Destructive Technologies and the Future of North American Continental Defence

15 NOVEMBER 2026

Sevastiana Roumelioti



Drone

1. Introduction

North America has long treated geography as a defensive asset since oceans, the Arctic and the size of the continent gave Canada, Mexico and the United States a margin of warning that few regions enjoyed. Emerging technologies are eroding that margin as they compress warning time, blur the line between conventional and nuclear operations and let an adversary reach critical systems without crossing a border in any traditional sense. This article asks how four technology sectors, namely artificial intelligence (AI) and autonomy, cyber-physical attack tools, precision counterforce and hy-

personic delivery and space-based systems, reshape the logic of continental defence and which policy choices would keep deterrence stable rather than brittle.

The analysis uses the strategic and stability framework of Sechser et al. (2019, p. 728-729), which separates peacetime stability (no incentive to race), crisis stability (no incentive to who strikes first) and wartime stability (no incentive to escalate within an ongoing conflict). *"Destructive"* and *"disruptive"* are used here in a functional sense. They are mentioned as a technology that qualifies when it shifts one of these three incentives, not because it is new. Because the most developed scholarship concerns NORAD and the Canada-United States relationship, the discussion centres on that bilateral core while Mexico's border security role and the Arctic as a stand-alone theatre are treated only indirectly and deserve separate study.

2. The Changing Threat Landscape

2.1 Artificial intelligence, autonomy, counterforce and delivery

Horowitz (2018, p. 36-57) argues that narrow AI is best understood as an enabling technology rather than a single weapon, so its effect on the balance of power depends on how effectively militaries integrate it. For continental defence the most relevant consequence is speed. Horowitz (2019, p. 764-788) shows that two features of lethal autonomous weapon systems, faster operational tempo and reduced human control, can feed arms races, weaken crisis stability and raise escalation risk once fighting begins. Altmann and Sauer (2017, p. 128-129) describe a related *"flash war"* dynamic in which interacting autonomous systems produce unplanned escalation faster than humans can intervene. Where warning times for hypersonic weapons are already short, machine speed sensing and engagement are attractive precisely because human decision windows are narrow and that attraction is the source of the risk. Johnson (2022, p. 439-477) extends the concern from tactical autonomy to strategic decision support. He argues that AI tools that displace human critical thinking, empathy and intuition become destabilizing if planners treat them as a remedy for human cognitive limits. For a binational command whose core function is to assess warning and recommend responses, the implication is that automation should shorten the path from detection to human decision rather than replace the decision.

Lieber and Press (2017, p. 9-49) contend that improvements in sensing, computing and precision have opened new possibilities for disarming strikes against nuclear arsenals once considered secure. If any party comes to believe that its forces or warning networks are vulnerable, incentives to strike first, or to use forces early, increase. Hypersonic glide vehicles sharpen this worry because their speed and maneuverability compress decision time and complicate tracking. Williams (2019, p. 789-813) analyses

scenarios for limiting hypersonic glide vehicles through asymmetric arms control, which indicates that the problem is recognized as one for negotiated restraint as well as defensive investment.

2.2 The capability/vulnerability paradox and near-peer and non-state dynamics

Schneider (2019, p. 841-863) offers a unifying idea. *States that invest heavily in a revolutionary technology gain relative power* but also become dependent on it and that dependence creates exploitable vulnerabilities and first-strike incentives on both sides. The incentive is strongest when dependence is high and adversaries can degrade the resource. North America's reliance on networked sensors, satellites and digital command systems arguably fits this pattern closely. The same architecture that makes continental defence more capable also creates attractive targets.

The literature reviewed here is written primarily around great power competition, above all with China and Russia. Talmadge (2017, p. 50-92), for example, assesses the risk of Chinese nuclear escalation in a conventional war with the United States. Non-state actors matter mainly as a second-order concern of cyber and autonomous tools lower the cost of harming infrastructure but the same organizational barriers that limit state operators also constrain them (Lindsay, 2013, p. 365-404; Slayton, 2017, p. 72-109). This article treats great power dynamics as the principal driver of continental risk.

3. North American Security Architecture

3.1 NORAD as a shared good

NORAD, in place since the late 1950s (Solomon & Fetterly, 2024, p. 542-556), is among the oldest bi-national defence arrangements in the world yet its economics have received little systematic study (Solomon, 2024, p. 521-526). That gap matters because modernization is a resource question as much as a technical one. The defence economics literature applies the joint product model of alliances. Allies jointly produce outputs that are partly public, benefiting everyone and partly private, benefiting one member and visible private benefits weaken the incentive to free ride (Berkok & Secrieru, 2024, p. 577-600). Berkok et al. (2024, p. 527-541) address a prior measurement problem of how to distinguish defence inputs within an alliance whose outputs are public goods only in part.

3.2 Burden sharing and modernization in extended deterrence of trilateral mechanisms

Solomon and Fetterly (2024, p. 542-556) quantify *burden sharing* between Canada and the United States using disaggregated spending on capital, labour and research and development and they compare Canada with its

Arctic Council peers. Their work frames the exploitation hypothesis, the claim that the larger ally bears a disproportionate share, as an empirical question rather than a political slogan. Berkok and Secrieru (2024, p. 577-600) add that modernization could yield sizable private economic benefits for Canada, including technology transfers and domestically produced inputs from sectors where Canada has a comparative advantage. If disruptive technologies raise the price of warning and defence, then the partner that captures industrial and technological benefits has a stronger reason to invest, while a partner that captures none has a stronger reason to hold back shaping alliance cohesion, not only capability.

Mehta (2021, p. 958-982) examines how emerging technologies affect extended deterrence and assurance. Canada and, in a different way, Mexico depend on U.S. capabilities for their security since technologies that alter the credibility of U.S. deterrence or the confidence of its partners therefore matter for continental defence, even when no attack occurs. The scholars reviewed for this article gives Mexico far less attention than Canada and that imbalance is itself a finding. **Trilateral coordination is thin relative to the bilateral NORAD relationship.** The recommendations in Section 6 therefore propose extending cooperation where Mexico's interests are clearest, in the resilience of shared infrastructure, rather than assuming symmetric defence institutions.

4. Case Studies

4.1 Cyber-physical threats to critical infrastructure

Energy grids and financial systems in North America are interconnected across borders and much of the relevant infrastructure is privately operated. Two influential analyses of the **Stuxnet operation**, the best documented case of a cyberattack causing physical damage.

Slayton (2017, p. 72-109) argues that the cyber offense-defence balance can be assessed only with respect to specific organizational skills and technologies. Offensive success, in her account, results mainly from poor defensive management and from the simpler goals of offense and it can be very costly to exert precise physical effects with cyber weapons. Her cost-benefit analysis of Stuxnet suggests the operation likely cost the offense much more than the defence. Lindsay (2013, p. 365-404) reaches a compatible conclusion of the complexity of weaponisation makes cyber offense less easy and defence more feasible, than commonly assumed and cyber options are most attractive when deterrence is intact. Stuxnet's payload was coded to target one specific control system (Lindsay, 2013, p. 388), which limited its reuse, yet the case also demonstrated that a cyberattack can cause kinetic damage (Lindsay, 2013, p. 402).

The implication for North America is twofold. First, *physical effects on infrastructure* demand well-resourced operators, which points toward state-

level adversaries and away from casual threats. Second, because success depends heavily on defensive management (Slayton, 2017, p. 72-109), *investment in operator skill and organizational resilience* is likely to pay higher returns than reliance on deterrence alone. Schneider's (2019, p. 841-863) argument adds a caution for the more the continent relies on digital systems for defence, the more tempting their disruption becomes in a crisis.

4.2 Space-based early warning and entanglement

Acton (2018, p. 56-99) shows that command, control, communications and intelligence (C4ISR) assets serving both nuclear and conventional missions are *"entangled."* Attacks on such assets in a conventional conflict, including assets located far from the theatre of operations, could be read as preparation for nuclear use. He identifies three escalation mechanisms: misinterpreted warning, a damage-limitation window and crisis instability. Talmadge (2017, p. 50-92) applies related logic to the risk of Chinese nuclear escalation in a conventional war with the United States.

Wilson and Rumbaugh (2024, p. 64-91) document a partial reversal of this entanglement in space. Between 2017 and 2019 the U.S. Air Force made decisions that separated nuclear from non-nuclear spacecraft and the authors conclude this outcome resulted less from a strategic choice than from acquisition reforms and bureaucratic dynamics. The broader lesson for NORAD is that architectural decisions taken for cost or programmatic reasons carry strategic consequences. Because the command relies on warning and assessment networks that cross the nuclear conventional divide, the design of those networks is a strategic decision even when it is not made as one. It follows that modernisation choices should be reviewed explicitly for their entanglement effects.

4.3 Arms control and oversight of institutional gaps

Traditional arms control counts discrete, verifiable objects such as launchers and warheads while software, autonomy and dual-use sensors resist that logic. Williams (2019, p. 789-813) shows that limits are conceivable for at least one category, hypersonic glide vehicles but that they would have to be asymmetric and technology specific. Sechser et al. (2019, p. 727-735) observe that emerging technologies affect peacetime, crisis and wartime stability differently, which implies that no single instrument will cover them. Talmadge (2019, p. 864-887) draws on Cold War evidence to ask whether technologies such as cyber, precision, stealth and remote sensing will drive escalation in future wars, a question that frameworks have yet to answer with confidence. **The governance gap lies less in the absence of rules than in the mismatch between slow, treaty-based processes and dual-use, software-defined capabilities.** Plus, both Horowitz (2019, p. 764-788) and Altmann and Sauer (2017, p. 117-142) both stress that speed and reduced human control are the features to regulate, not particular platforms.

5. Strategic Implications

5.1 Deterrence stability versus escalation economic and alliance risk

The literature converges on a common pattern of technologies that improve individual capability often reduce collective stability. Lieber and Press (2017, p. 9-49) describe capabilities that make disarming strikes more feasible. Schneider (2019, p. 841-863) explains why dependence on those capabilities creates first-strike incentives. Acton (2018, p. 56-99) shows how conventional operations can trigger nuclear fears while Horowitz (2019, p. 764-788) and Johnson (2022, p. 439-477) add speed and automation as amplifiers. The cyber cases pull the other way. Slayton (2017, p. 72-109) and Lindsay (2013, p. 365-404) suggest that some threats are more manageable than headlines imply. The overall picture is, therefore, mixed, not uniformly alarming and, it is important to mention that, policy should be targeted at the specific mechanisms, namely entanglement, speed and dependence, that the evidence supports.

Alliance cohesion depends partly on perceived fairness. Solomon and Fetterly (2024, p. 542-556) and Berkok and Secrieru (2024, p. 577-600) show that the seesaw of burden -benefit can be measured, which makes cohesion partly a matter of transparency. Mehta (2021, p. 958-982) adds that assurance, not only deterrence, is at stake when technologies change the perceived reliability of the larger partner.

6. Policy Recommendations

6.1 Short-term priorities

The short-term priorities of the recommendations should include to keep humans in the decision loop at warning and assessment loop. Even if automation should accelerate the detection and tracking, *the decisions with escalatory consequences should remain human* (Horowitz, 2019, p. 764-788; Johnson, 2022, p. 439-477). Secondly, *the establishment of bilateral incident-management protocols* for autonomous systems hare procedures that reduce the chance that interacting systems escalate an incident before humans can intervene (Altmann & Sauer, 2017, p. 128-129). Thirdly, with the investment in operator level cyber resilience, offensive success depends on defensive management, funding for skills and organizational practice at infrastructure operators should be treated as *defence spending* (Slayton, 2017, p. 72-109). Lastly, it is important to *publish burden-sharing metrics* for NORAD since disaggregated, transparent measures would replace slogans with evidence (Solomon & Fetterly, 2024, p. 542-556).

6.2 Medium- to long-term adjustments

On the other hand, as far as medium- and long-term changes apply the *review of modernization for entanglement* of very major decision affecting warning, communications, or space assets should include an assessment of nuclear conventional entanglement (Acton, 2018, p. 56-99; Wilson & Rumbaugh, 2024, p. 64-91). Moreover, the pursue of technology-specific arms control and hypersonic glide vehicles which are most *developed candidate* (Williams, 2019, p. 789-813). Lastly, design industrial policy to share benefits of technology transfer and domestic-content opportunities that *can sustain investment on both sides*, provided interoperability standards are protected (Berkok & Secrieru, 2024, p. 577-600).

6.3 Enhanced regional coordination

A trilateral track focused on shared infrastructure resilience, in energy and financial systems, would draw **Mexico** into continental security where its interests are clearest and where the cyber literature suggests defensive investment pays off (Slayton, 2017, p. 72-109). In parallel, the **United States** and **Canada** should treat NORAD modernization as an *alliance-management exercise* as well as a capability program, given the assurance concerns raised by Mehta (2021, p. 958-982).

6.4 Limitations and Directions for Future Research

Three limits qualify the argument. *First*, the analysis centers on the Canada–United States relationship because that is where the research is most developed. Even Solomon (2024, p. 521-526) notes that even NORAD's economics have received little systematic study and the literature reviewed here gives Mexico far less attention than Canada. The Arctic as a stand alone theater of operations is likewise treated only indirectly.

Second, the sources are written mainly around great-power competition. Lindsay (2013, p. 365-404) and Slayton (2017, p. 72-109) suggest that organizational barriers constrain non-state actors as well as states, which supports treating them as a second tear concern. That conclusion rests on a small number of cases, however and Stuxnet remains the best-documented example of a cyberattack causing physical damage. Whether cheaper autonomous and cyber tools will change that balance is an empirical question that the present evidence cannot settle.

Third, several of the article's policy proposals depend on assumptions that are still untested. The claim that industrial benefits sustain alliance investment (Berkok & Secrieru, 2024, p. 577-600) has not been weighed against the risk that sovereign technology development erodes shared standards. Similarly, Wilson and Rumbaugh (2024, p. 64-91) show that the separation of nuclear and non-nuclear spacecraft followed from acquisition reforms rather than strategy, so it is unclear whether a deliberate entanglement review would survive ordinary bureaucratic pressures. Research that

follows actual modernization decisions, rather than modeling them, would be the most useful next step.

Finally, assurance deserves more attention. Even Mehta (2021, p. 958-982) shows that technologies can alter partners' confidence in extended deterrence even when no attack occurs yet the literature reviewed offers little evidence on how Canadian or Mexican perceive that change.

7. Conclusion

Emerging technologies do not make North America uniformly less secure; they make certain mechanisms more dangerous. Speed and reduced human control **threaten crisis stability** (Horowitz, 2019, p. 764-788). Entanglement of warning networks **threatens wartime stability** (Acton, 2018, p. 56-99) while dependence on digital architecture creates first-strike incentives (Schneider, 2019, p. 841-863). Against these risks stand findings that **cyber operations against infrastructure** are harder than often assumed (Lindsay, 2013, p. 365-404; Slayton, 2017, p. 72-109) and that alliance economics can **be measured and managed** (Solomon & Fetterly, 2024, p. 542-556). The practical task for the three states is to target policy at the specific mechanisms of instability, so we can *preserve* human judgment, *review* architecture for entanglement, *invest* in resilience band keep the alliance's burdens and benefits visible.

Bibliography

Acton, J. M. (2018). Escalation through entanglement: How the vulnerability of command-and-control systems raises the risks of an inadvertent nuclear war. *International Security, 43*(1), 56-99. https://doi.org/10.1162/isec_a_00320

Altmann, J., & Sauer, F. (2017). Autonomous weapon systems and strategic stability. *Survival, 59*(5), 117-142. https://doi.org/10.1080/00396338.2017.1375263

Berkok, U. G., & Secrieru, O. (2024). NORAD modernization: Private benefits to Canada. *Defence and Peace Economics, 35*(5), 577-600. https://doi.org/10.1080/10242694.2023.2228565

Berkok, U. G., Secrieru, O., & Lee, K. P. (2024). On distinguishing defence inputs in an alliance – The case of NORAD. *Defence and Peace Economics, 35*(5), 527-541. https://doi.org/10.1080/10242694.2023.2209772

Horowitz, M. C. (2018). Artificial intelligence, international competition, and the balance of power. *Texas National Security Review, 1*(3), 36-57. https://doi.org/10.15781/T2639KP49

Horowitz, M. C. (2019). When speed kills: Lethal autonomous weapon systems, deterrence and stability. *Journal of Strategic Studies, 42*(6), 764-788. https://doi.org/10.1080/01402390.2019.1621174

Johnson, J. (2022). Delegating strategic decision-making to machines: Dr. Strangelove redux? *Journal of Strategic Studies, 45*(3), 439-477. https://doi.org/10.1080/01402390.2020.1759038

Lieber, K. A., & Press, D. G. (2017). The new era of counterforce: Technological change and the future of nuclear deterrence. *International Security, 41*(4), 9-49. https://doi.org/10.1162/ISEC_a_00273

Lindsay, J. R. (2013). Stuxnet and the limits of cyber warfare. *Security Studies, 22*(3), 365-404. https://doi.org/10.1080/09636412.2013.816122

Mehta, R. N. (2021). Extended deterrence and assurance in an emerging technology environment. *Journal of Strategic Studies, 44*(7), 958-982. https://doi.org/10.1080/01402390.2019.1621173

Schneider, J. (2019). The capability/vulnerability paradox and military revolutions: Implications for computing, cyber, and the onset of war. *Journal of Strategic Studies, 42*(6), 841-863. https://doi.org/10.1080/01402390.2019.1627209

Sechser, T. S., Narang, N., & Talmadge, C. (2019). Emerging technologies and strategic stability in peacetime, crisis, and war. *Journal of Strategic Studies, 42*(6), 727-735. https://doi.org/10.1080/01402390.2019.1626725

Slayton, R. (2017). What is the cyber offense-defence balance? Conceptions, causes, and assessment. *International Security, 41*(3), 72-109. https://doi.org/10.1162/ISEC_a_00267

Solomon, B. (2024). The political economy of NORAD. *Defence and Peace Economics, 35*(5), 521-526. https://doi.org/10.1080/10242694.2024.2349888

Solomon, B., & Fetterly, R. (2024). Canada and the NORAD: Economics and burden sharing. *Defence and Peace Economics, 35*(5), 542-556. https://doi.org/10.1080/10242694.2023.2232974

Talmadge, C. (2017). Would China go nuclear? Assessing the risk of Chinese nuclear escalation in a conventional war with the United States. *International Security, 41*(4), 50-92. https://doi.org/10.1162/ISEC_a_00274

Talmadge, C. (2019). Emerging technology and intra-war escalation risks: Evidence from the Cold War, implications for today. *Journal of Strategic Studies, 42*(6), 864-887. https://doi.org/10.1080/01402390.2019.1631811

Williams, H. (2019). Asymmetric arms control and strategic stability: Scenarios for limiting hypersonic glide vehicles. *Journal of Strategic Studies, 42*(6), 789-813. https://doi.org/10.1080/01402390.2019.1627521

Wilson, R. S., & Rumbaugh, R. (2024). Reversal of nuclear-conventional entanglement in outer space. *Journal of Strategic Studies, 47*(1), 64-91. https://doi.org/10.1080/01402390.2023.2249622