CANADIAN CENTRE FOR
CYBER SECURITY

Collective Cyber Defence: Protecting Canada in a Changing Threat Landscape

Daniel Couillard

Director General, Cyber Partnerships

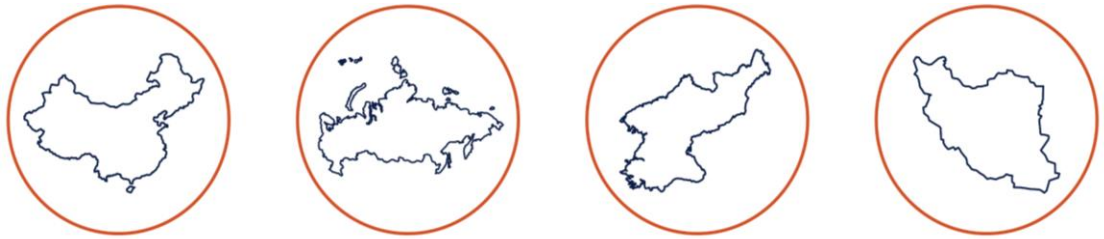
March 13, 2025

Who We Are: Canada's Cyber Security Authority

- We use our expertise to keep safe the **information and systems** that Canadians rely on every day.
- We work to protect and defend the country's valuable cyber assets and **lead Canada's federal response** to cyber security events.
- We believe cyber security is a **team sport**, built on strong partnerships across government, industry, and international allies.

Canada's technical authority on cyber security

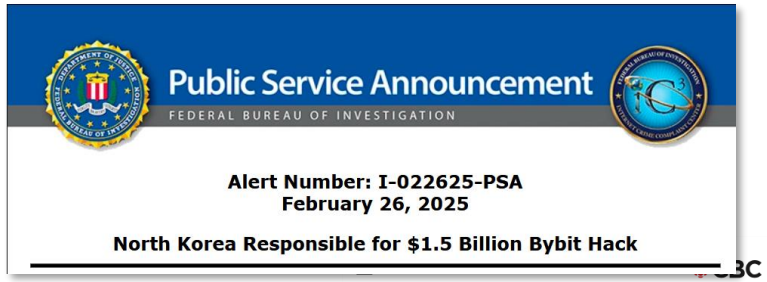
A New Era of Geopolitics – The Heightened Threat Environment



Espionage is only one half of the equation

Now, state-sponsored actors are also **spreading chaos**

INTRUSION → **DISRUPTION**



Understanding the Threat Landscape

Key narratives:

- Canada faces a growing cast of malicious actors—state-sponsored groups, cybercriminals, hacktivists.
- State adversaries are becoming more aggressive, using disruptive cyber operations.
- Cybercrime, led by ransomware, remains the top threat to Canadian critical infrastructure.

Persistent Threats: What's Not Changing

State-sponsored actors (China, Russia, Iran, North Korea) continue long-term cyber espionage and disruption campaigns

Cybercrime, led by ransomware, remains the dominant threat to critical infrastructure.

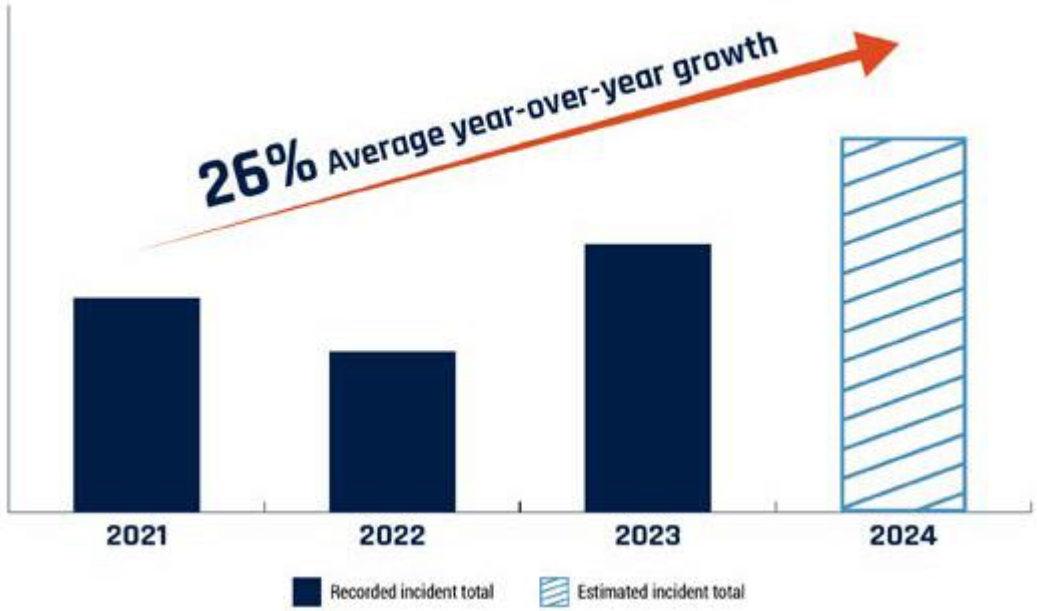
Hacktivism and opportunistic attacks flare during geopolitical events.

Cyber espionage and foreign interference continue to target sensitive sectors.

Evolving Threats: What's New

- Ransomware tactics are growing more aggressive—big game hunting, double extortion, and targeting supply chains.
- Increased use of Living-off-the-Land (LOTL) techniques makes detection harder.
- Focus on edge devices and supply chain vulnerabilities to gain access.

Relative growth from 2021 of Canadian ransomware incidents known to the Cyber Centre



AI: Transforming the Threat Landscape

- AI is making attacks **smarter, faster, and harder** to detect.
- Threat actors are using AI to:
  - Craft convincing **phishing and social engineering** attacks.
  - Generate **deepfakes** for disinformation.
  - **Automate** parts of the cyber attack lifecycle.
- Generative AI is lowering barriers for less-skilled attackers.
- AI systems are now a target themselves—subject to theft, tampering, and manipulation.

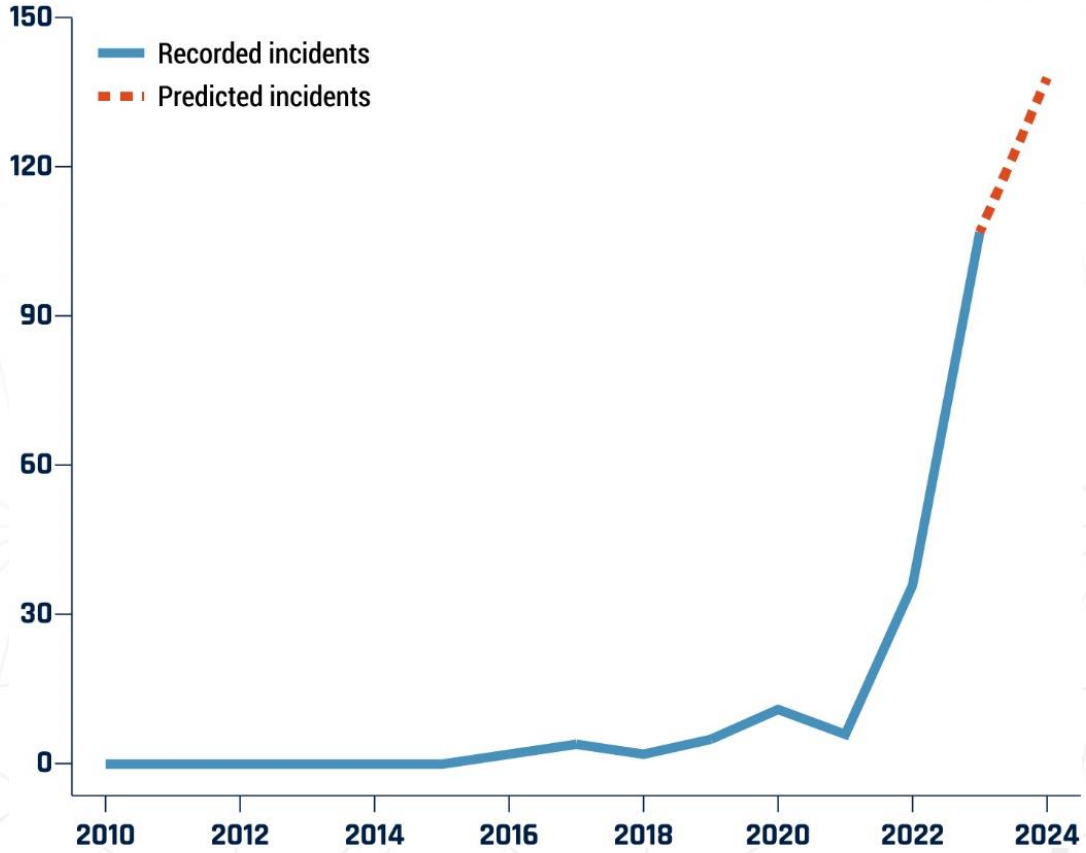


Figure 15: Publicly reported worldwide generative AI incidents resulting in harm or near harm (NCTA 2025-26).

BREAKING

NEWS – Threat Actors Leverage AI

THE WALL STREET JOURNAL.

Latest World Business U.S. Politics Economy **Tech** Markets & Finance Opinion Arts Lifestyle Real Estate Personal Finance Health

EXCLUSIVE ARTIFICIAL INTELLIGENCE Follow

Chinese and Iranian Hackers Are Using U.S. AI Products to Bolster Cyberattacks

Researchers outline malicious uses of AI after China-built AI platform DeepSeek upends international assumptions about Beijing's capabilities

By Dustin Volz Follow and Robert McMillan Follow
Jan. 29, 2025 5:00 am ET

Share Resize 29 Listen (2 min)

Google's new research sheds light on how foreign actors are using generative AI to boost their hacking efforts. PHOTO: STR/AGENCE FRANCE-PRESSE/GETTY IMAGES

SEARCH **FORTUNE** SIGN IN Subscribe Now

Home News Tech Finance Leadership Well Education Fortune 500

TECH· CYBERSECURITY

Microsoft says Iran, North Korea, Russia and China are beginning to use generative AI in offensive cyberattacks

BY FRANK BAJAK AND THE ASSOCIATED PRESS
February 14, 2024 at 7:49 AM EST

"Of course bad actors are using large-language models — that decision was made when Pandora's Box was opened," said Amit Yoran, CEO of the cybersecurity firm Tenable.
GETTY IMAGES

Forbes

FORBES > INNOVATION > CYBERSECURITY

Introducing GhostGPT—The New Cybercrime AI Used By Hackers

Davey Winder Senior Contributor
Davey Winder is a veteran cybersecurity writer, hacker and analyst.

Follow

0 Jan 23, 2025, 10:16am EST

GhostGPT is the cybercrime AI chatbot of choice. GETTY

A National Strategy for Collective Defence

Whole-of-Society Engagement

- Everyone has a role—governments, critical infrastructure, private sector, academia, and the public.

Agile Leadership

- Canada must adapt quickly to new threats with collaborative, flexible, and forward-looking strategies.

Cyber security isn't static—it requires *continuous innovation, investment, and partnership*.

Canada's National Cyber Security Strategy

Canada's strategy is built on three pillars:

1. **Work with Partners to protect Canadians and Canadian businesses.**
2. **Make Canada a Global Cyber Security Industry Leader.**
3. **Detect and Disrupt Cyber Threat Actors.**

- Together, these pillars support our vision of a **safe, secure**, and **prosperous** digital Canada.
- Initiatives like the **Canadian Cyber Defence Collective** (CCDC) bring public and private sectors together to solve national challenges.
- Protecting critical infrastructure and securing our economy require **unprecedented collaboration**.

Call to Action

Cyber Security is a Team Sport

- Our shared safety and prosperity depend on **collective resilience.**
- Canada's threat environment is evolving—so must our response.
- Through collaboration, information sharing, and joint action, we can protect Canada's digital future.

Let's work together

CONNECT WITH US


@cse_cst


partnerships-partenariats@cyber.gc.ca


www.cyber.gc.ca


@cybercentre_ca