VOLUME 9 · ISSUE 05

BALSILLIE PAPERS

Enhancing Bill C-8: Strengthening Canada's Cybersecurity Framework for Critical Infrastructure

Thomas Aaron Gries

JUNE 2, 2026

As Canada becomes increasingly digitalized, cyber threats against critical systems have escalated dramatically. Threat actors, many of whom are state sponsored, are actively targeting the critical infrastructure (CI) Canada relies on. Securing these systems is of the utmost importance to the safety of Canadians and the prosperity of Canadian society.

INTRODUCTION

As Canada becomes increasingly digitalized, cyber threats against critical systems have escalated dramatically. Threat actors, many of whom are state sponsored, are actively targeting the critical infrastructure (CI) Canada relies on. Securing these systems is of the utmost importance to the safety of Canadians and the prosperity of Canadian society. To address this, cybersecurity measures are being discussed by the federal government, but gaps in proposed Bill C-8 (An Act respecting cyber security) leave vulnerabilities in Canada's cybersecurity framework unaddressed. As of June 2, the bill had passed its third reading in the House of Commons and its second reading in the Senate.[1] Further consideration, or amendment of the bill, should be imperative before seeking Royal Assent.

BACKGROUND

Chinese Advanced Persistent Threats

Chinese-linked advanced persistent threats (APTs) are becoming an increasing risk to Canada. Of particular concern is the targeting of CI, notably by APTs Salt Typhoon and Volt Typhoon. Operating under China's Ministry of State Security, Salt Typhoon is a "programmatic campaign" that is actively positioning itself to disrupt communication, power and infrastructure sectors in the United States in the event of a US–China conflict.[2] Similarly, Volt Typhoon, also Chinese-linked, aims at maintaining long-term persistence in conducting attacks against Western CI.[3] This shift in strategy by the People's Republic of China is done with the intent to "slow the US military's response and sow societal panic" should a crisis occur.[4] While primarily targeting US systems, both APTs pose a significant threat to Canada. Salt Typhoon has been observed targeting Canadian infrastructure.[5] Additionally, because the United States and Canada maintain cross-border infrastructure such as oil and gas, an attack on American CI will likely have a spillover impact on Canadians.[6] To gain access to these systems, Salt Typhoon will target perimeter and edge devices, such as virtual private networks (VPNs), firewalls and routers, while Volt Typhoon exploits devices at their end-of-life (EOL) or end-of-service (EOS).[7] The use of perimeter and legacy devices allows these APTs to blend in with regular network traffic and evade detection and appears to be a favoured tactic of these threat actors.

Legacy Systems

Devices past their end-of-life or software past their end-of-service date are no longer supported by the manufacturer. These systems potentially have exploitable vulnerabilities threat actors can abuse, increasing risk for organizations utilizing these devices. These older systems often go unacknowledged by their owners due to the potential infrequent use of the device or software, or the high cost associated with decommissioning, updating or replacing of legacy devices.[8] For example, "most oil-and-gas companies in Calgary are seven to eight years behind [in] patching and securing their [computer] systems that control critical infrastructure because it would cost too much to have regular downtimes."[9] This is partially due to

Canada's current framework for cybersecurity infrastructure and upgrades. Much like the rest of its allies, Canada lacks regulation on how to manage legacy systems, advising users to replace their EOL/EOS devices while acknowledging it might not always be possible.[10] The closest to a hardline policy on legacy devices among Five Eyes nations are Australia's endoflife.date (a government-provided link to a catalogue of EOL devices)[11] and the US PATCH Act. This US legislation mandates that updates be implemented in a timely manner among certain critical industries, such as medicine. However, the act only applies to devices made post-2023, exempting 53 percent of current medical devices.[12] Canada and its allies lack regulation regarding legacy, patches and EOL/EOS systems, leaving organizations and individuals to monitor alerts from vendors to ensure their systems are up to date. This is cause for concern, especially considering the frequent targeting of such systems by Chinese APTs.

Critical Infrastructure

CI covers a broad range of sectors that ensure societal functioning and safety. These include crucial industries such as healthcare, transportation, water, energy and communications.[13] In the Communications Security Establishment Canada's (CSE's) 2025–2026 National Cyber Threat Assessment, these critical sectors are depicted as high-profile targets for APT groups and cybercriminals, and as a key vulnerability in Canadian national security. According to the assessment, "state-sponsored threat actors are very likely targeting Canada and allied countries to pre-position for possible future disruptive or destructive operations."[14] Given Chinese APTs' consistent targeting of CI and utilities, the need for adequate cybersecurity in Canadian critical systems is imperative.

However, many of these critical sectors lack sufficient cybersecurity protection or employ outdated systems. Of particular importance is the oil and gas industry. Due to increased automation of this sector's technology, oil and gas organizations are becoming more vulnerable to disruptions caused by cyberattacks.[15] In Canada, oil and gas accounts for five percent of GDP and employs more than 500,000 Canadians.[16] Any cyberattack on Canadian oil and gas would have negative consequences on the Canadian economy.

Furthermore, the National Cyber Threat Assessment emphasizes that, in addition to financial burden, cyberattacks risk negatively impacting the health and emotional well-being of citizens.[17] For example, a 2024 scan by the US Environmental Protection Agency revealed poor cybersecurity postures across nearly 100 drinking water systems. Should each of those unpatched systems, open internet portals and default passwords be exploited by threat actors, more than 26 million Americans would have their supply of drinking water impacted.[18] This is a threat in Canada as well. Data from 2025 shows that utility providers, including waterworks, faced "a rise in both frequency and severity of [cyber] incidents."[19]

Ransomware

While ransomware attacks are distinct from the strategic positioning of state-sponsored APTs and are primarily financially motivated, they too are a major cyber threat to Canadian CI and national security. In fact, because of the perception among threat actors that CIs will pay larger ransoms to prevent disruption, the CSE has identified ransomware as "almost certainly the top cybercrime facing Canada's critical infrastructure."[20] Such threats could have disastrous consequences for the health and well-being of Canadians. For example, in October 2023, five hospitals in Southwestern Ontario were the victims of a ransomware attack conducted by threat actor Daixin.[21] This attack saw the theft of employee and patient records and the delay of patient treatments, and cost the hospitals more than C$7.5 million, demonstrating the devastating impact ransomware attacks against Canadian CI can have on the stability of Canadian society through the disruption of essential services.[22]

Additionally, the CI of smaller municipalities is an appealing target to cybercriminals and, by extension, APTs. This is the result of municipal utility infrastructure often being hindered by smaller budgets, outdated systems and limited resources, including a lack of dedicated cybersecurity professionals on staff.[23] These threats to the CI of smaller municipal utility providers must be addressed to safeguard the Canadian people and economy.

CANADA'S CURRENT APPROACH TO CYBERSECURITY AND THE PROPOSAL OF BILL C-8

State Authority vs Regulation

Canada, like other allied nations, currently lacks private-sector regulation for cybersecurity implementation among CI providers. This is not to say that the Canadian government lacks legislation on the matter. The Communications Security Establishment Act (CSE Act) of 2019 provided the federal government authority to access federal and non-federal infrastructure to assist in cybersecurity protection.[24] While a significant development in Canadian cybersecurity, the act is primarily concerned with empowering the government with the authority to directly intervene in information infrastructure, with an emphasis on the communications sector, for national security purposes. However, the act does not establish sector-specific obligations for other CI systems, such as water and wastewater treatment, energy or transportation. Additionally, the act is designed to bestow authority on the federal government, not to implement cybersecurity regulations for Canadian organizations to follow. This leaves a regulatory gap concerning Canadian CI and cybersecurity implementation, with the government often providing considerations rather than concrete rules.

The Canadian Centre for Cyber Security (CCCS) currently maintains the Security Considerations for Critical Infrastructure on its public website, suggesting measures such as the installation of VPNs, firewalls, multi-factor authentication, network segmentation and isolation, the use of backups, the

development of an incident response plan and remaining informed of vendor updates.[25] While these recommendations are sound, they are not industry-specific and their implementation ultimately rests on the discretion of the CI owner or operator. Additionally, the CCCS offers cyber-readiness toolkits designed to "elevate the cyber security posture of Canada's CI."[26] Designed for CI, these toolkits are available to any organization, but they serve as guidance rather than a mandate, meaning organizations can choose not to implement the recommendations. Provincial approaches mirror this voluntary framework. For example, British Columbia recommends that vulnerabilities with a Common Vulnerability Scoring System (CVSS) score between 9.8 and 10 be patched within 72 hours of discovery and that "formal acceptance of risk is required for all instances in which patching cannot be completed during the recommended time frame."[27] This essentially allows organizations to opt out of security requirements.

However, this voluntary opt-in system is inadequate. The example of Calgary oil and gas companies above demonstrates that prioritization of cost over security recommendations can lead to lapses in cybersecurity health if there is no legislated mandate to enforce it. As such, Canada's lack of a formal regulatory framework for CI and cybersecurity, including the voluntary use of cybersecurity toolkits, and the lack of an enforceable cyber standard, results in a flawed cybersecurity ecosystem that leaves Canadian CI vulnerable to cyberattacks.

Bill C-8 and its Limitations

Due to the flaws in Canada's current cybersecurity framework, an overhaul is necessary. This is evidenced by the Government of Canada's multi-year, ongoing effort to introduce federal cybersecurity legislation. The first of these attempts was 2022's Bill C-26, An Act representing cyber security amending the Telecommunications Act and making consequential amendments to other Acts, which would "codify national security requirements for the telecommunications sector."[28] However, C-26 was not passed before Parliament was prorogued in January 2025, which ended the bill.[29] Since then, the Canadian government has introduced Bill C-8, which features much of C-26's regulatory requirements, while expanding its scope to include "sectors deemed central to national interests."[30] This paper focusses only on the first two parts of the bill, as the third part is a mandate for ministerial review of the act five years after its potential date of Royal Assent and is not germane to this discussion.[31] Part I of the bill empowers the federal government to ensure telecommunication providers take all measures "necessary to secure the Canadian telecommunication systems."[32] Part II of the bill, the Critical Cyber Systems Protection Act, is designed to safeguard Canadian CI through the mandatory compliance of CI owner/operators with cybersecurity standards set out by the act.[33] As such, Part II of C-8 addresses the CSE Act's lack of cybersecurity regulation for organizations, while addressing more than just the communication space. When viewed in tandem, C-8 serves as a natural continuation of the CSE Act by giving regulations to all CIs to follow. Such enhanced measures include implementing comprehensive cybersecurity programs, conducting annual risk assessments, the reporting of incidents within a period not to exceed 72 hours, and the improvement of organizational capacity to respond to incidents and mitigate risk.[34] Non-compliance

or violation of these cyber frameworks will result in monetary penalties.[35] While a national cybersecurity framework with enforcement is necessary, Bill C-8 needs further refinement to better serve all CIs and utility providers.

Lack of Sector Consultation

Part I of Bill C-8 is sector-specific, being tailored to "promote the security of the Canadian telecommunications system."[36] Part II, however, applies to sectors and operators the Governor in Council designates as vital to Canadian "national security or public safety."[37] Once designated as CI operators, these parties must adhere to a series of mandatory requirements to be completed within 90 days of designation, but may receive a deadline extension at regulator discretion.[38] These include the identification and management of cybersecurity risks within their operations and supply chains, the protection of their cyber systems from compromise, the detection of any cybersecurity incident with the potential to affect critical systems, and the minimization of the impact of cybersecurity incidents.[39] Operators must also report incidents to CSE Canada within a period prescribed by regulation not to exceed 72 hours, review and maintain their cyber program, store cybersecurity records within Canada, and comply with cybersecurity directions from the Governor in Council.[40]

What is concerning, however, is the lack of industry input regarding these regulations. While the bill's preamble does state the federal government's commitment to collaboration with stakeholders, there are minimal references to collaboration between legislators and CI providers in the development of baseline regulations and subsequent government directives.[41] Should the Governor in Council issue a directive measure toward a provider or a particular sector, the industry stakeholders do not receive input on whether those directives are reasonable, effective or necessary.[42] While the Governor in Council is able to amend or revoke directives, based on potential impacts on affected operators, public safety, financial impacts, the delivery of vital services, and "any other factor that the Governor in Council considers to be relevant," there is no mention of direct consultation with stakeholders.[43] The lack of a commitment to such cooperation could hinder the implementation of directives and the regulations that mandate them.

The Organisation for Economic Co-operation and Development has found that stakeholders, in general, "can provide valuable input on the feasibility and practical implications of regulations," and that stakeholder engagement can "build trust in government, strengthen democratic values, and encourage higher compliance with regulations, especially when stakeholders feel that policymakers considered their views."[44] Therefore, C-8's lack of stakeholder input, combined with the broad baseline regulations that do not account for sector-specific needs or means, could result in a "one-size-fits-all" approach, as stated by NDP MP Gord Johns, which would "lump together banks, telecoms, nuclear facilities, and energy co-operatives under a single compliance framework."[45] Such a lack of consultation and differentiation among stakeholders risks lowering compliance with C-8 regulation and, by extension, leaving cybersecurity gaps unaddressed.

No Accounting for Size

Small CI and utility providers are at significant risk of cyberattack. A US Chamber of Commerce survey in 2024 found that 60 percent of small businesses cited cybersecurity threats, including phishing, malware and ransomware, as a top concern.[46] Additionally, while adhering to increased cybersecurity regulation would increase costs for CI providers (including software, hardware, firewalls, professional audits, endpoint-detection and response, and consultation with cybersecurity security professionals),[47] the costs associated with cyber incidents are just as, if not more, significant. For example, cybersecurity platform ThreatConnect has found that smaller utility providers suffer the most severe financial impacts in the event of ransomware attacks. An average ransomware payment for a small provider can cost an organization up to 31 percent of its operating income. This is significantly greater than the ransomware costs for medium and large providers, which would face a 13 percent and two percent impact on operating income, respectively.[48] Even if these small providers understand the risk of cyber incidents, they still often lack the necessary financial resources to pay for upgrades to systems or hire IT professionals.[49]

However, despite these documented vulnerabilities and resource limitations, Bill C-8 does not consider organizational size when assessing preparedness or when administering penalties for non-compliance.[50] This oversight could put smaller businesses at a significant disadvantage as they attempt to fulfill their newfound obligations to secure themselves and their supply chains.[51] While Bill C-8 does set maximum penalties for non-compliance ("not more than $500,000, in the case of an individual; and $15,000,000, in any other case") it does not specify minimums.[52] This lack of specificity presents two concerns for small providers. First, due to limited resources at their disposal compared to larger firms, small CI providers are likely to find the "compliance obligations overwhelming."[53] Second, the absence of formal guidance on how organizational size factors into the determination of a non-compliance penalty creates regulatory uncertainty. Although regulators have discretion to impose smaller fees at the discretion of "any other factors that the Superintendent considers relevant,"[54] the lack of any formal consideration of size within the act means small providers still face unclear risk exposure. This is significant, as even relatively modest penalties would likely represent a much larger percentage of operating income for small utility providers compared to larger ones, as demonstrated by the ThreatConnect data on ransomware impacts.[55]

No Mention of Legacy Systems

C-8 does not detail procedures or regulations regarding legacy, EOL or EOS systems. Part I, regarding telecommunications, does authorize the government to prohibit providers from using or to mandate the removal of particular products, services, or facilities "provided by a specified person in, or in relation to, its telecommunications network or telecommunications facilities [and products]."[56] However, this appears to be aimed at barring trade with particular manufacturers, similar to the Canadian ban on Huawei products from all 5G networks in 2022.[57]

Additionally, the bill would require organizations to implement the following: "mapping vital systems; understanding new powers of applicable regulators; developing and implementing the necessary plans and training to improve cyber-resilience; and, creating capacity to respond to breaches and ensuing investigations to limit risk and liability."[58] While these measures contribute to Canadian cyber resilience, the lack of mention of legacy, EOL and EOS systems throughout the bill is a significant gap. This oversight is concerning, as Chinese APTs are known to target such systems. Leaving them unaddressed in a national cybersecurity framework leaves any organizations operating these systems at risk. An amendment to the legislation may provide high-level regulations for organizations to follow regarding EOL and EOS device management, while leaving the technical implementation at the organizational level. This approach would address the vulnerability of EOL and EOS devices while ensuring efficiency.

No Compensation or Incentives

By the Canadian government's own acknowledgement, the best way to mitigate the threats associated with legacy systems is the removal of outdated devices and software, and the upgrading of those systems.[59] Yet, despite the upgrading of hardware and software systems being the most effective way organizations can become more cyber resilient, Bill C-8 offers no form of financial compensation or incentive to facilitate those upgrades. According to Part I of the Bill: "No one is entitled to any compensation from His Majesty in right of Canada for any financial losses resulting from the making of an order under subsection (1) [the prohibition or removal of products at government's demand]."[60] This will likely result in communication and other CI providers being penalized for non-compliance, while still facing the burden of achieving compliance with the new regulations without assistance from the government. Considering these regulations will result in higher operational costs for organizations, having no financial compensation from the government could put these organizations (especially smaller services) at financial risk.[61] Additionally, the use of monetary penalties without any form of compensation or financial assistance, while potentially serving as a coercive mechanism to achieve compliance, is unlikely to foster trust between CI sectors and the government, and will place an even more onerous financial burden on private CI sectors.

POLICY RECOMMENDATIONS FOR BILL C-8 AND BEYOND

Tiered Approach to Cybersecurity Framework

- Bill C-8 should be amended to account for variation in CI provider size, revenue and resources.
- Because rural and small CI providers often face challenges of limited resources and IT support, a tiered system should be implemented that categorizes CI providers as small, medium or large, while also distinguishing between rural vs urban providers and municipal vs private providers to account for differences in provider capacity.

- Such a classification system could reflect existing models already used by the Government of Canada, such as the utility cost-sharing project, which invests in infrastructure based on the size, means and structure of the utility provider.[62]
- Different standards should be based on CI tiers. For example, while large, more critical, operators may be held to the 90-day compliance window, smaller operators may be granted a standard 180-day compliance window.
- The federal government should also consider industry- and sector-specific consultation when drafting future versions of Bill-C to ensure regulations are both effective and realistic.
- Critical sectors (small, medium and large) should be sub-categorized and tiered based on criticality to Canadian society. Criticality will be determined through criteria such as the provider's economic impact, population affected, and role in national security. The more critical the sector, the more government communication and regulation.
- Concrete cybersecurity resiliency measures, such as the segmentation of networks and the isolation of external access of systems to known/trusted hosts or networks, should be mandated across these tiered categories.

Financial Supports for Cybersecurity

- Due to Bill C-8's current lack of compensation for providers, financial support should be considered for CI providers.
- Tax credits for cyber-compliant CI providers could work as incentives to achieve cyber compliance. Similar programs exist regarding green energy development. Between 2024 and 2035, an estimated C$25.7 billion has been or will be made available as part of the Clean Electricity Investment Tax Credit, which gives a 15 percent credit to aid in green electricity generation and storage technologies.[63]
- The federal government should consider the implementation of the Accelerated Investment Incentive, which could see small and medium-sized enterprises receive tax benefits for capital investments. These investments could be made in cybersecurity software, hardware and services.[64]
- Consider the development of federal grants or co-ops to fund capital accumulation. Similar programs have existed in Canada, such as Ontario's Cybersecurity Preparedness Initiative and the Government of Canada's C$10.3-million funding of cybercrime initiatives. While both programs limited the accumulation of hardware, a new fund could be designed with software and hardware upgrades in mind.[65]

- Administration of federal funding may be based on the tiered structures established in Recommendation 1, with small and medium providers, particularly in rural or remote areas or those facing resource constraints, receiving priority.
- Canada already funds improvement of infrastructure through the Canada Critical Structure Program, demonstrating Canada's commitment to infrastructure resilience.[66] But without upgrades to EOL/EOS systems, these providers remain vulnerable, leaving Canada's existing investments in cyber innovation and CI vulnerable to APT influence. The allocation of funds to assist in EOL/EOS system replacements would be crucial in defending against APT attacks.
- Consider the reduction of monetary penalties for non-compliance should the CI provider self-report the situation in a timely manner (within 72 hours of discovery, in line with Bill C-8's current framework) and offer effective remediation plans.
- The creation of a fund pool that small and medium-sized CI providers can draw on to assist in achieving cybersecurity compliance.
- The money contributing to this fund could be generated from the penalties accrued from larger CIs' non-compliance.

Further Facilitation of Private and Public Partnerships

- While Bill C-8 commits to collaboration with stakeholders,[67] little is detailed about how such collaborations could be achieved.
- To assist in the burden of ensuring CI is adequately protected from APTs and other cybersecurity threats, the Government of Canada should work with cybersecurity firms to secure CI providers.
- Existing public-private liaison mechanisms administered by the CCCS should be expanded to aid organizations in achieving C-8 compliance.
- Canada should work with hardware and software providers to create a notification system that alerts users when their products are approaching EOL/EOS. This could be modelled after Australia's existing endoflife.date database, but enhanced through the use of notifications to registered CI operators.
- Canada already operates a cybersecurity-related notification, the CCCS Really Simple Syndication alert system, which provides subscribers with notifications and advisories on potential and existing cyber threats that impact Canadian infrastructure.[68]
- A similar notification system dedicated to EOL/EOS would inform Canadian CI providers when their existing systems are at risk, encourage system upgrades, and promote Canadian cyber resilience.

END NOTES

[1] Bill C-8, *An Act representing cyber security, amending the Telecommunications Act and making consequential amendments to other Acts*, 1st Sess, 45th Parl (as of April 21, 2026, at second reading in the Senate), https://www.parl.ca/LegisInfo/en/bill/45-1/C-8.

[2] "Inside Salt Typhoon: China's State-Corporate Advanced Persistent Threat," DomainTools, September 24, 2025, https://dti.domaintools.com/inside-salt-typhoon-chinas-state-corporate-advanced-persistent-threat; Chris Buckley and Adam Goldman, "How China's Secretive Spy Agency Became a Cyber Powerhouse," *The New York Times*, September 28, 2025, https://www.nytimes.com/2025/09/28/world/asia/how-chinas-secretive-spy-agency-became-a-cyber-powerhouse.html.

[3] txOne Networks, "The Latest Storm: Volt Typhoon and Supply Chain Vulnerabilities," May 2, 2026, https://www.txone.com/blog/volt-typhoon-and-supply-chain-vulnerabilities.

[4] Communications Security Establishment Canada, *National Cyber Threat Assessment 2025-2026*, 13, https://www.cyber.gc.ca/sites/default/files/national-cyber-threat-assessment-2025-2026-e.pdf.

[5] Catharine Tunney, "China-Backed Hackers 'Almost Certainly' Targeted Canada During Theft of Millions of Americans' Data," *CBC News*, September 5, 2025, https://www.cbc.ca/news/politics/salt-typhoon-canada-cyber-security-1.7625122.

[6] Canadian Centre for Cyber Security, *The Cyber Threat to Canada's Oil and Gas Sector* (2023), https://www.cyber.gc.ca/sites/default/files/cyber-threat-oil-gas-e.pdf.

[7] Canadian Centre for Cyber Security, *People's Republic of China Cyber Threat Activity: PRC Cyber Actors Target Telecommunications Companies as Part of a Global Cyberespionage Campaign*, Cyber Threat Bulletin, last updated June 19, 2025, https://www.cyber.gc.ca/en/guidance/cyber-threat-bulletin-prc-cyber-actors-target-telecommunications-companies-global-cyberespionage-campaign; txOne Networks, "The Latest Storm."

[8] Paul Asadoorian, "EOL Devices: Exploits Will Continue Until Security Improves," *Eclypsium*, September 3, 2025, https://eclypsium.com/blog/eol-devices-exploits-will-continue-until-security-improves.

[9] Andrew Seale, "Canadian Companies Struggle to Defend Against Data Breaches as Incidents Mount," *The Globe and Mail*, February 15, 2025, https://www.theglobeandmail.com/business/article-canadian-companies-struggle-to-defend-against-data-breaches-as.

[10] Canadian Centre for Cyber Security, *Obsolete Products – ITSAP.00.095, Awareness Series*, March 2023, https://www.cyber.gc.ca/en/guidance/obsolete-products-itsap00095.

[11] Australian Cyber Security Centre, "End of Support," last updated July 29, 2024, https://www.cyber.gov.au/protect-yourself/securing-your-devices/how-update-your-device-and-software/end-support.

[12] Steve Alder, "House Committee Hears New Concerns About Legacy Medical Device Cybersecurity," *HIPAA Journal*, April 8, 2025, https://www.hipaajournal.com/house-committee-concerns-legacy-medical-device-cybersecurity.

[13] "Canada's Critical Infrastructure (CI)," *Public Safety Canada*, last modified January 24, 2025, https://www.publicsafety.gc.ca/cnt/ntnl-scrt/crtcl-nfrstrctr/cci-iec-en.aspx.

[14] Communications Security Establishment Canada, *National Cyber Threat Assessment 2025–2026*, 5.

[15] "Cyber Threats for the Oil and Gas Industry," *Meriplex*, https://meriplex.com/cyber-threats-for-the-oil-and-gas-industry.

[16] Soha Sarfraz, "The Geopolitical Ramifications of Cyber Attacks On Canadian Energy Grids," NATO Association of Canada, March 27, 2024, https://natoassociation.ca/the-geopolitical-ramifications-of-cyber-attacks-on-canadian-energy-grids/.

[17] Communications Security Establishment Canada, National Cyber Threat Assessment 2025–2026, 6.

[18] Anna Ribeiro, "FDD experts warn EPA cyber grants are a 'drop in the bucket' as attacks escalate, call for expanded support," Industrial Cyber, August 26, 2025, https://industrialcyber.co/utilities-energy-power-water-waste/fdd-experts-warn-epa-cyber-grants-are-a-drop-in-the-bucket-as-attacks-escalate-call-for-expanded-support.

[19] M. J. Martin, "Canadian Municipal Cyber Attacks," *Vividcomm*, April 14, 2025, https://vividcomm.com/2025/04/14/canadian-municipal-cyber-attacks.

[20] Communication Security Establishment Canada, *National Cyber Threat Assessment 2025-2026*, 25.

[21] Communications Security Establishment Canada, *National Cyber Threat Assessment 2025-2026*, 25.

[22] "Southwestern Ontario Hospitals Cyberattack Cost Organizations at Least $7.5M," *CBC News*, last modified August 30, 2024, https://www.cbc.ca/news/canada/windsor/southwestern-ontario-hospitals-cyberattack-1.7308623.

[23] Bruce Rule, "Why Cybercriminals Target Small Utilities," *Tanium*, July 28, 2021, https://www.tanium.com/blog/why-cybercriminals-target-small-utilities.

[24] *Communications Security Establishment Act*, SC 2019, c13, ss 26-27, Justice Laws website, current to December 10, 2025.

[25] Canadian Centre for Cyber Security, *Security Considerations for Critical Infrastructure (ITSAP.10.100), Awareness Series*, July 2025, https://www.cyber.gc.ca/en/guidance/security-considerations-critical-infrastructure-itsap10100.

[26] Canadian Centre for Cyber Security, *Cyber Security Readiness Goals: Securing Our Most Critical Systems*, Version 1.0, October 29, 2024, 2, https://www.cyber.gc.ca/sites/default/files/cyber-readiness-goals-e.pdf.

[27] British Columbia Office of the Chief Information Officer, *OCIO Patch Guidelines: Vulnerability and Patch Management*, Version 2.2, February 18, 2021, 1, https://www2.gov.bc.ca/assets/gov/british-columbians-our-governments/services-policies-for-government/information-management-technology/information-security/defensible-security/ocio_patch_guidelines_-_2021-02-18.pdf.

[28] Catharine Tunney, "Senators amend error in cybersecurity bill that could have cancelled half of it," *CBC News*, December 6, 2024, https://www.cbc.ca/news/politics/cybersecurity-bill-c26-senate-amend-1.7401358.

[29] Sunny Handa, Wendy Mee, Ellie Marshall, John Lenz and Mallory Gallant, "House of Commons Re-Introduces Federal Cybersecurity Legislation," Blakes, June 23, 2025, https://www.blakes.com/insights/house-of-commons-re-introduces-federal-cybersecurity-legislation.

[30] Jaime Cardy, "From Bill C-26 to Bill C-8: House of Commons Reintroduces Key Cybersecurity Legislation," *Dentons Data*, July 8, 2025, https://www.dentonsdata.com/from-bill-c-26-to-bill-c-8-house-of-commons-reintroduces-key-cybersecurity-legislation.

[31] *Bill C-8, An Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts*, 1st Sess, 45th Parl, as passed March 26, 2026, House of Commons of Canada, 94, https://www.parl.ca/Content/Bills/451/Government/C-8/C-8_1/C-8_1.PDF.

[32] *Bill C-8*, ii.

[33] *Bill C-8*, ii, 23.

[34] Hélène Deschamps Marquis, Matt Saunders, Chloe Hughes-Légaré and Aaron Grech, "Bill C-8 revives Canadian cyber security reform: What critical infrastructure sectors need to know," *BLG*, July 28, 2025, https://www.blg.com/en/insights/2025/07/bill-c8-revives-canadian-cyber-security-reform-what-critical-infrastructure-sectors-need-to-know; Christi Thompson, "What Energy & Finance Businesses Need to Know About Canada's New Cybersecurity Law Bill C-8," *Expera Information Technology* (blog), August 5, 2025, https://www.experait.com/2025/08/05/what-energy-finance-businesses-need-to-know-about-canadas-new-cybersecurity-law-bill-c-8.

[35] *Bill C-8*, 16, 63.

[36] *Bill C-8*, 1.

[37] *Bill C-8*, ii.

[38] *Bill C-8*, 28–29.

[39] *Bill C-8*, 28.

[40] *Bill C-8*, 31, 36–37.

[41] *Bill C-8*, 23.

[42] *Bill C-8*, 31.

[43] *Bill C-8*, 32.

[44] Paul Davidson, Christiane Arndt-Bascle, Marie-Gabrielle de Liedekerke and Renny Reyes, "Improving Stakeholder Engagement and Evidence-Based Policy Making," *The Regulatory Review*, December 7, 2022, https://www.theregreview.org/2022/12/07/davidson-improving-stakeholder-engagement.

[45] *House of Commons Debates*, vol 152, no 33, 1st Sess, 45th Parl, October 3, 2025, https://www.ourcommons.ca/DocumentViewer/en/45-1/house/sitting-33/hansard.

[46] Jonathan Reed, "Cybersecurity dominates concerns among the C-suite, small businesses, and the nation," *IBM*, accessed January 26, 2026, https://www.ibm.com/think/insights/cybersecurity-dominates-concerns-c-suite-small-businesses-nation; Thaddeus Swanek, "Small Businesses Think Cyberattacks Are Biggest Threat, Survey Shows," *US Chamber of Commerce*, April 2, 2024, https://www.uschamber.com/small-business/new-survey-finds-small-businesses-think-cyberattacks-are-biggest-threat.

[47] Jason Miller, "The Cost of Cybersecurity and Creating an Achievable Security Budget," *BitLyft*, January 16, 2026, https://www.bitlyft.com/resources/the-cost-of-cybersecurity-and-creating-an-achievable-security-budget.

[48] Robert Walton, "Ransomware is a major threat to smaller utilities, manufacturers and health care providers: report," *Utility Dive*, April 18, 2023, https://www.utilitydive.com/news/ransomware-is-a-major-threat-to-smaller-utilities-manufacturers-and-health/647913.

[49] Rule, "Why Cybercriminals Target Small Utilities."

[50] Cardy, "From Bill C-26 to Bill C-8."

[51] Sabrina Charland, *Legislative Summary of Bill C-8: An Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts*, Pub No 45-1-C8-E (August 28, 2025), 25, https://lop.parl.ca/staticfiles/PublicWebsite/Home/ResearchPublications/LegislativeSummaries/PDF/45-1/PV_45-1-C8-E.pdf.

[52] *Bill C-8*, 63.

[53] Dale Smith, "A Cybersecurity Bill with Built-in Vulnerabilities," *CBA/ABC National*, September 17, 2025, https://nationalmagazine.ca/en-ca/articles/law/in-depth/2025/a-cybersecurity-bill-with-built-in-vulnerabilities.

[54] *Bill C-8*, 66.

[55] Walton, "Ransomware is a major threat to smaller utilities."

[56] *Bill C-8*, 2.

[57] Catharine Tunney and Richard Raycraft, "Canada bans Chinese tech giant Huawei from 5G network," *CBC News*, May 19, 2022, https://www.cbc.ca/news/politics/huawei-5g-decision-1.6310839.

[58] Deschamps Marquis et al., "Bill C-8 Revives Canadian Cyber Security Reform."

[59] Canadian Centre for Cyber Security, *Obsolete Products – ITSAP.00.095*.

[60] *Bill C-8*, 3.

[61] Charland, *Legislative Summary of Bill C-8*, 25.

[62] Housing, Infrastructure and Communities Canada, "Investing in Canada Infrastructure Program," last modified January 9, 2025, https://housing-infrastructure.canada.ca/plan/icp-pic-INFC-eng.html.

[63] Canadian Climate Institute, "Clean Electricity, Affordable Energy: How Federal and Provincial Governments Can Save Canadians Money on the Path to Net Zero," June 2023, https://climateinstitute.ca/wp-content/uploads/2023/06/Clean-Electricity-Affordable-Energy.pdf.

[64] Public Safety Canada, Canada's National Cyber Security Strategy: Securing Canada's Digital Future, January 2025, 19, https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg-2025/ntnl-cbr-scrt-strtg-2025-en.pdf.

[65] Public Safety Canada, "Call for proposals: Cyber Security Cooperation Program 2025," last modified October 2, 2025, https://www.publicsafety.gc.ca/cnt/ntnl-scrt/cbr-scrt/cprtn-prgrm/cll-prpsls-cybr-scrty-cprtn-prgrm/bckgrnd-en.aspx; Government of Ontario, "Cybersecurity Preparedness Initiative," published September 3, 2024, last updated January 27, 2025, https://www.ontario.ca/page/cybersecurity-preparedness-initiative.

[66] "Investing in Canada Infrastructure Program."

[67] *Bill C-8*, 23.

[68] Canadian Centre for Cyber Security, "Contact the Cyber Centre," last modified June 7, 2024, https://www.cyber.gc.ca/en/contact-cyber-centre.

Thomas Aaron Gries is a recent Master of Arts graduate in Global Governance from the University of Waterloo. He holds a Bachelor of Arts in History from the University of Lethbridge (2022). Thomas gained experience in policy and cybersecurity through the Balsillie School of International Affairs' fellowship program and an internship at the cybersecurity firm eSentire. He completed his Major Research Paper during an exchange at the University of Konstanz, Germany, and most recently interned with Canada's Permanent Mission to the WTO in Geneva, Switzerland. His academic interests focus on European history, geopolitics, and international relations.

BALSILLIE PAPERS

ISSN 2563-674X • doi:10.51644/BAP95

balsilliepapers.ca