IN BRIEF

Parliamentary Research Branch
Library of Parliament

Michel Rossignol
28 June 2001

Critical Infrastructure Protection and Emergency Preparedness

INTRODUCTION

Computer technology is now such a pervasive element of modern society that its benefits for governments, corporations, public utilities, and many other organizations are taken for granted. However, the computer age has also introduced new vulnerabilities. The technology is so widespread and interconnected in the banking, commercial, energy, and manufacturing sectors that any deliberate or accidental interference can have costly repercussions. Furthermore, any tampering with the computers managing public utilities such as hydroelectric plants and related infrastructure such as dams could cause serious environmental damage as well as major disruptions in commercial transactions and industrial production. A country's critical infrastructure could be the target of attacks by terrorist groups based at home or abroad, by foreign governments, and by criminal elements. The widespread disruptions caused by some recent computer hacking incidents are perhaps only a small sample of the impact a concerted effort to paralyze the essential infrastructure of a country through its computer systems could have. In the not-so-distant future, the capacity to wage offensive as well as defensive information technology warfare could become an increasingly important element of a country's ability to ensure its security, but this raises complex moral and ethical issues which are just starting to be debated.

INCREASED EMPHASIS IN THE UNITED STATES

In the meantime, the potential impact of just a few isolated attacks on a country's essential infrastructure has raised concerns within government and military circles. The United States in particular has devoted considerable efforts and resources to bolster its ability to deal with such attacks. Indeed, in the late 1990s, the United States became increasingly conscious that despite its great military power, it could still be very vulnerable to what has been called asymmetrical threats. Instead of directly confronting the United States, military forces, states or groups antagonistic towards the U.S. could launch terrorist strikes against that country's critical infrastructure in order to damage the economy and terrorize the population. To increase the impact of their actions on the civil population, antagonistic states and groups could also resort to terrorist attacks using weapons of mass destruction (WMD) including small nuclear bombs and chemical and biological agents. Thus, in conjunction with measures taken to protect its vital computer systems, the U.S. has also improved its capacity to deal with the consequences of terrorist attacks with weapons of mass destruction.

Given the emphasis on the protection of the population and the infrastructure within the continental United States, the measures taken by the U.S. government to counter asymmetrical threats are often grouped within what is called homeland defence. The key elements of homeland defence include two Presidential Decision Directives of 1998: PDD-62, which was aimed at increasing the capacity of civilian police and medical officials as well as some military units to deal with the consequences of WMD attacks; and PDD-63, which sought to improve the coordination of the various agencies involved in protecting information technology systems. These agencies include: the National Infrastructure Protection Centre (NIPC), within the Federal Bureau of Investigation (FBI), which is the focal point for threat assessment, warning, investigation, and response to threats to or attacks against the critical infrastructure; and the Critical Infrastructure Assurance Office (CIAO), housed within the Commerce Department, which is involved in the coordination of U.S. Government initiatives. The U.S. Space Command was designated as the lead organization for the protection of military computer systems. The complex inter-agency process involved in dealing with cyber-related issues was described in

the National Plan for Information Systems Protection issued by the U.S. Government in January 2000. The new Bush Administration also gives a high priority to critical infrastructure protection, but has announced its intention of producing a new version of the National Plan by late 2001.

Critical infrastructure protection is inevitably complex because it involves privately owned elements as well as government and military ones. Indeed, government and military systems represent a relatively small portion of the U.S. critical infrastructure when compared to the extensive privately owned and operated systems in the banking, commercial, and public utilities sectors. Thus, part of the efforts deployed by the U.S. Government to protect the infrastructure involves close cooperation with the private sector in order to: raise awareness of the issues; and improve coordination – between corporations and government agencies – of measures to deal with cyber attacks. However, the interconnection between computer systems does not end at borders, and the cooperation of other countries is also crucial in critical infrastructure protection.

CANADIAN INITIATIVES

Indeed, as already demonstrated on numerous occasions, hacking and other types of cyber attacks against U.S. systems can have serious repercussions for the critical infrastructure of many other countries. Banking, commercial, and government systems throughout the world are so interrelated that few countries can afford to neglect preparations to deal with the consequences of deliberate or accidental interference. Thus, in February 2001, Prime Minister Jean Chrétien announced the establishment within the Department of National Defence of the Office of Critical Infrastructure Protection and Emergency Preparedness (OCIPEP) which has the task of developing and implementing a comprehensive approach to the protection of Canada's critical infrastructure. The new agency encompasses the functions of what used to be called Emergency Preparedness Canada since it may have to deal with the consequences of disruptions in computer systems monitoring or the operation of physical elements of the critical infrastructure such as hydroelectric dams and oil pipelines. The emergency preparedness side of the agency will also continue to prepare for, and respond to, natural disasters and other situations unrelated to cyber attacks as Emergency Preparedness Canada did in the past. Indeed, a high level of preparedness will no doubt have to be maintained if only because of the possible increase in the number of extreme weather events due to climate change. However, the creation of a new agency is also aimed at bringing Canada's critical infrastructure protection up to speed in light of developments in the U.S. and in other countries. In terms of cyber attacks, Canada does not necessarily face as great a threat as the U.S. which is the main target of a number of antagonistic states around the world. However, Canada cannot afford to lag too far behind its allies in the protection of its critical infrastructure because there is always a possibility that terrorist groups could launch attacks against the U.S. through Canada. Besides, Canada might suffer collateral damage as a result of cyber or WMD attacks within the U.S., regardless of the route chosen by antagonistic states and groups to carry out their aggression.

Nevertheless, despite the creation of OCIPEP, the Solicitor General remains the lead minister for public safety in Canada. Indeed, as the minister responsible for OCIPEP, the Minister of National Defence will collaborate closely with the Solicitor General and other ministers to ensure a coherent and comprehensive national approach to critical infrastructure protection and emergency preparedness. Thus, the new office will not take over or coordinate the work of the Canadian Security Intelligence Service (CSIS) and the R.C.M.P. in assessing and dealing with the terrorist threat. It will instead cooperate with them and rely on their assessments of potential threats, as pointed out by Margaret Purdy, the Associate Deputy Minister of National Defence, who is responsible for OCIPEP within the department, during the 29 May 2001 meeting of the Standing Committee on National Defence and Veterans Affairs of the House of Commons. The office will also benefit from the ongoing work of organizations within the Department of National Defence involved in the protection of military and government computer systems. One of these organizations is the Communications Security Establishment (CSE) which advises government departments on network security by providing, for example, threat risk assessment support services.

However, as in the U.S., ensuring the security of military and federal government information technology systems is only one element of critical infrastructure protection. After all, as the Minister of National Defence pointed out in a 26 June 2001 speech during the World Conference on Disaster Management held in Hamilton, Ontario, only about 10% of Canada's critical infrastructure is owned or operated by the federal government. Although private

infrastructure owners and operators have developed their own information technology security programs, considerable work remains to be done to improve cooperation such as information-sharing between the public and the private elements of Canada's critical infrastructure. Thus, as part of its development of a National Framework for critical infrastructure protection, OCIPEP will not only work to improve the federal government's capacity to protect its information technology systems, but also develop partnerships with private infrastructure owners and operators and with business organizations such as the Canadian Chamber of Commerce and the Canadian Bankers Association. However, even if the protection of Canada's information technology systems against intentional disruptions is maintained at a high level, the country may still have to deal with major natural disasters and cannot afford to be complacent about emergency preparedness. Thus, on 26 June 2001, the Minister of National Defence also announced that the Government of Canada will begin consultations, led by OCIPEP, with the provinces and the territories and with the private sector in order to develop a National Disaster Mitigation Strategy aimed at saving lives and reducing the impact of disasters.

Indeed, the efforts deployed to protect information technology systems and to bolster emergency preparedness are in keeping with the growing recognition over the years that a country's security depends on more than its ability to defend itself against attacks by foreign military forces. In the absence of a sufficient capacity to counter the terrorist threat and to mitigate the effects of major natural disasters, a country could face serious social and economic disruptions which could seriously undermine its security. Thus, the protection of the critical infrastructure will likely continue to be a major preoccupation of the Canadian government for some time to come, especially because considerable work remains to be done in the development of closer cooperation between the public and private sectors.