Oscillation (ENSO) events of the past two decades, than due to greenhouse forcing of climate. ENSO events tend to depress Atlantic hurricane activity and change the distribution of tropical cyclones in the Pacific.

Other small-scale, intense disturbances such as tornadoes have notoriously serious reporting difficulties, but increased frequency of tornadoes on the Canadian Prairies appears to be related to above normal spring and summer temperatures, increasingly evident in the past two decades. These changes in the average temperatures seem to imply that the number of tornadoes might increase in the Canadian Prairies as a result of climate change.[14] This hypothesis has been studied in a seminal work by Etkin, and his findings concluded that there was a positive correlation between the generally accepted outcomes of ongoing climate change and an increase in tornado activity.

Wildfire increases in Yellowstone National Park from 1985–1990 have occurred as a result of trends in climatic conditions. In the boreal forests of central and northwestern Canada, the area annually disturbed by fire and insects has doubled in the past two decades compared to the previous 50-year period. This is related to statistically significant winter, spring and summer warming trends and probably more lightning. Other factors such as tree age, and fire fighting policy also could have contributed to this increase.[15]

Different regions of Canada can be affected by rainstorm floods, ice-jam floods and snowmelt floods. A shorter winter season under climate change may result in a reduced risk of snowmelt and ice-jam floods. The main concerns about increased flooding result from the fact that a warmer atmosphere can hold more moisture, and precipitation is expected to increase as a result. As well, the precipitation is expected to become more intense over smaller areas, which suggests greater flooding problems especially in smaller catchment areas.[16]

Conversely, regarding droughts, the concern is that with an increase in heavier rainfall events, the number of dry days between events may increase and drought will become more severe. This effect could be worsened by higher air temperatures and increased evaporation. Some general circulation model studies show reduced soil moisture values over the mid-North American continent, suggesting more frequent droughts in the future. For floods and droughts, other forms of change such as land use are also important factors in the changing severity of extreme weather events. For example, the reduction of woody vegetation, the urbanization of watersheds, increased areas of impermeable surfaces for highways and some other land use changes increase the amount of precipitation that quickly becomes surface runoff. Small rivers and streams in affected regions became increasingly "flashy" with higher peak floods and less flow in dry periods.

[14] Etkin, D. "Beyond the Year 2000. More Tornadoes in Western Canada? Implications from the Historical Record." Natural Hazards. V. 12 1995. pg. 27.
[15] Apps, M.J. et al. Boreal Forests and Global Change. Kluwer Academic Publishers, Dordrecht,. 548 pgs. 1995.
[16] White, R. & Etkin D. "Climate Change and the Canadian Insurance Industry." Natural Hazards. 16: 135-163, 1997.

Flood Trends in Canada

According to the Canadian Disaster database[17], the twelve provinces and territories experienced 204 reported major flooding situations between 1900 and 2002. About 58 percent of these floods have occurred in four provinces: Ontario (44 events), New Brunswick (29 events), Quebéc (27 events) and Manitoba (22 events).[18]

Flooding in Canada has resulted directly and indirectly in the deaths of at least 198 people and over several billion dollars of damage during the 20th century. Although floods can occur in every month of the year, about 40 percent occur in April and May, when several common flood mechanisms (e.g.: snowmelt runoff, storm rainfall and ice jams) are likely to occur concurrently, thereby increasing the likelihood of high water flows.

The Canadian Disaster database suggests that the number of flood disasters has increased through the 20th century with about 78 percent occurring after 1959.[19] This trend likely reflects several factors, perhaps most notably the shift in climate, although more accurate reporting of consequential flooding has also played a role. Also, during the 20th century, there has been an increase in the development of flood-prone lands due to the growth of Canada's population.[20] Urban sprawl places increasing strain on untested water and waste management infrastructure.

The Saguenay floods of 1996 are considered to have been the worst in Canadian history. These floods caused 10 deaths; destroyed 1,718 houses and 900 cottages; displaced 16,000 people; and resulted in $800 million in damages. The Red River flood of the following year was comparatively less severe, in large part due to the mitigating impact of the Red River floodway. Constructed in the 1960's at a cost of $60 million, the floodway has been pressed into service 20 times to reduce the impact of flooding. During the 1997 Red River flooding, some experts estimated that it prevented losses of more than $6 billion.[21] However, the 1997 Red River floods did result in over $150 million in damages. Floodwaters covered over five percent of Manitoba's farmland; destroyed millions of dollars worth of crops; and led the Canadian Forces to deploy more than 8,600 soldiers, 2,500 vehicles and 33 aircraft to assist civil defence workers.[22]

Impact of Floods on Canadian Critical Infrastructure

A trend of increasing damages from floods and other extreme weather-related hazards is expected in the future for three reasons.

---

[17] To access the Canadian Disaster database go to http://www.ocipep-bpiepc.gc.ca/disaster/search.asp?lang=eng
The Database currently lists 204 flood disaster instances in Canada during the entire 20th century. According to the database, 160 such instances have occurred after 1959.

[18] Brooks, G.R., Evans, S.G. and Clague, J.J.: 2001, Flooding, In G.R. Brooks (ed), A Synthesis of Natural Geological Hazards in Canada, Geological Survey of Canada Bulletin 548, Ottawa, pp, 101-143.

19 Ibid.

20 Ashmore, P. and Church, M.: The impact of climate change on rivers and river processes in Canada, Geological Survey of Canada Bulletin 555, Ottawa, 58 p.

[21] OCIPEP, *National Disaster Mitigation Strategy – Towards a Canadian Approach*, Ottawa, 2002, pg.7.

[22] Canadian Geographic, *Canada's Floods*, www.canadiangeographic.ca/SpecialFeatures/Floods/flood.htm

First, there will be more people living in larger but fewer urban centres. In the event of flooding, physical damage to property, especially in urban areas, is the major cause of tangible loss. Damage to crops, livestock and agricultural infrastructure can also be high in intensively cultivated rural areas.[23]

Second, changing climatic patterns with an associated increase in extreme flooding events are expected.[24] Different regions of Canada can be affected by rainstorm floods, ice-jam floods and snowmelt floods. A shorter winter season under climate change may result in a reduced snowpack in many areas and thereby a reduced risk of snowmelt and ice-jam floods. The main concerns about increased flooding result from the fact that a warmer atmosphere can hold more moisture, and as a result, precipitation is expected to increase. As well, precipitation is expected to become more intense over smaller areas, which suggests greater flooding problems especially in smaller catchment areas. For instance, precipitation over the Great Lakes was relatively higher and more variable for the period between 1940–1990 compared to the period between 1900–1940.

Third, an aging infrastructure that is more prone to damage will increase loss levels[25]. During the 1960s, governments in Canada spent 4.5–5 percent of GDP on infrastructure projects. That amount has now declined to 2 percent.[26] [27] These projects include many of the facilities that are integral parts of our urban systems–roads and bridges, water distribution and sewer networks, public buildings, and dams and dykes. Many of these water structures are now 30–45 years old, and may require major maintenance in the

[23] Smith, Keith. Environmental Hazards: Assessing Risk and Reducing Disaster. Routledge (London). 2000. p. 259.
[24] James Bruce, Ian Burton, Mark Egener. "Disaster mitigation and preparedness in a changing climate." May 1999
[25] Paul Kovacs, Howard Kunreuther. "Managing Catastrophic Risk: Lessons from Canada" April 2001
[26] Ibid.
[27] In Budget 2001, the GoC allocated $2 billion for the **Canada Strategic Infrastructure Fund** which will direct investment to projects of major national and regional significance, and will be made in areas that are vital to sustaining economic growth and supporting an enhanced quality of life for Canadians.
The GoC has also launched a **Border Infrastructure Fund (BIF)** which is critical to Canada's growing economic and trade relationship with the United States. The $600-million BIF will support the initiatives in the Smart Borders Action Plan by reducing border congestion and expanding infrastructure capacity over the medium term. The Plan is based on four pillars: (i) the secure flow of people, (ii) the secure flow of goods, (iii) secure infrastructure, and (iv) information-sharing and co-ordination in the enforcement of these objectives.
Finally, as part of the GoC's commitment to growth and the quality of life of all Canadians, the GoC launched a physical infrastructure program in 2000. In partnership with provincial, territorial and local governments, First Nations and the private sector, the **Infrastructure Canada Program (ICP)** is helping to renew and build infrastructure in rural and urban municipalities across Canada.

On September 30, 2002 the Speech from the Throne announced **a new 10-year infrastructure program**: "Working with provinces and municipalities, the government will put in place a ten-year program for infrastructure to accommodate long-term strategic initiatives essential to competitiveness and sustainable growth. Within this framework, it will introduce a new strategy for a safe, efficient and environmentally responsible transportation system that will help reduce congestion in our cities and bottlenecks in our trade corridors."

The programs are administered by the new federal **Department of Infrastructure.**

near and medium term. It is unclear how this activity will be financed. In the absence of required maintenance, all structures become more prone to damage. The flood infrastructure (both concrete and earthen) that now supports human settlements was often developed at the expense of naturally occurring flood mitigating infrastructure– wetlands, floodplains and other natural areas. Given the current trend in damages, it is unclear if the economic benefits associated with tradition settlements will outweigh the costs over the long term.

The effect of flooding on Canada's CI is largely dependent upon the affected area, although transportation, communications and some aspects of the service sector (particularly food production and delivery) have proven to be more prone to incapacity as a result of severe flooding. These were the most affected CI sectors during the Saguenay and Red River floods.

Despite our best efforts, Canadians and those critical infrastructure-related services they have come to depend upon, are, and will become more, vulnerable to extreme flood hazards.

Severe Storm Trends in Canada

This section will deal with three facets of the extreme storm threat to Canada's CI: tornadoes, hail storms, and ice storms. Though not an exhaustive list of the severe storm threats to domestic CI, these storm phenomena have been chosen because of their relative probability of occurrence and their potential for damage.

Tornadoes

Tornadoes can accompany severe convective weather events and produce significant damage as a result. This section will focus on the threat that tornadoes present as well provide some historical trends based on accumulated data. Canada has more tornadoes than any other country, with the exception of the United States.[28] As illustrated in Figure 3.0, Canada's "tornado alleys" are southern Ontario, Alberta, southeastern Quebéc and a band stretching from southern Saskatchewan and Manitoba through to Thunder Bay. The interior of British Columbia and western New Brunswick are also tornado zones.

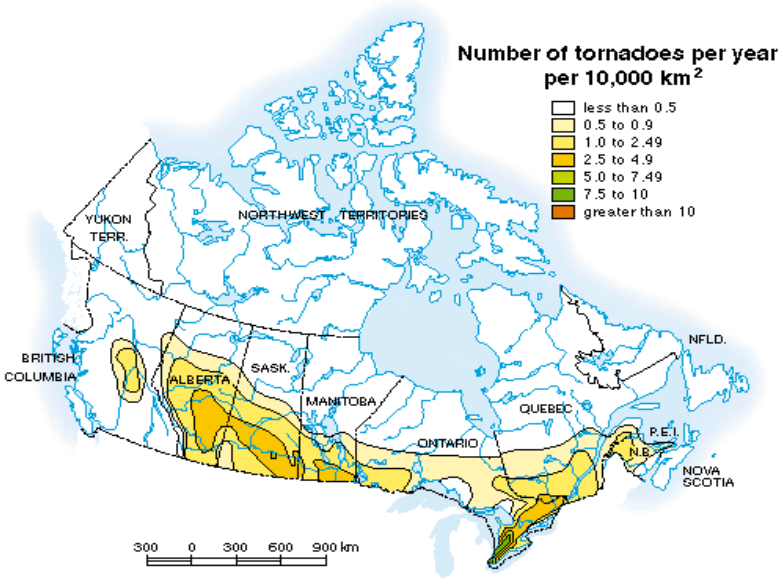
In Canada, during an average year, 80 tornadoes will cause two deaths and 20 injuries, plus tens of millions of dollars in property damage.[29] Southern Canada experiences about 60 of these tornadoes annually, although they rarely exceed intensity above category three out of six on the Fujita scale.[30]

As stated above, the study by Etkin predicts that tornadoes in Canada's prairies will likely increase given the continuing effects of global warming.[31]

---

[28] Grazulis, T.P.. Significant Tornadoes, 1880-1989. 526 pgs.
[29] http://www.mb.ec.gc.ca/air/summersevere/tornadoes.en.html
[30] Environment Canada. "CO2/Climate Report" Fall 2002 Issue. Pg. 4.
Tornado intensity is gauged (somewhat subjectively) by the Fujita Scale, which classifies tornado intensity on a six level scale.
[31] Etkin, D. "Beyond the Year 200. More Tornadoes in Western Canada? Implications from the Historical Record." Natural Hazards. V. 12 1995. pg. 27.

Figure 3.0



Hailstorms

Hailstorms pose a serious threat of damage to property and crops.[32] Hailstorms are a warm-season phenomena, typically occurring between May and September, associated exclusively with severe thunderstorms.[33]

The most costly Canadian hailstorm occurred on 7 September 1991 in Calgary, Alberta, causing an estimated $360 million in insured damage and $450 million in total damage.[34] On average, hailstorms destroy roughly three percent of Canada's prairie crops each year. Costs are conservatively estimated at $100 million annually. National hail climatologies (e.g. the number of hail days per year in Canada) serve as a foundation for most hail risk analyses. Analyses of hailstorm patterns have shown that Alberta, B.C., Saskatchewan and Quebéc are the provinces with the most reported hail activity.[35] Although national hail climatologies cannot be used to determine hailstorm severity or to infer damage, they are used to help identify vulnerable regions and areas where mitigation efforts (e.g. hail suppression) should be concentrated.

There are no indications that hailstorm activity in Canada has risen significantly due to climate change.[36]

---

[32] Paul, A. 1991a. 'A review of hail climatology on the Great Plains', *Twenty-fifth Annual Congress of the Canadian Meteorological and Oceanographic Society*, Winnipeg, Manitoba, June.
Etkin, D.A. and Maarouf, A. 1995. 'An overview of atmospheric natural hazards in Canada', *Proceedings of a Tri-lateral Workshop on Natural Hazards*, Merrickville, Canada, 11–14 February.

[33] LaDochy, S. and Paul, A. 1986. 'A climatology of hail for the southeastern prairies', *Twentieth Annual Congress of the Canadian*
Meteorological and Oceanographic Society, Regina, Saskatchewan, 5 June.

[34] IBC 1997. *Facts of the General Insurance Industry in Canada*, Insurance Bureau of Canada, Toronto, 37 pp.

[35] Etkin, David, and Soren Erikbrun, A note on Canada's hail climatology: 1977–1993. International Journal of Climatology. V. 19, 1999. p. 1370.

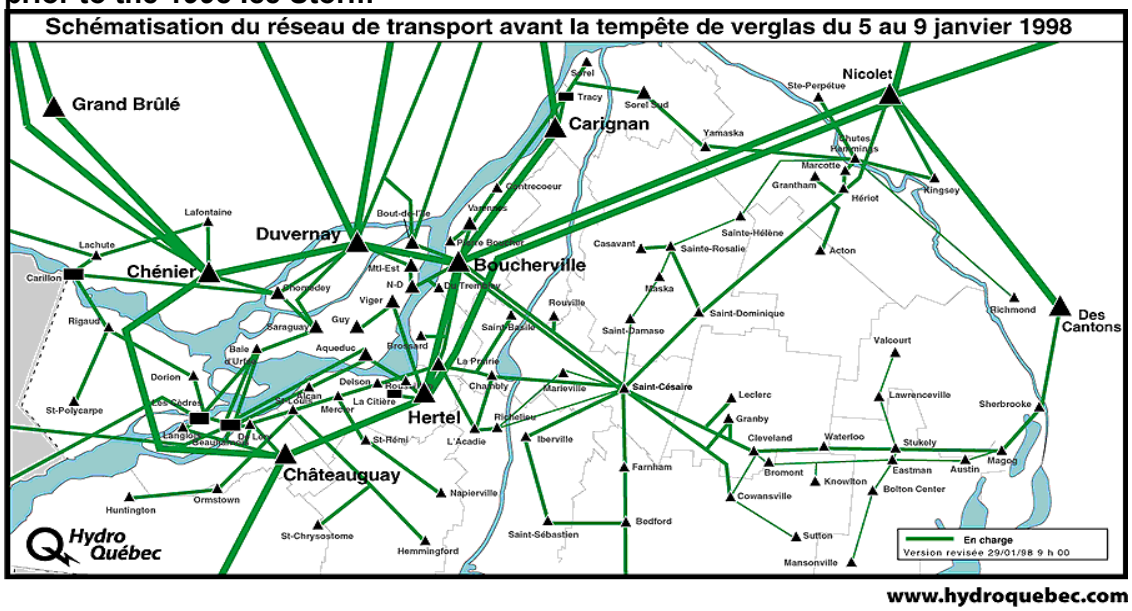
[36] Environment Canada. "CO2/Climate Report" Fall 2002 Issue. Pg. 4.

Ice Storms

Ice storms remain an important part of the natural threat environment of Canada. Studies have shown that severe winter storms in Canada, notably ice storms, may increase by as much as 30 percent by the end of the 21st century.[37]

In January 1998, an ice storm of unprecedented intensity struck eastern Ontario, western Quebéc and parts of New Brunswick, Nova Scotia and Prince Edward Island. The storm created massive and protracted power failures, particularly in Ontario and Quebéc (see Figure 4.0). This storm led to emergencies in which thousands of people had to be moved into temporary shelters and an extensive, coordinated program to restore normalcy was implemented. The costs associated with this disaster were the largest in Canadian history for a natural disaster, with the loss approximating $5.4 billion.[38] All levels of government were involved in responding to this emergency and approximately 15,000 military personnel were deployed to assist–the largest deployment of Canadian military forces since the Korean War.

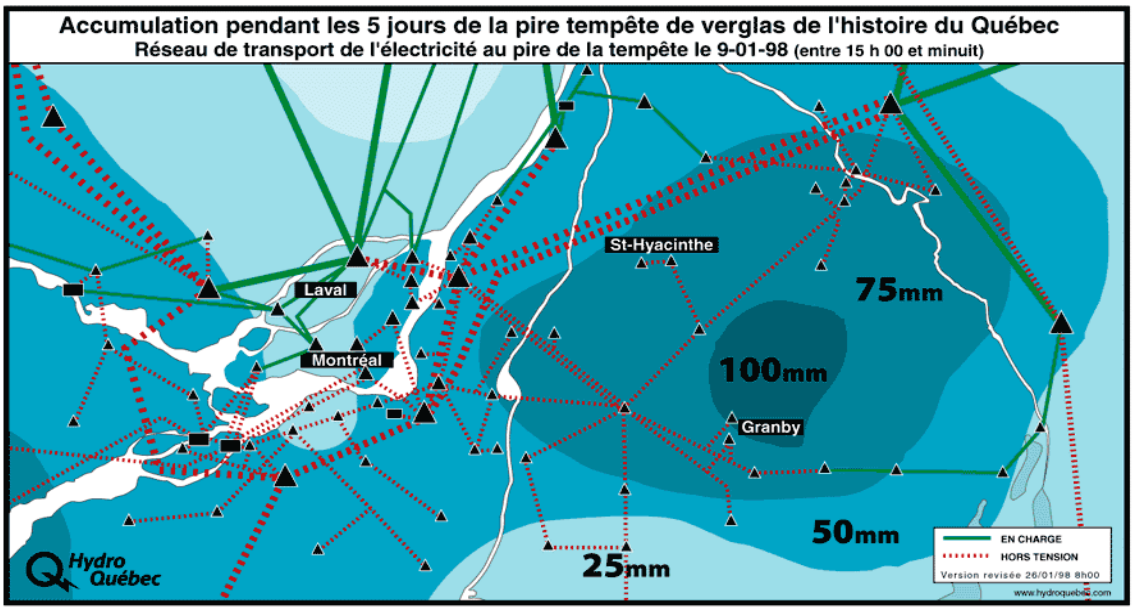
Figure 4.0 – Hydro-Quebéc map of power lines in the southern Quebéc region prior to the 1998 Ice Storm



The ice storm of 1998 felled millions of trees; 120,000 kilometres of power and phone lines; 130 major transmission towers; and 30,000 telephone poles. Ontario Hydro estimated that 600,000 customers and their dependents (amounting to 1.5 million people) were without electrical power in eastern Ontario at the height of the storm. In Ontario and southern Quebéc, 1,291,500 residences (affecting approximately 3,228,750 people) were without power, some for up to four weeks.[39] Hydro-Québec had to rebuild, not simply repair, its electricity transmission grid.

[37] Cubas et al. Climate Change 2001: The Scientific Basis. Cambridge Press. 2001. Chapter 9.
[38] Canadian Disaster database.
[39] Environment Canada, *Ice Storm '98*, www.msc-smc.ec.gc.ca/events/icestorm98/icestorm98_e.html

Figure 4.1 – After the Ice Storm of 1998 - Ice accumulation and its impact upon power lines in southern Quebéc during the 1998 Ice Storm.



Although the 1998 Ice Storm was created by a series of atmospheric coincidences, the real possibility of a future ice storm, with the potential to create similar damage, cannot be dismissed.[40] While severe ice storms often involve multiple factors, one key factor is the presence of moist air slightly above the freezing point over-riding cold air near the surface. Another is persistence. Under warmer climates, the frequency of moist air masses in southern Canada in mid-winter is likely to increase.[41] Although this is by no means conclusive, it does represent an increased potential for an increased prevalence of ice storms in Canada.

Impact of Severe Storms on Canadian Critical Infrastructure

Severe storms can significantly affect the reliability and overall security of Canada's CI. Although forecasting technology has allowed experts to accurately track and predict the severity of storms, overall understanding of their impact upon CI remains limited. Moreover, current predictive methodologies regarding the cascading effects of a CI incapacity or failure are limited.

The infrastructure sectors most prone to some level of incapacity due to certain severe storms have been telecommunications, energy service delivery, transportation, and emergency services. Transportation networks, especially in major urban centres, can become choked, whereas in rural communities, roadways and access points can be entirely blocked, given the lack of transportation infrastructure redundancy. Emergency services are also particularly susceptible to the effects of severe storms as wide-impact storms can place tremendous strains on communities with limited emergency response services.

[40] Lecomte, Eugene, et. al. Ice Storm '98. Institute for Catastrophic Loss Reduction. December 1998. p. 7.
[41] Zhang et al. "Spatial and temporal characteristics of heavy precipitation events over Canada." Journal of Climate. V. 14: 1923-1936. 2001.

Geomagnetic Storms

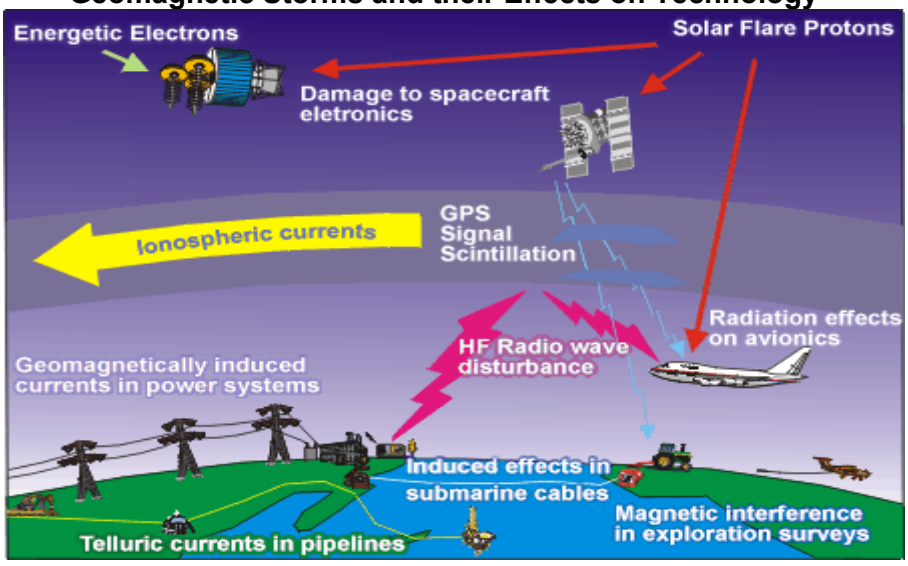
This section will elaborate on the prevalence of *geomagnetic storms* and their potential to impact upon various aspects of Canada's CI.

In 1989, a strong geomagnetic storm overloaded Hydro-Québec's power grid, deactivating reactive power compensators at several power stations and causing the system to collapse. Equipment was rendered useless (much of it having to be replaced rather than repaired), service was out for several hours and millions of dollars worth of generated power was wasted.[42]

Impact of Geomagnetic Storms on Canadian Critical Infrastructure

Geomagnetic storms, although infrequent, have the potential to severely impair CI (see Figure 5.0). Geomagnetic storms occur when sunspots on the surface of the sun erupt and impact the Earth's magnetosphere, thereby disturbing solar wind and reducing the global magnetic field. In Canada, it has been demonstrated that power systems, pipelines, and communications are at risk from the damaging effects of geomagnetic storms. Consequences of geomagnetic storm activity can include widespread power failures, pipeline corrosion, the shutdown of cable systems, an increased drag on satellites, inaccurate navigational sensors, and the potential loss of millions of dollars in revenue.[43] Geomagnetic storms also disrupt telephone and cable lines, submarine cables and the geosynchronous satellites used for telecommunications and global positioning systems.[44]

Figure 5.0
Geomagnetic Storms and their Effects on Technology[45]



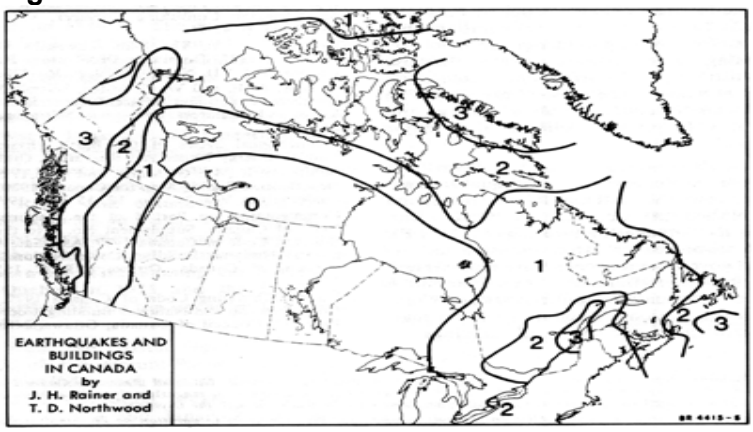
Earthquake Trends in Canada

[42] OCIPEP, *Threat Analysis: Geomagnetic Storms – Reducing the Threat to CI in Canada*, www.ocipep.gc.ca/emergencies/other/TA02-001_E.html
[43] Ibid.
[44] Ibid.
[45] http://www.spaceweather.gc.ca/effects_e.shtml

Each year, seismologists with the Geological Survey of Canada record and locate more than 1,000 earthquakes in western Canada. The Pacific Coast is the most earthquake-prone region of the nation (See Figure 6.0). In the offshore region to the west of Vancouver Island, more than 100 earthquakes of magnitude 5 or greater (large enough to cause damage had they been closer to land) have occurred during the past 70 years.

There is evidence that the Juan de Fuca and North America plates are currently locked together, causing pressure to build up in the earth's crust. It is this squeezing of the crust that causes the 300 or so small earthquakes in southwestern B.C. each year, and the less-frequent (once per decade, on average), damaging crustal earthquakes (e.g. the 7.3 magnitude earthquake on central Vancouver Island in 1946). At some time in the future, these plates will snap loose, generating a huge offshore "subduction" earthquake–one similar to the 9.2 magnitude earthquake in Alaska in 1964, or the 9.5 magnitude earthquake in Chile in 1960.[46] Current crustal deformation measurements in this area provide evidence that major seismic activity off the west coast of Canada is a ubiquitous threat.[47] Geological evidence indicates that huge subduction earthquakes have struck this coast every 300-800 years.[48]

Figure 6.0



Seismic zoning map for Canada, 1970. Probability of damaging earthquakes: Zone 0 -- negligible; Zone 1 -- small; Zone 2 -- moderate; Zone 3 -- greatest.[49]

Eastern Canada has a relatively low rate of earthquake activity (See Figure 6.0). Nevertheless, large and damaging earthquakes have occurred in the region in the past and will inevitably occur in the future. Seismologists have expressed concern about the potential damage of an earthquake in eastern Canada, given that less research has been devoted to the possibility of such an occurrence.

Although groundshaking is the major source of earthquake damage, secondary effects such as landslides, the liquefaction of saturated sandy soils, flooding of low-lying areas and tsunamis or tidal waves washing over coastlines can also cause deaths and

[46] http://www.pgc.nrcan.gc.ca/seismo/eqinfo/eq-westcan.htm
[47] http://www.pgc.nrcan.gc.ca/geodyn/eqpro.htm
[48] http://www.pgc.nrcan.gc.ca/seismo/hist/mega.htm
[49] http://www.nrc.ca/irc/cbd/cbd208e.html

massive destruction to property and the environment. In recent years, large buildings, roadways and other infrastructures have been built on reclaimed land, steep slopes and unstable soils. Such areas are at high risk of being damaged by a large earthquake. This also means that, in the future, earthquakes in such built-up areas could affect more people and cause more damage than in the past.[50]

Impact of Earthquakes on Canadian Critical Infrastructures

Ongoing research by scientists, engineers and emergency preparedness officials has produced quantifiable insights into what effects earthquakes can have on various structures. This research has resulted in improvements to the National Building Code of Canada, with modern buildings in earthquake-prone areas having built-in earthquake resistance to help limit damage and injuries. Increasing focus on the vulnerability of essential lifeline services (including power lines, water supply, sewage disposal, communications, oil and gas pipelines, and transportation facilities) both within a building and throughout urban centres, is required. Interruption of such services due to an earthquake can pose severe hardship to a community or a threat to the health and safety of the population.

Should a long-predicted earthquake of extreme magnitude occur near the mainland of B.C., or near the city of Vancouver, its effect could be catastrophic to the CI network of the region. Moreover, given the relative unlikelihood of major seismic activity in eastern Canada, mitigative activity vis-à-vis the threat of earthquakes on CI has been limited and therefore, the potential for damage (should the unlikely occur) could be considered high. Besides providing adequate strength and ductility to resist ground motion, it may be advisable to introduce multiple paths or loops in a distribution network in order to provide alternate paths of supply. These redundancy measures will limit the regions that can be affected by a failure or interruption at one point of a network.[51]

Tsunami Trends in Canada

Triggered by an offshore earthquake, volcano or mudslide, tsunamis will start off small in the open sea but amplify in size as they reach shallow water.

In 1964, a tsunami, triggered by a 9.2 magnitude earthquake in Alaska, travelled down the coast causing significant damage, finally coming inshore at Port Alberni, B.C. By the time the wave reached the end of its journey, deep in the interior of Vancouver Island, the tsunami's waters were seven metres high. It devastated the lower reaches of the town, damaging 320 buildings and causing $10 million dollars damage. Since then, there have been no major tsunamis in Canada, but a risk remains. The British Columbia Provincial Emergency Program states that a tsunami of this magnitude will undoubtedly happen again.

Impact of Tsunamis on Canadian Critical Infrastructures

[50] http://www.safeguard.ca/earthquakes/en_can.html
[51] http://www.nrc.ca/irc/cbd/cbd208e.html

The threats to Canadian CI from tsunamis should be considered low. Tsunamis are relatively rare compared to other natural hazards; however, they do present a threat to maritime infrastructures, notably ports and shipping yards. They also present a general threat to the transport and telecommunication sectors of those regions vulnerable to tsunamis.

Forest Fire Trends in Canada

Canada is covered with trees over two-fifths of its landmass. Every year, millions of dollars are spent managing and protecting the trees and with good reason: Canada is the world's largest exporter of wood and paper products with 10 per cent of the world's forests. Forestry operations employed 352,000 people in 1999–more Canadians than any other industry–earning a total of $11.8 billion. More than 300 communities across Canada depend on forestry. It is a key to the economy of many provinces, especially British Columbia, New Brunswick, and Ontario.

On average, 10,000 forest fires burn 2.5 million hectares of forest in Canada each year. In the last 10 years, forestry researchers have recorded a significant increase in the amount of area burned by fires, an increase fuelled mostly by climate change.[52] A longer forest fire season, brought on by rising annual temperatures, will severely affect the forest industry, especially if trees that are ready to be harvested are continually ravaged. If climate models used by scientists predict correctly, there will be no significant changes in the amount of rain and moisture to compensate for the longer forest fire season. While most forest fires in Canada are caused by lightning or carelessness, the additional few degrees of heat that would ensue would cause enough dryness to create a situation where more blazes, and more serious blazes, are more likely to occur.[53]

Impact of Forest Fires on Canadian Critical Infrastructures

Recent forest fires in Quebéc caused Hydro-Québec officials to shut down power to over 500,000 customers for extended periods when the fires got too close to transmission lines.[54]

Forest fires present a significant threat to CI, particularly to oil pipelines in the West, and to energy transmission and telecommunications across the country. They also place a strain on the services and safety sectors in affected areas.

Epidemics

Certain health hazards pose a threat to Canadians and Canadian CI. By far, the worst natural disaster in the country's history, as measured by the death toll, was the epidemic of Spanish influenza, which followed World War I. This flu epidemic killed 50,000

[52] http://www.marnieko.com/flames.htm
[53] Ibid.
[54] http://ca.news.yahoo.com/020705/6/nh5l.html

Canadians (20 million people worldwide) from 1918 and 1925.[55] Influenza is no longer considered to be a significant epidemic threat; however, other potential health concerns include West Nile virus and Foot and Mouth Disease (FMD). An analysis of the threat of anthrax and smallpox to Canada is included in the malicious threat section of this paper.

West Nile virus

The West Nile virus is a flavivirus that is spread by female mosquitoes. They require a blood diet to produce eggs and most species breed on standing or stagnant water. Mosquitoes may become infected with the WN virus after feeding on the blood of infected birds. The virus is stored in the salivary glands of the mosquito and may be injected into humans while they are blood feeding. Symptoms of infection include fever, headaches and body aches; however, most people infected with the virus experience only mild illness and recover fully, and others may not experience any symptoms. The two most serious health complications of the virus are meningitis and encephalitis (inflammation of the brain). At this time, there is no licensed human vaccine for the WN virus; although, recent reports state that a vaccine may be available in the U.S. within the next three years.

In Canada, the West Nile (WN) virus was first detected in birds during the summer/fall of 2001. The first human case of the virus contracted in Canada appeared in September 2002. West Nile virus has the potential to negatively affect Canada's health care sector; however, the threat level from this virus is considered low. The mosquito season in Canada is relatively short compared to that of other regions where the WN virus has been detected; therefore, Canadians have a decreased likelihood of becoming infected.

Impact of West Nile Virus on Canadian Critical Infrastructures

To date, WN virus has not negatively impacted Canada's health care sector; however, laboratories have been occupied with testing hundreds of samples, largely from birds, and in particular, crows. During the summer and early fall, hospitals may see an increase in patients with flu-like symptoms due to the WN virus, but the majority of these cases will be remedied quickly and without serious consequences for the patient. These cases are not likely to overwhelm hospitals or affect the health care system's ability to provide assistance.

Foot and Mouth Disease (FMD)

Foot and Mouth Disease is an extremely contagious, viral disease for which the symptoms are vesicles or blisters that occur mainly in the mouth or on the feet of cloven-hooved animals. Cattle, sheep, pigs and goats are highly susceptible to FMD, especially if they live in a country where FMD is not endemic. There are seven strains of the virus, which can only be differentiated in a laboratory. An area affected by FMD can become extensive due to the virus' ability to be transferred in several ways. FMD can spread by direct or indirect contact between infected animals, through the air, mechanically through the movement of infected animals and through the ingestion of infected meat. The disease is not normally fatal because it only kills approximately five percent of infected animals; however, due to the lasting, negative effects on an infected animal that has survived the disease (such as decreased milk production, decreased pregnancy rates, weight loss and lameness), infected animals are usually destroyed. Presently,

[55] *Ibid.*, 16.

vaccination is being considered as an alternative preventative and control measure, because it is safe to consume meat from animals that have been vaccinated against FMD.

Those commodities deemed capable of transmitting FMD are denied access to free countries unless tested or treated in some manner. In Canada for the year 2000, the value of exports subject to an potential FMD-related embargo was estimated at $5.4 billion. But losses from export embargoes, while dramatic for a country such as Canada, can represent only a small portion of the total national impact.[56]

The most recent FMD outbreak occurred in the United Kingdom from 19 February 2001 to 30 September 2001. During this crisis, approximately 10,512 premises were negatively affected and 4,200,000 animals were slaughtered.

Canada has been free of FMD since 1952 and, as a result, the threat level to Canadian CI sectors is considered low. Canada has strict FMD-prevention guidelines, which are administered partly by the Canadian Food Inspection Agency (CFIA). For example, immediately after a country has confirmed the presence of FMD within its borders, Canada bans all imports of commodities[57] from that country. The CFIA also oversees the Foot and Mouth Disease Strategy[58], which is part of an overall management strategy for responding to a FMD outbreak in Canada.

Impact of Foot and Mouth Disease on Canadian Critical Infrastructures

The CI sectors that can be negatively affected during a severe outbreak of FMD are: transportation, government services and emergency management. In addition to FMD's negative effects on CI sectors and emergency management resources, an outbreak can cause severe distress among the public and producers (including financial losses) and can affect consumer confidence in the agricultural industry's products.

FUTURE TRENDS

The primary effect of natural hazards on CI is the physical interruption of communications, power and transportation networks and the strain these natural threats place on the safety and security of the affected region's population.

The cost of natural disasters in North America has increased dramatically since the mid-1980s, in spite of the goal of the International Decade for Natural Disaster Reduction (the 1990s) to reduce the costs of natural disasters by 50 percent by the year 2000. Although an increase in the number of storms may play a role in these disasters, the increasing costs are largely the result of increased vulnerability.[59]

In recent years, the death toll due to natural disasters in Canada has decreased, while the economic costs of the damage have increased. For example, the Saguenay and

[56] http://www.inspection.gc.ca/english/anima/heasan/fad/fmd/sumsome.shtml
[57] http://www.inspection.gc.ca/english/anima/heasan/fad/fmd/prodliste.shtml
[58] http://www.inspection.gc.ca/english/anima/heasan/fad/fmd/fmdtoce.shtml
[59] Pielke and Downton, Precipitation and damaging floods: Trends in the United States, 1932-1997. Journal of Climate, 13:3625-3637. 2000.

Red River floods and the 1998 Ice Storm claimed relatively few lives, but cost the Federal Government approximately $6.7 billion. This trend may be the result of two divergent factors. The Canadian response to natural disasters has been tried and tested, and coordinated responses to them have become more sophisticated and better implemented. However, the cost of securing our domestic infrastructure has risen greatly as Canadian CI has become more complex and interconnected. As our physical CI elements become more intertwined with the cyber environment, the ripple effects which emanate from a critical incident arising from a natural hazard become more widespread across the CI sectors, and its overall effects and costs can increase. Moreover, the ability of first responders, emergency managers in the public and private sector, and policy makers to react in a timely matter becomes increasingly compromised.

Reports indicate that the process of rapid climate change will continue, and even accelerate, over the course of the 21st century. The effects of climate change have been forecasted by some to be greater in Canada than in any other country, with mean temperatures rising 5–10 °C by the end of the 21st century. These changes will likely bring shifting weather and climate patterns, resulting in more extreme weather events. All of these symptoms may present additional stresses on the country's infrastructure.

For example, the total number of winter storms is expected to decrease, but intense winter storms are predicted to increase five to thirty percent.[60] The increased cost of heating and maintenance during the winter is exacerbated by the similarly increasing costs of energy consumption during the summer. In October 2002, the Independent Market Operator (IMO) of Ontario warned that, due to steadily increasing summer temperatures, electricity consumption was outstripping the province's ability to supply affordable energy and that periodic power outages may become the norm for some Ontario residents during future summer months.[61]

Expansion of urban development and economic activity into more remote parts of the country may also increase the risk of disaster. As the urbanization of underdeveloped lands continues, pressure may be placed upon infrastructure that lacks the redundancy and robustness to safely support these bourgeoning communities.

Finally, the increasing shift to wireless technology may make the telecommunications and information infrastructure less vulnerable to storms and other natural events like the 1998 Ice Storm, because the system will be less reliant on transmission lines. Wireless technology is still reliant on transmission towers, but the time and costs related to repairing the system will be reduced.

ACCIDENTAL THREATS

HISTORY

It is difficult to cover the spectrum of potential accidental incidents to Canadian CI. They include human-error, mechanical failures and computer programming errors. To date,

[60] Environment Canada, *The Science of Climate Change*, 69.
[61] http://www.theimo.com/imoweb/pubs/pressReleases/pr_mspReport_2002oct07.pdf

accidental incidents have primarily been physical-based errors or mishaps. The result is often a reduced level of capacity over a critical time period.

Transportation accidents were the third-most prominent source of disasters in Canada in the 20th century. The worst accident in Canadian history occurred in 1917 when two ships carrying ammunition collided in Halifax Harbour. The resulting explosion killed 1,963 people and destroyed more than 300 blocks of the city.[62]

Train derailments are potentially most disruptive because of their often volatile cargo and because they travel through urban areas. In 1979, a CP Rail train carrying a cargo of caustic soda, propane, chlorine, styrene and toluene derailed in Mississauga, causing an explosion and fire, releasing chlorine gas. More than 240,000 residents were forced from their homes, and six nursing homes and three hospitals had to be evacuated. A similar accident occurred in Firdale, Manitoba, in May 2002, when a collision with a truck caused a train carrying benzene and plastics to derail and catch fire. The fire released benzene into the environment, forcing the evacuation of nearby farms, and had to be extinguished with water bombers due to the intensity of the heat and the levels of airborne toxins at the accident site.

In April 2000, a fire at a cement products factory in Toronto demonstrated the possible repercussions of a large scale fire in the chemical industry. Although the prevailing winds carried the resulting toxic cloud out over Lake Ontario, making evacuation unnecessary, it highlighted the risks posed by accidents in the chemical sector. (There are currently 170 industrial facilities handling large amounts of chemicals in the Greater Toronto Area alone.[63])

Even seemingly small accidents can have serious implications. In 1999, a Bell technician dropped a wrench while working in a telephone switching station in downtown Toronto. The small fire that resulted caused at least 113,000 phone lines to go out in Toronto's downtown business section, including lines to emergency service centres, and disrupted phone services as far away as Ottawa, Halifax, and Chicago. 9-1-1 emergency lines had reduced capacity but remained available. The outages also caused service from bank machines, electronic credit card systems, and Interac to be negatively affected. Other services which saw their regular operations affected including; computerized traffic lights; stock exchange trading (nearly $1 billion in electronic trading was lost); and several major data networks and Internet portals were brought offline due to the outages.

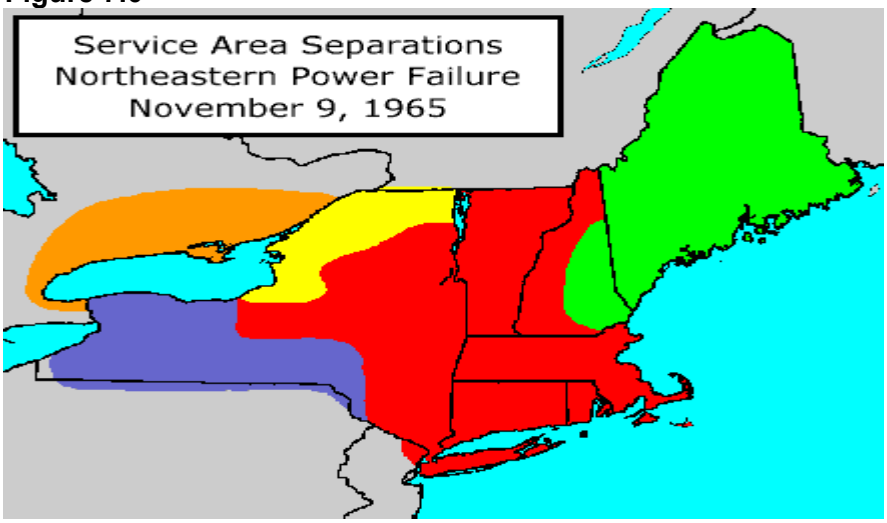
In 2001, a hunter's bullet breached the trans-Alaska pipeline. The resulting rupture allowed more than one million litres of crude oil to escape, causing environmental damage and reducing North Slope oil production to five percent of normal levels.

The single, largest electricity blackout in history, known as the Great Northeast Blackout, occurred in 1965, when a faulty relay at the Sir Adam Beck Station in Niagara Falls, Ontario, caused a key transmission line to disconnect. This failure triggered a sequence of escalating line overloads which raced down the main trunk lines of the grid, separating major generation sources from load centres and weakening the entire system with each subsequent separation. The cascade effect spread across the interconnected power

[62] Canadian Disaster database
[63] 'Mapping city's chemical caches' Toronto Star, May 8, 2002.

grid. As the blackout spread across the U.S. Northeast, power generating stations in the New York City area automatically shut themselves off to prevent the surging grid from overloading their turbines. Within 15 minutes, the entire Ontario-New York-New England grid system was down. (see Figure 7.0)

Figure 7.0



Areas of separation at 5:17 PM EST
9 November 1965

Orange: Ontario Hydro System
Yellow: St. Lawrence – Oswego
Blue: Western New York
Red: Eastern New York - New England
Green: Maine and part of New Hampshire
The green area did not lose power during the blackout.[64]

Three regional reliability councils were formed in the wake of the 1965 northeast blackout:

- *Northeast Power Coordinating Council (NPCC)* was formed in January 1966.
- The Federal Power Commission's blackout report was issued in June 1967, creating the *National Electric Reliability Council*. It has since been expanded into the *North American Electric Reliability Council (NERC),* which was formed in June 1968.

Impact of Accidental Threats on Canadian Critical Infrastructures

Accidents can interrupt service and supply of telecommunications and energy, disrupt transportation networks (e.g. creating bottlenecks in rail networks), dislocate hundreds or thousands of people, and cause injury or death. For telecommunications and power grids, a failure in one part of the network can cause cascading failures across a much wider area.

[64] http://www.cmpco.com/about/system/blackout.html

The increasing interconnectedness of CI means the impact of an accident is greater and more widespread than before. For example, in 2000, the Port of Montreal handled more than one million 20-foot-equivalent units (TEU's), equalling 9,205,120 tonnes of cargo. The port serves markets in Ontario, Quebéc, and the U.S. Northeast and Midwest.[65] The accidental sinking of a ship in the Montreal harbour could freeze activities on the docks, disrupting rail traffic across North America and causing ships to be denied entry to the port or be diverted to other ports. Recently, a collision between two cargo ships near Montreal prompted an overnight shutdown of the St. Lawrence Seaway.[66]

Where people are forced to evacuate their places of business (e.g. farms, offices and factories), economic and financial losses can be considerable. For example, the Firdale train derailment in 2002 left many farms in the area untended, leading to livestock deaths and unplanted fields.

The accident and fire at the Bell station in Toronto in 1999 affected more than 113,000 phone lines. The Hospital for Sick Children was forced to use two-way radios, 9-1-1 service was reduced, traffic lights at 550 intersections were affected and businesses were unable to take orders or contact staff. Trading value on the Toronto Stock Exchange (TSE) fell by nearly $1 billion, and the exchange was forced to close its derivatives trading floor. The Interac system was also affected by the blackout, leaving consumers in the downtown core without access to bank machines or direct payment services.

The Great Northeast Blackout of 1965 left 30 million people across 200,000 square kilometres without power. Urban centres, which are heavily dependent on electricity for lighting, transportation, elevators and traffic lights, were paralyzed. Hundreds of thousands of commuters were stuck in Manhattan and forced to camp out in hotel lobbies or their offices. Ten thousand people were trapped between stations in the subway system. Had the blackout lasted into a second day, serious logistical, health and security problems could have developed.

Accidents which lead to large numbers of people injured, killed or displaced have the potential to overwhelm the health care system. Although no one was killed in the Mississauga train derailment, 139 ambulances and several buses were held on standby for an expected flood of casualties. Had there been large numbers of injured, they would have had to travel to outlying hospitals for treatment, because three local hospitals had been evacuated.

Although leading software companies have recently committed themselves to improving the latent security of the products they bring to market, there remains a significant threat to the security of information networks due to poorly secured software. According to @Stake, a U.S. IT security consultancy, 70 percent of security defects are due to flaws in software design. For example, Code Red exploited a coding error in the way Microsoft's web-server software handles non-Roman characters.[67] In addition, the vast majority of users employ common software platforms and programs (Microsoft products being the most ubiquitous) and there exists a significant vulnerability to information networks.

[65] Port of Montreal, www.port-montreal.com/english/featfr-t.htm
[66] http://www.ocipep.gc.ca/opsprods/dob/dob02-165_e.html
[67] "Tools of the Trade." The Economist. V. 365, No. 8296. Oct. 26.

Flaws in software are considered vulnerabilities, rather than a threat *per se*. That said they do make up a significant portion of a holistic risk equation. As such, this paper will examine tbe software vulnerabilities because of the threat they pose to our increasingly on-line economy. Though usually not intentionally created, software vulnerabilities pose a significant risk because users tend to place a certain degree of trust in commercially available software packages. This trust can translate into the user placing sensitive proprietary information in a vulnerable, exploitable position. It is the contention of some experts, that with proper mitigative engineering, many potential security gaps could be prevented.

FUTURE TRENDS

Accidents are, by definition, unforeseen. Therefore, it is difficult to predict future trends in accidents involving CI.

The Transportation Safety Board of Canada (TSB) recently expressed concern regarding rail safety in Canada, particularly in the high-volume rail corridor in southern Ontario. In particular, it warned of the danger of main-track collisions due to ineffective warning of main-track switch positions and the existence of non-signalled track. Furthermore, the train control system remains vulnerable to breakdowns from signal error, and the system is unable to detect, correct or compensate for operating errors. These factors are aggravated by the proliferation of small railway companies in Canada, which lack the resources and safety programs of the national rail carriers. The risk of a serious rail accident, with the associated dangers of a chemical spill and disruption of service, remains.[68]

In the same report, the TSB expressed concern over the increase in aircraft maintenance-related incidents and accidents. The report stated "shortcomings in the human performance aspects of keeping aircraft airworthy appear to be on the rise. Inadequate supervision of apprentices and failure to follow appropriate maintenance procedures and practices...have recently been identified in investigations of fatal accidents involving aircraft serviced at Canadian maintenance facilities."[69] If this trend is not addressed, the danger of air safety incidents may increase.

The North American hydro grid is more interconnected today than it was at the time of the Great Northeast Blackout. "This interconnectedness has increased the ability of the grid to withstand unexpected disruptions as managed by coordinated real-time monitoring across North America." Officials have gone to great lengths to ensure that the entire breadth of the North American electricity grid is carefully monitored for fluctuations and special protection systems are in place. This work is therefore making the possibility of another massive blackout that would leave large areas of North America without power, remote.

Microsoft is now making a particular effort to improve the standards for security in its software. According to a report in the *Economist,* Microsoft company president Bill Gates issued a rare memo to all employees stating that the company had recommitted

[68] Transportation Safety Board of Canada, *Key Safety Issues – 2001*, http://www.tsb.gc.ca/en/index.asp
[69] Ibid.

itself to ensuring the security of its products. However, the work the programmers are doing now will not be reflected in the company's products for one to two years.[70]

With the increased scrutiny in both the public and private sectors on CI protection and business continuity planning, the telecommunications sector has put in place plans, procedures, and in many cases multiple system redundancies, which may make accidental threats to CI less likely. The initiatives begun by the telecommunications sector may generate similar actions by all CI sectors to enhance the robustness of their infrastructure elements. These measures will help to make most CI sectors less prone to the negative impacts of accidents on CI facilities and networks.

MALICIOUS THREATS

HISTORY

Physical Attacks on Infrastructure

Infrastructure has long been a target for malicious attack, whether for criminal, military or political purposes. Infrastructure supports society, delivering a range of services upon which individuals and other sectors depend. Any damage or interruption causes ripples across the system. Attacking infrastructure, therefore, has a "force multiplier" effect, allowing a small attack to achieve a much greater impact. For this reason, CI structures and networks have historically proven to be appealing targets for vandals, criminals and terrorists.

Historically, Canada has experienced physical attacks on critical infrastructure elements. While the motives behind these attacks have differed, their effects have been equally damaging.

One motive behind a malicious attack may be vandalism. In April 2002, a 14-year-old boy tampered with a railway switch in Stewiacke, N.S., causing a Via Rail train to derail and collide with a commercial building. Twenty-four people were hospitalized as a result.

Attackers may also act for personal motives. Weibo Ludwig and Richard Boonstra were convicted in 2000 of vandalizing and bombing an oil well owned by the Suncor Corporation in Alberta in the late 1990s. Ludwig blamed his family's ongoing health problems on the pollution generated by local oil and gas industries.

The FBI and other U.S. agencies are currently investigating the possibility that an electrical outage at a Utah Power relay station on the final day of the Olympic Games was caused by an explosive device. Although investigators have not confirmed that the explosion was the result of a bomb, the security fence surrounding the station was cut, suggesting that there was some malicious involvement.

[70] "Tools of the Trade." The Economist. Oct 24th 2002

The al-Qaeda terrorist attacks of 11 September 2001 on the symbols of American power and influence had the additional result of affecting a significant portion of local - and regional - CI elements and networks. The attacks had wide-ranging effects on local infrastructure, such as regional telecommunication service, the global financial networks, and local and international transportation infrastructure.

Currently there is no specific information that would lead Canadian law enforcement agencies to conclude that the level of threat for potential malicious physical attacks to CI is greater than low. However, the consequences resulting from a physical attack on Canadian CI are growing due to the increased dependence upon the collection of products and services that make up the CI network and the fact that the CI sectors are becoming increasingly *interdependent*, as telecommunications and cyber elements continue to underwrite them. Information technology has changed the way operations are performed, controlled and monitored throughout the Canadian CI network. Increasingly, various components of the infrastructure are automated and rely on remote monitoring and control systems in the conduct of their operation. A single physical attack at a strategic point may now have the potential to disrupt an entire system as well as interdependent sector systems.

Impact of Malicious Physical Attacks on Canadian Critical Infrastructure

Physical attacks on CI may impede the delivery of services, such as power, transportation and health care. As discussed above, because of the impact such a disruption has on a wide cross-section of society, an attack on physical infrastructure magnifies the impact of the initial attack.

For example, the explosion at the Utah Power electrical plant during the 2001 Salt Lake City Olympic Games caused a power outage that left 33,000 homes in Salt Lake, Davis and Tooele counties without power for nearly one hour and later sparked a fire at the Tesoro oil refinery in North Salt Lake. Smoke from the fire was so thick that Interstate 15 had to be closed. During the power outage, the airport ran on emergency generators, although flight operations were not affected.

In the immediate aftermath of the 11 September 2001 attacks in New York City, the local emergency services sector was dealt a serious blow when hundreds of responders were killed under the collapsing towers of the World Trade Centre (WTC).[71] Local communication was disrupted leading several wireless carriers to donate mobile phones and pagers to emergency personnel.[72] The attacks hindered local emergency transportation and taxed the resources of the local health infrastructure.

The attacks of 11 September, 2001 impacted CI in two ways. First, CI facilities and operations were directly disrupted by the physical impact of the attacks. The WTC housed, and was surrounded by, a number of key businesses that support CI. The destruction of the WTC area caused the disruption of business operations vital to several CI sectors including banking and finance, transportation, and communications. It is not known what effect the destruction of other firms in the WTC area might have had on the legal, health, business and public sector communities. It is difficult to ascertain the impact the Pentagon attack had on government continuity.

[71] Multiple sources.
[72] ComputerWorld.com, 12 September 2001.

Second, the decisions that CI regulators, owners and users made in response to the attacks also impacted CI. The U.S. Government was responsible, through the Federal Aviation Authority (FAA), for issuing the first ever national grounding of commercial aircraft immediately following the attacks. Owners of infrastructure such as financial markets and market participants altered the financial and banking sector by deciding to temporarily close key markets as a safety precaution. Increased demand for telephone and Internet connections forced carriers to truncate their services to avoid crashing their networks.

Biological Threats to Canadian Critical Infrastructure

There is currently much speculation as to the degree to which terrorist organization and nation-states are actively seeking out chemical and biological weapons. Following the initial September 11 attacks, the U.S. was once again put on heightened alert by the anthrax outbreaks.

Smallpox has also become a sensitive issue, with several countries reportedly holding stores of the deadly disease.

Anthrax

Anthrax is an acute infectious disease caused by the spore-forming bacterium *Bacillus anthracis*. Anthrax most commonly occurs in wild and domestic lower vertebrates (cattle, sheep, goats, camels, antelopes, and other herbivores), but it can also occur in humans when they are exposed to infected animals or tissue from infected animals.[73]

Although the inhaled form of anthrax is often cited as a potential biological weapon, there are limitations to its use. The bacteria are found in nature, but it is difficult to find strains that will cause serious disease. And once such a strain is found, it's dangerous to handle.

Subsequent to the September 11 attacks in New York and Washington, American law enforcement and health officials discovered that *Bacillus anthracis* spores had been intentionally distributed through the postal system, causing 22 people to be infected with anthrax, leading to the deaths of five of them.

Despite the panic that ensued after several envelopes containing anthrax spores were received through the mail in the U.S., sending the bacteria in letters does not make an effective biological weapon. Spores of anthrax tend to clump together and fall to the ground, so they aren't easily inhaled. When sent through the mail, the spores are often mixed with light powder that can be inhaled, but sometimes the spores are simply spread on the paper.

To be released as a weapon, the clumps of anthrax spores would have to be ground down to a size that can be inhaled easily, freeze-dried and delivered in an aerosol spray from an aircraft. A standard crop-dusting plane, however, would not be suitable. The spraying equipment used to deliver insecticide onto fields produces droplets that are too large to be absorbed through the lungs.

[73] http://www.cdc.gov/ncidod/dbmd/diseaseinfo/anthrax_g.htm

Even after it's delivered, the bacteria's behaviour is somewhat unpredictable. It normally has an incubation period of up to seven days, but could take up to 60 days to develop. And unlike other potential biological weapons, such as smallpox or plague, anthrax cannot be transmitted from person to person, so it will not spread through a population after it has been released.

Were a virulent strain of the anthrax bacteria to get into the Canadian agricultural system, its effects could be far-reaching and devastating. Anthrax is a named disease under the Health of Animals Act, and the general protocol for the release of the disease into a herd of cattle calls for the infected animals to be destroyed. However, those animals found to be uninfected–though in contact with the infected carrier–would merely be required to be quarantined. Though this technique is medically sound, it might not alleviate public health concerns.

Smallpox
Smallpox was officially declared eradicated in 1980 by the World Health Organization (WHO). However, that diagnosis was apparently premature as the virus is now considered one of the world's top six viruses that pose a threat to public health.[74] Since naturally occurring smallpox bacteria has been eradicated, the type of smallpox that would presumably be released as a biological agent would be a genetically altered version with properties significantly different than those found in the natural species.

A biological attack using the smallpox virus has the potential to be devastating to Canada's CI and would, according to some estimates, kill approximately 30 percent of those whom it infects. In a worst-case scenario, an outbreak of smallpox could negatively affect health care services, transportation, government and the economy. Some reports have stated that it could take up to one year to recover from a smallpox attack. Smallpox was recently put back on the list of diseases under surveillance by Canadian health officials for possible outbreaks.[75]

The threat level of a smallpox outbreak is currently considered low. The virus should only be located in two places in the world: the Centres for Disease Control and Prevention (CDC) in Atlanta, Georgia, and the State Research Centre of Virology and Biotechnology in Novosibirsk, Russia. However, it is not known if terrorists or other states[76] have obtained the virus. It is only known that smallpox stocks do exist in the world and that terrorist organizations may view the virus to be an effective weapon of mass destruction.

CYBER ATTACKS ON CANADIAN CRITICAL INFRASTRUCTURE

Malicious computer-based threats to Canadian CI are characterized by a number of elements which make them both difficult to predict and detect:

[74] http://www.hc-sc.gc.ca/pphb-dgspsp/publicat/ccdr-rmtc/01vol27/dr2704ea.html
[75] http://www.canada.com/health/story, 17 August 2002.
[76] Recent media reports indicate that four countries may possess smallpox stocks. The reports cite U.S. intelligence sources and list Iraq, North Korea, Russia, and France as states who have smallpox stocks. French officials have denied the reports. (Source: http://www.washingtonpost.com/wp-dyn/articles/A5113-2002Nov4.html, 4 November 2002)

- The problem of actor identification is particularly difficult in a domain where maintaining anonymity is easy and where there are sometimes time lapses between the intruder action, the intrusion itself, and the actual effects. In addition, the continuing proliferation of sophisticated computer technologies into the mainstream population makes assigning attribution increasingly difficult

- The threat is not restricted by political or geographical boundaries. Attacks can originate from anywhere in the world and from multiple locations simultaneously. Investigations and back tracking through a web of false leads and unwittingly slaved systems can be time consuming and resource intensive to pursue.

- The threat environment is extremely fluid. The window of time between the discovery of vulnerabilities and the creation of a new tool or technique to exploit the vulnerability is rapidly decreasing.

- The technology employed for attacks is simple to use, inexpensive, and widely available. Computer intruder tools and techniques are widely available on computer bulletin boards and various web sites as are encryption and anonymity tools.

- These methods of attack have become increasingly automated and more sophisticated resulting in more damage from a single attack.

- The tools used in attacks are often similar or identical to, those technologies which are employed to ensure network reliability.

- The cost required to develop a significant attack capability continues to decrease.

- Publicly and privately controlled infrastructures are becoming increasingly networked/interconnected/interdependent and, as a result are becoming more vulnerable to a diverse number of threats. The phenomena make it harder to differentiate between the author or authors of electronic attacks as well as other system-related malfunctions. While lead federal agencies have had some notable successes in ascertaining the identity of malicious code authors, tracking down and apprehending them has proven more difficult, costly and resource intensive. Ironically, the very innovations that are spurring economic development and driving globalization are rendering users vulnerable to more diverse threats.

Statistics for 2002 compiled by the Computer Emergency Response Team Coordination Center (CERT/CC) at Carnegie Mellon University suggests that there are 147 million host computers.[77] Industry estimates suggest that this represents a total global Internet community that encompasses anywhere from 445–533 million users. These numbers are expected to almost double by 2004. A new network is added to the Internet every 30 minutes.

Increasingly, everything from the delivery of energy to our homes and businesses to the effectiveness of our health care systems is tied to the reliability of information systems and networks. In this respect, Canada's information infrastructure has become a

[77] http://www.cert.org

fundamental cornerstone of our society's quality of life. The more technologically advanced a society becomes, the more reliant it becomes on that technology, which, without proper safeguards in place, can be easily exploited and corrupted. Any computer network linked to the Internet is vulnerable to attack. These attacks can be routed through the Internet, an authorized or unauthorized modem connection, or via insider access by a party with malicious intent. Moreover, attacks can be directed at multiple targets for information and intellectual property, be they on a computer, on a web site, or on a system network.

The Actors, their Tools and their Methods

In the cyber environment, geographic borders are meaningless, which makes tracking, investigation, apprehension and prosecution difficult. There are actors in the cyber environment who have displayed a willingness to contravene national legal frameworks and hide in the relative anonymity of cyberspace. These actors, in many cases, are armed with the latest technology with which they attempt to inflict the greatest damage to those networks and systems upon which we have become so reliant.

It should be noted that there is a limited ability on the part of government departments and agencies to collect, collate, analyze and synthesize in real-time the modest amount of substantive qualitative information on actors, their actual and potential capabilities, intended targets, and recorded attempts to penetrate or attack assets or systems.[78]

Script kiddies

Script kiddies are considered to be on the lowest rung on the hacker social ladder. They download readily-available code from the Internet rather than writing their own. Script kiddies can cause significant harm, often without understanding the tools and methods they are using, as well as the potential impact of their actions.[79] It may be argued that script kiddies pose a greater threat than the more competent hackers do, simply because there are many more of them and they have such ready access to so many sophisticated tools to facilitate their activities. Since there are so many fewer truly gifted hackers, the probability that one of them will attack a specific target is much lower, even though the potential damage is greater. The lesson for IT security officials is that applying patches to address vulnerabilities exploited by the latest hacking tools will generally defeat the script kiddies, the greater threat, but not the most experienced hackers, who are more likely to discover new weaknesses.[80] According to the RCMP, the typical script kiddie is a 12 to 16-year-old boy who finds some hacking code on a web site and decides to try it out. Frequently, the motive is curiosity or teenage bravado.

Hackers

Professional hackers, in contrast, have the skills to effectively use more sophisticated automated tools to carry out their activities. Whether motivated by financial gain or the challenge of breaking through defences, hacker attacks are increasing in volume and

[78] Derived from consultations with officials from the Communications Security Establishment, 4 February 2003.
[79] Criminal Analysis Branch, RCMP, "Hackers: a Canadian police perspective" www.rcmp-grc.gc.ca/crim_int/hackers_e.htm
[80] Derived from consultations with officials from the Communications Security Establishment, 4 February 2003.

sophistication and appear to be better coordinated. The rapid and widespread dissemination of new exploit tools has made it possible for even the most unsophisticated individuals to take advantage of these technologies. The evidence suggests that hacker groups are better organized, more highly skilled and far more active than terrorist groups in exploiting vulnerabilities within critical information infrastructures.

Malicious insider actors
The "insider" or trusted employee is perceived by many experts to be a greater threat than is the traditional "outsider" hacker. According to a number of surveys in Canada and the United States, the majority of computer security problems are the result of wrongful activity by persons inside an organization who have full access to information systems, both in government and business. A survey released in February 1999 by Ernst & Young revealed that 70 percent of computer system security breaches originate from an internal source within a company.

Hacktivism
Hacktivism is generally considered to involve the use of computer attacks for political, social or religious purposes. Indeed, hactivists are motivated by a wide range of social and political causes. Some anti-globalization, environmental and labour rights activists see the Internet as a tool that will allow them to achieve their goals through malicious, or criminal, means. In the past, these activities have been limited to basic DoS attacks or the defacing of web sites. While historically these activities have been limited to basic DoS attacks or the defacing of web sites, there is a developing trend of a direct relationship between political conflicts and increased malicious cyber activity. For example, during NATO's 1999 Kosovo campaign, hackers from Yugoslavia attacked the official NATO site and other sites in NATO-member countries. Chinese hackers joined the fray after the Chinese embassy in Belgrade was bombed by the U.S. Air Force, by attacking the U.S. Departments of Energy and the Interior and the National Park Service. As a result of the same incident, the White House site had to be shut down for three days after suffering a sustained DDoS attack. The ongoing disputes between India and Pakistan over Kashmir have also prompted major cyber activity.

IT networks and systems are valuable in delivering political messages. Reports of malicious cyber activity during world political and economic summits are increasing.

Terrorists
Terrorists are attracted to high-volume targets whose disruption would have symbolic, economic, financial, political or tactical consequence. As such, if terrorist were to employ cyber means to achieve their ends, the most likely targets might include networks, routers, and servers.

OCIPEP's analysis of al-Qaeda's cyber capabilities reveals that the terrorist organization is not likely to be a viable threat, although those sympathetic to their cause may prove to be a more noteworthy threat.[81] Bin Laden's choice to use Afghanistan as a base for his operations limited al-Qaeda's ability to use that country as a base for malicious cyber activity. Therefore, a potential cyber terrorist attack by the al-Qaeda group, or their sympathizers, against the West would most likely have to be launched or coordinated outside Afghanistan.

[81] http://www.ocipep.gc.ca/opsprods/other/TA01-001_E.asp

However, there has been significant, albeit unsubstantiated, reporting that bin Laden and his al-Qaeda organization are sophisticated users of computer and telecommunication technology. For example, it has been reported that al-Qaeda personnel use the Internet for sending encrypted communications.

Interestingly, in the wake of the 11 September 2001 attacks, bin Laden reportedly gave a statement to Hadmid Mir (editor of the Ausaf newspaper) indicating that:

> Hundreds of young men had pledged to him that they were ready to die and that hundreds of Muslim scientists were with him and who would use their knowledge in chemistry, biology and (sic) ranging from computers to electronics against the infidels. He said they had no atom bombs and missiles but the passion for jihad was more important than those weapons.[82]

While bin Laden' s comments that his organization was prepared to use experts with knowledge of computers to launch further attacks are noteworthy, there is no history of al-Qaeda engaging in cyber attacks and no information suggesting that it has already prepared itself for such action. Bin Laden's vast financial resources, however, would enable him or his organization to purchase the equipment and expertise required for a cyber attack and mount such an attack in very short order.

Open source reports have indicated that members of al-Qaeda have computer science/information technology expertise and/or education. There is insufficient information available to determine the specific intentions of these individuals, the al-Qaeda unit in which they exist, or the al-Qaeda organization, with respect to whether or not they are planning to, or may in the future plan to, engage in malicious cyber-based activities/attacks.

In short, the lack of available information does not allow a determination as to whether or not such attacks are being planned. However, the information that has been compiled, in combination with recent experience, would indicate that al-Qaeda, in spite of their potential to employ cyber means to conduct terrorism, will use IT assets for communications and information gathering, but that they have rarely moved beyond physical attacks on a variety of symbolic targets.

A recent study issued by the Centre for Strategic and International Studies (CSIS) contends that the threat from cyberterrorism is "overstated". The paper argues that few critical infrastructures are vulnerable because computer networks and critical infrastructures are distinct entities with sufficient buffers between them to counter the damaging effects of a malicious cyber attack.[83] The report goes on to find that "modern industrial societies are more robust than they appear at first glance. Critical infrastructures, especially in large market economies, are more distributed, diverse, redundant and self-healing than a cursory assessment may suggest, rendering them less vulnerable to attack. In all cases, cyber attacks are less effective and less disruptive than physical attacks. Their only advantage is that they are cheaper and easier to carry

[82] http://www.ocipep.gc.ca/opsprods/other/TA01-001_E.asp

[83] Lewis, James A. "Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats". Center for Strategic and International Studies. December 2002 http://www.csis.org/tech/0211_lewis.pdf

out than a physical attack. A cyber-attack does not cause damage that rises above the threshold of the routine disruptions that every economy experiences, it does not pose an immediate or significant risk to national security."[84]

However, a report by the CIA on the cyber threat to U.S. interests revealed that there is some concern over terrorist groups employing cyber techniques to attack domestic targets. According to the report, "cyberwarfare attacks against our critical infrastructure systems will become an increasingly viable option for terrorists as they become more familiar with these targets, and the technologies required to attack them. Various terrorist groups–including al-Qaeda and Hezbollah–are becoming more adept at using the Internet and computer technologies, and the FBI is monitoring an increasing number of cyber threats. The groups most likely to conduct such operations include al-Qaeda and the Sunni extremists that support their goals against the United States. These groups have both the intention and desire to develop some of the cyberskills necessary to forge an effective cyber attack. Aleph, formerly known as Aum Shinrikyo (i.e. the group responsible for the Sarin gas attack in a Tokyo subway in 1995) is reputed to be the terrorist organization that places the highest level of importance on developing cyber skills. These could be applied to cyber attacks against the U.S. This group identifies itself as a cyber cult and derives millions of dollars a year from computer retailing."[85]

State-sponsored malicious actors

State-sponsored hacking has long been a concern to Western governments and business. The increasing dependence of every governmental and business function on networked systems makes Western society vulnerable to remote attacks by hostile governments. There are data indicating that nation states are developing the tools and expertise to engage in highly sophisticated cyber activity. A number of these hostile actors may be willing to use cyber tools and techniques to replace traditional threat-related operations. Foreign intelligence agencies mount cyber attacks for a variety of reasons: to gather political or economic intelligence, to steal trade secrets, or to disrupt another country's infrastructure.[86] Within Canada, there have been no reported incidents of a state-sponsored computer-based attack or intrusion on domestic CI that have resulted in serious loss of network integrity or financial repercussions.[87] However, analysts note that activities of hostile states or intelligence service would be difficult to detect. Their objective is different–because of the major political ramifications–from hackers and terrorist groups in that they rarely want to leave any evidence or "message" for the victim of the intrusion.

Denial-of-service (DoS)

DoS attacks are explicit attempts by attackers to prevent legitimate users of a service from using that service. Examples include attempts to "flood" a network, thereby preventing legitimate network traffic; attempts to disrupt connections between two machines, thereby preventing access to a service; attempts to prevent a particular individual from accessing a service; and attempts to disrupt service to a specific system or person. DoS attacks can also be costly. Mafiaboy's (the nickname of a young hacker

[84] Ibid.
[85] http://www.fas.org/irp/congress/2002_hr/020602cia.html
[86] *Canadian Security Intelligence Service 2001 Public Report*, www.csis.gc.ca/eng/publicrp/pub2001_e.html
[87] Derived from consultations with officials from the Communications Security Establishment, 28 January 2003.

from Montreal) attacks on several major e-commerce web sites cost US$1.7 billion in lost revenue and repairs.

Distributed denial-of-service (DDoS)
Recently, a distributed denial-of-service (DDoS) attack was detected by monitoring agencies in North America. This attack targeted the 13 root Domain Name System (DNS) servers that provide worldwide address translation for the Internet. Some experts warned that this represented a disturbing trend, where attackers were targeting the infrastructure, the very hardware, of the Internet itself, which is relatively insecure. Other experts have argued that the root DNS servers are some of the most secure/robust portions of the Internet, in part due to their redundancy. Regardless, the attack was considered disturbing because, (1) it targeted all or nearly all of the root DNS servers, and (2) it was successful to an extent–several of the servers were disabled, while others experienced significant performance impacts, (3) the attack was either halted by the attackers themselves, or was a half-hearted attack in the first place. Officials from CSE contend that a similar attack against Canadian core routers could be similarly successful.

War Driving
More businesses are moving to wireless computer networks in their offices, because the systems are inexpensive and easy to set up and replace. However, the shift to wireless technology is making networks even more vulnerable to intrusion compared to wired networks. Malicious actors have started war driving, patrolling the streets with a laptop, wireless network adapter card and antenna, trolling for nearby networks. To date, it is believed that most war drivers have exploited network vulnerabilities to steal corporate bandwidth rather than attack networks. However, the same technology could allow a hacker to gain access to sensitive applications and data.

Worms and Viruses
The frequency of new worms and viruses is increasing, and will continue to do so. The costs associated with them can be significant. (see Figure 8.0).[88] Price Waterhouse Coopers estimates hackers, worms and viruses caused almost US$1.6 trillion in downtime and recovery costs in the year 2001 alone.[89]

On 25 January 2003, global internet traffic slowed to a crawl as a virus-like worm exploited a known flaw in Microsoft SQL Server 2000 (see Figure 1.0). The attack used a buffer overflow to execute code on a vulnerable SQL Server, causing that system to randomly seek out other computers to infect and in the process consume massive amounts of bandwidth.[90] The worm, called "Sapphire" or "SQL Slammer," specifically targeted UDP port 1434 in order to find SQL Servers to compromise. In doing so, the worm affected such disparate CI sectors as the banking and finance, transportation, communications, safety and emergency services, and government services. North American Automated Teller machine service was intermittently interrupted, several North

[88] Price Waterhouse Coopers - E-Privacy: Solving the On-Line Equation 2001
http://www.pwcglobal.com/extweb/pwcpublications.nsf/4bd5f76b48e282738525662b00739e22/ed95b02ac583d4e480256a380030e82f/$FILE/E-privacy+brochure.pdf
[89] Price Waterhouse Coopers - E-Privacy: Solving the On-Line Equation 2001
http://www.pwcglobal.com/extweb/pwcpublications.nsf/4bd5f76b48e282738525662b00739e22/ed95b02ac583d4e480256a380030e82f/$FILE/E-privacy+brochure.pdf
[90] http://www.betanews.com/article.php3?sid=1043499036

American airport hubs were forced to postpone or cancel flights when their online services were negatively impacted, and a 9-1-1 call centre outside Seattle, Washington, which services fourteen fire departments, two police stations and a community of 164,000 people was taken offline as a result of the worm. Global internet traffic was significantly compromised by the Slammer worm. Five of the 13 Domain Name Servers were taken offline as a result of the magnitude of informational requests made by the Slammer worm. Voice over IP and other capacity intensive services were particularly hit hard.

Figure 8.0

Incident	Date	Time to Spread	Cost
Cascade	1990	3 years	US$ 50M
Concept	1995	4 months	US$ 60M
Melissa	1999	4 days	US$ 300M
I Love You	2000	1 day	US$ 8B
Code Red	2001	Hours	US$ 2.6B
Slammer	2003	1 Hour	US$ 1B

- Losses from downtime and recovery costs in 2001 were US$1.6T
- FBI and Computer Security Institute survey found average loss of 600 respondents was $13M

Internet security company, Mi2g estimates the Slammer/Sapphire worm has so far resulted in approximately US$1 billion in cleanup costs and economic damage, which includes things like lost commerce and productivity due to Internet outages and system problems.[91] The fact that the worm did not include a harmful payload is fortunate, but it could easily have done so. The nature of the vulnerability was such that it enabled an attacker to execute arbitrary code with system privileges (i.e. higher than the Administrator account). In summary, while Slammer diminished system and network availability, had it included a malicious payload it could have significantly compromised the confidentiality and integrity of all data accessible by the compromised host. Furthermore, the time and effort involved in clean-up and recovery would have been considerably more resource-intensive.[92]

Impact of Malicious Cyber Attacks on Canadian Critical Infrastructures - Cyber

Cyber attacks on CI cost billions of dollars in lost intellectual property, maintenance and repair, lost revenue, and increased security. Cyber attacks can corrupt information through viruses, worms and data tampering; disclose confidential information and trade

[91] http://news.com.com/2100-1001-982955.html?tag=fd_top
[92] http://www.auscert.org.au/render.html?it=2730

secrets; steal telephone and Internet services; and interrupt a company's ability to deliver services to its clients.

Beyond the direct impacts, cyber attacks reduce the public's confidence in the security of Internet transactions and e-commerce, damaging corporate reputations and reducing the efficiency of the economy. It is estimated that most attacks are never reported because the victims fear a loss of consumer confidence and damage to their reputations, or are afraid of encouraging more attacks.

Due to the crosscutting and rapidly changing nature of the threat and limitations in the ability to detect, monitor and report, it is difficult to establish a complete picture of the computer-based threat to CI. As a result, there are a number of uncertainties in the data contained in threat assessments and qualitative information remains anecdotal making it difficult for the intelligence and enforcement community to generate effective analysis of the changing nature of the threat and degree of risk.

Currently, there are also no consolidated statistics at the federal or provincial level regarding computer-based threats or incident rates. There are acknowledged limitations in the detection technology and process that make it difficult to define the scope and degree of the threat. Threat trends analyses are also inhibited by the lack of baseline knowledge of normal activity on critical networked systems. As a result, most of the available threat data is very generic and based heavily on U.S. monitoring and reporting.

Traditional methodologies for addressing threats are often ineffective in detecting and analyzing computer-based threats. Technology impacts strategic analysis in terms of shorter time frames to indicate changing trends relating to threat activity.

Impact of Malicious Cyber Attacks on Canadian Critical Infrastructures - Physical

Cyber attacks can result in costly *physical* damage. A cyber attack in 2000 caused an Australian sewage plant to release raw sewage into the local environment, which cost $11,460.00 to clean up, and $154,000 in further monitoring and upgraded security.[93]

According to Riptech, a corporate Internet security firm, all of its clients experienced some form of attack during the first half of 2002. Although more than 99% of attack events were directed against web site content, as discussed above, there is still a considerable cost involved in ensuring that systems were not tampered with. Approximately 23% of clients suffered one or more severe attacks during the reporting period, down from 43% in the prior six-month period. This decline likely reflects improved security at client firms; those that did not improve their security suffered higher rates of severe attack.[94] In its Q3-Q4 2001 report, Riptech estimated that 39% of attacks were targeted (against the victim firm), while 61% were opportunistic (the attacker scanning randomly selected networks).[95] No comparable data were presented for the first half of 2002. Attacks targeted various industries differently: power and energy

[93] Green, Glenis. "Hacker caused sewage overflows, court told" Courier Mail (Australia). 17 October 2001. Pg. 11.
[94] Riptech Inc., *Riptech Internet Security Threat Report: Attack trends forQ1 and Q2 2002*, Jul. 2002.
[95] Riptech Inc., *Riptech Internet Security Threat Report: Attack trends for Q3 and Q4 2001*, Jan. 2002.

companies were the most likely targets, followed by financial services providers, high tech companies and non-profit organizations.[96]

The year 2002 may have been a relatively quiet for virus attacks, but security experts say that this is likely to be the calm before the storm. Experts have predicted that in 2003, the new breeds of computer attacks, such as a Warhol worm[97] and a flash worm[98], are likely to emerge that are capable of knocking out millions of computers around the Internet in a matter of minutes.

F-Secure ranked nine attacks in 2001 as Level 1–the most serious ranking–but only two as of late 2002. In 2001 there were 43 Level 2 attacks, dropping to 13 by late 2002.[99] However, these numbers do not indicate that 2002 was by any means a more secure year for the online community. New worm variants have provided security experts with new challenges. The Linux-based Slapper worm included an innovation that is likely to reappear in a more dangerous form in the future: it establishes a peer-to-peer network among affected servers, enabling a hacker to take over the servers and use them to attack another Web location, known as a distributed denial of service attack (DDoS). Another watermark security event in 2002 was the attack on the root servers of the domain name system (DNS). While the attack caused little damage, security experts say it was marginally effective in that it did manage to negatively impact five of the thirteen root servers.

FUTURE TRENDS

While incidents of terrorism have been very rare in Canada, the 11 September 2001 attacks have served to heighten our awareness of the threat to, and vulnerabilities within Canada's physical and cyber infrastructure (and the nexus points where the two interconnect). As such, the likelihood of a serious, deliberate and targeted attack on a Canadian critical infrastructure system must be given due consideration. Until infrastructure elements are hardened, and a greater appreciation of their interdependence is developed, the threat of an attack on Canadian infrastructure must be dealt with the utmost seriousness.

The water, transportation and oil pipeline systems make appealing targets, given their diffuse nature and the difficulty of effectively protecting them from attack.

---

[96] Riptech Inc., *loc. cit.*, Jul. 2002.

[97] http://www.cs.berkeley.edu/~nweaver/warhol.html
The study which examined the "Warhol" worm concluded that the worm would first use a list of 50,000 or so sites to start the infection from (this list would be built by scanning in advance), and then use a clever co-ordinated scanning technique to scan and infect the rest of the Internet. Simulations estimated such a worm could infect one million vulnerable servers in significantly less than 15 minutes, using plausible estimates of the scan rate a worm could achieve.

[98] http://www.silicondefense.com/flash/
The "flash" worm proposes that a determined malicious code writer could create, with relative ease, a list of *all* or almost all servers with the relevant service open to the Internet *in advance* of the release of the worm. This would speed the spread of the worm to almost 15 seconds.

With response times to critical internet threats currently at approximately 2 to 3 hours, this would make both the Warhol and flash worms particularly damaging to the cyber environment.

[99] http://www.f-secure.com/news/items/news_2002121700.shtml

Cyber crime and the criminal and terrorist use of information technology are significant issues for law enforcement. A sophisticated information infrastructure, a large pool of potential hackers within the country and heavy reliance on computer-based CI are all factors in making computer-based crime a serious threat to Canada. The spread of high speed Internet access, which allows a home computer to remain connected to the Internet all day, will provide more attack opportunities for hackers and will mean more potential victims to be exploited for DDoS attacks.

According to Riptech, the rate of cyber attack on its clients increased substantially over the first half of 2002. Attack activity against its clients was up 28 percent over the second half of 2001, which represents a projected annual growth rate of 64 percent. Daily attack volumes fluctuated more than in the previous six-month period, but the trend was toward a consistent increase in cyber attack activity during the first half of 2002.[100] Riptech's conclusion to its Q3–Q4 2001 report remains valid: "Overall, these findings strongly suggest that attack activity is severe, diverse, and steadily increasing."[101]

The growing adoption of wireless technology will continue to introduce new vulnerabilities and points of access for attackers. As discussed above, wireless systems are currently more vulnerable than wired networks, partly because users are not properly protecting themselves, and partly because of ineffective built-in protection technologies.

CONCLUSION

Critical infrastructure underpins every sector of society and the economy providing all the basic services upon which we depend. Because it supports society as a whole, the impact of a disruption in a CI sector can have potentially far-ranging effects. Moreover, the potential for widespread impact is growing, as the different sectors of the CI become increasingly interdependent. More than ever, the impact of an event on one sector is felt in other infrastructure sectors.

Four factors contribute to Canada's vulnerability to the vast spectrum of threats. First, Canada's population, built environment, and wealth, are increasingly concentrated in a small number of highly vulnerable areas and many such communities are at risk from multiple hazards. Second, climate change may increase the frequency and severity of extreme weather events. Third, Canada's built environment is aging and is more susceptible to damage. Fourth, communities are increasingly more reliant on advanced technologies that are frequently disrupted during disasters.

The process of global climate change is providing new and distinct challenges for emergency managers in Canada. Canada's aging infrastructure should be tested by an increase in severe natural phenomenon. Therefore, it will precipitate the need for a layered approach to infrastructure protection.

The increased urbanization of Canadian communities, and the concomitant need for additional vital, uninterrupted, services for Canada's bourgeoning cities raises the possibility that our critical infrastructure is more vulnerable than ever. Moreover, we

[100] Riptech Inc., *loc. cit.* Jul. 2002.
[101] Riptech Inc., *loc. cit.*, Jan. 2002, 12-13.

remain equally susceptible to human-error, mechanical failures, and computer programming errors.

The threat environment has become more complicated by the advent of new technologies which have empowered all people with the ability to more efficiently access, and manipulate computer-based information stores. This presents new challenges in the form of cyber-based threat actors who, be it accidentally or maliciously, can impose significant costs on private and public computer networks.

Finally, the terrorist attacks of September 11 confirmed what the security and intelligence community had long feared, which is that malicious actors, motivated by a multitude of reasons, would be willing to use deadly force to strike at the fabric of our post-industrial society. Those events have altered the way in which emergency management professionals, policy-makers, and the owners and operators of CI conduct their affairs because the possibility, regardless of how remote, that an event on an equally grand scale might occur again precipitates the need for robust and flexible mitigation, preparedness, response and recovery plans.

Canada's future safety, security and economic well-being will depend on our ability to predict and respond to threats to these critical assets. It is a stated goal of the Government of Canada to assist in coordinating federal, provincial and municipal resources in order to enhance the robustness of Canadian CI networks and facilities. Actions to secure CI will be ongoing and will have to evolve in relation to development and implementation of new technologies.

ANNEX A: KEY ORGANIZATIONS IN CANADIAN CRITICAL INFRASTRUCTURE PROTECTION

Although individual organizations have been involved in addressing various aspects of critical infrastructure protection (CIP), for many years, these activities have largely been limited particularly to the areas of emergency preparedness, telecommunications and IT security. It is only recently that the issue of CIP has begun to be approached in a coordinated manner. Cooperation among agencies and organizations in specific areas is well established but the broad range of vulnerabilities and their interdependencies is only now becoming fully recognized. This realization is mainly due to three factors: the result of the extensive preparations for the Year 2000 (Y2K) and the concomitant recognition of interdependencies; the growing reliance of all sectors of the economy on the public Internet; and the dramatic increase in terrorist and criminal activities directed both towards cyberspace and traditional infrastructures.

Effective critical infrastructure protection requires coordinated action across industry and at all levels of government. The effort in Canada is being spearheaded by a relatively small number of lead agencies, most of which have historically had some role in national or civil defence, in fighting crime, or in countering computer/communications threats. This section provides an overview of the key organizations involved in protecting Canada's critical infrastructure.

FEDERAL GOVERNMENT LEAD AGENCIES

The summaries below are extracted from the published mandates of the departments and agencies.

The Office of Critical Infrastructure Protection and Emergency Preparedness (OCIPEP)

The *Office of Critical Infrastructure Protection and Emergency Preparedness* (OCIPEP) was established in February 2001. OCIPEP is a civilian organization in the National Defence portfolio that combines the responsibilities of the former *Emergency Preparedness Canada* with broad expertise gained during the preparations for Y2K and the increasing recognition of the need for a comprehensive approach to protecting critical infrastructure. The Office is charged with developing and implementing a comprehensive approach to protecting Canada's critical infrastructure in both its physical and cyber dimensions, regardless of the source of threats and vulnerabilities. It also acts as the government's primary agency for ensuring national civil emergency preparedness.

In fulfilling its mandate, the Office aims to:

- build partnerships with the private sector, the provinces, territories and municipalities, and key international partners, the U.S. in particular;
- promote dialogue among Canada's critical infrastructure owners and operators and foster information sharing on threats and vulnerabilities;
- provide a focal point for the federal government's own cyber incident analysis and coordination efforts and support federal departments and agencies in meeting their responsibilities for protecting their IT systems and networks;

- promote other areas of cooperation such as raising awareness, enhancing education and training, and promoting information technology security research and development; and
- achieve an appropriate level of national civil emergency preparedness.

The Communications Security Establishment (CSE)
As the cryptology and information technology security (ITS) technical authority, the Communications Security Establishment (CSE) is responsible to:

- In consultation with the Treasury Board of Canada Secretariat and other departments, develop operational standards and technical documentation as it relates to Signals Intelligence (SIGINT), Communications Security (COMSEC), and ITS in terms of system certification and accreditation, risk and vulnerability analysis, product evaluation, system and network security analysis.
- Provide advice and assistance to departments on operational standards and technical documentation developed by CSE.
- Provide security engineering services, technical and operational assistance to support the design, implementation and operation of government and national IT systems and infrastructure elements.
- Develop and provide specialized SIGINT and ITS training, especially with respect to COMSEC, network vulnerabilities and relevant technical safeguards.
- Test, inspect and evaluate IT products and systems to identify risks, vulnerabilities and appropriate mitigation, and conduct related technical research and development.
- Certify private sector test and evaluation facilities.
- Assess and report on the application of COMSEC and ITS technical safeguards in both the public and private sectors, upon request or when mandated by security standards.
- Manage the distribution of SIGINT, cryptographic equipment, accountable publications and key material. Operate key management systems. Maintain the national inventory of personnel cleared for access to SIGINT.
- Represent the Government of Canada on national and international SIGINT and ITS committees and negotiate agreements with allied agencies.

CSE provides technical advice, guidance and services to the Government of Canada to maintain the security of its information and information infrastructures. CSE is recognized for is expertise in information assurance and is a trusted supplier of made-for-Canada solutions to protect information, and services to assess the security of IT products, systems and networks.

In fulfilling its IT security mandate CSE helps to protect Canada's electronic information assets and information infrastructures by:

- supporting the development of IT security policy and standards for the Government;
- analyzing vulnerabilities in IT products, systems and networks, and recommending appropriate countermeasures;
- approving cryptographic, computer and network security products and systems for the protection of electronic information and electronic commerce;
- developing and supporting the development of IT security products, systems and services; and

- providing IT security consulting services and support to the federal government, and to other levels of government and Canadian organizations.

CSE's ITS programme provides leadership and support to many secure e-government initiatives including Critical Infrastructure Protection, the Government of Canada Information Protection Co-ordination Centre and the Government of Canada Public Key Infrastructure initiative. CSE's mandate under the National Defence Act has recently been amended to allow the collection of communications of a legitimate foreign intelligence target located abroad if those communications go into or out of Canada and to provide the necessary technical assistance to those responsible for Canadian government computer systems and networks in order to effectively protect them from mischief, unauthorized use or interference.

Department of the Solicitor General of Canada (SolGen)
The Solicitor General Portfolio is responsible for protecting Canadians and helping to maintain Canada as a peaceful and safe society.
The Portfolio consists of the Department and four agencies including the Royal Canadian Mounted Police (RCMP) and the Canadian Security Intelligence Service (CSIS).

SolGen's National Security Directorate has three divisions: the Security Policy Division, the Counter-Terrorism Division and the Technology and Lawful Access Division.

The Royal Canadian Mounted Police (RCMP)
The *Royal Canadian Mounted Police* (RCMP) is the Canadian national police service and an agency of the *Ministry of the Solicitor General of Canada*.

The mission of the RCMP's Technical Operations Directorate is to provide policy, advice and management to predict, research, develop and ensure the availability of technical tools and expertise which enable front-line members and our partners to:

- prevent and investigate crime and enforce the law
- protect against terrorism
- operate in a safe and secure environment

The Royal Canadian Mounted Police (RCMP) Technical Security Branch (TSB) is part of the Technical Operations Directorate and is responsible, as mandated in Treasury Board policy, for the following aspects of physical and information technology security within the federal government:

1. In consultation with Treasury Board Secretariat (TBS) and other departments, developing the operational standards on physical and information technology security for the approval of Treasury Board, and advising on their application;
2. Developing, approving and issuing technical documents on physical and information technology security, and advising on their application;
3. Providing advice on threat and risk assessments for physical sites and information technology environments, when requested;
4. Advising departments on physical security, when requested;
5. Advising departments, other than the Department of National Defence, on information technology security, when requested;
6. Carrying out specialized training on physical and information technology security;
7. Reviewing and advising on counter-technical intrusion security, when requested;

The Canadian Security Intelligence Service (CSIS)
The primary objective of the *Canadian Security Intelligence Service* (CSIS) is to investigate and report on threats to the security of Canada. CSIS's mandate is to collect, analyze and retain information or intelligence on activities that may, on reasonable grounds, be suspected of constituting threats to the security of Canada, and to report to and advise the Government of Canada. CSIS also provides security assessments, on request, to all federal departments and agencies, with the exception of the RCMP. CSIS does not have law enforcement powers; therefore, all law enforcement functions are the responsibility of police authorities.

The Treasury Board Secretariat (TBS)
The *Treasury Board Secretariat* (TBS) is a central government agency. Its mission is to help the Government of Canada manage its human, financial, information and technology resources. Its responsibilities for the general management of the government affect initiatives, issues and activities that cut across all policy sectors managed by 22 operating departments and some 100 other organizational entities.

Of particular interest in the context of this report is the Secretariat's responsibility for the *Government Security Policy* (ref. 3) (which applies to protection of the federal government's information assets) and its derivative technical security policies, standards and guidelines that are developed in close consultation with the Communications Security Establishment and the Royal Canadian Mounted Police. In addition, TBS leads the implementation and policy development work of Government of Canada Public Key Infrastructure (GoC/PKI) initiative.

Industry Canada
Industry Canada has a number of responsibilities relating to research, regulation, licensing and operation of telecommunications in Canada. In general, these powers are granted under three Acts of Parliament: the Telecommunication Act, the Radiocommunication Act and the Industry Canada Act. Industry Canada maintains an *Emergency Telecommunications Operations Centre* (EOC) in Ottawa and in five regional offices. In an emergency, the EOC works with the *Government Emergency Operation Centre* and provincial emergency coordination centres to coordinate telecommunications services.

Based on this emergency response expertise and on expertise with respect to security issues around e-commerce, Industry Canada has been identified by OCIPEP as the sectoral lead for CIP activities focused on the telecommunications sector. The department will be developing additional activities that focus on partnering with industry around CIP, as well as working closely with OCIPEP on CIP issues and the telecommunications industry sector.

Natural Resources Canada
Based on this emergency response expertise and on expertise with respect to security issues around e-commerce, NRCan has been identified by OCIPEP as the sectoral lead for CIP activities focused on the energy and utilities sector. The department will be developing additional activities that focus on partnering with industry around CIP, as well as working closely with OCIPEP on CIP issues and the energy and utilities industry sectors.

Transport Canada
Based on this emergency response expertise and on expertise with respect to security issues around e-commerce, Transport Canada has been identified by OCIPEP as the sectoral lead for CIP activities focused on the transportation sector. The department will be developing additional activities that focus on partnering with industry around CIP, as well as working closely with OCIPEP on CIP issues and the transportation industry sector.

Health Canada
Health Canada collaborates internationally and with its provincial and territorial counterparts to protect the health of Canadians against current and emerging health threats. Through its *Health Intelligence Network*, the Department works with other levels of government and the health care system in the surveillance, prevention, control and research of disease outbreaks across Canada and around the world.

By administering the Food and Drugs Act, Health Canada helps protect Canadians from potential health hazards by releasing Advisories and Warnings on foods, drugs, medical devices, natural health products and consumer products, and by providing information and policies on Novel and Genetically Modified Foods and Nutrition Labelling.

The Department also works to maximize the safety and effectiveness of biologics and biotechnology products such as blood, tissues and reproductive technologies in the Canadian marketplace and health system.
In addition, Health Canada negotiates agreements regarding hazardous materials in the workplace, performs medical assessments for pilots and air traffic controllers and conducts environmental health assessments.

In a national health emergency or disaster, Health Canada's *Office of Emergency Services* is responsible for supporting emergency health and social services in the provinces, territories or abroad. It manages the National Emergency Stockpile System (NESS), which includes emergency supplies and medical and pharmaceutical supplies. The Office is responsible for the Emergency Operations Centre which responds to calls for emergency assistance from provincial and territorial governments and from other parts of the Government of Canada. To ensure that emergency officials across Canada are always ready, this Office develops procedures and training assistance.

PROVINCIAL, TERRITORIAL AND MUNICIPAL ROLES

Because of the large number of organizations involved at the provincial and municipal levels of government, no detailed breakdown of individual organizations will be attempted in this report. Instead, an overview of the more general approaches is presented.

Critical infrastructure protection and emergency preparedness in the provinces and territories has traditionally focussed more on the human and physical infrastructure, rather than cyber protection. That is now changing somewhat, though there are still quite different perspectives depending on whether one comes from an emergency preparedness or an IT background. Provincial and territorial responsibility is assigned to an existing ministry that varies from administration to administration. Typically,

responsibility tends to be lodged in the Ministry of Municipal Affairs or the Ministry of the Solicitor General.

Both federally and provincially, there has traditionally been close liaison with municipalities in areas such as emergency preparedness, as the municipalities traditionally play a major role in responding to emergencies through the fire, police and ambulance services.

Every province and territory also has an Emergency Measures Organization (EMO), which manages any large scale emergencies (prevention, preparedness, response and recovery) and provides assistance and support to municipal or community response teams as required.

Government of Canada departments and agencies support the provincial or territorial EMOs as requested or manage emergencies affecting areas of federal jurisdiction. From policing, nuclear safety, national defence and border security to the protection of our environment and health, many federal departments and agencies also work to prevent emergencies from happening or are involved in some way in a response and recovery effort.

Emergencies are dealt with first by local officials, such as hospitals, fire departments, police and municipalities. If they need assistance, they request it from the provincial or territorial EMO, who in turn seek assistance from the Government of Canada if the emergency escalates beyond their resource capabilities.

Requests from the provinces to the Government of Canada are managed through the Office of Critical Infrastructure Protection and Emergency Preparedness (OCIPEP), which maintains close operational links with provincial and local emergency authorities and maintains inventories of resources and experts in various fields. In practice, it can take just a few minutes for the response to move from the local to the national level and the right resources and expertise identified and triggered.

A list of the Canadian Provincial and Territorial Emergency Management Organizations follows:

British Columbia
BC Inter-Agency Emergency Preparedness Council
BC Provincial Emergency Program

Alberta
Emergency Management Alberta

Saskatchewan
Saskatchewan Emergency Planning

Manitoba
Manitoba Emergency Management Organization

Ontario
Emergency Measures Ontario

Québec
Québec Ministère de la Sécurité

New Brunswick
New Brunswick Emergency Management Organization
On-line Public Safety Advisories

Newfoundland & Labrador
Newfoundland Emergency Measures Division

Nova Scotia
Nova Scotia Emergency Measures Organization

Prince Edward Island
Prince Edward Island Emergency Measures Organization

Northwest Territories
Northwest Territories Emergency Measures Organization

Yukon
Yukon Emergencies Measures Organization

As well, there exists a National CIO Subcommittee on Information Protection (NCSIP) which is comprised of provincial and territorial representatives. This body makes recommendations to provincial/territorial Chief Information Officers on IT security related issues.

OCIPEP is now cooperating closely with the provinces even to the extent that in some provinces, federal and provincial teams are being co-located, thus sharing facilities and knowledge.

BIBLIOGRAPHY

Apps, M.J. et al. *Boreal Forests and Global Change*. Kluwer Academic Publishers, Dordrecht, 548 pgs. 1995.

Ashmore, P. and Church, M.: "The impact of climate change on rivers and river processes in Canada", *Geological Survey of Canada Bulletin* 555, Ottawa, 58 p.

Brooks, G.R., Evans, S.G. and Clague, J.J.: 2001, "Flooding", In G.R. Brooks (ed), A Synthesis of Natural Geological Hazards in Canada, *Geological Survey of Canada* Bulletin 548, Ottawa, pp, 101-143.

Cubas et al. *Climate Change 2001: The Scientific Basis*. Cambridge Press. 2001. Chapter 9.

Cyberthreat - (Canadian Internet Security Environment), Warwick Publishing

Environment Canada. "CO2/Climate Report" Fall 2002 Issue. Pg. 4.

Environment Canada, *The Science of Climate Change*, Apr. 2001, 24. Online at www.msc.ec.gc.ca/saib/climate/Climatechange/CC_presentation_e.PDF

Etkin, D. "Beyond the Year 200. More Tornadoes in Western Canada? Implications from the Historical Record." *Natural Hazards.* V. 12 1995. pg. 27.

Etkin, David. "Risk transference and related trends: driving forces towards more mega-disasters." Environmental Hazards 1 (1999), pp. 69-75. Elsevier Science Ltd.

Etkin, David, and Soren Erikbrun, "A note on Canada's hail climatology: 1977–1993." *International Journal of Climatology*. V. 19, 1999. p. 1370.

Etkin, D.A. and Maarouf, A. 1995. "An overview of atmospheric natural hazards in Canada", *Proceedings of a Tri-lateral Workshop on Natural Hazards*, Merrickville, Canada, 11–14 February.

Grazulis, T.P. *Significant Tornadoes, 1880-1989.* 526 pgs.

Green, Glenis. "Hacker caused sewage overflows, court told" Courier Mail (Australia). 17 October 2001. Pg. 11.

IBC 1997. "Facts of the General Insurance Industry in Canada", Insurance Bureau of Canada, Toronto, 37 pp.

James, Bruce, Ian Burton, Mark Egener. "Disaster mitigation and preparedness in a changing climate." May 1999

Paul Kovacs, Howard Kunreuther. "Managing Catastrophic Risk: Lessons from Canada" *Institute for Catastrophic Loss Reduction*. April 2001

LaDochy, S. and Paul, A. 1986. 'A climatology of hail for the southeastern prairies', *Twentieth Annual Congress of the Canadian Meteorological and Oceanographic Society*, Regina, Saskatchewan, 5 June.

Lecomte, Eugene, et. al. Ice Storm '98. *Institute for Catastrophic Loss Reduction*. December 1998. p. 7.

Lewis, James A. "Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats". Center for Strategic and International Studies. December 2002 http://www.csis.org/tech/0211_lewis.pdf

"Mapping city's chemical caches" *Toronto Star*, May 8, 2002.

OCIPEP, *National Disaster Mitigation Strategy – Towards a Canadian Approach*, Ottawa, 2002, pg.7.

Ontario Hydro. ICE Report: 1998 Ice Storm.

Paul, A. 1991a. 'A review of hail climatology on the Great Plains', *Twenty-fifth Annual Congress of the Canadian Meteorological and Oceanographic Society*, Winnipeg, Manitoba, June.

Pielke and Downton, "Precipitation and damaging floods: Trends in the United States, 1932-1997." *Journal of Climate*, 13:3625-3637. 2000.

Smith, Keith. *Environmental Hazards: Assessing Risk and Reducing Disaster.* Routledge (London). 2000. p. 259.

"Tools of the Trade." *The Economist.* V. 365, No. 8296. Oct. 26. 2002

White, R. & Etkin D. "Climate Change and the Canadian Insurance Industry." *Natural Hazards.* 16: 135-163, 1997.

Zhang et al. "Spatial and temporal characteristics of heavy precipitation events over Canada." *Journal of Climate.* V. 14: 1923-1936. 2001.

Internet Sources

AusCERT - "Business Impact Assessment - Possible Slammer hiatus" http://www.auscert.org.au/render.html?it=2730

Beta News - "MS SQL Server Worm Cripples Internet" http://www.betanews.com/article.php3?sid=1043499036

Office of Critical Infrastructure Protections and Emergency Preparedness - Canadian Disaster Database http://www.ocipep.gc.ca/disaster/default.asp

Canadian Food Inspection Agency (CFIA) - Foot and Mouth Disease http://www.inspection.gc.ca/english/anima/heasan/fad/fmd/prodliste.shtml

http://www.inspection.gc.ca/english/anima/heasan/fad/fmd/fmdtoce.shtml
http://www.theimo.com/imoweb/pubs/pressReleases/pr_mspReport_2002oct07.pdf

Canadian Geographic - "Canada's Floods"
www.canadiangeographic.ca/SpecialFeatures/Floods/flood.htm

CBC News - "Earthquakes in Canada"
http://cbc.ca/news/indepth/earthquake/canada.html

Central Maine Power - The Great Northeast Blackout of 1965
http://www.cmpco.com/about/system/blackout.html

Centers for Disease Control - Anthrax FAQ's
http://www.cdc.gov/ncidod/dbmd/diseaseinfo/anthrax_g.htm

The CERT® Coordination Center (CERT/CC)
http://www.cert.org

Criminal Analysis Branch, RCMP, "Hackers: a Canadian police perspective"
www.rcmp-grc.gc.ca/crim_int/hackers_e.htm

Environment Canada - Ice Storm '98
http://www.msc-smc.ec.gc.ca/media/icestorm98/index_e.cfm

F-Secure - "F-Secure Corporation's Data Security Summary for 2002"
http://www.f-secure.com/news/items/news_2002121700.shtml

Health Canada – "Bio-terrorism and public health"
http://www.hc-sc.gc.ca/pphb-dgspsp/publicat/ccdr-rmtc/01vol27/dr2704ea.html

The Independent Market Operator
http://www.theimo.com/imoweb/pubs/pressReleases/pr_mspReport_2002oct07.pdf

National Research Council of Canada – "Earthquakes and Buildings in Canada"
http://www.nrc.ca/irc/cbd/cbd208e.html

News.com - "Counting the cost of Slammer," 31 January 2003
http://news.com.com/2100-1001-982955.html?tag=fd_top

Natural Resources Canada - Earthquakes and Plate Tectonics in Western Canada
http://www.pgc.nrcan.gc.ca/seismo/eqinfo/eq-westcan.htm

Natural Resources Canada - Earthquake Processes
http://www.pgc.nrcan.gc.ca/geodyn/eqpro.htm

Natural Resources Canada - Effects on Technology/Geomagnetic Hazards
http://www.spaceweather.gc.ca/effects_e.shtml

Natural Resources Canada - Giant Megathrust Earthquakes
http://www.pgc.nrcan.gc.ca/seismo/hist/mega.htm

Office of Critical Infrastructure Protections and Emergency Preparedness - "Threat Analysis: Al-Qaida Cyber Capability"
http://www.ocipep.gc.ca/opsprods/other/TA01-001_E.asp

Office of Critical Infrastructure Protections and Emergency Preparedness - "OCIPEP Daily Brief," 15 October 2002
http://www.ocipep.gc.ca/opsprods/DOB/DOB02-165_e.html

Office of Critical Infrastructure Protections and Emergency Preparedness - "Threat Analysis: Geomagnetic Storms – Reducing the Threat to CI in Canada"
www.ocipep.gc.ca/emergencies/other/TA02-001_E.html.

Port of Montreal
www.port-montreal.com/english/featfr-t.htm

Price Waterhouse Coopers, *E-Privacy: Solving the On-Line Equation 2001*
http://www.pwcglobal.com/extweb/pwcpublications.nsf/4bd5f76b48e282738525662b00739e22/ed95b02ac583d4e480256a380030e82f/$FILE/E-privacy+brochure.pdf

Silicon Defense - "Flash Worms: Thirty Seconds to Infect the Internet"
http://www.silicondefense.com/flash/

Transportation Safety Board of Canada - "Key Safety Issues – 2001"
www.tsb.gc.ca/

Washington Post - "4 Nations Thought To Possess Smallpox," 4 November 2002
http://www.washingtonpost.com/wp-dyn/articles/A5113-2002Nov4.html

Weaver, Nicholas C, "Warhol Worms: The Potential for Very Fast Internet Plagues"
http://www.cs.berkeley.edu/~nweaver/warhol.html

Yahoo News - "Hydro-Quebéc cuts power to 500,000 after forest fire nears transmission line"
http://ca.news.yahoo.com/020705/6/nh5l.html