Submission to the Standing Committee on Public Safety and National Security

Bill C-8

An Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts

Author:
Suchet Mittal
Policy Analyst
AI Governance and Safety Canada

Submitted by:
Wyatt Tessari L'Allie
Executive Director
AI Governance and Safety Canada

Date:
January 23rd, 2025

Introduction

AIGS Canada is a nonpartisan not-for-profit and a community of people across the country, working to ensure that advanced AI is safe and beneficial for all. Since 2022 we have provided government with public interest AI policy recommendations, such as our submissions to ISED and TBS, and our testimony and detailed briefs for the AI & Data Act. Last Fall we published *Preparing for the AI Crisis: A Plan for Canada*, our white paper outlining where AI is headed, the likely crisis points, and why Canada is well placed to lead a global solution.

Artificial intelligence (AI) has shown significant unanticipated improvements in capability, and the acceleration is expected to continue. These gains have transformed the landscape of both cyberdefence and cyberattacks. In the near future, we could see AI being utilized to automate the full cyberattack chain, from identifying targets to operationalising the attack.[1] A recent event exemplified these risks when American frontier AI lab Anthropic reported that their frontier model "Claude" was utilized in an automated cyberespionage campaign targeting American companies and the government.[2]

In light of the new risks that AI presents, **AIGS Canada supports the central cybersecurity objective of Bill C-8: strengthening the resilience of Canada's critical cyber systems and vital services**. We welcome the establishment of a baseline framework in the Critical Cyber Systems Protection Act (CCSPA) that is explicitly aimed at managing cyber risks, including risks associated with supply chains and the use of third-party products and services (CCSPA s. 5(a)), and operationalized through mandatory cyber security programs that must include steps to identify and manage those supply-chain/third-party risks (CCSPA s. 9(1)(a)). We also support the introduction of mandatory incident reporting to the CSE within a period set by regulation not exceeding 72 hours (CCSPA s. 17), which can strengthen national situational awareness and coordination as threat patterns evolve.

Building on this strong starting point, this submission has two goals: (1) highlight AI as a risk multiplier for cyber threats and as a new supply-chain/third-party dependency category in the context of the CCSPA, and (2) the proposal of two amendments following from the insights of AI's expected impact. We address each point in turn below.

AI's Impact on Cyber Risk

Advanced AI systems are reshaping the cyber threat environment in ways that amplify existing risks and introduce new structural vulnerabilities, particularly through their effects on attacker capabilities and third-party dependencies.

---

[1] Caleb Withers, "Tipping the Scales," Centre for New American Security, September 23, 2025, https://www.cnas.org/publications/reports/tipping-the-scales.
[2] See: https://www.anthropic.com/news/disrupting-AI-espionage

1. Risk multiplication: AI could increase an attacker's scale, targeting accuracy, and iteration speed, while significantly reducing the cost and effort required to conduct sophisticated cyberattacks. Notably, the leverage that AI lends could asymmetrically favor attackers over defenders due to the lower cost of failure for attackers. A failed attack is significantly less critical than a failed defence, making AI a viable cyberoffence tool despite problems with reliability.

2. Third-party dependencies: As AI systems are increasingly integrated into Canada's critical cyber infrastructure to improve efficiencies, vulnerabilities of the models themselves or the environments they operate in could affect the confidentiality, integrity, or availability of critical cyber systems. For example, vendor-side updates to a base model could present unforeseen security vulnerabilities due to behaviour drift (unexpected change in an AI model's behavior), or introduce unforeseen and/or novel security vulnerabilities.

Recommendations

These observations necessitate two amendments to the currently proposed text of Bill C-8.

1. Prevent telecom security orders from undermining cybersecurity: Bill C-8 gives the Minister of Industry significant power to address threats to the Canadian telecommunications system, including the power to impose conditions on network products/services and to compel a provider to "do a specified thing or refrain from doing a specified thing" (Telecommunications Act, proposed s.15.2(2)(m)). However, absent a clear statutory constraint, these broad order-making powers could inadvertently reduce telecommunications security (for example, by requiring measures that weaken the encryption of networks). Noting the cyberattack capabilities that AI models are now making widely available, even minor and/or temporary security vulnerabilities could result in significant insecurity.

Echoing Citizen Lab's recommendation, AIGS Canada suggests adding an interpretive clause to s. 15.2 to clarify that, for improved certainty, the Minister is not permitted to make an order that would compromise the confidentiality, integrity, or availability of a telecommunications facility/service, or transmission facility.

2. Clarify how modern digital services fit within CCSPA's supply-chain and third-party risk requirements in the early implementation guidance. AI and ML services are rapidly becoming embedded in operational workflows across all Schedule 1 sectors. Vendor-side updates can change behavior without local approval, making them a distinct supply-chain risk. **The implementation guidance should make clear that CCSPA s. 9(1)(a) applies to adaptive, remotely updated third-party services, and to integrations with broad access**. This includes, for example, supplier-side updates that change service behaviour without a local software change; or integrations (e.g. plugins/connectors/agent tooling) that expand effective access or potentially create new data-exfiltration pathways. These are direct instances of the supply-chain/third-party risk concept that Parliament has already embedded in the cyber security program requirements under CCSPA s. 9(1)(a).