ACRAIS Daily Cybersecurity & AI Brief — 2026-11-07

Evidence-led intelligence, including frontier AI where available

Edition: 2026-11-07 | Status: Verified and published

Executive summary

ACRAIS evidence-led daily intelligence digest for 2026-11-07. Includes 7 cybersecurity and 7 AI source-linked updates. 1 AI items reference frontier AI or superintelligence. Summaries reflect the original source metadata; consult linked primary sources for details.

Cybersecurity Intelligence (7)

1. Cyber threat bulletin: PRC-sponsored cyber activity against Canadian provincial, territorial, Indigenous, and municipal governments

Canadian Centre for Cyber Security public intelligence item. Review the authoritative source for complete context and recommended action.

Practical takeaway: Review the original source and assess relevance before taking action.

Source: Canadian Centre for Cyber Security - https://www.cyber.gc.ca/en/guidance/cyber-threat-bulletin-peoples-republic-china-sponsored-cyber-activity-against-canadian-provincial-territorial-indigenous-and-municipal-governments

2. Threat detection for SharePoint vulnerabilities

Canadian Centre for Cyber Security public intelligence item. Review the authoritative source for complete context and recommended action.

Practical takeaway: Review the original source and assess relevance before taking action.

Source: Canadian Centre for Cyber Security - https://www.cyber.gc.ca/en/news-events/threat-detection-sharepoint-vulnerabilities

3. The cyber threat to Canada’s water systems: Assessment and mitigation

Canadian Centre for Cyber Security public intelligence item. Review the authoritative source for complete context and recommended action.

Practical takeaway: Review the original source and assess relevance before taking action.

Source: Canadian Centre for Cyber Security - https://www.cyber.gc.ca/en/guidance/cyber-threat-canadas-water-systems-assessment-mitigation

4. AL26-027 - Critical vulnerability impacting Google Brotli – CVE-2026-111497 [2026-10-28]

Canadian Centre for Cyber Security public intelligence item. Review the authoritative source for complete context and recommended action.

Practical takeaway: Review the original source and assess relevance before taking action.

Source: Canadian Centre for Cyber Security - https://www.cyber.gc.ca/en/alerts-advisories/al26-027-critical-vulnerability-impacting-google-brotli-cve-2026-111497

5. AL26-028 – Ongoing Help Desk Voice Phishing Campaign Targeting Canadian Organizations [2026-10-28]

Canadian Centre for Cyber Security public intelligence item. Review the authoritative source for complete context and recommended action.

Practical takeaway: Review the original source and assess relevance before taking action.

Source: Canadian Centre for Cyber Security - https://www.cyber.gc.ca/en/alerts-advisories/al26-028-ongoing-help-desk-voice-phishing-campaign-targeting-canadian-organizations

6. Mozilla security advisory (AV26-1131)

Canadian Centre for Cyber Security public intelligence item. Review the authoritative source for complete context and recommended action.

Practical takeaway: Review the original source and assess relevance before taking action.

Source: Canadian Centre for Cyber Security - https://www.cyber.gc.ca/en/alerts-advisories/mozilla-security-advisory-av26-1131

7. JetBrains security advisory (AV26-1132)

Canadian Centre for Cyber Security public intelligence item. Review the authoritative source for complete context and recommended action.

Practical takeaway: Review the original source and assess relevance before taking action.

Source: Canadian Centre for Cyber Security - https://www.cyber.gc.ca/en/alerts-advisories/jetbrains-security-advisory-av26-1132

ASI / SI — Superintelligence Watch (0)

No verified ASI/SI breakthrough is established by this brief. Topic mentions are research references, not evidence of superhuman capabilities.

No qualifying source-linked items in this edition.

AGI — General Intelligence (0)

No qualifying source-linked items in this edition.

Frontier & Advanced AI (1)

1. The Hiroshima AI Reporting Framework Organisations developing advanced AI systems can participate by submitting a report. By sharing information, they will facilitate transparency and comparability of risk mitigation measures.

OECD.AI public intelligence item. Review the authoritative source for complete context and recommended action.

Practical takeaway: Review the original source and assess relevance before taking action.

Source: OECD.AI - https://oecd.ai/en/transparency/overview

Applied AI (0)

No qualifying source-linked items in this edition.

AI Safety, Governance & Risks (6)

1. AI Shopping Assistants Pose Fraud Risks During Black Friday

OECD.AI public intelligence item. Review the authoritative source for complete context and recommended action.

Practical takeaway: Review the original source and assess relevance before taking action.

Source: OECD.AI - https://oecd.ai/en/incidents/2026-11-04-ae8d

2. AI-Generated Deepfake Videos Used in Victorian Election Campaigns Spread Misinformation

OECD.AI public intelligence item. Review the authoritative source for complete context and recommended action.

Practical takeaway: Review the original source and assess relevance before taking action.

Source: OECD.AI - https://oecd.ai/en/incidents/2026-11-04-e17c

3. West Virginia Sues Snap Inc. Over AI-Driven Child Exploitation and Sextortion Deaths

OECD.AI public intelligence item. Review the authoritative source for complete context and recommended action.

Practical takeaway: Review the original source and assess relevance before taking action.

Source: OECD.AI - https://oecd.ai/en/incidents/2026-11-05-f894

4. AI-Generated Images Used in Volunteer Recruitment Scam at Shengang Mazu Park

OECD.AI public intelligence item. Review the authoritative source for complete context and recommended action.

Practical takeaway: Review the original source and assess relevance before taking action.

Source: OECD.AI - https://oecd.ai/en/incidents/2026-11-05-188e

5. AI Voice Cloning Scam Targets Elderly Woman in Volos

OECD.AI public intelligence item. Review the authoritative source for complete context and recommended action.

Practical takeaway: Review the original source and assess relevance before taking action.

Source: OECD.AI - https://oecd.ai/en/incidents/2026-11-05-080a

6. AI, Data & Privacy Data and privacy are primary policy issues for AI.

OECD.AI public intelligence item. Review the authoritative source for complete context and recommended action.

Practical takeaway: Review the original source and assess relevance before taking action.

Source: OECD.AI - https://oecd.ai/en/site/data-privacy

Responsible-use note

This brief supports awareness and defensive action. Verify applicability and consult original sources before high-impact decisions.