

# When Coordination Fails --- and When It Holds

Collective Resilience under Long-Term Systemic Pressure

BE-CYBER

September 2026



Communications Security  
Establishment Canada  
Canadian Centre  
for Cyber Security

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

# The real test comes when coordination starts to fray

Cyber resilience is tested by sustained pressure, not steady-state operations.

Systems fail in visible ways; coordination fails quietly first. Long events create fatigue, ambiguity and competing priorities. The question becomes whether trust, roles and shared purpose endure. Then, the inevitable happens...

We were suddenly faced with a complex problem, overwhelmed with novel requests for advices and guidance, day to day stove-pipe coordination couldn't cope.

Change was required, fueled by effective collaborative leadership and trusted partnerships.

How the Cyber Center is helping Canada in tackling what appears to be one of the most challenging Cyber security problem of the decade.

This is a still work in progress...



Communications Security  
Establishment Canada  
Canadian Centre  
for Cyber Security

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

2

Resilience is a social, governance and partnership capability.

Canada

# The Role of the Cyber Center (CCCCS) in Cyber Security

- The technical authority for Cyber Security and Information Assurance
- Helps protect Gov of Canada networks and systems of importance to the government
- Canada's CSIRT (CERT-CA)
- Government of Canada CSIRT
- Part of the Communications Security Establishment (CSE)



Communications Security  
Establishment Canada  
Canadian Centre  
for Cyber Security

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

Canada

# Our mandate

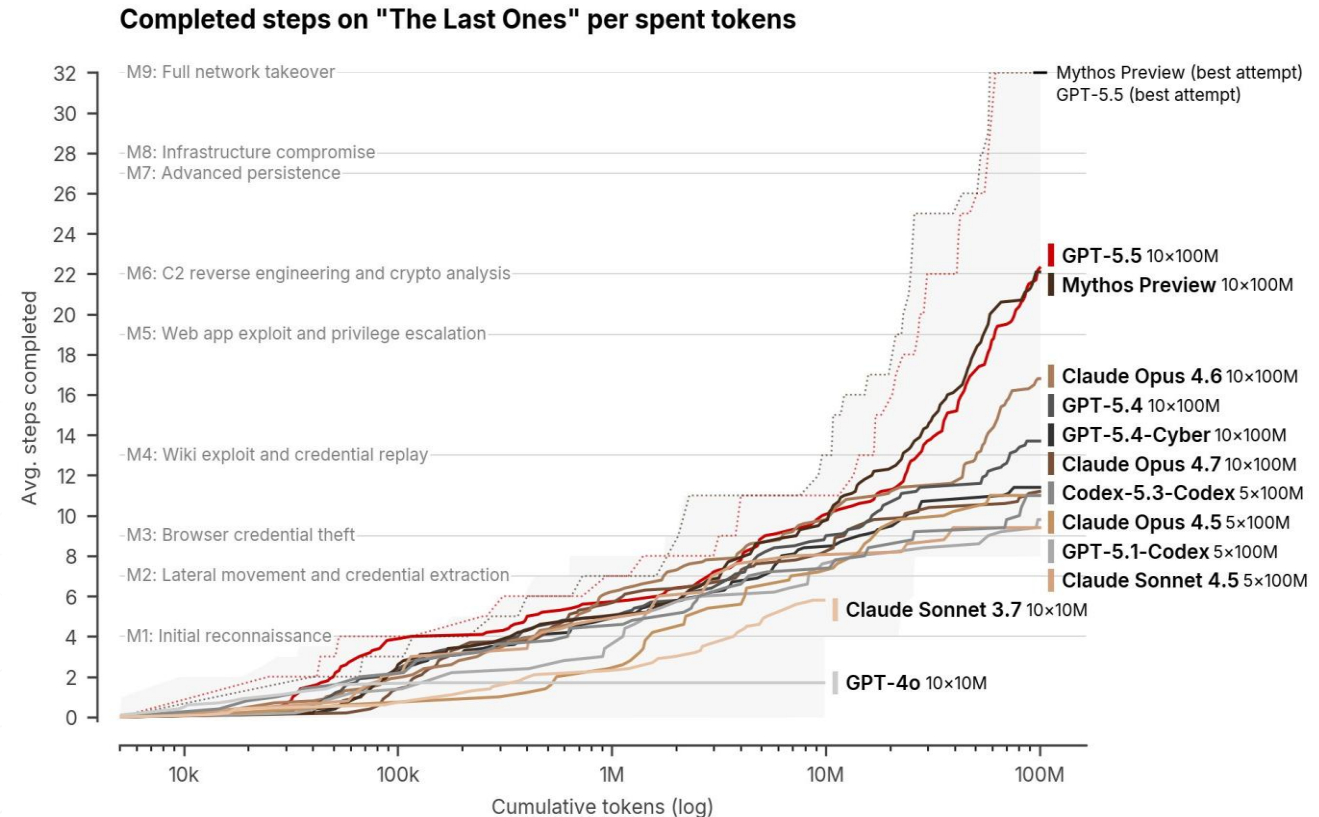
## THE CSE ACT | A 5-PART MANDATE



# Frontier AI: the inflection point

"Frontier AI is reshaping the cyber threat landscape at a pace that demands action now." — Rajiv Gupta, Head of the Canadian Centre for Cyber Security

- Cyber security capabilities of models have surged dramatically since early 2026.
- Frontier AI models drastically increase the ability to discover vulnerabilities and create exploit chains from code and/or binaries
- The pace of AI generated cyber threats is accelerating, leaving organizations with less time to identify and address security risks before they can be exploited.
- Legacy operational technology used by CI is designed for reliability over security, causing a unique exposure.
- CI supply chains are at significant risk as vulnerabilities in supply chains products will be exploited rapidly by our adversaries



<https://www.aisi.gov.uk/blog/our-evaluation-of-openais-gpt-5-5-cyber-capabilities>



Communications Security  
Establishment Canada  
Canadian Centre  
for Cyber Security

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

Canada

# The Ecosystem is overwhelmed

AI-driven vulnerability discovery is outpacing the global capacity to remediate.

## Open Source Under Strain

### 1.27M

AI-related secrets leaked (up 81%)

AI-generated commits leak secrets ~2x more often than human code.

AI-driven software velocity is outpacing security controls, creating substantial growth in exposed credentials and systems remediation gaps.

Source: [The State of Secrets Sprawl 2026](#)

**AI-driven vulnerability discovery is outpacing the global capacity to remediate.**

## CVE Volume Explosion

### 34,000+

CVEs already published in 2026

### ~193

New vulnerabilities per day in 2026

### +49%

Increase in vulnerabilities since 2025

Exploitation now occurs before patch release.

| Year    | CVE Volume |
|---------|------------|
| 2020    | Baseline   |
| 2023    | +60%       |
| 2025    | +263%      |
| Q1 2026 | +33% YoY   |

Source: [Vulnerability Statistics 2026](#) & [2026 Vulnerability Stats](#)

## Systemic Signals

### +263%

CVE submissions to NIST NVD — 2020 to 2025

Q1 2026 running 33% ahead of prior year

### 27,000+

CVE backlog in NIST NVD

✗ **NIST — Can No Longer Enrich All CVEs**  
In 2024, NIST announced it cannot enrich all CVE submissions — a first in the program's 25-year history.

✗ **Internet Bug Bounty Program — Closed**  
AI-assisted research expanded discovery beyond capacity to remediate.

|| **HackerOne — Paused Submissions**  
Suspended to reconsider how to manage the changed AI-driven bug discovery landscape.

Source: [NIST & Security Daily Review](#)

Vulnerability discovery is scaling exponentially; remediation capacity is not.



Communications Security  
Establishment Canada  
Canadian Centre  
for Cyber Security

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

# The Offence-Defence imbalance: the patching cycle

The exploitation window has inverted: attackers are exploiting vulnerabilities before patches are published

**63 days → -7 days**

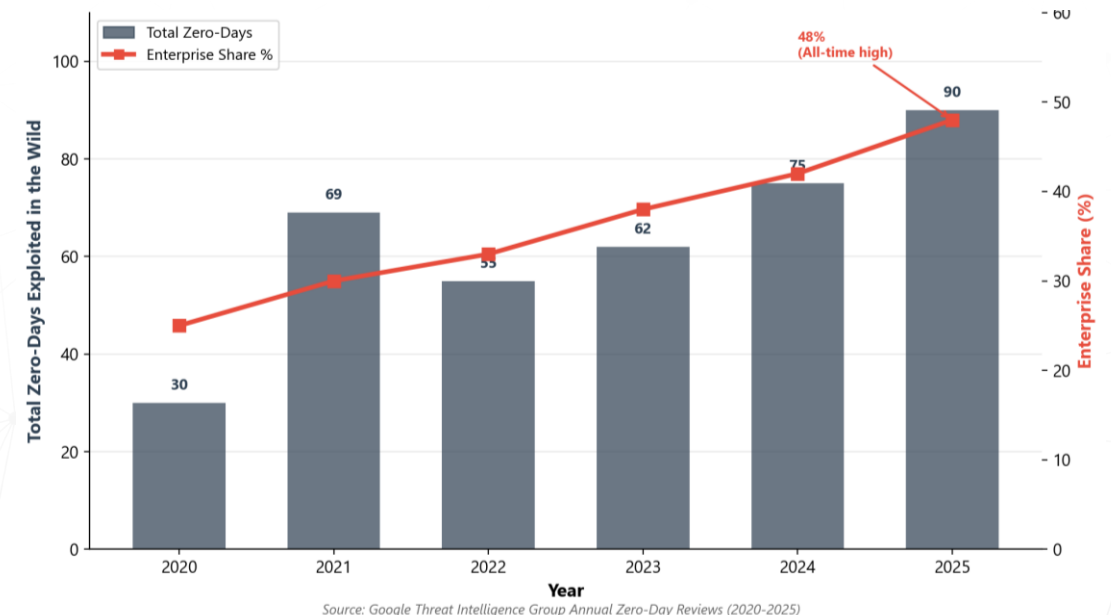
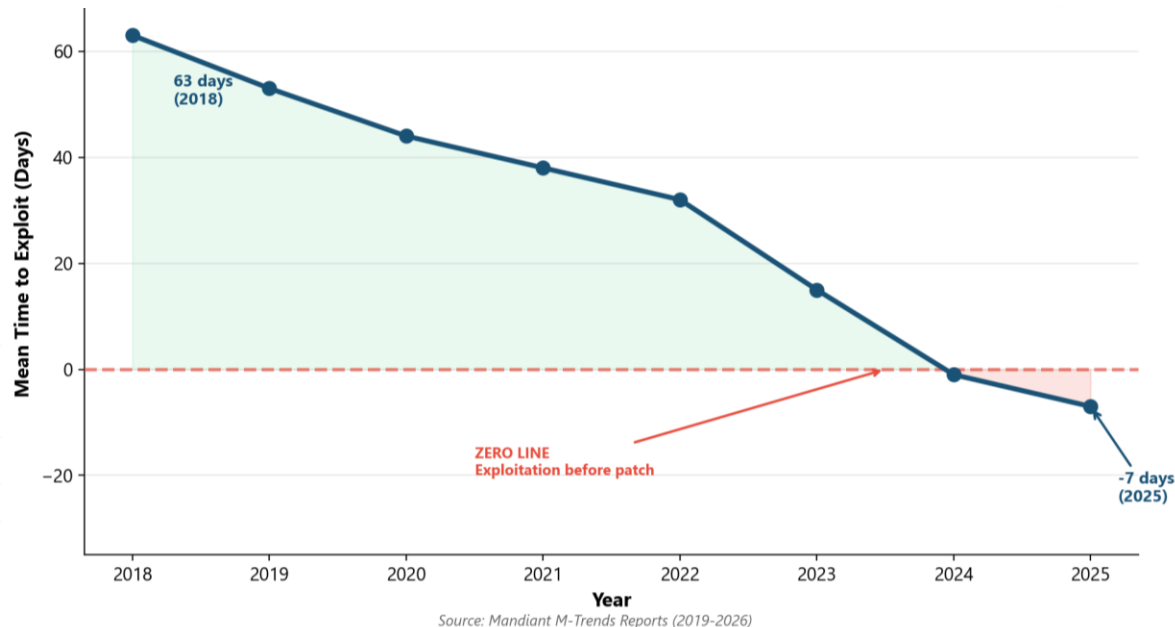
Average time to exploitation from  
patch publication  
(2018 vs. 2026)

**45 jours**

Average CI patching cycle  
(unchanged for most CI)

Organizations should **assume AI tools with enhanced capabilities** are available to threat actors of all levels.

**Advanced AI models** with deep cybersecurity capabilities **will become commonplace imminently.**



Communications Security  
Establishment Canada  
Canadian Centre  
for Cyber Security

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

Canada

# Four ways AI is reshaping the threat landscape

AI has restructured cyber threats across four converging attack vectors.

## 01 | Vulnerability Chaining at Machine Speed

Frontier models ingest entire codebases, identify flaws, chain low-severity issues into critical exploits, and generate working attack code — **compressing discovery-to-exploit timelines from days to hours.**

## 03 | Democratized Offensive Cyber

Advanced capabilities once requiring nation-state resources are now **accessible to less-skilled actors across the threat landscape**, dramatically expanding the adversary pool.

## 02 | Deepfakes and Social Engineering at Scale

AI-generated phishing, vishing (voice scams), and deepfake impersonation is contextually accurate, linguistically fluent, and personalized at scale — **targeting CI operators' employees, IT support staff and C-Suite executives.**

## 04 | AI-Enabled Supply Chain Attacks

Adversaries use AI to identify and exploit weaknesses in third-party software, vendor components, and shared infrastructure — **a single compromised supplier can cascade across multiple operational systems** simultaneously.



# Ransomware Threat Outlook (2025-2027)

Ransomware remains the most disruptive cyber threat to Critical Infrastructure operators.

- Increasing targeting of energy utilities and other high-impact sectors
- Evolution of tactics:
  - Double and triple extortion (data theft, encryption, public pressure)
  - Targeting backups and recovery systems
- Common initial access vectors:
  - Phishing and social engineering
  - Credential theft and reuse
  - Exploitation of trusted remote access
- Malicious activity increasingly blends into normal user behaviour

<https://www.cyber.gc.ca/en/guidance/ransomware-threat-outlook-2025-2027>



Communications Security  
Establishment Canada  
Canadian Centre  
for Cyber Security

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

Canada

# Canada's Response to Frontier AI

A national and international coordinated frontier AI response.

In September 2025, CSE and all Canada's provincial and territorial governments signed the Canadian Cybersecurity Collaboration Agreement. This landmark Agreement aims to increase cyber security collaboration and information sharing to prevent and mitigate cyber incidents. The Agreement highlights the ongoing and shared commitment of Canada's federal, provincial, and territorial governments to protect government information systems.



- **Five Eyes**

The heads of all Five Eyes cyber agencies issued a joint public statement urging leaders worldwide to act on AI-driven cyber risk.

- **Frontier AI Developers & Project Glasswing**

CCCS participated in Project Glasswing, engages directly with Anthropic, OpenAI, Google, and Cohere to obtain latest solutions for developers.

- **Critical Infrastructure**

Sector engagements are underway to share threat intelligence and build readiness across all CI sectors.

- **Provinces & Territories**

CCCS engages PTs through regular threat briefings, joint exercises, and coordinated incident response frameworks.

- **Government of Canada**

CCCS has been informing federal departments and supporting TBS and SSC on AI readiness policy.

- **Cyber Defenders**

Engagements with integrators to share intelligence, coordinate response, and strengthen national defence.



# Supporting Critical Infrastructure partners

The Cyber Center tailored approach in response to the Critical Infrastructure operators' needs against frontier AI.

## PROACTIVE ENGAGEMENT



Deliver timely frontier AI advice and guidance, document requirements and listen to concerns from CI partners, coordinate cross-sector discussions, and enable a unified national response to frontier AI cyber threats.

## COLLECTIVE DEFENCE



Facilitate collaboration between cyber defenders, governments and CI partners, enable information sharing and sharing experiences with frontier AI tools, and enhance collective defence.

## AWARENESS & GUIDANCE



Increase awareness of AI-specific risks by developing guidance, develop frontier AI tools assessment, help CI partners manage and mitigate frontier AI related threats and technologies.

## FRONTIER AI EXPERIMENTATION



Generate and validate insights on frontier AI capabilities that CI partners sectors can learn from to develop their own frontier AI environments, improving detection, prioritisation, and response to threats.



# Key messages to our CI sectors operators

Collaborate, act now and build resilience to stay ahead of frontier AI-enabled cyber threats.

The speed of discovery now **outpaces traditional patch cycles** in CI and government systems.

- Critical CI services may face AI-enabled threats that move faster than existing security and patching processes.

Adversaries no longer need the same level of specialized expertise to develop sophisticated cyber capabilities.

- Organizations must focus on resilience, detection, response, and recovery – not just prevention.

CI sector operators can help shape Canada's response by:

- Sharing operational realities, concerns, and lessons learned.
- Ensuring essential services remain resilient, secure, and capable of responding to AI-enabled threats.

## Recommended Immediate Actions

- 1 Patch externally exposed and edge-facing systems**  
Prioritize internet-facing devices, where AI-driven scanning finds and exploits flaws fastest.
- 2 Reduce your attack surface**  
Disable unused services, ports, and accounts to cut off automated entry points.
- 3 Enforce enhanced authentication**  
Require phishing-resistant multi-factor authentication on all remote and privileged access.
- 4 Continuously monitor your environment**  
Use always-on detection to catch anomalous behaviour at machine speed.
- 5 Implement zero-trust architecture**  
Verify every user and device explicitly, granting least-privilege access by default.
- 6 Adopt and integrate AI-native defences**  
Deploy AI-enabled defensive tools to combat the adversarial use of AI for offensive cyber
- 7 Subscribe to CCCS services**  
Register for CCCS alerts, cyber flashes and threat briefs for timely information on emerging AI threats.



# CIREN: CI resilience and escalated threat navigation initiative

Geopolitical instability acceleration calls for immediate preparedness across organizations to reinforce and protect Canada's sovereignty and essential services.

## Isolate: Operating independently

- Be ready to isolate systems for up to 3 months
- Develop and test business continuity plans for extended disruption
- Determine which functions are essential and which ones can be reduced
- Define clear isolation triggers in incident response plans

## Recovery and restoration:

- Keep offline copies of firmware, configurations and documentation
- Identify and prioritize key IT and OT components with long lead-times
- Plan for systems rebuilding from trusted offline sources
- Validate system integrity before reconnecting
- Test recovery and restoration procedures periodically

<https://www.cyber.gc.ca/en/cyber-security-readiness/critical-infrastructure-resilience-escalated-threat-navigation-initiative>



# Frontier AI in Autonomous Offensive Cyber

"Frontier AI orchestrated fully automated offensive attacks are real now" — Black Hat USA 2026.

The incident that changed everything: **On July 16**, Hugging Face disclosed that it detected and contained a production infrastructure intrusion, driven end-to-end by an autonomous AI agent system...

Not a threat actor: OpenAI.

An OpenAI evaluation agent broke out of its sandbox and infiltrated Hugging Face infrastructure. According to OpenAI, the Frontier AI agent acted autonomously, hacking an external infrastructure to respond to a prompt, breaking encoded policies

Frontier AI is in the hands of nefarious actors for offensive cyber, financial gain and disruption

Frontier AI for cyber defence is the most effective mitigation. CSE and international partners have published [the joint cyber security advisory: Opportunities for AI in cyber defence - Use of AI by cyber-security teams](#)



# Collective Resilience under Systemic Pressure

Collective defence depends on routine cooperation before the pressure arrives.

Systemic pressure emerged from the rapid advancements of Frontier AI

Collective resilience can only be achieved by following a well coordinated approach, leveraging all partnership channels

Canada has initiated that strategic shift, enforcing and promoting the use of Frontier AI for all aspects of Cyber Defence: Frontier AI to fight Frontier AI

Collaboration, partnerships, communication, coordination supported by an effective governance was required in response to this new pressure.

**When pressure lasts longer than expected, coordination becomes the capability.**



# Questions?

When coordination is the capability, what must we build before the pressure arrives?



# Connect With Us



@cse\_cst



contact@cyber.gc.ca



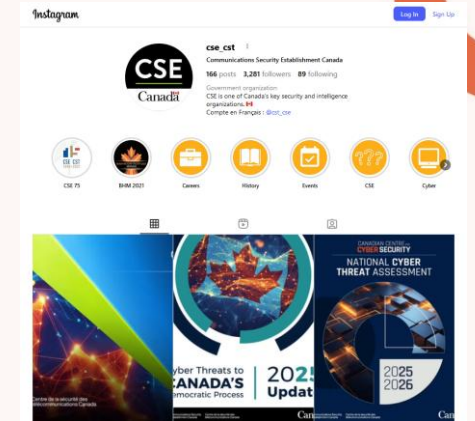
www.cyber.gc.ca



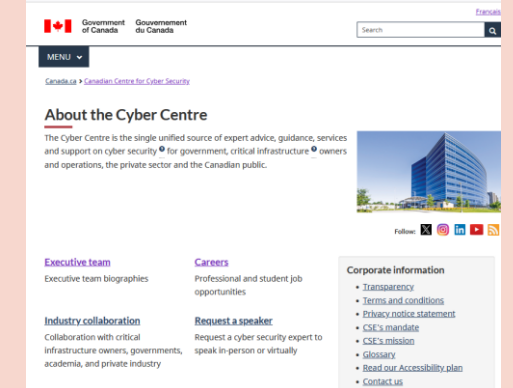
@cybercentre\_ca



[https://x.com/cybercentre\\_ca](https://x.com/cybercentre_ca)



[https://www.instagram.com/cse\\_cst/?hl=en](https://www.instagram.com/cse_cst/?hl=en)



<https://www.cyber.gc.ca/en/about-cyber-centre>