CIIP Country Surveys

Canada

Canada

Concept of CIIP and Description of System

In Canada, CI is defined as "those physical and information technology facilities, networks, and assets whose disruption or destruction would have serious impact on the health, safety, security, and economic well-being of Canadians or on the effective functioning of governments in Canada".[1] Based on efforts made in anticipation of Y2K, the Critical Infrastructure Protection Task Force (CIPTF, see below) modified its results to settle on a characterization of CI/CII in six critical sectors. These critical sectors are the following ones:[2]

- (Tele-) Communications,
- Government,
- Energy and utilities,
- Financial services,
- Safety,
- Transport.

CIIP Initiatives and Policy

CIIP Initiatives

The Canadian government has recognized the importance of CIIP and that all elements of the CI are highly dependent on information technology.[3] This adds a new set of CII vulnerabilities and risks to natural hazards such as risk of earthquakes, floods, or ice storms. In the late 1990s, Canada intensified its CIIP efforts. The following list gives an overview of the main initiatives taken:

[1] Grenier, Jacques. "The Challenge of CIP Interdependencies". *Conference on the Future of European Crisis Management.* (Uppsala, Sweden, 19-21 March 2001). http://www.ntia.doc.gov/osmhome/cip/workshop/ciptf_files/frame.htm.

[2] http://www.epc-pcc.gc.ca/critical/index_e.html.

[3] Purdy, Margaret. *Cyber-Sabotage for Government. Speech at the Ottawa Congress Centre.* (Ottawa, 20 February, 2001).

National Infrastructure Risk Assessment (NIRA)

The National Contingency Planning Group (NCPG) was formed in October 1998. Part of its mandate was to develop a National Infrastructure Risk Assessment (NIRA). The NIRA's objective was to better position Canada for the transition to the year 2000. It set out to examine critical Canadian infrastructures.[4] In May 1999, excerpts of the NIRA were published in the book "Canada's Critical Infrastructure: An Overview".

Y2K Efforts

Later, the NCPG was given the mandate to monitor and coordinate federal organizations through the Y2K transition. One of the groups formed under the NCPG was the Infrastructure Analysis Group (IAG). Its mandate was to predict potential impacts of any Y2K failures on the Canadian infrastructure and critical government functions.[5] Drawing on lessons from the Y2K roll-over period, the Canadian federal government in April 2000 created the interdepartmental Critical Infrastructure Protection Task Force (CIPTF). The Task Force was charged with the development of proposals for a national CIP/CIIP policy framework.[6]

Strategic Infrastructure Initiative (SII)

The Treasury Board Secretariat[7] leads the Strategic Infrastructure Initiative (SII) in partnership with key departments and agencies. The SII will satisfy the government's accountability for the security of its IT infrastructure and allow it to meet its government on line objectives. Under the responsibility of the Chief Information Officer, the SII is focusing on designing a robust IT security architecture, establishing optimal IT security standards and practices, and developing the capabilities needed to more fully protect government-held information and communications with Canadians.

CIIP Policy

Based on the perception of the new risks such as IT dependencies/ interdependencies, spectacular terrorism, and mass casualty/urban

[4] National Contingency Planning Group. *Canadian Infrastructures and their Dependencies*. (March 2000), iv.

[5] National Contingency Planning Group. (March 2000), iv.

[6] http://www.dnd.ca/archive/2001/feb01/06protect_b_e.htm.

[7] http://www.tbs-sct.gc.ca.

destruction attacks, the federal government has taken several steps towards a better risk management policy.[8]

Government-on-line (GoL)

The government will put in place a technology and policy framework that protects the security and privacy of Canadians in their electronic dealings with their government. This is part of the GoL policy. Canadians will be able to transmit applications and financial transactions securely on-line and in real-time. GoL must address the principal security requirements for electronic transactions (data integrity, data confidentiality, availability, authentication, and non-repudiation).

"All Hazards" Approach

The establishment of the Office of Critical Infrastructure Protection and Emergency Preparedness (OCIPEP, see below) implicated the merging of the CIP/CIIP and emergency preparedness functions. With this process, the Canadian government pointed to the new national security policy agenda, which went beyond the realm of cyberspace. The setting of the new national security agenda was also influenced by the lessons learned from the 1998 ice storm affecting Eastern Canada and Quebec. The Canadian policy emphasizes decentralized, collaborative "bottom-up" approaches, because most of the CI/CII are under the jurisdiction of provincial governments or owned by the private sector.[9] The "all hazards" approach to CIP/CIIP in Canada adds a heightened awareness of physical infrastructure threats analogous to recent discussions on US homeland security.[10] The OCIPEP sees Canada's CI/CII potentially affected by both physical and virtual threats. It is also fully recognized that Canada's CI are heavily dependent on IT.

National Critical Infrastructure Protection Program (NCIPP)

The events of 11 September 2001 have accelerated the implementation of the National Critical Infrastructure Protection Program (NCIPP). The Canadian government is working on this program together with the provinces and the territories. The overall aim is to identify CI/CII of national interest, so that appropriate measures can be taken to protect them and

[8] http://faso.nrcan.gc.ca/newsfe_e.htm.

[9] Dependability Development Support Initiative (DDSI). *Global Overview – Countries, International and Inter-Governmental Organisations*. (version April 2002), 19.

[10] Dependability Development Support Initiative, Global Overview, (version April 2002), 16.

to mitigate and plan for the potential impact in case of failures. The objective of the NCIPP is to catalogue elements of the physical infrastructure as well as of cyberspace that could be at risk from a variety of hazards.[11] The government seeks to involve the provincial, territorial, and local authorities in this process, since it is crucial that these authorities be aware of CI/CII and of the possible significant impacts to their region in case of failures.

Law and Legislative Action[12]

The Constitution Act

This act defines the areas of federal and provincial authority and determines the leadership responsibilities of the different governmental agencies for emergency preparedness.

The Emergency Preparedness Act

This act is a major element of the federal framework. It charges Canadian ministers with the responsibility of making plans for emergencies that may fall under their jurisdiction.

The Emergencies Act

This act is a multi-part statute describing four types of national emergencies: (1) public welfare emergencies (including severe natural disasters and major accidents affecting public welfare), (2) public order emergencies (emergencies that constitute threats to the security of Canada), (3) international emergencies (acts threatening Canada's sovereignty, security, or territorial integrity), (4) war emergencies (real or imminent armed conflict against Canada or its allies).

Following 11 September 2001, Canada is reviewing its legislation, as are many other countries. A new OCIPEP legislative is being drafted to replace the Emergency Preparedness Act. The new legislation will include provisions for CIIP.

[11] http://www.gov.yk.ca/depts/community/pdf/3200-1129web.pdf.

[12] For this section, the author is indebted to ÖCB (ed.), *International CEP Handbook: Civil Emergency Planning in the NATO/EACP Countries 1999–2000*, (Stockholm, 2000), 33–36.

Organizational Analysis

Public Agencies

Office of Critical Infrastructure Protection and Emergency Preparedness (OCIPEP)

The Office of Critical Infrastructure Protection and Emergency Preparedness (OCIPEP) is Canada's main governmental organization responsible for CIP/CIIP. The OCIPEP, being embedded within the Department of National Defence, has the ability to call on specialized computer security expertise within the military and national security community. The Office is headed by the associate deputy minister of national defense.[13] The OCIPEP has the objective of developing and implementing a comprehensive approach to protecting Canada's CI/CII. The Office is also the government's primary agency for ensuring national civil emergency preparedness and therefore also encompasses the existing functions of Emergency Preparedness Canada.[14] However, the OCIPEP has no law enforcement and no investigative power. Its approach includes promoting awareness and education, research and development, information-sharing, and partnerships with other governments and the private sector.[15]

National CIO Subcommittee on Information Protection (NCSIP)

In 1998, the National CIO Subcommittee on Information Protection (NCSIP) was established at the behest of the Public Sector Chief Information Officer's Council (PSCIOC), representing all federal, provincial, and territorial governments and a Municipal Information Systems Association (MISA) representative. This forum enables participating governments to exchange information, policies, security awareness program practices, and architecture initiatives related to information protection.

Cooperation between Public and Private Sectors

Canada's CIIP policy is based on a broadly collaborative approach. The Canadian government seeks to create partnerships with private sector actors to enhance information-sharing between the public and the pri-

[13] The Minister of National Defence is responsible for the OCIPEP.

[14] http://www.epc-pcc.gc.ca/whoweare/index_e.html.

[15] Dependability Development Support Initiative, Global Overview (version April 2002), 19.

vate sectors.[16] The current policy postulates that the CIIP challenge has to be tackled by efforts on the part of the federal government and the provinces and territories, as well as individual CII owners. One part of that approach is international collaboration (above all with the US).[17] The public-private partnership approach of the Canadian government is largely based on the structures and contacts developed during the Y2K rollover. During this period, the Canadian government worked together with private actors responsible for the security of CII.[18]

OCIPEP Approach

An important cooperation approach in Canada between the public and private sectors are the regular meetings of OCIPEP and representatives of CI/CII. These meetings are a trigger for the building of trust and for fostering information-sharing. OCIPEP's tries to create Information Sharing and Analysis Centres (ISACs) within governments and within infrastructure sectors.[19]

Information Operations Working Group (IOWG)

The Information Operations Working Group (IOWG) is an activity of the Department of National Defence.[20] The group seeks to build partnerships with industry actors as part of its own CIP/CIIP efforts. The IOWG addresses the Department's own dependence on civilian communications infrastructure.[21]

[16] Dependability Development Support Initiative, Global Overview (version April 2002), 20.

[17] "Cyber-Sabotage for Government", speech by Margaret Purdy at the Ottawa Congress Centre, 20 February 2001.

[18] Dependability Development Support Initiative, Global Overview (version April 2002), 20.

[19] "Cyber-Sabotage for Government", speech by Margaret Purdy at the Ottawa Congress Centre, 20 February 2001 and http://www.cfcsc.dnd.ca/irc/nh/nh9798/0034.html.

[20] http://www.dnd.ca.

[21] Dependability Development Support Initiative, Global Overview (version April 2002), 20.

Early Warning

CanCERT

The OCIPEP provides subscribers with a range of services designed to support responses to computer security breaches. The OCIPEP promotes the collection, analysis, and reporting of statistics on Canadian IT security incidents. The CanCERT team and its subscribers are contributors to these goals.[22] CanCERT is a member of the international Forum of Incident and Security Response Teams (FIRST).

Research and Development

Research and development (R&D) in the field of CIIP is largely financed by the private sector, and partly by the public sector. The following are some of the most important government-funded R&D activities:[23]

The OCIPEP promotes CIIP R&D across the branches of the Canadian government. The OCIPEP encourages collaborative work among governments, the industry, and academia to address crucial requirements in such areas as intrusion detection.[24]

The Canadian National Research Council (NRC) operates the Institute for Information Technology (IIT) and the Institute for Microstructural Sciences (IMS). These institutes conduct their research mostly in collaboration with private firms and universities.

Research at the Communications Research Centre (CRC) is focused on advanced communications. The research programs provide a technical basis for the development of regulations and standards in support of telecommunications and broadcast policy.

The Networks of Centers of Excellence (NCE) is a unique federal program in Canada that facilitates partnerships between industry and universities.

The Defence Research and Development Branch of the Department of National Defence Research and Critical Infrastructure Protection has several responsibilities. They include facilitating and enhancing the ability of decision-makers to make informed decisions on defense policy.

[22] http://www.cancert.ca.

[23] Dependability Development Support Initiative, Global Overview (version April 2002), 22.

[24] Purdy, *Cyber-Sabotage for Government*.