Carleton University
Infrastructure Resilience Research Group (IRRG)
Office of the Dean, Faculty of Engineering and Design

RECOMMENDED READINGS

PREPARED BY:

Felix Kwamena, Ph.D. Adjunct Research Professor / Director, IRRG

&

Jerry Shelest, M A, IRRG Research Associate

The IRRG is aware that subject matter experts, practitioners, students, and others are busy with current and developing projects and has provided the following list of readings to share knowledge of potential interest in support of efforts relating to the resilience, security, and risk management of critical infrastructure assets and networks.

STRATEGIC POLICIES AND LEADERSHIP

1. **Prime Minister Carney – Davos WEF Speech on Middle Powers**
CBC News/Office of the Prime Minister – January 20, 2026
https://www.cbc.ca/news/politics/mark-carney-speech-davos-rules-based-order-9.7053350
https://www.pm.gc.ca/en/news/speeches/2026/01/20/principled-and-pragmatic-canadas-path-prime-minister-carney-addresses
Summary: PM Carney's Canada's Path address at the Worl Economic Forum articulates Canada's position as a middle power navigating a rapidly changing world, noting the rules-based international order, trade diversification, and relationships with major power during a period of significant geopolitical realignment.

2. **Prime Minister Carney – New Strategic Partnership with the People's Republic of China**
Office of the Prime Minister – January 16, 2026
https://www.pm.gc.ca/en/news/speeches/2026/01/16/prime-minister-carney-delivers-remarks-after-forging-new-strategic
Summary: Canada is forging a new strategic partnership with the PRC, noting terms of bilateral cooperation across trade, investment, and areas of mutual interest wile acknowledging areas of ongoing tension and difference.

3. **Prime Minister Carney – New Partnership with Qatar**
Office of the Prime Minister – January 18, 2026
https://www.pm.gc.ca/en/news/speeches/2026/01/18/prime-minister-carney-secures-new-partnership-qatar-increase-trade

Summary: PM Carney secures a new partnership with Qatar on trade, investment, and defence cooperation, signaling Canada's diversification of strategic partnerships in the Gulf region as part of a broader foreign policy reorientation.

4. **Prime Minister Carney – Launch of Canada's First Defence Industrial Strategy**
Office of the Prime Minister – February 17, 2026
https://www.pm.gc.ca/en/news/speeches/2026/02/17/prime-minister-carney-announces-launch-canadas-first-defence-industrial
Summary: Announcement of Canada's Defence Industrial Strategy, setting out the framework for domestic defence production, industrial capacity, and sovereign capability development. This is a direct response to allied pressure on defence spending and recognition that Canada's industrial base must be able to support its own security commitments.

5. **Prime Minister Carney – Remarks to Business Leaders in Mumbai**
Office of the Prime Minister – February 28, 2026
https://www.pm.gc.ca/en/news/speeches/2026/02/28/prime-minister-carney-delivers-remarks-business-leaders-mumbai
Summary: Remarks at a Mumbai business roundtable focused on Canada-India economic and investment ties, noting energy transition, technology cooperation, and talent mobility as the three pillars of the deepening bilateral relationship.

6. **Prime Ministry Carney – Partnership with India on Energy, Talent, and Technology**
Office of the Prime Minister – March 2, 2026
https://www.pm.gc.ca/en/news/speeches/2026/03/02/prime-minister-carney-secures-ambitious-new-partnership-india-focused
Summary: Formal announcement of an ambitious Canada-India partnership with focus on energy, talent, and technology cooperation, setting out commitments across clean energy development, skilled worker pathways, and digital economy collaboration.

7. **Prime Ministry Carney – Remarks to Media in Sydney, Australia**
Office of the Prime Minister – March 4, 2026
https://www.pm.gc.ca/en/news/speeches/2026/03/04/prime-minister-carney-delivers-remarks-media-sydney-australia
Summary: Media remarks covering the Canada-Australia bilateral relationship, shared Five Eyes commitments, and the broader Indo-Pacific strategy within which both countries are deepening cooperation on trade, defence, and critical minerals.

8. **Prime Minister Carney – Address to Both Houses of Australia's Parliament**
Office of the Prime Minister - March 5, 2026
https://www.pm.gc.ca/en/news/speeches/2026/03/05/prime-minister-carney-delivers-address-both-houses-australias-parliament
Summary: Address to the Australian Parliament and invited dignitaries, outlining the Canada-Australia strategic relationship in the context of a shifting global order, noting shared values,

democratic resilience, and the importance of like-minded nations deepening cooperation across security, trade, and technology.

9. **Canada and the Indo-Pacific: Middle Power Strategy in a Contested Region**
Centre for International Governance Innovation (CIGI) – 2025-2026
https://www.cigionline.org/topics/indo-pacific/
Summary: CIGI's Indo-Pacific research hub aggregates policy analysis, commentary, and research on Canada's strategic positioning in the region, covering trade diversification, security partnerships, critical minerals, and the governance of emerging technologies.

ARTIFICIAL INTELLIGENCE

AI Governance and Policy

1. **America's AI Governance Gap Needs Independent Oversight**
RealClearPolicy (Hewlett Foundation) – April 3, 2026
https://www.realclearpolicy.com/articles/2026/04/03/americas_ai_governance_gap_needs_independent_oversight_1174471.html
Summary: The U.S. faces a structural governance deficit when AI is being rapidly embedded in critical infrastructure, defence networks, and public services, noting that AI tools could be used to attack hospitals, power grids, and air traffic control systems.

2. **How 2026 Could Decide the Future of Artificial Intelligence**
Council on Foreign Relations – January 12, 2016
https://www.cfr.org/articles/how-2026-could-decide-future-artificial-intelligence
The report examines the governance, accountability, and geopolitical competition dimensions of AI, noting that over 80% of critical infrastructure in the US, UK, and Germany have deployed AI-generated code into the production of medical devices and energy networks despite associated security risks rated as moderate or high, raising the question of who bears legal responsibility for AI system actions.

3. **AI Governance: What Organizations Need to Know in 2026**
MLT Aikins – March 4, 2026
https://www.mltaikins.com/insights/ai-governance-what-organizations-need-to-know/
Summary: Western Legal perspective documenting Ontario's January 2026 joint publication by the Information and Privacy Commissioner and the Human Rights Commission of six principles for responsible AI use, covering accountability, transparency, fairness, privacy by design, security, and safety. It also mentions Manitoba's AI taskforce consideration and British Columbia's regulatory posture.

4. **State of AI Trust in 2026: Shifting to the Agentic Era**
McKinsey – March 25, 2026
https://www.mckinsey.com/capabilities/tech-and-ai/our-insights/tech-forward/state-of-ai-trust-in-2026-shifting-to-the-agentic-era
Summary: Based on a survey of approximately 500 organizations, the report documents the transition from generative to agentic AI, systems executing complex, autonomous actions with minimal human oversight. Almost two-thirds of respondents cite security and risk concerns as the top restriction to scaling agentic AI.

5. **Responsible AI Adoption in Canada's Public Sector**
KPMG Canada – March 2026
https://kpmg.com/ca/en/insights/2026/03/responsible-ai-adoption-in-canadian-public-sector.html
Summary: Research-based analysis of AI adoption across federal, provincial, and municipal governments, that notes that only 22% of Canadian public sector organizations have implemented AI tools, while nearly half of public servants already use AI in daily work without oversight.

6. **Canadian Artificial Intelligence Safety Institute**
Innovation, Science and Economic Development Canada (ISED) – 2026
https://ised-isde.canada.ca/site/ised/en/canadian-artificial-intelligence-safety-institute
Summary: The Canadian AI Safety Institute (CAISI) conducts leading research in collaboration with industry, the National Research Council, and the international Network of AI Safety Institutes, and its mandate covers studying how advanced AI systems work, identifying risks from impersonation, fraud, and systems that may hinder human oversight.

7. **Introducing the Agent Governance Toolkit: Open-Source Runtime Security for AI Agents**
Microsoft Open Source Blog – April 2026
https://opensource.microsoft.com/blog/2026/04/02/introducing-the-agent-governance-toolkit-open-source-runtime-security-for-ai-agents/
Summary: A Microsoft release of the first open-source framework addressing all ten The Open Worldwide Application Security Project (OWASP) agentic AI risks, timed to the EU AI Acts's high-risk obligations taking effect in August 2026. The toolkit maps technical controls to OWASP risk categories.

8. **2026 Public Sector Cyber Outlook: Identity, AI, and the Fight for Trust**
Palo Alto Networks – January 28, 2026
https://www.paloaltonetworks.com/blog/2026/01/public-sector-cyber-outlook/
Summary: It analyses AI integration in the public sector security operations, predicting federal security operations centres will evolve toward hybrid human-AI operations with autonomous agents triaging alerts and initiating containment responses.

Carleton University
Infrastructure Resilience Research Group (IRRG)
Office of the Dean, Faculty of Engineering and Design

AI and Workforce

1. **Research Finds That AI Has Already Replaced Work for 20 Percent of Jobs**
Futurism/NBC News – April 12, 2026
https://apple.news/ATKUectcpSkK5VQGp6k7czg
Summary: A survey finds one in five full-time workers report AI has taken over parts of their job. Goldman Sachs data shows AI eliminating roughly 16,000 jobs per month in the U.S.

2. **Skilled Older Workers Turn to AI Training to Stay Afloat**
The Guardian – 2026
https://apple.news/ATx5Xx5ukStStAGlPbEoykw
Summary: Workers with degrees, expertise and experience are unable to find employment and are turning to AI training to meet employer expectations about AI fluency.

AI Security Risks

1, **Former National Cyber Director: Anthropic's 'Mythos' AI Can Hack Nearly Anything and We Aren't Ready**
Fortune – April 23, 2026
https://fortune.com/2026/04/23/anthropic-mythos-ai-cybersecurity-critical-infrastructure-kemba-walden/
Summary: Acting National Cyber Director argues that an unreleased Anthropic model is 83% successful in autonomously discovering zero-day vulnerabilities across virtually any operating system or browser, chaining exploits, and covering its tracks. He calls for effort to protect under-resourced critical infrastructure.

2. **Hacker Uses Claude and ChatGPT to Breach Multiple Government Agencies**
Cybersecurity News/Gambit Security – April 2026
https://cybersecuritynews.com/hacker-uses-claude-and-chatgpt-to-breach/
Summary: A lone attacker compromised nine Mexican government agencies between December 2025 and February 2026, using AI as core operational tools. Claude Code generated remote commands that allowed one person to work at the scale and speed of a specialist team.

3. **AI is Coming to the Ottawa Police Service**
CBC Ottawa – 2026
https://apple.news/A78sHNoNuQ5GGmXNuaXy5Gg
Summary: The Ottawa Police Board is unveiling a new AI policy in April 2026. The policy aims to protect Charter rights while leveraging AI for faster crime resolution.

4. **Linux Lays Down the Law on AI-Generated Code**
Tom's Hardware – April 2026
https://www.tomshardware.com/software/linux/linux-lays-down-the-law-on-ai-generated-code-yes-to-copilot-no-to-ai-slop-and-humans-take-the-fall-for-mistakes-after-months-of-fierce-debate-torvalds-and-maintainers-come-to-an-agreement
Summary: Linux kernel maintainers have formalised a pragmatic AI code policy. Developers bear full legal and reputational accountability for everything they submit.

AI Strategy and Business

1. **OpenClaw is Coming for Businesses**
Ey/Various – 2026
https://apple.news/AIWasXVubS2eSVQyfdps4AA
Summary: Executives are trying to layer AI onto their existing businesses rather than ripping up old models and reimagining them. It challenges organizations to think structurally about AI transformation rather than treating it as an incremental technology upgrade.

2. **Cisco's President on the New Rules of AI Capitalism**
Semafor – 2026
https://apple.news/ASMCSAVuiTJ-pyXZcqU8zlw
Summary: Cisco's president argues the tech world is underestimating the amount of AI infrastructure needed (in power, cooling, networking, and physical space) which will create significant supply constraints and investment opportunities in the near term.

3. **Directive on Automated Decision-Making**
Treasury Board of Canada Secretariat – 2019, amended and in force.
https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=32592
Summary: This is the Government's instrument governing the use of automated decision systems, including AI, in federal decision-making. It establishes a four-level impact assessment framework, requiring transparency, human oversight, and recourse mechanisms as impact of automated decisions on individuals increases. The Directive is increasingly references as a benchmark by provincial government and regulatory bodies.

Carleton University
Infrastructure Resilience Research Group (IRRG)
Office of the Dean, Faculty of Engineering and Design

CYBERSECURITY

Threat Landscape and Critical Infrastructure

1. **FBI Warns of Iranian-Affiliated Cybersecurity Threats on U.S. Infrastructure**
Spectrum News – April 7, 2026
https://spectrumlocalnews.com/nc/triad/technology/2026/04/07/fbi-iranian-affiliated-cybersecurity-threats-u-s--critical-infrastructure
Summary: A joint federal advisory from the FNI, CISA, NSA, EPA, Department of Energy, and U.S. Cyber Command confirms Iranian-affiliated actors are actively targeting water, wastewater, and energy systems. It recommended mitigations centering on network isolation and multifactor authentication.

2. **FBI Reports Cyber Threats to Critical Infrastructure Intensify as U.S. Cybercrime Losses Hit $21 Billion**
Industrial Cyber – April 8, 2026
https://industrialcyber.co/reports/fbi-reports-cyber-threats-to-critical-infrastructure-intensify-as-us-cybercrime-losses-hit-21-billion-exposes-risk/
Summary: FBI's 2025 Internet Crime Report documents a sustained and deliberate campaign by state-aligned actors from China, Russia, Iran, and North Korea against critical infrastructure, with goal of pre-positioning for disruption during geopolitical conflict. Office of the Director of National Intelligence's Annual Threat Assessment 2026 reinforces this picture, identifying cyberspace as a primary arena of modern conflict.

3. **Cybersecurity Considerations 2026**
KPMG – April 6, 2026
https://kpmg.com/sa/en/insights/ai-and-technology/cybersecurity-considerations-2026.html
Summary: Identifies eight priority areas for cybersecurity leadership in 2026, and key themes include the strategic elevation of the CISO role, management of AI agents and service accounts, convergence of cyber and physical threat domains, and extending third-party risk management to cover ai systems and IoT devices throughout the supply chain.

4. **OT Threat Landscape 2026: What OT Cybersecurity Defenders Need to Know**
Dragos – April 2, 2026
https://www.dragos.com/blog/ot-threat-landscape-2026
Summary: Deals with the evolution of adversary operations across industrial control environments and noting that adversaries are moving beyond device-level targeting toward systematic mapping of control loops, preparing for future operational disruption rather than just data theft.

5. **SANS 2026 Report Flags Cybersecurity Skills Crisis**
Industrial Cyber – April 6, 2026
https://industrialcyber.co/reports/sans-2026-report-flags-cybersecurity-skills-crisis-putting-critical-infrastructure-and-ot-sectors-at-measurable-breach-risk/
Summary: Based on responses from practitioners, the report identifies a structural workforce crisis, with 60% of organizations reporting inadequate skill levels and 27% attributing actual breaches to capability gaps. It discusses AI erosion of entry-level career pathways and resulting risk to long-term workforce sustainability.

6. **Cyber Risk Trends for 2026: Building Resilience, Not Just Defenses**
SecurityWeek – April 3, 2026
https://www.securityweek.com/cyber-risk-trends-for-2026-building-resilience-not-just-defenses/
Summary: This strategic assessment argues the organizational imperative is resilience engineering rather than perimeter defence and makes recommendations across four domains: AI risk management, quantum readiness, third-party assurance, and board-level incentive structures.

7. **EU ICT Supply Chain Security Toolbox Adopted**
European Commission Digital Strategy – February 13, 2026
https://digital-strategy.ec.europa.eu/en/library/toolbox-improve-ict-supply-chain-security
Summary: This deals with the adoption of the toolbox by the EU Network and Information Systems (NIS) Cooperation Group that harmonises supply chain cybersecurity risk management across EU member states. The framework provides a structured methodology for identifying, assessing, and mitigating Information and Communication Technologies (ICT) supply chain risks.

8. **Cybersecurity Requires Collective Resilience**
Harvard Business Review – February 18, 2026
https://hbr.org/2026/02/cybersecurity-requires-collective-resilience
Summary: This report draws on the 2024 CrowdStrike incident to argue for three necessary organisational shifts: from protection to coordination, from internal continuity to service continuity, and from third-party risk management to co-resilience.

9. **From Bill C-26 to Bill C-8: Canada's Cyber Law Reboot Explained**
Security Brief Canada – March 2, 2026
https://securitybrief.ca/story/from-bill-c-26-to-c-8-canada-s-cyber-law-reboot-explained
Summary: An account of the legislative history behind Canada's long-delayed critical infrastructure cybersecurity framework. It traces Bill C-26 introduction and near-passage and revival as Bill C-8. It frames the legislation against the threat environment document in the National Cyber Threat Assessment 2025-2026.

10. **National Cyber Threat Assessment 2025-2026**
Canadian Centre for Cyber Security – October 2024
https://www.cyber.gc.ca/en/guidance/national-cyber-threat-assessment-2025-2026
Summary: The threat intelligence publication covers state-sponsored cyber threats from China, Russia, Iran, and North Korea, ransomware, AI to enhance malicious cyber activity, and pre-positioning in Canadian critical infrastructure as an emerging priority threat.

Quantum Computing and Cryptographic Resilience

1. **Mitigating the Government of Canada to Post-Quantum Cryptography: Security Policy Implementation Notice**
Treasury Board Secretariat/Canadian Centre for Cyber Security – October 2025
https://www.canada.ca/en/government/system/digital-government/policies-standards/spin/migrating-government-canada-post-quantum-cryptography.html
Summary: This is the directive for the PQC transition, establishing mandatory milestones for federal departments and agencies.

2. **Roadmap for the Migration to Post-Quantum for the Government of Canada (ITSM.40.001)**
Canadian Centre for Cyber Security
https://www.cyber.gc.ca/en/guidance/roadmap-migration-post-quantum-cryptography-government-canada-itsm40001
Summary: Sets the Canadian government's transition milestones: departmental PQC migration plans, annual progress reporting, and full migration to be completed by 2035.

3. **National Quantum Strategy Roadmap: Quantum Communication and Post-Quantum Cryptography**
Innovation, Science and Economic Development Canada
https://ised-isde.canada.ca/site/national-quantum-strategy/en/national-quantum-strategy-roadmap-quantum-communication-and-post-quantum-cryptography
Summary: The strategy outlines plans for raising awareness of the CRQC threat, supporting PQC standardisation and adoption, building a national quantum network test bed with satellite and ground fibre-optic links, and developing domestic manufacturing capacity for quantum components.

4. **NIST Releases First Three Finalized Post-Quantum Encryption Standards**
NIST – August 2024
https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards
Summary: The reference document for the post-quantum cryptography transition globally and in Canada where NIST standards serve as the basis for the Cyber Centre's ITSP.40.111 cryptographic algorithm recommendations.

5, **Quantum Security is Turning into a Supply Chain Problem**
Help Security – February 20, 2026
https://www.helpnetsecurity.com/2026/02/20/post-quantum-cryptography-supply-chain-priority/
Summary: Argues that the quantum cryptographic threat is a supply chain problem. As long as suppliers and embedded technologies continue using quantum-vulnerable cryptography the threat continues.

5. **A Guide to International Post-Quantum Cryptography Standards**
Akamai – 2026
https://www.akamai.com/blog/security/guide-international-post-quantum-cryptography-standards
Summary: Most PQC guidance assumes organizations operate in a single regulatory jurisdiction. Akamai's comparative analysis is useful for Canadian critical infrastructure operators, particularly in financial services, telecommunications, and energy.

6. **Quantum Threat Timeline Report 2024**
Global Risk Institute – December 2024 (the work is published annually)
https://globalriskinstitute.org/publication/2024-quantum-threat-timeline-report/
The report provides a timeline for the development of computers that could break public-key cryptography. The report is used by governments and financial institutions to calibrate PQC migration timelines.

INSIDER THREATS AND HUMAN FACTORS IN SECURITY

1. **CISA Urges Critical Infrastructure Organizations to Take Action Against Insider Threats**
CISA – January 28, 2026
2026 https://www.cisa.gov/news-events/news/cisa-urges-critical-infrastructure-organizations-take-action-against-insider-threats
Summary: A formal announcement stating insider threats take two forms: calculated harm and unintentional mistakes. Emphasises fostering a reporting culture rather than a surveillance culture, and that people are the first and best line of defence.

2. **CGN Reports Cybersecurity Maturity Becoming Prerequisites in Critical Infrastructure and Industrial Supply Chains**
Industrial Cyber/Canadian Cybersecurity Network – April 9, 2026
https://industrialcyber.co/reports/ccn-reports-cybersecurity-maturity-becoming-prerequisite-in-critical-infrastructure-industrial-supply-chains/
Summary: Cybersecurity is a gatekeeping function for economic participation with insurers declining coverage, supply chains enforcing security standards, and legal frameworks expanding duty of care. This reflects the convergence of forces defining Canadian critical infrastructure security in 2026.

3. **Annual Report on Insider Threats: Identification and Prevention 2026-2027**
ACSMI – March 2026
https://acsmi.org/blogs/annual-report-on-insider-threats-identification-amp-prevention-2026-2027-original-data
Summary: It quantifies the cost of insider threats and provides a three-layer prevention model and describes agentic AI as amplifying insider risk.

4. **Insider Threats: Turning 2025 Intelligence into a 2026 Defence Strategy**
Flashpoint – February 9, 2026
https://flashpoint.io/blog/insider-threats-2025-intelligence-2026-strategy/
Summary: The report analyses instances of insider threat, noting how adversaries exploit human vulnerabilities. It also states that AI tools will be used to both detect and perpetrate insider threat.

5. **Insider Threat Mitigation for U.S. Critical Infrastructure Entities**
National Counterintelligence and Security Center (NCSC/NITTF) - September 2024
https://www.dni.gov/files/NCSC/documents/nittf/20240926_Insider-Threat-Mitigation-for-US-Critical-Infrastructure.pdf
Summary: It states insider threat must be understood alongside cyber and supply chain threats, not in isolation.

6. **Policy on Government Security – Personnel Security**
Treasury Board Secretariat
https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=16578
Summary: The policy is the government framework governing personnel security (security screening, reliability status, security clearances, and handling of personnel security information) and establishes the legal and procedural framework for federal government insider threat mitigation programs.

PHYSICAL SECURITY AND CUBER-PHYSICAL CONVERGENCE

1. **Transport Canada: Drone Safety – Regulations and Enforcement**
Transport Canada
https://tc.canada.ca/en/aviation/drone-safety
Summary: This provides the full legal framework governing drone operations in Canadian airspace.

Carleton University
Infrastructure Resilience Research Group (IRRG)
Office of the Dean, Faculty of Engineering and Design

SUPPLY CHAIN SECURITY AND THIRD-PARTY RISK

1. **2026 Supply Chain Risk: Five Critical Reality Checks**
Cyber Strategy Institute – February 19, 2026
https://cyberstrategyinstitute.com/2026-supply-chain-risk-report/
Summary: Analysis of how supply chain ransomware has advanced toward continuous third-party data theft and operational disruption and identifies identity artifacts at the vendor level. It also recommends hard-wiring automatic kill-switches as a design requirement.

2. **Information and Communications Technology Supply Chain Risk Management**
CISA
https://www.cisa.gov/information-and-communications-technology-supply-chain-risk-management
Summary: CISA and the Canadian Centre for Cyber Security routinely co-publish Five Eyes advisories, and the CISA framework is effectively the operational standard against which Canadian critical infrastructure operators are measured.

3. **Supply Chain Risks Top of Mind 2026**
ISC2 – January 8, 2026
https://www.isc2.org/Insights/2026/01/cybersecurity-predictions-for-2026
Summary: The ISC2 conducts synthesis of supply chain risk, quantum computing, and identity-based attack landscape, and its cybersecurity workforce studies include Canadian data. It recommends building resilience through supply chain mapping and continuous evaluation.

4. **Secure-by-Design**
CISA – April 2023
https://www.cisa.gov/resou+++rces-tools/resources/secure-by-design
A joint advisory by cybersecurity agencies of the U.S., Australia, Canada, the U.K., New Zealand, and Germany established the principle that technology manufacturers should bear primary responsibility for the security of their products. The advisory calls for software vendors to eliminate classes of vulnerabilities.

Carleton University
Infrastructure Resilience Research Group (IRRG)
Office of the Dean, Faculty of Engineering and Design

WORKFORCE DEVELOPMENT, CERTIFICATION, AND PROFESSIONAL STANDARDS

5, **Closing the skills gap in cybersecurity: Why Canada must embrace collaborative education and hands-on learning**
Canadian Cybersecurity Network – continuing.
https://canadiancybersecuritynetwork.com/cybervoices/closing-the-skills-gap-in-cybersecurity-why-canada-must-embrace-collaborative-education-and-hands-on-learning and similarly,
https://www.cyber.gc.ca/en/education-community/cyber-skills-development
Summary: Canada faces an estimated shortage of 25,000 to 100,000 cybersecurity professionals, and the report argues that educators, industry leaders, and government agencies must collaborate to build needed practical skills through internships, co-op programs, and competitions.

6. **2026 Cybersecurity Workforce Research Report by SANS | GIAC**
SANS | GIAC – March 11, 2026
2026 Cybersecurity Workforce Research Report | SANS Institute and other training programs at https://www.sans.org/
Summary: The issue has changed from the numbers of workers but their capability, and the idea that system breaches are due to capability gaps.

7. **Communications Security Establishment Canada Annual Report 2024-2025**
Communications Security Establishment Canada – 2025
https://www.cse-cst.gc.ca/en/accountability/transparency/reports/communications-security-establishment-canada-annual-report-2024-2025
Summary: This provides a snapshot of the state of Canada's national cybersecurity workforce.

8. **Best Cybersecurity Certifications in 2026: 14 Credentials Ranked by Career Impact & ROI**
Axis Intelligence – March 8, 2026
https://axis-intelligence.com/best-cybersecurity-certifications-2026/
Summary: This provides an analysis of leading professional certifications with costs as they exist as of March 2026.

9. **What is the CyberSecure Canada Certification?**
CIRA - January 20, 2022
https://www.cira.ca/en/resources/news/cybersecurity/what-cybersecure-canada-certification/
Summary: The CyberSecure Canada certification, established by ISED and the CSE, is a voluntary program for SMEs. Drawing from the CCCS' Baseline Cyber Security Controls for Small and Medium Organizations which were released a few years ago, it outlines some of the steps businesses can take to protect their networks, data, and customers.

Carleton University
Infrastructure Resilience Research Group (IRRG)
Office of the Dean, Faculty of Engineering and Design

LEGAL, LIABILITY, AND INSURANCE FRAMEWORKS FOR CYBER INCIDENTS

1. **CCN reports cybersecurity maturity becoming prerequisite in critical infrastructure, industrial supply chains**
Industrial Cyber/Canadian Cybersecurity Network - April 09, 2026
https://industrialcyber.co/reports/ccn-reports-cybersecurity-maturity-becoming-prerequisite-in-critical-infrastructure-industrial-supply-chains/
Summary: It states quotes on cyber liability insurance as a mechanism to provide the clearest statement on how Canadian law and insurance markets are converging to make cybersecurity governance a commercial need.

2. **CyberSpace - Global cyber expectations for 2026: New laws, regulations, and increased severity of incidents? Part 1**
CMS Law – January 29, 2026
https://cms-lawnow.com/en/ealerts/2026/01/cyberspace-global-cyber-expectations-for-2026-new-laws-regulations-and-increased-severity-of-incidents-part-1
Summary: The law firm analyses the 2026 legal landscape, with detailed treatment of U.K. and E.U. developments.

3. **What you need to know about mandatory reporting of breaches of security safeguards**
Office of the Privacy Commissioner of Canada – current
https://www.priv.gc.ca/en/privacy-topics/business-privacy/breaches-and-safeguards/privacy-breaches-at-your-business/gd_pb_201810/
Summary: This provides an authoritative guide to mandatory breach reporting obligation under PIPEDA, noting when a breach must be reported, what constitutes a real risk of significant harm, the reporting obligation timeline, content requirements for breach reports, and the interaction between reporting and notification to affection individuals. It also notes record-keeping obligations and common compliance failures.

SPACE AND SATELLITE INFRASTRUCTURE SECURITY

1. **Space Security, and Why It Matters to Your Organization**
QA Blog, ISACA - February 27, 2026
https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2026/space-security-and-why-it-matters-to-your-organization
Summary: The report describes space security as a governance and compliance concern rather than purely technical. The European Apace Agency has shifted toward space resilience, removing reliance on the U.S.

2. **National Quantum Strategy roadmap: Quantum communication and post-quantum cryptography**
Innovation, Science and Economic Development Canada – current
https://ised-isde.canada.ca/site/national-quantum-strategy/en/national-quantum-strategy-roadmap-quantum-communication-and-post-quantum-cryptography
Summary: The strategy includes the QEYSSat satellite project, one of the first global tests of satellite-based secure quantum communication.

3. **With space infrastructure at risk, experts call for cybersecurity by design, tight governance, supply chain accountability**
Industrial cyber - October 07, 2025
https://industrialcyber.co/threat-landscape/with-space-infrastructure-at-risk-experts-call-for-cybersecurity-by-design-tight-governance-supply-chain-accountability/
Summary: Applies security-by-design and supply chain accountability principles familiar from OT/ICS security to the space infrastructure domain, and it notes that space systems operate as a system of systems, with each system representing a potential point of failure.

4. **Satellite Hacking: The Hidden Cyber Warfare Above Our Heads**
BQP Simulation – January 2026
https://www.bqpsim.com/blogs/satellite-hacking-cyber-warfare
Summary: It provides an overview of satellite hacking attack vectors, including compromised ground stations, software supply chain attacks, GPS spoofing, signal jamming, command hijacking, and payload exploitation. Most satellites were designed without cybersecurity in mind and run on proprietary protocols developed before modern cryptographic standards.

INTERNATIONAL DEVELOPMENT, CRITICAL INFRASTRUCTURE RESILIENCE, AND CYBERSECURITY

1. **Wartime Ukraine offers global lessons on the future of cyber resilience**
Atlantic Council – March 19, 2026
https://www.atlanticcouncil.org/blogs/ukrainealert/wartime-ukraine-offers-global-lessons-on-the-future-of-cyber-resilience/
Summary: Sustained cyber warfare has transformed Ukraine's digital environment into the most comprehensive available case study on how national infrastructure can endure under persistent cyber-kinetic pressure. Ukraine's next national cybersecurity strategy could invest systematically in regional-level cyber capacity.

2. **When data centres become targets: It's time to treat AI infrastructure as critical infrastructure**
World Economic Forum – April 2, 2026
https://www.weforum.org/stories/2026/04/ai-infrastructure-critical-infrastructure/
Summary: Drawing on March 2020 drone strikes illustrates that data centres have evolved from commercial real estate to strategic national assets, and cyber defence and access control are no longer sufficient.

3. **Critical Undersea Infrastructures: A Framework to Address Threats in a Post-Physical Context**
Georgetown Journal of International Affairs – February 12, 2026
https://gjia.georgetown.edu/2026/02/12/critical-undersea-infrastructures-a-framework-to-address-threats-in-a-post-physical-context/
Summary: It provides a governance framework for protecting subsea infrastructure in a "post-physical" threat environment," where "bad actors" exploit the maritime domain, jurisdictional complexity to conduct activities below the threshold of conventional warfare. It recommends a shift to multi-stakeholder approaches modelled on alignment between state and private maritime operators.

4. **Global Cybersecurity Index**
International Telecommunication Union – 2024
https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx
Summary: The Index is a benchmark of national cybersecurity capacity, covering 193 countries across five categories: legal measures, technical measures, organizational measures, capacity development, and cooperation. It identifies the institutional and regulatory infrastructure that distinguishes resilient from vulnerable nations and provides country-level data that enables development practitioners to identify where capacity-building investment will have the greatest marginal impact.