Conference Report

Future Directions for Critical Infrastructure Protection for Canada

On 17-18 November 2000, the Centre for Conflict Studies of the University of New Brunswick hosted a ground-breaking event: the first public academic conference on Critical Infrastructure Protection (CIP) in Canada. The conference brought together some three dozen experts from all levels and many branches of government, the business community, public utilities and academia. The conference began with a reception on the evening of the 17th. Formal sessions began the next morning.

Margaret Purdy, Deputy Secretary to the federal Cabinet for Security and Intelligence delivered the keynote address. Ms Purdy explained the origins of the Critical Infrastructure Protection Task Force (CIPTF), its mandate and its general findings. The first of these is that a whole new approach to CIP is needed because Canada's CI are now so electronically interdependent. The second is that Canada's CI are not adequately protected. Third, Canada needs a national strategy for CIP. Fourth, the federal government can lead by example, putting its own house in order first. But it cannot impose a rigid, regulated standard on the other players. Rather, it needs to establish partnerships with the provinces and the private sector. Finally, there is a need for awareness, training and education and research and development. Ms Purdy closed her talk by posing some key questions: How do we engage the private sector in CIP? Is there a role for auditors and the insurance industry in motivating key players? How do we get government and business to think on "Internet Time" so they will respond quickly to the fast-changing threat and vulnerability environment? How do we approach the challenge of collecting intelligence on individuals and groups who might attack Canada's CI? How should we characterize CIP - as a security and intelligence issue, a technology or economic issue, or as an emergency planning issue? Will we be able to achieve the necessary level or horizontal cooperation to meet the CIP challenge?

Drawing upon a study he conducted for Solicitor General Canada in 1999, Dr David Charters, Director of UNB's Centre for Conflict Studies, started his presentation by offering a definition of CI: "Interdependent, interactive, interconnected networks of institutions, services, systems and processes that meet vital human needs, sustain the economy and maintain continuity of and confidence in government." He then surveyed the Canadian CI inventory, identifying those components which have a high level of criticality: electrical power, oil and natural gas industries and distribution, water purification and sewage treatment, hospitals and health care services, emergency services, financial services, telecommunications, air, rail and road transportation systems and the food industry, among others. He drew attention to their inter-dependencies and their potential vulnerabilities to a range of threats, from natural disasters and accidents to deliberate disruption and sabotage. The consequences of such events could be catastrophic, if the right CI are "taken down." But, he closed by emphasizing that while vulnerability implies risk, that is not the same as a threat, which was addressed by the following speaker.

Dr Tim Smith of the Canadian Security Intelligence Service presented a "Threat Assessment" on Canadian CI. He identified three broad threats: espionage/sabotage; terrorism; and what he called "Hacktivism." In the fields of espionage/sabotage and terrorism, traditional means are being supplemented by Ôcyber' means. One consequence of that is the difficulty in identifying the source of cyber attacks, since these can be routed through several countries before reaching the target. Smith drew attention to the fact that a number of countries are developing cyber-warfare capabilities. He pointed out that terrorist attacks on computer-related targets are not a new phenomenon; the earliest incidents date back to the 1980s. He also drew distinctions between actual terrorism and sabotage. Terrorist attacks include an element of coercion, which is not present in all cyber attacks. Smith argues that terrorists will use cyber attacks in the future, either by gaining the capabilities themselves or by hiring them. He defined Hacktivism as the conjunction of hacking and activism, in which the Internet is used for politically motivated purposes short of terrorism. This is currently the most common cyber threat, as demonstrated by the recent demonstrations against "Globalization," which were mobilized in part by information-sharing among activist groups on the net. Those protests were accompanied by cyber attacks on a number of corporations. Smith concluded by suggesting that the problem is likely to grow.

David Black, of the RCMP's Technical Security Branch (TSB), described the RCMP's role in IT Security and Threat Assessment. He opened his presentation with a description of a recent bank fraud incident in the UK, in which the bank was robbed electronically. He went on to highlight the range of electronic threats, from viruses - by far the largest problem - to other forms of malicious software, to Denial of Service attacks. To deal with these problems the RCMP's TSB has a mandate to develop new IT Security techniques, to prevent, detect, investigate and prosecute technological crimes that threaten Canadian CI. The Branch is the lead agency on physical and IT security, but it works in close cooperation with the Criminal Intelligence Directorate, the Economic and Technological Crime Sections and the Technical Operations Branch. It shares the IT Security Research and Development mission with the Canadian Police Research Centre, which is housed in the National Research Council. The TSB itself has a 24/7 incident response capability. The RCMP, CSIS, CSE and DND are working jointly to set up a pilot Government Infrastructure Protection Coordination Centre (GIPCC) in December 2000.

Katie Tolan, Canadian representative at the US National Infrastructure Protection Centre (NIPC) in Washington, DC, explained the American approach to CIP. The list of American CI's is similar to Canada's: government operations; telecommunications; power; transportation; banking and finance; water; and gas and oil storage and delivery. The US government approach is outlined in two Presidential Decision Directives: 62 and 63 (1998). PDD 62 highlights the new threats to CI, made possible by changes in access to information, new tools (computers and other IT elements), globalization and interdependencies, all of which combine to make threats hard to predict. Threats fall into three categories: unstructured (insider crime, hackers); structured ("hacktivists," economic espionage and organized crime); and national security threats (terrorists, intelligence agencies and "Information Warriors"). PDD 63 sets the policy framework and goal: to create a secure government information system by 2003. The Critical

Infrastructure Assurance Office (CIAO) was established to implement PDD 63. It created lead agencies in each sector and established public-private sector partnerships. For example, information sharing committees have been established in the financial services, telecommunications and electrical power sectors. The NIPC, created in 1998, operates under the authority of the Attorney General. It has four key responsibilities: warning (24/7), response, assessment and investigation. In addition, it is to share and disseminate information, and to train cyber investigators for government and the private sector. Although it is housed in the FBI, it is a multi-agency body, and will eventually include the private sector. This reflects the fact that in the CIP field national security is a shared public-private responsibility. Ms Tolan closed her presentation with data showing the dramatic rise in computer intrusion cases, indictments, arrests and convictions.

Brenda Hensler-Hobbes was serving at the time of the conference on the CIPTF. Her presentation focused on a number of key issues the TF had addressed up to that time. She briefly reviewed the historical background to CIP, and drew attention to its new dimensions. What has changed is increased: reliance on IT; interdependencies; vulnerabilities; and impact of disruption and destruction. Her review of threats was consistent with those identified by earlier speakers. She explained that the TF had surveyed activities related to all aspects of national CIP, and had reached several conclusions. First, there is no comprehensive approach to CIP: no overall policy and no operational framework. Second, CIP efforts in government and the private sector are uneven. Third, Canada is not well-prepared to detect and respond to deliberate actions either using cyber means or targeting the cyber dimension of CIP. Finally, it concluded that while Canada is well placed to handle the threat and impact of natural disasters and accidents on the physical aspects of CI, it is not well-prepared to deal with the cyber impacts. Ms Hensler- Hobbes identified four elements needed for a national CIP strategy: leadership by example; building creative and sustainable partnerships; developing effective, targeted CIP programmes; and developing a national CIP policy and operational capabilities. She stressed the importance of public-private sector partnerships, since the majority of CI is not owned and operated by the federal government. Balancing issues of ownership and accountability, she concluded that the federal government's role should be leadership to foster, but not to control, cooperation on CIP.

John McCallan, the Regional Director for Emergency Preparedness Canada in New Brunswick, gave the conference a briefing on the relevant legislation and on the basic principles of Canadian emergency preparedness. The *Emergency Preparedness Act* defines the functions and responsibilities of the minister responsible for EPC (the Minister of National Defence) and establishes the EPC program. The Emergencies Act defines four types of emergencies: public welfare - natural disasters or accidents; public order - internal security threats; international - foreign threats or coercion; and war. He then discussed the four basic principles: response devolves upon the lowest level competent to deal with the given emergency; planning embraces preparations to deal with all types of hazards and emergencies; plans and arrangements are based on established structures and procedures; and the Canadian approach combines centralized direction and coordination with decentralized implementation and response.

Danny Keizer, Director of Strategic Initiatives and Security for the Government of New Brunswick addressed the issue of collaboration on protection of information and IT assets. In the first part, he discussed the rise of threats and incidents, including website attacks and viruses. Both have shown dramatic increases over the last two years. There also have been many attempts at intrusion of government communications via the Internet. He noted that the "Loveletter" virus in May 2000 affected 7,600 provincial government desktop computers across Canada (about two percent of the total). This caused some provincial and federal government departments to shut down their email systems for a week. In the second part of his presentation, Mr Keizer explained the work of the Subcommittee on Information Protection (SCIP), an initiative of the National Public Sector Chief Information Officers Council. SCIP consists of representatives from the federal government, each provincial and territorial government, and the Municipal Information Systems Association. It's mandate is to share information and set goals and priorities on information protection, and to create, develop and support operational procedures. SCIP has initiated several projects, including development of: a security awareness strategy; an operational capability with a Canadian Information Protection Coordination Centre; a common approach to secure electronic service delivery; Canadian information security classification standards; a Canadian security impact assessment guide; incident response standards and procedures; and a Canadian intrusion detection system (an engineering research pilot project).

The final presentation of the conference was delivered by Maren Hansen of CanCERT - the private sector Computer Emergency Response Team, operated by the Ottawa-based firm, EWA-Canada. Her presentation was built around three themes: structured communication across sectors; research and development; and education. Emphasizing the lack of boundaries in networks and thus in incidents, and the fact that hackers work together and learn from each other, those responding must work together - nationally and internationally. In particular, there is a need for widespread private sector consultation. More R&D is needed, if only to keep pace with the hackers, who are doing their own R&D. Computers and networks have been developed for use rather than security, which now requires much more attention. There are vulnerabilities at all levels of the IT infrastructure: communications and services; operating systems; and applications. Ms Hansen pointed out that the response timeline currently is well behind the hacker's tool development and exploitation timeline. The aim of responders should be to develop and apply counter-measures sooner in the timeline, to limit exposure to attacks and intrusions. Industry must be proactive in reducing vulnerabilities, in finding ways to handle the huge volume of data to be analyzed and in providing ways to correlate incident data. Ms Hansen stressed the need for a broad-based approach to CI security education, combining: common sense awareness training; computer and network security; law and technology; psychology; strategic and conflict studies.

A number of common key themes emerged from the conference. The advent of the networked world has changed the nature of CIP, but Canada is not yet well-prepared to deal with the changing (ie., cyber) threats or their consequences. Before it can be properly prepared, the federal government will have to articulate a national policy, develop a national strategy and establish an operational framework. The federal

government can lead by example, and secure its own parts of the CI, but can only coordinate its efforts with those of other sectors; it cannot direct them. Therefore, partnerships and teamwork with other levels of government and with the private sector are essential. Research and development will be essential to keep pace with the threat and to provide "early warning" and rapid response, but this means that governments and business will have to be able to "think on Internet time." This, in turn, will require a new broad-based approach to IT security education.

The urgency of the CIP issue and the timeliness of the conference is evident from the fact that the federal government has moved quickly to establish a national CIP capability. In December 2000, it activated the Government Information Protection Coordination Centre. In February 2001, it established the Office of Critical Infrastructure Protection and Emergency Preparedness, under the leadership of our keynote speaker, Ms Margaret Purdy.