



www.ddsi.org

National Dependability Policy Environments

CANADA

Report Version: Final
Report Preparation Date: 1 November 2002
Classification: Public
Preparation led by: RAND Europe (NL)

Contract Start Date: 1 June 2001 Duration: 18 months
Project Co-ordinator: RAND Europe (NL)

Partner: RAND Europe (NL, Project Coordinator); King's College London (UK);
Cell Network (S); IABG (D); Almaweb (I); LINK (P); ELIAMEP (GR);
Ernst Basler + Partner (CH), Isdefe (E)



IST-2000-29202

Project funded by the European Community
under the “Information Society Technology”
Programme (1998-2002)

Table of Contents

Overview of the Country’s Information Infrastructure 3
Main ICT Regulatory and Legal Developments 4
Assessment of Phenomena Undermining Dependability 5
Government Initiatives Aimed at Tackling Cyber-Security 5
Industry and Other Non-Government Activities Related to Dependability 8
Public-Private Partnerships 8
Research and Development 9

Overview of the Country's Information Infrastructure

This section provides a high level summary of social, political, and economic trends concerning the Internet, and information and communications networks. In terms of ICT intensity in Canada, the private sector spends 45.8 percent of its total R&D spending on ICT.¹ In 2000, the contribution of ICT to Canada's GDP accounted for 5.1 percent of the total.² The share of ICT related employment as part of the total employment force stands at 3.6 percent. ICT manufacturing exports totalled 28.10 billion EUROS.³ Overall ICT penetration in households stood at 57 percent in 2000, whilst the number of Canadian SMEs⁴ connected to the Internet in Q2 2000 was 69 percent.

The number of Internet hosts stands at 3.9 million, whilst the number of websites per 1000 population is 24.7. The number of secure server per 100,000 population is 12.8.⁵ The number of telecommunications access paths per 100 inhabitants in 1999 stood at 88.1.⁶ The volume of B2B e-trade was 9.57 billion EUROS in 1999.⁷ The volume of B2C trade over the same period was 1.035 billion EUROS. With regards to wireless penetration, there are 17.6 Cellular Mobile Subscribers per 100 inhabitants⁸

As a developed country, Canada is placed consistently high within the Group of Eight (G8) on indicators of information and communications technology penetration. Much of this growth is fostered by the extensive links between the Canadian economy and that of the United States. In particular, the US is the main market for Canadian ICT exports, accounting for 84.2 percent of total foreign sales in 2000.⁹ ICT exports to the European Union have also increased, though only marginally (8.2 percent to 8.3 percent), between 1993 and 2000. Exports to the Asia-Pacific region fell during the same period from 8.9 percent to only 4.3 percent. Canada has a large trade deficit in ICT – though this has declined between 1999 and 2000. This deficit stems from the structure of the Canadian ICT sector (populated by foreign multinational enterprises and offshore parts dependencies) and from imports of semiconductors.

The growth of the Internet is facilitated in Canada by a strong government commitment to spreading the benefits of electronic commerce and network access to the entire population. Consistent with this objective, the federal government implements policies designed to encourage high levels of internet connectivity and e-commerce development. To quote an OECD fact sheet on Canadian electronic commerce policies:

¹ Information and Communications Technology Branch – Industry Canada, The ICT Sector in Canada, October 2001, 2.

² The ICT Sector in Canada, 1.

³ The ICT Sector in Canada, 3.

⁴ SME refers to Small- and Medium-Sized Enterprises.

⁵ Organisation for Economic Co-operation and Development, Communications Outlook 2001, Chapter 5 – “Internet Infrastructure”, 100-101.

⁶ Communications Outlook 2001, Table 4.2 “Telecommunications Channels per 100 Inhabitants in the OECD Area,” 81.

⁷ Industry Canada, Canadian Internet Commerce Statistics Summary Sheet, 2 March 2001, 1.

⁸ Organisation for Economic Co-operation and Development, Information Technology Outlook 2000, cited in Information Technology Association of Canada, IT in Canada: An Overview (Updated November 20, 2000), “International Comparison of Cellular Mobile Subscribers.”

⁹ The ICT Sector in Canada, 3.

“Canada set a goal of becoming a world leader in electronic commerce by the Year 2000 and has implemented supporting strategies both domestically and internationally. Domestically, Canada released The Canadian Electronic Commerce Strategy in September 1998, presenting a broad ten-part agenda based on four themes: building trust in the digital market place, clarifying market rules, strengthening the information infrastructure and realising opportunities. Canada has the foundation for a world-class electronic commerce framework, with policies or legislation on key issues such as cryptography, consumer protection, tax neutrality, privacy, E-signatures, public key infrastructure and standards”.¹⁰

Activities designed to accelerate Canadian ICT sector development were also driven by concerns with Y2K vulnerabilities. To address this problem, the Canadian government established Task Force Year 2000, comprised of Chief Executive Officers from major Canadian firms charged with assessing the nature of Y2K vulnerabilities facing Canadian industry. National surveys conducted under this task force’s auspices contributed greatly to vulnerability assessments later used for critical infrastructure protection planning.

Main ICT Regulatory and Legal Developments

As noted above, a national strategy designed to give Canada world leadership in e-commerce applications and markets was launched in 1998. Two important initiatives undertaken to implement this strategy focused on the E-Business (e-commerce) environment and upon the electronic delivery of government services (E-Government).

In October 1998, the Canadian Government issued a comprehensive policy statement on the conduct of electronic commerce seeking to address security, law enforcement, national security, and consumer protection concerns. Civil liberties issues arising from the necessity to “police” the public Internet was also addressed in the document.¹¹ In October of the following year, the federal government reiterated its goal of ensuring access to public information via the Internet in the Speech from the Throne. Three objectives were articulated during that address: improvement of the service to Canadians, acceleration of the growth in electronic commerce, and the exploration of new electronic means of delivering government services directly to citizens.

An initiative was launched to integrate government services – and their delivery – both horizontally (at the federal level) and vertically (through provincial and subsidiary levels of government). This was designed to build a secure and reliable digital infrastructure for the delivery of information and services. Establishment of a single point of access to government information, and legislation addressing legal and policy uncertainties surrounding electronic commerce were both designed to enhance the transparency and flexibility of the information infrastructure.

In terms of standards, the Canadian government identified at an early stage that their development was a key part of its electronic commerce strategy. To this end, the government chose to work through established organisations (most notably CSA International) to voice Canadian interest in the development of open and easily formulated electronic commerce standards. Other entities involved in implementing Canadian government strategy are the Standards Council of Canada (SCC, a federal Crown Corporation),

¹⁰ OECD Fact Sheet, *CANADA*, 1

¹¹ OECD Fact Sheet, *Canadian CIP Initiatives*, 1.

the Telecommunications Standards Advisory Council (TSACC), and the Electronic Commerce Council of Canada (ECCC).

Alongside this initiative was a programme designed to establish a multi-agency effort for strengthening the security of critical infrastructures. This effort focused around the Critical Infrastructure Protection Task Force, which began its work in April 2000. The Task Force concluded its work in March 2001, with recommendations for a successor structure designed to integrate public and private sector critical infrastructure protection efforts. The details of these recommendations are addressed in Section 4 of this note.

Assessment of Phenomena Undermining Dependability

Canada has a highly-developed awareness of the state of the cyber-threat. Much of this experience stems from the simple fact that Canadian society is highly dependent on computers for its daily functioning. The development of the Internet has led to a number of hacking and web-defacement episodes, as well as to the occurrence of a number of denial of service (DoS) incidents. Linked to these incidents is a growing awareness – fuelled by both the Y2K and 1999 ice-storm experiences – of the extensive interdependencies of key infrastructures on IT networks and technologies.

Canadian statements of cyber-threat typically track those of the United States. The “all hazards” approach to CIP adopted in Canada, however, adds a heightened awareness of physical infrastructure threats more analogous to recent US homeland security discussions. As stated by Margaret Purdy, threats in the “e-environment” are real and serious.¹²

The United States Department of Defense admits it identified 22,000 attacks on its systems in 1999 – of which 20,000 came from recreational hackers. The February 2000 Distributed Denial of Service attack against eBay, Yahoo, and Amazon, etc. resulted in at least US\$1.2 billion (EUR 1.34 billion) in lost revenue. The hack of October 2000 affected Microsoft’s high-level, internal network for several days, reportedly providing access to the source-code for one product in the early stages of development. Since February 2001, cyber-actors representing Israeli and Palestinian interests have conducted a cyber-war or e-jihad in the Middle East and beyond. They have defaced each other’s Web sites and have launched denial-of-service attacks and malevolent viruses at each other. Each of these activities indicates a heightened awareness of the cyber-threat, while at the same time also couching responses in terms of national priorities to mitigate disaster damage. This is the critical heart of the Canadian “all hazards” approach to CIP and dependability.

Government Initiatives Aimed at Tackling Cyber-Security

On February 5 2001, the Prime Minister of Canada announced the creation of the Office of Critical Infrastructure Protection and Emergency Preparedness (OCIPEP). The Office was established in continuation of the work of the Critical Infrastructure Protection Task Force promulgated in April 2000. As stated by Prime Minister Chrétien:

“The protection of Canada’s critical infrastructure from the risks of failure or disruption is essential to assuring the health, safety, security, and economic well being of Canadians. I am confident that these new measures will enable the Government of Canada to provide

¹² Margaret Purdy, *Cyber- Strategy for Government*, 5.

national leadership on this important issue and ensure our preparedness to deal with emergencies. We will also be able to build strong partnerships to ensure the protection of our shared North American Infrastructure.”¹³

In creating this office, Canada adopted an “all hazards” approach to critical infrastructure protection, conflating critical infrastructure disturbances with the occurrence of natural disasters such as ice storms or floods. Critical infrastructures were defined as encompassing six sectors: energy and utilities (such as electrical power, 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, emergency services) and Government (including major government facilities, information networks or assets).¹⁴

Seven key functions were defined for OCIPEP. These were monitoring of critical infrastructures for disruptions due to natural disasters or criminal/terrorist activity through a new **Infrastructure Protection Co-ordination Centre** (IPCC, to be staffed and operated around the clock), issuance of alerts, advisories, and information notes on threats and incidents affecting critical infrastructures, based on continuous analysis of threats, incidents, and infrastructure vulnerabilities, dissemination of advisories to federal agencies and departments, and co-ordination of responses to malicious code, IT threat, and other cyber-incidents, co-ordination of conference-calls involving stake holders during a critical infrastructure disruption. Also defined as OCIPEP functions are the response to *ad hoc* queries by industry and/or government on threats to critical infrastructure integrity, provision of early warning, guidance, and assistance associated with maintaining functionality in critical infrastructures in the face of threats to infrastructure operation and collection and consolidation of intrusion detection and malicious code data for pattern and trend analysis in order to characterise co-ordinated attacks
OCIPEP was also embedded within the Department of National Defence (DND).

OCIPEP is headed by an Associate Deputy Minister of National Defence - Margaret Purdy – a career public servant. The office inherits the Emergency Preparedness roles previously undertaken by Emergency Preparedness Canada. While a component of DND, OCIPEP remains a civilian agency, making it comparable to foreign entities with critical infrastructure protection roles such as the National Infrastructure Protection Center (NIPC) in the US and the National Infrastructure Security Co-ordination Centre (NISCC) in the United Kingdom. One factor differentiating OCIPEP from its US and UK counterparts is the fact that it does not have primarily a law enforcement focus. The Royal Canadian Mounted Police (RCMP) and the Department of the Solicitor-General maintain cognisance over investigations into criminal disruption of infrastructure systems and installations.

Associate Deputy Minister Purdy characterised the OCIPEP structure as combining key elements of the US CIP interagency approach into one office:

“[T]he Office I now manage will be roughly equivalent to Dick Clark’s (US Director of Cyber-space Security) role, FEMA (the US Federal Emergency Management Agency), the CIAO (the US Department of Commerce’s Critical Infrastructure Assurance Office),

¹³ Prime Minister of Canada, Prime Minister Announces Office of Critical Infrastructure Protection and Emergency Preparedness, 5 February 2001: www.pm.gc.ca/default.asp?Language=E&page=newsroom&sub=newsreleases&doc=emergency.20010205_e.htm

¹⁴ Critical Infrastructure Protection Fact Sheet, www.ocipep.gc.ca/critical/index_e.html

FedCert (the US Federal Government's Computer Emergency Response Team operated by the General Services Administration), and the non-investigative roles of the NIPC".¹⁵

This comparison is apt because of the close integration of critical infrastructure protection policy and response in the United States and Canada. In important terms, the Canadian office represents an "opposite number" to which the US critical infrastructure protection effort can respond, co-ordinate, and share actions and lessons learned.

As described by OCIPEP documentation, the agency leverages its efforts through a multi-part approach to protecting critical infrastructures. The components of this approach include awareness and education, research and development on CIP, information Sharing, partnerships with other Governments and the private sector, fostering sector-to-sector CIP relationships.

Importantly, one must emphasise here the "horizontal" nature of the partnerships being formed with other governments (international and provincial) and with the private sector. Each of the five dimensions identified above involves the use of existing relationships in order to advance CIP objectives, or the creation of new links – sometimes necessitating new legal or administrative approaches to bring them into being. The long-term efficacy of the new legal and policy frameworks still remains to be demonstrated.

The merging of the CIP and emergency preparedness functions points to the "greater than Cyber" nature of the new national security policy agenda. Indeed, the design for OCIPEP is influenced by the lessons learned from the 1998 ice storm affecting Eastern Canada and Quebec. In turn, severe floods in 1996 and 1997 also pointed to the importance of advance planning and consequence management efforts in order to mitigate the worst affects of infrastructure disruptions.¹⁶ Because most critical infrastructures are under the jurisdiction of provincial governments and/or owned by the private sector, Canadian federal policies necessarily emphasise decentralised collaborative "bottom up approaches".¹⁷ OCIPEP serves as a facilitator for these efforts – intentionally positioned as an intermediary institution empowered to fuse emergency preparedness and early warning functions where critical infrastructure threats overlap with those of natural disasters and accidents.

Similar to other countries, Canada does not seem to have exploited the lessons learned from the Y2K experience in addressing the country's dependability on information infrastructures. In order to prepare the country to tackle with the Millennium Bug, Project Solstice was launched. Although it originally came from the criminal intelligence arm of the Royal Canadian Mounted Police, this initiative involved also the Department of National Defence, Canadian Security Intelligence Canada and Canadian Law Enforcement. As the scope of Solstice's work expanded beyond the initial criminal intelligence realm, its goals and objectives increased as well. Among the various initiatives, the Solstice Project was able to identify the critical infrastructures with which the Canadian government had to establish a two-way communication. It also engaged their representatives in exchange information about "best practices" in protecting against threats associated with Y2K. These information-exchange and the general awareness of the country's dependability from information infrastructures are the two main results of this experience, which should probably be taken into consideration by OCIPEP

¹⁵ Margaret Purdy, Associate Deputy Minister, National Defence, remarks at "The Partnership for Critical Infrastructure Security, Annual Meeting and Public Policy Briefing," (20-22 March 2001): 2.

¹⁶ Remarks by James Harlick, Assistant Deputy Minister, National Defence, to the Cyber-Sabotage Conference 2001, Ottawa, Ontario (19 September 2001), 3.

¹⁷ Cyber-Sabotage Conference 2001, 6.

Industry and Other Non-Government Activities Related to Dependability

As noted in the previous section, privately-owned critical infrastructures are the central focus of consequence management and prevention efforts. The interconnections between infrastructures in Canada and the United States highlight the importance of non-governmental organisations to fostering an enhancement in critical infrastructure protection. Common infrastructures such as energy, transportation, and telecommunications each have industry-organisations designed to articulate stakeholder interests in dialogue with national governments. A good example of such organisations is the North American Electricity Reliability Council. The Council co-ordinates between and among North American electric utilities, facilitating information-sharing among business competitors, and transmitting potentially significant operational information to government authorities as an input to national security decision-making.

The Canadian government – through OCIPEP – seeks to create partnerships with private sector entities to enhance information-sharing between the public and private sectors. These links can also serve to facilitate sharing between the United States and Canada – in a way reinforcing official contacts between the two countries – and making sure that information generated during a CIP investigation is not lost. Other partners identified as important for the implementations of CIP and emergency preparedness plans include professional associations, chambers of commerce, insurance companies, and audit/verification professionals.

Public-Private Partnerships

The Canadian government has recognised the importance of partnerships – both between the private sector and government and between sectors – as a crucial enabler of enhanced critical infrastructure protection. OCIPEP conducts regular contact meetings with representatives of critical infrastructures. These meetings are designed to build trust and foster information sharing in both pre-event planning and incident response situations. In turn, OCIPEP's longer-term work on developing a CIP alert and warning system depends on a free flow of incident data (alongside forensic analytical products) deriving from natural and deliberately-triggered infrastructure disruptions.

The Information Operations Working Group (IOWG) – an activity of the Department of National Defence – has begun initiatives as part of its own CIP drive to seek partnerships with industry.¹⁸ This group addresses the Department's own dependencies on civilian communications infrastructures, and seeks to improve information assurance through outreach and joint activities.

Much of the Canadian approach to relations with the private sector in this area on CIP is based on the structures and contacts developed during the Y2K rollover. During that process, the Government of Canada worked with key private sector organisations and associations responsible for securing critical infrastructures, including the financial sector, the energy infrastructure sector, telecommunications firms, transportation firms, and health care providers. Each of these establishments is now involved in planning to secure critical infrastructures from disruption.

¹⁸ IOWG, www.csis.gc.ca/eng/operat/io2e.html (visited on 11 December 2001).

Research and Development

Canadian research and development on ICT comprises two parts: a portion financed by the private sector, and a second, smaller portion funded by the public sector. In 1999, privately funded ICT R&D totalled 3.93 billion EUROS.¹⁹ Obviously, it is inappropriate to evaluate all of the R&D expenditures as being targeted for critical infrastructure purposes. Nonetheless, where expenditures are in the network control, semiconductor, standards, or computer equipment (and telecommunications equipment) areas, they can meaningfully be linked to continuing CIP objectives.

Federally-funded R&D in the ICT area is performed through governmental research centres, and with industry and universities in research partnerships. Many ICT R&D projects have been funded by the Government of Canada. These include CANARIE (the Canadian Network for the Advancement of Research, Industry and Education) – a private-public sector partnership designed to accelerate development of Canadian advanced networks and derived services. In 1997, CANARIE established CA*netII, a national broadband network that gave the Canadian research community access to early-phase development projects on next-generation applications suitable for future broadband networks. CANARIE is now spending 49.10 million EUROS to develop the CA*net3, the world's first national optical R&D Internet. Offering up to 40 gigabits/second data transmission rates, this network will provide unparalleled capability to conduct collaborative work in advanced networking applications, research, and ultra-high speed information exchange. Network-related R&D on other access technology, namely wireless and optical and network management applications, is also funded through CANARIE.²⁰

A second project is NRC (the Canadian National Research Council). This operates two research groups addressing ICT: the Institute for Information Technology (IIT) and the Institute for Microstructural Sciences (IMS). Research conducted at these institutions is mostly done in collaboration with private firms and Canadian universities. Both NRC bodies are involved in the CA*net3 effort.

The CRC (Communications Research Centre) is a federally-funded laboratory dedicated to advanced communications R&D, whose research programmes provide a technical basis for the development of regulations and standards in support of telecommunications and broadcast policy.

PRECARN (Pre-Competitive Applied Research Network) is an industry-driven, not-for-profit consortium, national in scope, which sponsors, manages, and disseminates the results of long-term pre-competitive research projects in the area of intelligent systems and robotics. PRECARN has engaged over 1,200 individuals and 100 companies in a suite of major research projects at the leading edge of intelligent systems and robotics research.

TPC (Technology Partnerships Canada), in partnership with the private sector, invests in high-risk, near-market development and demonstration projects across Canada. TPC invests an annual budget of C\$300 million (EUR 214.5 million) in priority areas such as environmental technologies, biotechnologies, aerospace and defence, advanced manufacturing, and leading information and communications technologies.

NCE (Networks of Centres of Excellence) is a unique federal program comprising partnerships between industry and universities, designed to connect excellent research with industrial know-how and investment

¹⁹ Information Technology Association of Canada, [IT in Canada: An Overview](#) (visited on 20 November 2000). Slide 12.

²⁰ OECD Paper on Canadian ICT Policies and Programs, *CANADA*, 3.

capital. Five centres within the NCE address ICT areas. These are: the Canadian Institute for Telecommunications Research (CITR), the Institute for Robotics and Intelligent Systems (IRIS), Micronet, the Canadian Institute for Photonics Innovations (CIPI), and the Geomatics for Informed Decisions Network (GEOIDE).

The Defence Research and Development Branch of the Department of National Defence has several responsibilities, including facilitating and enhancing the ability of decision-makers to make informed decisions on defence policy, force generation, and procurement by providing expert scientific and technological knowledge (including on information security).

OCIPEP is charged with co-ordinating government-wide research and development on CIP issues across the Canadian government, and is likely to use the structure of federal ICT research institutions and activities to accomplish this end. Collaborative work is the focus of OCIPEP efforts, with the objective of leveraging timely investments in areas likely to yield tangible benefits for critical infrastructure protection.