TRIPLE HELIX

Overcoming Canada’s Disorganized and Ineffective Approach to Cyber Security Standards

by Alexander Rudolph, W. Alec Cram, Windhya Rankothge, Michael Davie

October 2025

POLICY PERSPECTIVE

Overcoming Canada’s Disorganized and Ineffective Approach to Cyber Security Standards

by Alexander Rudolph, W. Alec Cram, Windhya Rankothge, Michael Davie

October 2025

This article is supported by Amazon Web Services (AWS)

Prepared for Triple Helix
Suite 200, 8 York Street, Ottawa, ON K1N 5S6 Canada www.cgai.ca/triple_helix

ISBN: 978-1-77397-356-2

Overcoming Canada's Disorganized and Ineffective Approach to Cyber Security Standards

On 6 February 2025, the government of Canada released its new *National Cyber Security Strategy*. The strategy outlines the government of Canada's long-term goals to improve cyber security for Canadians, including through the use of international cyber security standards as a guide in these efforts. Despite the intent to offer better cyber security standards, the Strategy substantively addresses the concept only four times and lacks detail or clarification regarding how the government intends to use them. At this stage, the description amounts to little more than acknowledging the importance of cyber security standards. As a result, there is insufficient direction and guidance for the federal bureaucracy, businesses, and civil society on how the federal government intends to use cyber security standards and engage with the standardization community. Ineffective management of cyber security standards risks increasing the costs for businesses to work with the Government of Canada and risks leaving gaps in Canadian cyber security.

Canada and all countries benefit from the collaborative, international development of cyber security standards. Historically, Canada and many other countries have significantly benefited from a lot of the work done on cyber security standards by the United States' National Institute of Standards and Technology (NIST). However, in the United States, the NIST is significantly downsizing under President Trump, which has greatly limited its capacity to develop standards in cyber security and future security needs, such as post-quantum cryptography. This loss of contributions creates a need both domestically and internationally, which Canada appears prepared to address with the *National Cyber Security Strategy*. The lack of specificity in the planning and integration of cyber security standards in the strategy presents an opportunity for the government to reinvigorate and innovate its approach to cyber security standards.

This paper will introduce standardization and cyber security standards, including how the federal government of Canada currently makes use of standards in federal policy and procurement. This critical assessment highlights inefficiencies with the government's approach to cyber security standardization in terms of the effects on policymaking and procurement. The paper ends with recommendations to improve the federal government's approach to cyber security standardization by drawing upon the best practices of other countries. In particular, a reorganization of the government of Canada's management of cyber security standardization would reduce costs for the government and businesses working with the government and ensure that Canada has strong cyber security protections of critical services.

Canada's National Cyber Security Strategy and Cyber Security Standards

Since the wide adoption of the Internet in the 1990s, cyber security and cyber security standards have increasingly become important to ensure that both the public and private sectors maintain a baseline of cyber security that will protect an organization and those it serves. Despite recognizing and increasingly using cyber security standards, the federal government has taken an ad hoc approach to the promotion and development of cyber security standards, with most of this work occurring at the regulatory level. Although the *National Cyber Security Strategy* recognizes that cyber security standards are important to achieving national cyber security objectives, the federal government must change its approach to improve coordination and treat cyber security standards as a national security priority.

Further, the federal government has yet to explain why cyber security standards are a national security issue. There is also a lack of clarity on how the Government of Canada contributes to the design, implementation, and overall management of cyber security standards in federal policymaking. Since 1970, the government of Canada has delegated the leading role of standards development and promotion to the Standards Council of Canada (SCC) as the crown corporation in charge of voluntary standardization (standards an organization can choose as opposed to legally required ones). But there is no single federal authority in charge of mandatory cyber security standards, which are instead delegated to sector-specific federal departments or agencies, such as Health Canada for health-related standards or Accessibility Standards Canada.

The *National Cyber Security Strategy* has committed the government of Canada to renewing its leadership on cyber security issues to make it agile. This is partly due to a previous federal government review into how it achieves its policy objectives, which noted a broad lack of engagement from government leadership, contributing to little coordination and harmonization of efforts across the government. This siloed approach leads to redundancy and inefficiencies as the federal departments and organization working with standards are unsure of what the rest of the government is doing and what they should be doing. Industry is caught in the middle, trying to make the best decisions in an environment where the government is unable to provide certainty and clarity. Despite recognizing the importance of cyber security standards, the strategy is silent on how the federal government intends to exercise its leadership related to cyber security standards.

Adding to these concerns, the *National Cyber Security Strategy* lists the SCC as the policy lead for cyber security standards, which would encompass a major increase to SCC's portfolio as a crown corporation typically reserved for the government. All other policy areas listed are led by a Minister, which means the federal government is effectively giving its policy powers on cyber security standards to a crown corporation without the mandate to do so. This brings into question the government's ability to achieve its own stated objectives to use cyber security standards to achieve *National Cyber Security Strategy* objectives.

What are Cyber Security Standards?

Standards "[establish] accepted practices, technical requirements and terminologies" for various different fields that "provide guidelines, characteristics or requirements for products, processes or services." A Public Services and Procurement Canada official once stated that standards were meant to "have an objective, performance-based statement of how a product should behave for a specific outcome." Standards are usually developed by a committee or group of stakeholders in the field of interest, which is then approved by a recognized international standards body. Some common international standards include International Standards Organization (ISO) 27001 and 27002 on information security management and control, which governments and organizations have adopted internationally.

In Canada, the SCC is the national authority in charge of voluntary standardization. Being the national authority on voluntary standardization means that the SCC accredits standards developing organizations (SDOs), approve standards that are created by these SDOs, which then become a National Standard of Canada (NSC). Industry, the public sector, and civil society adopt cyber security standards voluntarily because they are strong, reliable guides to adopting cyber security practices that protect an organization. It helps organizations adopt best practices before they have to learn them independently. One such voluntary cyber security NSC in which the federal government has played a role is CyberSecure Canada's CAN/DGSI 104 baseline cyber security controls for small and medium enterprises. However, not all standards are the same. Whereas most standards are voluntary, Federal and provincial governments can make them mandatory by turning them into law, regulations, or contractual obligations. In addition, while many laws and regulations require organizations to adopt cyber security practices, cyber security standards provide a mechanism to prove and demonstrate compliance.

Cyber security standards can impact organizations in a variety of ways, with consequences on contracts and vendor agreements being two particularly common. Private and public organizations alike often use cyber security standards in contracts in order to ensure a sufficient level of cyber protection in the product or service during procurement. When an organization like the government of Canada purchases digital technology – e.g., a cloud service – cyber security standards provide a common language for the procuring agency and the supplier to both agree on an appropriate level of security to protect government systems. This can also occur when acquiring cyber insurance, which often requires organizations to maintain certain practices such as the implementation of particular cyber security standards. However, while the government of Canada regularly uses cyber security standards to help inform its decisions, the federal government has played a comparatively minimal role in cyber security standardization compared to other sectors.

A significant reason for this minimalist approach is that the government's authorities, responsibilities, and accountabilities for standardization management are distributed unevenly across the government.

The Diffusion of Federal Government Cyber Security Standardization

Canada does not have a single, federal agency in charge of cyber security standardization, but the responsibilities for cyber security standards is diffused across the federal government with unclear responsibilities. This is particularly problematic as a lack of clear coordination and responsibilities greatly diminishes the federal government's ability to accomplish its objectives laid out in the *National Cyber Security Strategy*. This is particularly shown with the decline of the Canadian General Standards Board (CGSB).

In 1934, the Government of Canada created the Canadian General Standards Board (CGSB) as one of the first public organizations to oversee the government's approach to developing, assessing, and using standards. Today, CGSB still operates as the internal component of Public Services and Procurement Canada (PSPC) that provides standards services and development for the federal government, but its work has been significantly reduced over the years. Ten years ago, an SCC official described the CGSB as "a very useful organization 40 to 50 years ago," but its catalogue of standards and offerings has diminished since this time due to more up-to-date alternatives. This is largely because the core of standardization activities occurs outside of the federal government and is conducted by SCC and other accredited organizations. Traditionally, CGSB was used when the federal government sought standardization in a specific area to serve the government's needs. Although CGSB has contributed to standards in related areas like electronic records as documentary evidence, they have had little to no contributions to the federal government's recent efforts such as CyberSecure Canada or the Canadian Program for Cyber Security Certification (CPCSC).

Despite still being around today, inefficiencies identified in CGSB and Canada's overall approach to standardization led to the creation of the Standards Council of Canada (SCC) in 1970. The *Standards Council of Canada Act* established SCC as a federal Crown corporation to "promote efficient and effective voluntary standardization in Canada." SSC fulfills its mandate by supporting subject matter experts in the development of standards and by accrediting standards development organizations and conformity assessment bodies, which can include certification bodies and testing laboratories, and promoting public-private cooperation in voluntary standardization. The Minister of Industry, Science and Technology oversees and directs SCC, and does so at arm's length. Historically, this approach has benefited Canada, with standardization contributing to overall labour productivity and GDP growth. SCC has estimated that growth in standardization contributed $5.86 billion to the country's economy in 2019 alone. As a Crown corporation (not a government department), SCC is a largely independent organization, primarily funded by Parliamentary appropriations and supplemented by revenue generated from its operations. Although independent, SCC regularly works with federal and provincial governments as part of its mandate to provide policy and technical expertise on standards. While SCC is indeed the largest Canadian organization overseeing voluntary standards development, there is no similarly comprehensive organization to oversee the development of mandatory standards for the federal government. Instead, the federal government involves multiple other government organizations to address voluntary and mandatory standardization activities.

Suiting similar needs as the CGSB, Accessibility Standards Canada was created in 2019 under the *Accessible Canada Act* to specifically create accessibility standards for federally regulated entities and organizations. Accessibility Standards Canada has contributed to developing accessibility standards for information and communications technology (ICT) and is currently developing accessible and equitable artificial intelligence (AI) systems standards as well. Amid a renewed interest in the federal government's standards making mechanisms, the Council of Canadian Innovators have gone so far as to recommend that the CGSB and Accessibility Standards Canada be dissolved or incorporated into the SCC or another accredited standards body. Although the government cannot easily dissolve Accessibility Standards Canada as it would require legislative change, there is a growing belief that the current lack of coordination between institutions and mechanisms across the government hinders its ability handle standards sufficiently and effectively, particularly concerning cyber security standards.

Since the creation of SCC in 1970, government of Canada agencies have predominantly taken a minor role in standards development and promotion, with certain areas of specialized involvement. Despite developing a generally favorable reputation in the federal government and industry, SCC is not without flaws. A 2019 audit of SCC by the Auditor General of Canada identified major deficiencies in its corporate governance, but noted they met the criteria in all other areas and provided recommendations for improvements. Historically, due to the broadly cross-cutting nature, standards have not been under the purview of one particular minister's portfolio but have been most closely associated with the Minister of Industry due to SCC reporting to Parliament through Industry Canada. This is particularly the case with cyber security standards, whereby the *National Cyber Security Strategy* itself says the SCC is the cyber security standards policy lead, but as a crown corporation, its policy and governance levers are limited compared to a department like ISED. Adding further ambiguity. SCC as a crown corporation reports to Parliament through the Minister of ISED and cyber security standards only represents a fraction of their work. Lastly, it is unclear that the mandate of the new Minister of AI and Digital Innovation includes a role in cyber security standards or the *National Cyber Security Strategy*.

As it currently stands, SCC has been tasked with a policy lead on cyber security standards with ministry-level objectives, but their tools are significantly limited due to being a crown corporation and not a government department. While SCC is the cyber security standards lead for Canada, there is significant potential for greater involvement by the government to increase the adoption of proven cyber security standards and align the government's activities with international best practices. Further complicating SCC's position as policy lead on standards, SCC plays no role in determining federal government policy related to the use of standards for government services and activities. When it is not ministry-level policy planning and direction, on a day-to-day basis, most of the activities related to cyber security standards in the federal government are governed by the Treasury Board Secretariat (TBS), the Canadian Centre for Cyber Security (CCCS), and Shared Services Canada (SSC).

Treasury Board Secretariat

Technical, operational, and procurement activities related to cyber security standards are distributed across the federal government, but it is the Treasury Board Secretariat that establishes overarching strategic policies, frameworks, and mechanisms that departments must adhere to in the conduct of their work. In particular, the Treasury Board Secretariat holds administrative and regulatory oversight over the federal government, setting what standards and policies must be followed. This means that as much as SSC and the Canadian Centre for Cyber Security (CCCS) provide recommendations and guidance on what cyber security practices must be followed, TBS determines if these recommendations or guidance become mandatory government of Canada policy. These policies also affect how the federal government spends its money, which means that TBS has significant influence on determining the security requirements for products procured by the government. Examples of such policy frameworks which affect all of the government include the Enterprise Cyber Security Strategy and the Policy on Service and Digital.

Canadian Centre for Cyber Security /Communications Security Establishment

CCCS launched in 2018 as a part of the Communications Security Establishment (CSE) to serve as the Government of Canada's technical authority on cyber security and help protect the Government and Canadians. As part of its work, CCCS is the public-facing organization of CSE that works closely with industry and the rest of the federal government to provide expert guidance and assistance in the oversight of cyber security. CCCS and CSE's primary role related to cyber security standards is to serve as the technical experts in determining what cyber security standards meet the needs for the federal government, such as in the Cloud Service Provider (CSP) Information Technology Security (ITS) Assessment Process (ITSM.50.100). This is problematic for the federal government's management of cyber security because the ITS assessment is based on ITSG-33, an aging risk management framework. Described as "obsolete" by retired Vice-Admiral Ron Lloyd, ITSG-33 is mandated by TBS so that "departments ensure security is considered right from the start." Although CCCS and CSE could recommend this change, any change to this or other government-wide mandated frameworks would have to be done by TBS, which highlights the minimal policymaking abilities of the government's technical experts. The Minister of National Defence oversees CCCS and CSE.

Shared Services Canada (SSC)

SSC was created in 2011 under the *Shared Services Canada Act* to centralize the management of the government's information technology. As part of its many activities, SSC has sought to standardize information technology, including related to security, and provides guidance to federal government departments related to cyber security standards. This work has been particularly important for cyber security standards and compliance related to cloud services as the federal government has significantly increased its adoption of cloud computing following the adoption of the cloud-first strategy in 2018, with subsequent updates to the strategy in 2023. One key SSC mechanism is the Service, Program and Procurement Review Board (SPPRB), which approves cyber and IT standards recommendations and security assessment and authorization recommendations for all new enterprise services. The SPPRB relies on recommendations from the Security Risk Management Board (SRMB), whose mandate includes reviewing, analyzing and managing medium to high-risk cyber and IT security issues and risks that could affect the government of Canada's IT infrastructure. This has meant that SSC has been on the frontlines of ensuring that the federal government's information technology is secure, but SSC follows the direction and guidance of CCCS/CSE and TBS. SSC is overseen by the Minister of Government Transformation, Public Works and Procurement.

There are multiple federal government organizations who play important roles in cyber security standards, but most of their activities are siloed. A lack of coordination or mechanism to align their activities with government of Canada priorities makes achieving national objectives related to cyber security standards incredibly difficult.

Current Federal Government Policy Direction on Cyber Security Standards

What has been shown to this point is that the government of Canada has consistently stressed how critical cyber security standards are. The government of Canada uses cyber security standards for many purposes, including as tools to achieve policy objectives, to help guide and determine the appropriate security needed for the federal government, and to verify that software and hardware have the appropriate cyber security controls for government use. However, no fewer than four ministries are actively involved and the processes are siloed, with minimal to no coordination between relevant government agencies and departments.

Canada's 2025 *National Cyber Security Strategy* does little to address this lack of coordination, but seeks to leverage the existing system to achieve new objectives without any indication of change or plans to make this happen. The strategy itself directly mentions the role of cyber security standards to achieve Canadian cyber security policy objectives in four instances:

1. For Canada to continue working with international partners to champion international law, norm-based behaviour, and international standards in cyberspace;
2. Work with international partners to coordinate labelling and reciprocal recognition of Canadian standards related to Internet of Things;
3. Promote the "widespread adoption of strong cyber security standards and practices"; and
4. Work with "stakeholders as part of the Global Coalition on Telecommunications to foster diverse supply chains as well as secure and interoperable standards in the telecommunications sector."

SCC has the tools to contribute to these objectives as an organization involved domestically and internationally in cyber security standards promotion, but its ability to influence or mandate the adoption, use, coordination, or integration into the government of Canada's procurement or other activities is significantly limited. SCC has had success as a crown corporation, but its success in its mandate of promoting and developing standards should not be confused with having the tools or authority of the crown or federal government to achieve these policy objectives. Due to the siloed approaches that lack coordination, if SCC were to achieve success in these objectives, it would be unlikely to have much of an effect on the federal government's activities.

Whereas the central focus for this paper is cyber security standards, this lack of coordination and complex administration and governance is typical of the Government of Canada's overall administration of cyber security. VAdm (ret'd) Lloyd articulated this recently, illustrating how the complex, overlapping, and at times redundant authorities, responsibilities, and accountabilities between TBS, ISED, SSC, and CCCS/CSE lead to poor management of the federal government's digital systems.

There are multiple problems with the federal government's approach to cybersecurity standards being distributed across the regulatory level of government, with no coordination at the policy level. One of the primary impacts of this is on industry. Businesses increasingly become unsure of what requirements or standards to follow.

Further, this lack of coordination where redundancy or overlap with international or other standards occur can lead to inefficiencies and make Canadian businesses less competitive. This is especially onerous for small and medium-sized businesses, who lack the resources and often the knowledge to navigate this complex regulatory arrangement. For policymakers and members of the government, the intricate, disorganized system makes it difficult to address or understand who is responsible. This leads to further entrenchment of the lack of coordinated action on cybersecurity standards, and forfeiture of the federal government's role in cybersecurity standards policy to the SCC.

Recommendations for Policymakers

In response to the cyber security standards concerns noted above, policymakers need to take immediate action to ensure this lack of coordinated activity does not negatively impact achieving the *National Cyber Security Strategy*. We have framed what we believe to be the necessary, related steps within four key groups of activities, which we outline below: recognition, responsibility, process management, and communication.

1. **Recognition of the importance of cyber security standards**. The first step is to increase clarity and transparency in regard to the role of cyber security standards within the federal government ecosystem. Fundamental to this activity is to draw attention to the role of cyber security standardization by clearly establishing and formally documenting what cyber security standards are (and what they are not), why they are important, and what role they play in government initiatives. By establishing a foundational understanding of the importance of cyber security standards, less ambiguity and confusion on the practicalities of standards setting and use is likely to emerge.

2. **Responsibility for overseeing cyber security standards.** Next, the Minister of Industry should appoint a Cyber Security Standards Task Force within ISED that reports directly to her and would be responsible for facilitating, coordinating, and overseeing the various groups and organizations associated with cyber security standards. Formal guidelines should be established regarding decision rights and accountabilities for cyber security standards within the government.

   Establishing and maintaining a formal list of existing cyber standards in place for various government entities and initiatives is of particular importance. Such a listing should be accessible to stakeholders and transparent regarding the sources and uses of particular cyber standards. A full, formal mapping of the federal government's landscape and use of cyber security standards will help policymakers and those working with standards to understand the current state and direction of standardization across the federal government. In addition, this will help assist with further standardization by creating a common operating picture of where the federal government is with cyber security standards. It will also provide a better understanding of what standards private industry should prioritize if they wish to work with or sell to the federal government.

Further, since regulatory fragmentation and redundancy complicate compliance (e.g., Quebec enforces its own data protection laws), this group could spearhead the harmonization and reconciliation of federal and provincial regulations to facilitate a more cohesive intergovernmental cyber security and privacy governance structure.

Finally, ethical and legal dilemmas surrounding emerging technologies, such as surveillance and privacy, must be carefully navigated. By establishing a Cyber Security Standards Taskforce, advice can be offered to policymakers to strike a balance between innovation, individual rights, and best practices.

3. **Cyber standards process management:** Although clarity on the standards that are currently relevant to government entities is important, it is also critical that there is a process in place to anticipate what new standards will be required in the future and identify older standards that should be discontinued or amended. Establishing an agile and responsive cyber standards lifecycle management process is essential to address the ongoing changes associated with technology risks and avoiding obsolescence. The Cyber Security Standards Task Force should partner with SCC and CCCS to study the current process by which cyber security standards are managed and how an agile and responsive lifecycle management process can be implemented. This should include formal consultation with stakeholders to elicit feedback on existing gaps and changing risks.

   As part of this activity, a formal working group between the Task Force, SCC, and CCCS should be established to examine and plan for the standards-related challenges associated with emerging technologies. Canada's current cybersecurity policies were not designed to handle AI-driven threats, quantum decryption risks, or cloud-based services. Several key challenges must be addressed to ensure a secure digital future (please see the **appendix** for an overview of these risks).

   Further changes will emerge in the coming years, and ongoing diligence will be required to keep on top of what new standards will be required. Despite the existing measures, the rapid evolution of cyber threats necessitates an ongoing re-evaluation of existing approaches. The previous Canadian government had taken steps in this direction with the introduction of the *AI and Data Act* (*AIDA*) under Bill C-27, which sought to regulate high-impact AI systems. As the prorogation of Parliament ended this work, the government of Canada and 45th Parliament should introduce legislation to appropriately regulate AI and update privacy laws. However, more comprehensive updates will be required to address future risks.

4. **Communication and engagement:** Canada faces a cyber security skills shortage, with the demand for trained professionals far outpacing the supply of new graduates. This leaves the public and private sectors vulnerable to attack, financial loss, and operational disruption. Expanding cyber security education and training programs will be crucial to closing this gap. Cultivating a path for tomorrow's cyber experts to be part of public sector standards management is a difficult challenge, as private sector job opportunities are currently plentiful. However, by communicating the importance of cyber standards within government activities and establishing cyber-specific career progressions within government, tomorrow's cyber leaders can be increasingly recruited to join this important initiative.

   Another important activity is the strengthening of public-private collaboration. Critical infrastructure sectors—such as energy, finance, and healthcare—require better threat intelligence sharing to defend against sophisticated attacks. As cyber security standards are increasingly established, monitored, and communicated, collecting and disseminating threat data with stakeholders becomes easier. By knowing what to look for and who it impacts, cyber standards form a foundation from which a more sophisticated form of incident response can emerge.

Conclusion

Canada's cyber security future hinges on proactive adaptation to emerging threats. Key priorities include accelerating the adoption of post-quantum cryptography, refining AI governance frameworks, streamlining cloud security regulations, and investing in workforce development. However, the Government of Canada has shown that its bureaucratic coordination mechanisms are insufficient to face many of these new threats at the speed of relevance. The next five years will be critical in determining whether Canada can maintain its cyber security resilience in an increasingly complex threat landscape. By modernizing policies and bureaucratic frameworks to better address issues such as cyber security standards, foster collaboration, and embrace cutting-edge security technologies, Canada can safeguard its digital infrastructure against AI, quantum, and emerging risks. The time to act is now—before adversaries gain the upper hand.

Appendix: Emerging Technology Challenges

1. Generative AI and Deepfakes

The rise of generative AI presents both opportunities and risks for cyber security. While AI can enhance threat detection and automate security responses, it also enables sophisticated cyberattacks, including AI-generated phishing scams and deepfake impersonations. In response, the government of Canada has sought to develop new regulations to ensure transparency in AI-generated content. The previously proposed *AIDA* framework included provisions for accountability in AI deployments, particularly in high-risk sectors.

However, regulating AI without stifling innovation remains a challenge. Deepfake technology, in particular, poses a significant threat to national security, elections, and corporate fraud prevention. Future standards may require digital watermarking and authentication protocols to distinguish real from synthetic media. Enforcement will be difficult, as deepfake detection tools struggle to keep pace with rapidly improving generative AI models.

2. Quantum Computing Threats

Quantum computing, while still in its early stages, threatens to break traditional encryption methods, rendering current cybersecurity defences obsolete. Recognizing this, Canada is expected to adopt the post-quantum cryptography (PQC) standards being developed by the NIST. Transitioning to quantum-resistant encryption will be a massive undertaking, requiring updates to government, financial, and critical infrastructure systems.

The shift to PQC will be costly and complex, particularly for organizations relying on legacy systems. Additionally, Canada must coordinate with international partners to ensure compatibility with global quantum security standards. Failure to act swiftly could leave sensitive data vulnerable to future quantum-enabled cyberattacks.

3. Cloud Security and Hybrid Work Risks

The accelerated adoption of cloud computing, fueled by hybrid work models, has introduced new security challenges. While cloud providers offer robust security features, misconfigurations and unauthorized access remain major concerns. To address this, Canada is moving toward Zero Trust Architecture (ZTA), which enforces strict identity verification and least-privilege access controls.

Another critical issue is data sovereignty. Many Canadian organizations rely on U.S.-based cloud providers, raising concerns about foreign surveillance and legal jurisdiction. SSC's *Cloud Adoption Strategy* aims to promote secure cloud adoption while ensuring sensitive data remains within Canadian borders. However, vendor lock-in and shadow IT, such as employees using unauthorized cloud apps, further complicate compliance efforts.

4. Supply Chain Threats

Supply chain cyber security has emerged as a critical national security concern, with increasingly sophisticated cyber threats targeting the interconnected systems that support Canada's economy and public services. Recognizing this, the government of Canada is advancing its *Enterprise Cyber Security Strategy*—a whole-of-government approach designed to strengthen cyber resilience across departments and agencies. This includes enhancing standards for secure procurement, vendor risk management, and digital infrastructure protection.

Modernizing supply chain cyber security will be a complex and resource-intensive effort, especially for sectors dependent on legacy technologies and global suppliers. The government must also ensure alignment with international cyber security frameworks to maintain interoperability and trust in cross-border trade. Delays in implementing robust supply chain protections could expose Canada to cascading cyber incidents, threatening critical infrastructure, economic stability, and public trust.

About the Author

Alexander Rudolph Alexander Rudolph is a Ph.D. Candidate in the Department of Political Science at Carleton University and an expert on Canadian cyber policy. His research examines the grand strategy, conflict, and competition in cyberspace and how states attempt to maintain their monopoly on violence in the digital domain. He applies sociology, information security, and open-source intelligence methods to investigate the strategic thought and doctrine of cyber conflict and how it influences the creation of cyber force structures in military and intelligence organizations. He obtained his MA in Political Science at Carleton University, where he wrote his thesis on Canada's emerging offensive cyber operations posture following Strong, Secure, Engaged. His methods improve existing methods of analysis of cyber conflict by introducing hacker-informed perspectives on cyberspace and cyber conflict.

In addition to his academic work, Alex is an American-Canadian ex-pat and a frequent contributor to Canadian and international discussions on cyber conflict. He has more than 10 years of experience working for non-profits in the public education and advocacy sectors as a project manager and analyst. Recently, he has worked as a researcher and market analyst in defence consulting and presently works in Ottawa as a policy advisor and consultant.
As one of Canada's leading Canadian Armed Forces cyber defence policy researchers, Alex created **Canadian Cyber in Context**, the first newsletter dedicated to following updates and providing in-depth analysis of Canadian cyber defence.

Alec Cram is an Associate Professor of Emerging Technologies in the School of Accounting & Finance at the University of Waterloo. His research explores the behavioural and emotional responses of employees to technology-based control initiatives, namely cybersecurity and algorithmic management. Alec's work has been published in a variety of outlets, including MIS Quarterly, Information Systems Research, Journal of Management Information Systems, Journal of the Association for Information Systems, Information Systems Journal, and European Journal of Information Systems. He serves as associate editor at the Information Systems Journal and holds the J. Page R. Wadsworth Junior Chair in Accounting and Finance.

Windhya Rankothge received her PhD in Information Technology and Communication in the year 2017 from the University of Pompeu Fabra, Barcelona. Her research interests are in Cybersecurity Governance, Risk, and Compliance Engineering. Dr. Windhya has published her research work in numerous journals and conferences, and she is an IEEE Senior member. Also, she has served different international research communities as a reviewer, advisor, and executive committee member. Currently, she serves as a voting member for the IEEE MGA Awards and Recognition (ARC) Committee, a voting member (member-at-large) for the IEEE Women in Engineering (WIE) Global Committee.

Michael Davie, CD, is a cybersecurity engineer with Amazon Web Services (AWS), where he leads AWS Compliance and Security Assurance in Canada. Prior to joining AWS in 2021, he spent seven years working in cyber defence at the Communications Security Establishment (CSE) and fifteen years as a Signals Officer in the Canadian Armed Forces. Michael is a graduate of the Royal Military College of Canada, holds graduate degrees in engineering and law, and has been a licensed Professional Engineer (P.Eng.) since 2009.

Canadian Global Affairs Institute

The Canadian Global Affairs Institute focuses on the entire range of Canada's international relations in all its forms including trade investment and international capacity building. Successor to the Canadian Defence and Foreign Affairs Institute (CDFAI, which was established in 2001), the Institute works to inform Canadians about the importance of having a respected and influential voice in those parts of the globe where Canada has significant interests due to trade and investment, origins of Canada's population, geographic security (and especially security of North America in conjunction with the United States), social development, or the peace and freedom of allied nations. The Institute aims to demonstrate to Canadians the importance of comprehensive foreign, defence and trade policies which both express our values and represent our interests.

The Institute was created to bridge the gap between what Canadians need to know about Canadian international activities and what they do know. Historically Canadians have tended to look abroad out of a search for markets because Canada depends heavily on foreign trade. In the modern post-Cold War world, however, global security and stability have become the bedrocks of global commerce and the free movement of people, goods and ideas across international boundaries. Canada has striven to open the world since the 1930s and was a driving factor behind the adoption of the main structures which underpin globalization such as the International Monetary Fund, the World Bank, the World Trade Organization and emerging free trade networks connecting dozens of international economies. The Canadian Global Affairs Institute recognizes Canada's contribution to a globalized world and aims to inform Canadians about Canada's role in that process and the connection between globalization and security.

In all its activities the Institute is a charitable, non-partisan, non-advocacy organization that provides a platform for a variety of viewpoints. It is supported financially by the contributions of individuals, foundations, and corporations. Conclusions or opinions expressed in Institute publications and programs are those of the author(s) and do not necessarily reflect the views of Institute staff, fellows, directors, advisors or any individuals or organizations that provide financial support to, or collaborate with, the Institute.