POLICY BRIEF

Eastern Europe and Transatlantic Network
EETN

Impact of Digital Technologies upon Strategic Stability: Relevance to Canada

Vladimir Gorodkov

February 4, 2026

Introduction

Strategic stability is commonly understood as a condition in which no major power perceives an incentive to initiate a first nuclear strike, even during moments of acute crisis. Historically, this condition rested on mutual vulnerability and the assurance of unacceptable retaliation, reinforced by clear signalling of deterrent postures and relatively predictable patterns of crisis behaviour. During the Cold War, strategic stability was formalized through arms control and arms reduction negotiations between the United States and the Soviet Union. Over time, the concept expanded beyond bilateral nuclear deterrence to include missile defence, anti-satellite capabilities, hypersonic weapons, and mechanisms for managing escalation in crises (Bracken, 2013).

This framework is being fundamentally reshaped by the advent of digital capabilities such as cyber intrusions, artificial intelligence (AI), and quantum communications (Bolt, 2025). Unlike the relatively static assumptions of mutual vulnerability in Cold War–era stability models, this emerging digital era introduces fluid, adaptive, and opaque threat environments, compresses decision-making time, and decreases predictability through automation and machine-enabled decision processes, particularly in crisis situations involving hybrid operations and attacks on critical infrastructure.

Emerging technologies affect strategic stability in three broad and interrelated ways:

1. Digital technologies can strengthen deterrence by improving how quickly and accurately states detect threats and coordinate responses across military domains (Lloyd, 2025).

2. These technologies also make it easier to carry out low-level offensive actions, such as cyber attacks and disinformation, which lowers the threshold for confrontation and increases the risk of escalation

(Mussington, 2019).

3. Technological capacity and the protection of digital infrastructure have become central to national resilience and are now integral to a state's overall strategic posture (Baldoni, 2025).

Implications for Canada

Canada does not possess an independent nuclear strike capability. Nevertheless, as a middle power embedded in key defence and intelligence alliances such as NATO, NORAD, and the Five Eyes partnership, it plays a meaningful role within the broader architecture of collective deterrence. Canada's vast territory, extensive coastline, access to the Arctic, and significant economic and technological capacity give it strategic relevance despite its status as a non-nuclear state. As a result, strategic stability has been an enduring, if sometimes implicit, concern of Canadian defence and security policy since the end of the Second World War (Lagasse, 2008).

Canada has an opportunity to reinforce this role by investing in digital, AI, and quantum ecosystems, leveraging its geography, energy base, and education (Fitz-Gerald and Padalko, 2025). In this context, Canada must ensure its digital systems – and those of its allies with which it interoperates – are resilient, secure, and credible. If digital vulnerabilities degrade Canada's contribution or degrade allied trust, Canada's strategic posture is weakened.

In practical terms, digital technologies shape Canada's role in deterrence through alliance operations, particularly in North American defence. Cyber vulnerabilities, uncertain attack attribution, and increased reliance on automation raise the risks of miscalculation within shared systems such as command, communications, and early warning. Over-confidence in the digital sphere produces the risky escalation behaviour (Schneider, Schechter, and Shaffer, 2023). If Canadian capabilities are insufficiently resourced, equipped, or integrated, they risk weakening collective deterrence rather than reinforcing it.

These risks are most visible in Canada's North. Limited connectivity and sparse infrastructure in the Arctic are often treated as social challenges, but they directly affect early warning, command and control, satellite links, and data flows (Ahmmed, Alidadi, Zhang, Chaudry, and Yanikomeroglu 2023). Addressing these gaps is therefore not only a matter of development, but of reliability: Canada's ability to act as a willing, capable, and dependable partner in collective defence.

Many of Canada's key partners are already moving more decisively on digital technologies that shape strategic stability. NATO has formalized an updated AI strategy to accelerate AI adoption for defence and secure interoperability across Allied systems, including standards and workforce development (NATO 2024). The United States rapidly pushes forward in modernizing its cyber and AI-enabled command systems as a core component of its military posture, and the United Kingdom and France are investing in sovereign cyber, AI, and secure data infrastructures to reduce reliance on external platforms (Budnig and Wilner, 2024). Canada has taken initial steps, such as establishing a Canadian Armed Forces Cyber Command and articulating an AI strategy for defence, but defence digital modernization efforts have historically lagged in funding and capability development compared with partners (Rudolph, 2025). Without clearer prioritization of secure data infrastructure, sovereign compute capacity, and defence digital research and development (R&D), Canada risks falling behind its closest allies.

Policy Challenges and Security Risks

Cyber-attacks' low attribution certainty weakens deterrence: when states cannot confidently identify the responsible actor, it becomes more difficult to determine when and how to respond. The structural opacity of cyberspace significantly erodes the credibility and effectiveness of traditional deterrence strategies (Mussington).

For Canada, this poses a policy challenge: how to develop credible attribution frameworks (within NORAD, NATO, Five Eyes, etc.) capable of distinguishing state from non-state activity and identifying hostile actions that deliberately remain below conventional thresholds.

Digital technologies **compress decision-making time, enable fast automated actions, and raise the possibility of machine-speed escalation**. Autonomous systems and AI in nuclear delivery and command and control systems (C2) may increase risk of miscalculation (Horowitz, Scharre, and Velez-Greene, 2019).

Canada must therefore ensure that its C2 systems retain human oversight and that interoperability with allies does not inadvertently breed vulnerabilities (e.g., automated triggers, pre-delegation).

Dependence on global supply chains for digital infrastructure, cloud services, and data centers increases vulnerability to disruption, compromise, or foreign interference (Baldoni. The core policy challenge is to secure continuous and trusted access to critical technologies, whether through domestic capacity or reliable allied arrangements. Loss of assured control over command, intelligence, or data infrastructure would weaken deterrence credibility for both Canada and its partners.

Concentration of critical AI capabilities in a small number of foreign corporate ecosystems (Rohozinksi, 2025) poses a significant risk to Canada's role in maintaining strategic stability. As military planning, intelligence assessment, and national-security decision-making become increasingly dependent on proprietary platforms controlled abroad, Canada's autonomy in crisis response and cyber defence diminishes. The loss of sovereign control over essential cognitive infrastructure weakens the country's ability to verify information, ensure the integrity of digital systems, and maintain credible contributions to deterrence within alliances.

Policy Recommendations for Canada

Drawing on these implications, I recommend the following for Canada's strategic-stability posture:

1. Strengthen cyber-resilience of defence and alliance infrastructure

Canada should invest in hardening, segmenting, and stress-testing its own defence and C2 digital systems, while preserving human oversight, so that it remains a reliable and secure contributor to allied deterrence and crisis-management architectures. That includes redundant systems, frequent attack-surface audits, and adoption of Alliance-wide standards.

2. Invest in digital sovereignty and secure data-ecosystem

Canada should become a trusted hub for secure data infrastructure (especially given its geography, clean-energy base, and stable governance) and host climate-resilient digital infrastructure for NATO and other collective defence partners, such as AI-focused data centres. Policies should include support for domestic cloud and edge capabilities, supply-chain diversification, cryptographic sovereignty (post-quantum readiness), and standards for trusted allied-interoperability.

3. Pursue targeted "AI sovereignty"

Canada should focus on developing small, domain-specific AI models on secure domestic infrastructure, emphasizing niche specialization rather than competition with frontier systems (Rohozinksi). This requires investment in specialized AI defence applications, rigorous algorithm-auditing capacity, and diversified digital supply chains to reduce dependence on external platforms.

4. Develop norms for the digital domain

Canada should play a proactive role among allies in developing norms around digital operations, offensive cyber use, automation in decision-loops, and escalation-control protocols. Technology alone does not determine stability – what states make of it does (Nadibaidze and Miotto, 2023). Thus Canada should convene practical crisis panels that include digital escalation scenarios, pre-delegation boundaries, and notify and de-conflict protocols. Funding priorities could include wargaming cyber-nuclear escalation (Schneider et. al.) or assisted by AI crisis decision making simulations.

Conclusion

For Canada, digital technologies are now central to 21st century deterrence, defence, and alliance credibility. They enhance capability but also compress decision-cycles, blur attribution, and inject instability into strategic calculations. Canada therefore requires a holistic approach in adopting this new technology: strengthening cyber-resilience and digital sovereignty, shaping Allied governance of digital escalation, and investing in targeted capacities aligned with its middle-power role. By building reliable, interoperable, and sovereign AI capabilities, Canada can strengthen NATO and NORAD operations and position itself as a trusted provider of high-assurance analytical tools. In doing so, it helps shape a digital era of strategic stability that supports both national interests and alliance commitments.

References

Ahmmed, T., Alidadi, A., Zhang, Z., Chaudhry, A. & Yanikomeroglu, H. (2023). The Digital Divide in Canada and the Role of LEO Satellites in Bridging the Gap. Electrical Engineering and Systems Science. https://www.researchgate.net/publication/359235314_The_Digital_Divide_in_Canada_and_the_Role_of_LEO_Satellites_in_Bridging_the_Gap (Accessed Jan 30, 2026)

Baldoni, R. & Luna, G. D. (2025). Sovereignty in the Digital Era: The Quest for Continuous Access to Dependable Technological Capabilities. IEEE Security & Privacy, 23(1), 91–96. https://ieeexplore.ieee.org/document/10871167/ (Accessed Jan 30, 2026)

Bolt, P.J. (2025). Strategic stability in a new era. Frontiers in Political Science, 2025-01, Vol.6. https://www.researchgate.net/publication/387703616_Strategic_stability_in_a_new_era

Bracken, P. J. (2013). The second nuclear age: strategy, danger, and the new power politics. New York: St. Martin's Griffin. ISBN: 9780805094305.

Budning K. & Wilner A. (2025). Synthetic Environment in Canada's Defence Future. Canadian Global Affairs Institute. https://www.cgai.ca/th_pp_synthetic_environment (Accessed Jan 30, 2026)

Fitz-Gerald, A. & Padalko, H. (2025). Canada's Opportunity to Redefine Its Defence, and Its Value to Allies. Centre for International Governance Innovation. https://www.cigionline.org/articles/canadas-opportunity-to-redefine-its-defence-and-its-value-to-allies/ (Accessed Jan 30, 2026)

Horowitz, M.C., Scharre, P., Velez-Green, A. (2019). A Stable Nuclear Future? The Impact of Autonomous Systems and Artificial Intelligence. https://arxiv.org/abs/1912.05291 (Accessed Jan 30, 2026)

Lagasse, P. (2008). Canada, Strategic Defence, and Strategic Stability: A Retrospective and Look Ahead. International Journal (Toronto), 63(4), 917–937. https://www.jstor.org/stable/40204429

Lloyd, R. (2025). Empowering Defence in the Digital Age. The Canadian Global Affairs Institute. https://www.cgai.ca/th_pp_empowering_defence_in_the_digital_age (Accessed Jan 30, 2026)

Mussington, D. (2019). Strategic Stability, Cyber Operations and International Security. Centre for International Governance Innovation. https://www.cgai.ca/th_pp_empowering_defence_in_the_digital_age (Accessed Jan 30, 2026)

Nadibaidze, A., & Miotto, N. (2023). The Impact of AI on Strategic Stability is What States Make of It: Comparing US and Russian Discourses. Journal for Peace and Nuclear Disarmament, 6(1), 47–67. https://www.tandfonline.com/doi/full/10.1080/25751654.2023.2205552

NATO. (2024). Summary of NATO's revised Artificial Intelligence (AI) strategy. https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2024/07/10/summary-of-natos-revised-artificial-intelligence-ai-strategy (Accessed Jan 30, 2026)

Rohozinski, R. (2025). Who Controls the AI Future? SecDev Flashnote. https://flashnote.secdev.com/p/who-controls-the-ai-future?r=2b0v1b&utm_campaign=post&utm_medium=web&showWelcomeOnShare=true&triedRedirect=true (Accessed Jan 30, 2026)

Rudolph A. (2025). New Canadian Defence Investments: What's the Impact on Cyber? Canadian Cyber in Context. https://www.cyberincontext.ca/p/new-canadian-defence-investments (Accessed Jan 30, 2026)

Schneider, J., Schechter, B. & Shaffer, R. (2023). Hacking Nuclear Stability: Wargaming Technology, Uncertainty, and Escalation. International Organization, 77 (3):633-67. DOI:10.1017/S0020818323000115