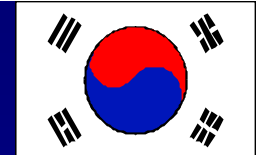


Creating Trust in Critical Network Infrastructures

# Canadian Case Study

Michael Harrop





## Overview of Presentation

- Outline of the Canadian environment
- Organisations involved in infrastructure protection
- Legal issues
- The importance of network infrastructures to the Canadian economy
- Examples of network infrastructure dependencies
- Protection of the enterprise
- Conclusions and Suggestions for Further Study





## The Canadian Environment

- Three levels of government each with distinct responsibilities
- Vast country (almost 7% of the world's land mass)
- 31 million people spread over 10 million sq. km.



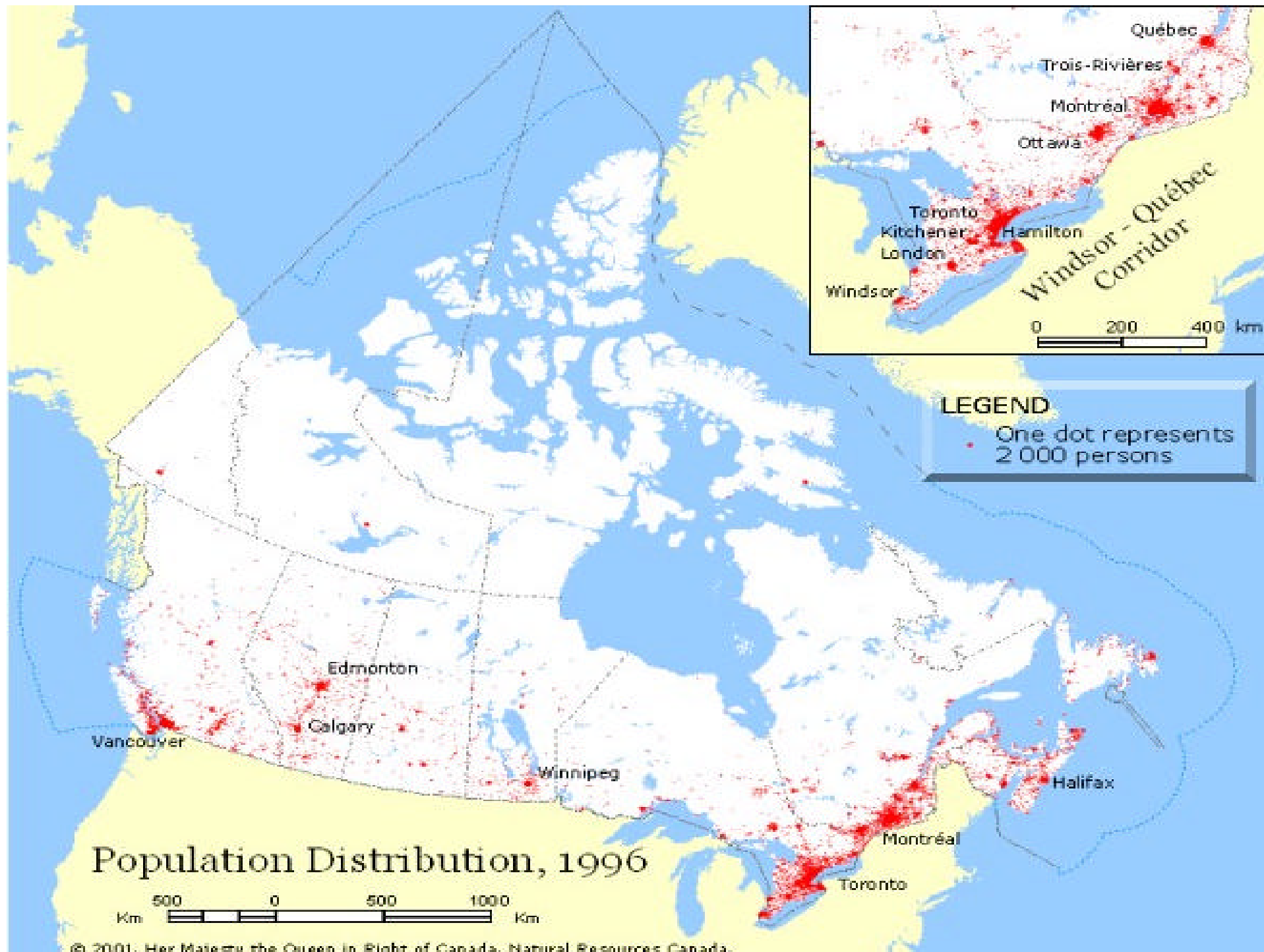




## The Canadian Environment

- Population largely concentrated in urban centres but rural and remote parts of the country must also be served







## The Canadian Environment

- The environment (i.e. the geography, population distribution, the remoteness of some communities, and the size of the country) presents serious challenges to providing telecommunications





## Key Organizations in Canadian Critical Infrastructure Protection

- Federal Organizations:
  - Office of Critical Infrastructure Protection and Emergency Preparedness (OC�PEP)
  - Communications Security Establishment (CSE)
  - Royal Canadian Mounted Police (RCMP)
  - Industry Canada
- Provincial & Municipal Organizations
- Non-government Organizations



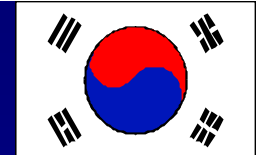




## Legislation

- Legal issues relating to networks and data security are addressed functionally under various sections of the Criminal Code.
- Canada has signed the Council of Europe Convention on Cyber-Crime and is active in the G8 Lyons Group on High-Tech Crime.
- The Canadian government is now examining what changes to current criminal law might be required in order to implement the Council of Europe convention.





## Telecommunications and Network Services

- Teledensity - 92.1 access lines per 100 of population
- 562 existing or emerging wireline competitive carriers, 14 wireless providers, and 187 satellite and other providers
- 3.7 million households with Internet service
- 51% of households have at least one regular Internet user





## The importance of networks to the Financial Services- 1

- 3000 financial services organizations, all heavily dependent on telecommunications
- LANs, MANs, WANs, Private, Shared and Public networks
- 5 million transactions Inter-bank transactions\_per day with average value in excess of \$135 million
- 1999 settlements totalled more than 30 times GDP





## The importance of networks to the Financial Services- 2

- Interac (Private Network)
  - *Over 2 billion transactions (Cdn\$94.9 billion in sales) in 2001*
  - *10.8 million direct debit transactions on busiest single day*
- Credit cards (on-line authorization)
  - *1,226 million transactions valued at \$121.8 billion in 2001*





## The importance of networks to the Financial Services- 3

- **PC/Internet Banking**
  - *47.2m transactions in 2000*
  - *increase of 74% over 1999*
- **Telephone Banking**
  - *74.0m transactions in 2000*
- **E-Commerce**
  - *\$7.2 billion in Internet orders in 2000*





## The importance of networks to government

- Increasing reliance on Internet for service delivery at all levels of government
  - *Over 11m income tax returns filed electronically in 2001*
  - *The Government of Canada web site receives almost 4 million page requests per week.*
  - *The online Job Bank is receiving 100,000 visitors to every day*





## Critical Infrastructure Dependencies - 1

- The National Telecommunications Infrastructure
- The Electricity Industry
- Internet Services





## Critical Infrastructure Dependencies - 2

- **Examples of other industries that would be seriously affected by network failure:**
  - *Financial Services*
  - *Government*
  - *The Oil and Gas Industry*
  - *Surface Transportation - land and marine*
  - *Air Transportation and Airports*
  - *Food Production and Distribution*
  - *Health Care*



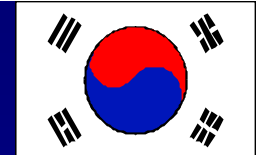




## Protecting the Enterprise from Network Attacks- 1

- *Insider* threats constitute the dominant threat to networks and end-systems for most organizations
- A consistent, enterprise-wide approach to security is essential
- Network security must protect the network, end-systems and applications using network facilities; and support the provision of services to protect user data in transit for both insider and external threats.





## Protecting the Enterprise from Network Attacks- 2

- Good perimeter defence is absolutely essential to protecting each part of the enterprise
- Perimeter defence can be applied in layers
- Perimeter defence is not enough. You still need to protect the data at all times, whether in storage or in transit.





# Conclusions and Suggestions for Further Study





## The importance of networking infrastructures to the Canadian economy

- *Both public and private sectors are highly dependent on networking infrastructures for their day-to-day operations, and this dependence is growing*
- *Although both sectors are increasingly relying on the public Internet for service delivery, to a large extent, Canadian organizations appear to be still using traditional communications channels, rather than the Internet, for their most critical applications*





## Work is needed to address the criticalities.....

- *We need to re-examine infrastructure criticalities to identify the points of risk and to determine how to protect them*
- *We need for a coordinated approach that addresses both the emergency measures aspects and the cyber security aspects of infrastructure protection*





.... and understand the interdependencies

- *Critical Infrastructure Protection comprises many facets, the interdependencies of which are not yet well understood. Much work needs to be done to identify the interdependencies and the potential implications of those interdependencies*





## The robustness of networks

- *Traditional carrier networks are relatively robust: the Internet much less so*





## The risk to network infrastructures

- *Traditional network infrastructures are at risk as a result of the changed communications environment*



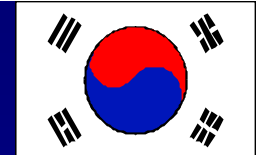




## The impact of Internet-based threats

- *Critical infrastructures are at risk from Internet-based threats.*
- *There is a need for aggressive defensive measures to protect systems and information from attack and for much more effort to be put into ensuring the “correctness” of networking software and systems*





## The application of cyber-crime laws

- *Cyber-crime laws and their application are not consistent from country to country. There is a need for greater consistency in cyber-crime laws and in their application*





## Summary

- Many sectors of the economy are highly dependent on networks.
- The critical network infrastructure is vulnerable to attack which, if realized, could have a devastating effect.
- Much work needs to be done to get a better understanding of the criticalities and interdependencies.
- Greater international cooperation is needed to fight cyber crime.





**Thank You**

