Canada

Last Updated: October 2021

CYBERSECURITY POLICY

Strategy Documents

National Cyber Security Strategy: Canada's Vision for Security and Prosperity in the Digital Age

Government of Canada

Strategy to strengthen three pillars: Security and resilience; Cyber Innovation; and Leadership and Collaboration through an approach rooted in a sustained commitment to:

- Protect the safety and security of Canadians and our critical infrastructure;
- Promote and protect rights and freedoms online;
- Encourage cyber security for business, economic growth, and prosperity;
- Collaborate and support coordination across jurisdictions and sectors to strengthen Canada's cyber resilience;
- Proactively adapt to changes in the cyber security landscape and the emergence of new technology.

Source

2018

Strong, Secure, and Engaged: Canada's Defence Policy

National Defence Ministry

- The most sophisticated cyber threats come from the intelligence and military services of foreign states
- Potential adversaries, including state proxies and non-state actors, are rapidly developing cyber means to exploit the vulnerabilities inherent in the C4ISR systems (command, control, communications, computers, intelligence, surveillance, reconnaissance) on which militaries depend

Source

2017

Royal Canadian Mounted Police Cybercrime Strategy

Royal Canadian Mounted Police

Identifies three pillars, provides 15-step action plan

1. Identify and prioritize cybercrime threats through intelligence collection and analysis
2. Pursue cybercrime through targeted enforcement and investigative action
3. Support cybercrime investigations with specialized skills, tools, and training

Source

2015

National Strategy for Critical Infrastructure

Public Safety Canada (PS)

- The Strategy is to be read in conjuction with the Action Plan for Critical Infrastructure.
- The objectives of the Strategy are to:
  - build partnerships;
  - implement an all-hazards risk management approach; and
  - advance the timely sharing and protection of information among partners.

Source Source 2

2010

Implementation Frameworks

National Cross Sector Forum 2021-2023 Action Plan for Critical Infrastructure

Public Safety Canada (PS)

Canada

Last Updated: October 2021

- The Action Plan reaffirms the Government's commitments to work closely with critical infrastructure sector partners, provinces and territories towards a more secure and resilient Canada.
- The Plan builds upon progress made through past action plans, identifies new activities based on the changing threat environment, and will support a collaborative approach to enhance the security and resilience of Canada's critical infrastructure.
- The Action Plan continues to support the three strategic objectives identified in the National Strategy for enhancing the resilience of critical infrastructure in Canada:
    - Building partnerships;
    - Sharing and protecting information; and,
    - Implementing an all-hazards risk management approach.

Source Source 2

2021

Canada's implementation of the 2015 GGE norms

[In this report, Canada shares] some of the best practices it has identified and the lessons it has learned on the implementation of previously recognized voluntary, non-binding norms of responsible State behavior endorsed by the UN General Assembly, in case this is useful to other UN member States as they seek to implement the 11 norms laid out in the 2015 GGE report.

Source

2019

Action Plan 2010-2015 for Canada's Cyber Security Strategy

Government of Canada

- Outlines plan of implementation towards the three pillars
- Specifies deliverables and timelines, specifying lead actors

Source

2013

STRUCTURE

National Centre or Responsible Agency

Canadian Centre for Cyber Security

Government of Canada

- Canada's authority on cyber security; unites operational cyber security expertise from Public Safety Canada, Shared Services Canada, and the Communications Security Establishment into one organization
- Acts as National CERT, and the Government of Canada CIRT (Computer Incident Response Team), working in close collaboration with government departments, critical infrastructure, Canadian businesses and international partners to respond to and mitigate cyber events
- Focuses on five key areas:
    1. To **inform** Canada and Canadians about cyber security matters, as a single, clear, trusted source of information on cyber security for Canadians and businesses
    2. To **protect** Canadians' cyber security interests through targeted advice, specific guidance, direct hands-on assistance, and strong collaborative partnerships
    3. To **develop** and **share** specialized cyber defence technologies and tools resulting in better cyber security for all Canadians
    4. **To defend** cyber systems, including government systems, by deploying sophisticated cyber defence solutions. We have over 70 years of experience in defending Canadian government systems
    5. To **act** as the operational leader and government spokesperson during cyber security events. Our expertise and access puts us at the forefront of cyber security in Canada

Source

Key Positions

Canada

Last Updated: October 2021

Minister of Public Safety and Emergency Preparedness
Public Safety Canada (PS)
Source

Minister of Foreign Affairs
Government of Canada
Source

Minister of National Defence
Government of Canada
Source

Dedicated Agencies and Departments

Cyber Crime Fusion Centre
Royal Canadian Mounted Police
Centre intended to

- Address key analytical cybercrime gaps;
- Better assess and help respond to criminal cyber incidents;
- Provide a more comprehensive understanding of cybercrime threats and risks; and
- Publish an annual report on cybercrime and describe the work done on collecting and analyzing statistics

Source

2011

Cyber Threat Evaluation Centre
Communications Security Establishment

- Responsible for the detection, analysis, and assessment of cyber threat activity on nationally important networks
- Composed of technical and analytical specialists

Source

2011

LEGAL FRAMEWORK

Legislation

Personal Information Protection and Electronic Documents Act (PIPEDA)

- Federal privacy law for private-sector organizations
- Requires an organization maintain a record of every breach of security safeguards

Source

23 June 2015 (amended); 13 April 2000

Criminal Code of 1985
Includes provisions on unauthorized use of computer

Canada

Last Updated: October 2021

- 342.1 fraudulently and without colour of right, (a) obtains, directly or indirectly, any computer service
- 342.2 possession of device to obtain unauthorized use of computer system or to commit mischief
- 430 (1.1) mischief in relation to computer data

Source

19 June 2017 (amended)

COOPERATION

Multilateral Agreements

Budapest Convention

PARTY

Source

1 November 2015 (entry into force)

UN Processes

Represented at the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security

Source

2012/2013, 2016/2017

Expressed views to the Annual Report of the UN Secretary-General on Developments in the Field of Information and Telecommunications in the Context of International Security

Source

2013, 2014, 2015, 2016, 2017

Expressed Views at the Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security

Source Source 2

2019/2020

Bilateral and Multilateral Cooperation

Resolution on Working Group on Cooperative and Confidence Building Measures for Cyberspace, Inter-American Committee against Terrorism

Presented by Chile, Colombia, Perú, Costa Rica, Canada, Guatemala and Mexico

Prepare a set of draft confidence-building measures, based on UN GGE reports to enhance interstate cooperation, transparency, predictability and stability and to reduce the risks of misperception, escalation, and conflict that may stem from the use of ICTs

Source

10 April 2017

Memorandum of Understanding, Canada-India

Public Safety Canada

Cooperation in the field of Information Communication Technology and Electronics

Source

Canada

Last Updated: October 2021

April 2015

Global Forum on Cyber Expertise, Member

A global platform for countries, international organizations and private companies to exchange best practices and expertise on cyber capacity building

Source

2015 (established)

Sweden-Canada Agreement

Defence Research and Development Canada

Long-term agreement on cooperation in science and technology in the field of societal security, including on cyber security and critical infrastructure.

Source

September 2014

Cybersecurity Action Plan Between Public Safety Canada and the Department of Homeland Security (US)

Public Safety Canada

Three goals:

1. Enhanced cyber incident management collaboration
2. Engagement and information sharing with private sector
3. Continued cooperation on public awareness

Source

October 2012

Select Activities

Cyber Security Cooperation Program

Government of Canada

- Three year, $1.5 million initiative
- Offer grants and contributions to owners and operators, industrial and trade associations, academics and research organizations in support of eligible projects

Source

4 February 2014

GetCyberSafe national public awareness campaign

2011

Membership

- **Commonwealth**
- **Group of Seven (G7)**
- **International Telecommunications Union (ITU)**
- **North Atlantic Treaty Organization (NATO)**
- **Organization for Security and Co-operation in Europe (OSCE)**

Canada

Last Updated: October 2021

Organization of American States (OAS)

United Nations (UN)