Building Trust in an AI-Driven World

March 2026

Communications Security Establishment Canada
Canadian Centre for Cyber Security

Centre de la sécurité des télécommunications Canada
Centre canadien pour la cybersécurité

Canada

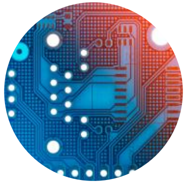
Cyber Centre's Role in Cyber Security

- Part of the Communications Security Establishment (CSE)
- Foreign intelligence, Cyber Operations
- Technical Authority for Cyber Security and Information Assurance
- Canada's CSIRT (CERT-CA)Government of Canada CSIRT

AI Is Transforming the Way we Work, but…

- Without investment in security, results can be incorrect, misleading or biased.
- Cyber threat actors use AI to increase stealth, lower costs and build scale.

Protect the Model's Privacy & Integrity



Protect the Model's IT System

Block Adversary Use of AI

Protect Privacy & Integrity

Ensure AI tools are used safely, with strong privacy protections and develop clear expectations for AI suppliers

Secure AI Engineering & Supply Chain Processes

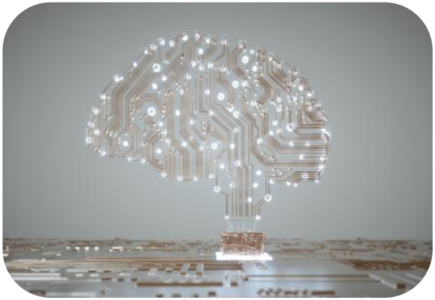
Use Human-in-the-Loop Oversight & Execution Control

Maintain Operational Resilience Against Model Drift, Bias & Overreliance

Protect the Model's IT System

Harden the AI Infrastructure

Access to your AI platform gives threat actors powerful capabilities to analyze and exploit your data



Conduct Testing to Identify Modifications

Without sufficient and continuous testing, modifications to AI systems can remain undetected

Safeguard Against Data-Poisoning

Understand how your model is trained, the data sets used by agents and protect them

Set strong controls on who has access to your AI system

An AI system can be used as an oracle to extract sensitive information

Protect Against Adversaries

AI has fundamentally tilted the playing field to benefit threat actors

Every attack can be thoroughly researched, automated and obfuscated

Keep Ahead of New Attacks; Quickly Deploy Mitigations

We are learning how to use AI and so are threat actors. Update your defences continuously.

Defend Against Deepfake & Impersonation

Threat actors use AI-powered deepfakes to impersonate, shape opinions and manipulate.

?