The Many Shades of Canadian Deterrence

by Alex Wilner
August 2022
POLICY PERSPECTIVE

THE MANY SHADES OF CANADIAN DETERRENCE

by Alex Wilner

August 2022
Deterrence is experiencing a renaissance. Russia’s war against Ukraine has jolted NATO out of its decades-long stupor. China’s diplomatic, economic and military prodding of the Pacific region, along with its advancements in emerging and disruptive technologies in hypersonic weapons, artificial intelligence (AI) and robotic platforms, has renewed talk of great-power competition and a global arms race. The nuclear weapons taboo is dissolving, with even pacifist nations like Japan exploring their use and utility. And the risk of crisis and conflict in space and cyber-space have led to calls to extend deterrence to these emerging domains of warfare. Some observers conclude that we’re in the midst of a Cold War redux.

The attention placed on deterrence is welcome. When done right, deterrence entails an absence of conflict. In practice, it rests on using a combination of threats, like the sting of retaliation and/or the hindrance of defence and denial, to convince an adversary to forgo an unwanted action. Related concepts like compellence and coercion can influence an adversary in other ways, too, including through the promise of incentives, the pain of economic exclusion and the reputational cost of delegitimization.

Drawing deterrence parallels between today and the Cold War is tempting. After all, the West won that conflict without engaging directly with its primary adversary, the Soviet Union, for nearly 50 years. Deterrence played a large part in our eventual success.

However, brushing off Cold War deterrence concepts for renewed application to contemporary conflict will only get us so far. Deterrence theory and practice have evolved a great deal since then. Some of the dynamics currently in play, including, cyber- and grey-zone conflict and the nexus between emerging technologies and coercion weren’t evident during the Cold War. But even the challenges that did exist then and continue apace today, like nuclear proliferation, information warfare and conflict in outer space, have evolved in ways that warrant a more modern approach to deterrence. The sum of these developments is that deterrence theory and practice have progressed in dramatic ways over the past several decades. Scholars have advanced novel deterrence concepts, theories and frameworks beyond the traditional notion of kinetic punishment, military retaliation and strategic weapons, including in areas like denial, delegitimization and resilience. Innovations in cross-domain deterrence, which bridges the digital-physical divide, along with lessons for managing international relations drawn from criminal deterrence and deterring terrorism and insurgency, have likewise been made.

Where does this leave Canada? Strong, Secure, Engaged (2017), Canada’s defence policy, identified the “re-emergence of deterrence” as a cornerstone of Canada’s ability to shape international engagements across the domains of conflict. Now, in the midst of a major review of Canadian national defence and security, cyber-security, infrastructure protection and foreign affairs, we have an opportunity to better put the logic of contemporary deterrence into practice.
While Canada has some of the pieces and tools already in place to advance its contemporary coercive goals, we should also think bigger, more broadly and more creatively about the types of military and non-military capabilities, strategies and relationships we need to research, develop, build and apply to extend our deterrence more concretely within and beyond the backdrop of renewed great-power competition.

Six contemporary domains of deterrence – nuclear, conventional, space, cyber, information environment and emerging technology – are explored in greater detail below.

**Nuclear Deterrence**

A re-think of nuclear deterrence and policy is justified. For starters, “nuclear” appears only a dozen times in SSE, often tucked into CBRN, a misnomer derived from the post-9/11 world that falsely lumped chemical, biological, radiological and nuclear weapons together. Given Russia’s nuclear **sabre-rattling**, the lessons Ukraine and others are learning about the consequences of forgoing (or returning) nuclear weapons, China’s nuclear **expansion**, ongoing weapons programs in North Korea and Iran and given the risk that proliferation will spread to other countries, like **Saudi Arabia** or **Taiwan**, Canada should again treat nuclear deterrence as its own phenomenon.

To this end, Canadian nuclear deterrence will stem from Ottawa’s foreign relations. As in the Cold War, the American nuclear umbrella, effectively provided twice under both NATO and **NORAD**, will suffice to provide Canada with a viable nuclear deterrent in the (very) unlikely event it is needed.

Ensuring Washington’s nuclear guarantee continues well into the future and in line with Canadian national interests and sovereign control, however, will require that Ottawa catch up to and **work more closely with the U.S.** on modernizing NORAD. Canada’s newly unveiled **NORAD Modernization Plan** provides a good starting point, promising both much-needed funding and political attention. In terms of deterring both conventional and nuclear threats, two parts of Canada’s plan – “detection” and “technology-enabled decision making” – should be more closely aligned with coercion and deterrence.

In the first case, Canada’s stated objective is to provide “significant investments” in new capabilities better able to detect threats to North America, including through improved early warning radar, space-based surveillance and next-generation sensors. The chief purpose is to enhance “our knowledge of the situation and allow Canada to be notified sooner and more accurately” of inbound threats. But a secondary deterrent objective presents itself. Demonstrating these new detection capabilities (without revealing sensitive technology) may give adversaries extra pause. Simply possessing detection capabilities isn’t usually enough to deter unwanted action: adversaries need to better appreciate these capabilities and understand the difficulty they will have in conducting certain activities. Accordingly, as these new capabilities are constructed, Canada (with the U.S.) should explore how best to communicate their possession using a
combination of open technical tests, tailored speeches and reports and joint displays of technological prowess. Ambiguity won’t easily serve Canada’s deterrent objective.

In the second case, Canada’s plan for NORAD includes leveraging technology, like AI, to increase the speed of our response, by providing decision-makers with a faster, more comprehensive understanding of information and data collected from all-domain sensors. From a nuclear and conventional deterrent perspective, emphasis should be placed on jointly establishing the connected battlespace (CB, also referred to as joint all-domain command and control). CB is an emerging framework that aims to enable “pan-domain connectivity and awareness” between various military assets,” achieve greater control and co-ordination by leveraging several technologies like low Earth-orbit satellites, unbeauteous sensors, cloud computing and AI, and “collect, process, and disseminate large quantities of data in real time” allowing decision-makers to “respond to threats faster ... than their adversaries.” CB enables deterrence, including of the nuclear variety. Once a bilateral CB framework is fleshed out, developed and built, the connected battlespace should be able to address Canada’s emerging nuclear deterrence challenges, including those related to advancements in hypersonic missile technology, improvements in missile defence and greater physical access to the Arctic.

**Conventional Deterrence**

Conventional conflict, for the purposes of this article, refers to military engagements short of nuclear conflict but excluding cyber-attacks and disinformation campaigns. Conventional deterrence entails dissuading a would-be attacker from conducting an unwanted military engagement.

During the Cold War, the importance of nuclear deterrence long overshadowed conventional deterrence. Today, however, with the nuclear hangover largely lifted, new and innovative frameworks for conventional deterrence are being explored. The war in Ukraine provides ample examples of its complexity. In the months leading up to Russia’s initial onslaught, the U.S. and its allies tried to deter Russia’s invasion altogether, with a range of economic, diplomatic and military threats and by promising to assist Ukraine in repelling Russian forces. Unfazed, President Vladimir Putin invaded anyway. More time and much research are needed to understand what the West might have done better to deter hostilities, but the fact that Putin felt comfortable upending the global order by launching Europe’s greatest war in generations “suggests a deterrence failure of epic proportions.”

And yet, even in failure the war holds other lessons for contemporary conventional deterrence, compellence and coercion. Today, in Ukraine, we’re witnessing the early effects of an active deterrence-by-denial campaign. Deterrence works by weighing on an adversary’s cost-benefit calculus: adding costs, in the form of retaliation, can tip the scales towards deterrence, just as stripping away the benefits, by way of effective defence, can too. In Ukraine, the former process didn’t pan out, but the latter still might. The process is an example of intra-war deterrence – coercion that takes place within, rather than before, a conflict. By supporting Ukraine with
immense quantities of lethal aid, including sophisticated weapons systems and diplomatic and financial support, the West is attempting to deny Russia the victory it expected and still badly needs. Every minute Ukrainians continue to fight costs Putin. The coercive objective is to convince Russia that the cost of continuing the war outweighs the benefits. We want to compel Putin to consider and accept a ceasefire, and to think twice next time he contemplates launching a war of aggression.

The future of conventional deterrence may well centre on denying adversaries the fruits of their labour. Like conventional deterrence, the logic of denial was largely ignored during the Cold War as a result of a conceptual focus on nuclear weapons, whose effect could not be credibly denied. "Deterrence by Denial," the 2021 book I co-edited with Andreas Wenger, finds that “new conceptual ground long dormant during the Cold War is being uncovered, leading to new proposals of and discoveries in deterrence by denial.” Today, we are at the rising dawn of deterrence by denial.

This may be especially relevant in scenarios in which great powers threaten weaker states. While history is replete with examples of the weak compelling the strong to accept a loss and cease a military engagement, the difference today is that this approach might be used in advance of a conflict to deter hostilities altogether. Ukraine is making itself impossible to swallow. Taking note, Taiwan, with U.S. prodding, is adopting a “porcupine” strategy against China, threatening it with failure in the hopes of deterring an invasion. Not to be outdone, China is applying the strategy, too, denying the U.S. and its allies easy access to the western Pacific. And Iran, pointing towards U.S. difficulties in Iraq, Syria and Afghanistan, is attempting something similar to stave off Israeli and American plans to halt its nuclear weapons program.

In response to these trends, Canada needs to add more denial to its coercive mix. For the moment, the process rests in the realm of ideas and conceptual innovation. DND, DRDC, CAF, defence-minded academics and others need to simply think about contemporary denial within the context of Canadian national defence policy. What technology or equipment currently in hand might Canada uniquely leverage to deny adversaries the fruits of their labour, as we are doing today in Ukraine? Flipping the equation around, how might we undermine and circumvent an adversary’s use of denial against us, as we are currently attempting vis-à-vis China? Conceptual innovation should help identify next steps, including by highlighting the R&D and procurement mechanisms Canada might develop next to build and secure dual-purpose tools, useful both for projecting power and denying adversaries. Finally, Canada might consider developing new alliance partnerships, in concert with traditional allies, to reinforce and signal our determination to defend like-minded democracies against aggression, uphold the rules-based order and deny adversaries their strategic and tactical objectives. To this end, Japan should be Canada’s first stop. Not only is it already a longstanding American ally and founding member of the Quadrilateral Security Dialogue – which includes the U.S. and Australia, another Canadian ally – but Japan will also figure prominently in any future allied engagement meant to deny China its regional and global ambitions. Canada and Japan have strong diplomatic relations and robust trade agreements; a military nexus should be explored next.
Cyber-Deterrence

Effectively deterring adversaries in cyber-space remains a major hurdle. The difficulty pivots on three core elements: the intent and resolve to punish adversaries for their aggression, inside and beyond cyber-space; the credible capability to do so; and a communicative posture that defines cyber red lines and the costs adversaries will suffer in ignoring them. The U.S. is several years ahead of Canada in conceptualizing cyber-deterrence and building the tools and prerequisites to do so. That provides us with an advantage to learn from our ally. Importantly, the Canadian government is currently reviewing and renewing the National Cyber Security Strategy (2018). Ensuring cyber-deterrence is baked into the strategy will require that Canada pursue three avenues in tandem.

First, building cyber-deterrence intent will require that Canada develop its own national cyber-deterrence posture. Canada has never done anything like this before. In all of our past (and ongoing) conflicts, we’ve relied on our allies to provide us with coercive cover. That has worked well to date. But cyber-space is different. We might be able to leverage the power of our alliances to deter especially nefarious forms of cyber-aggression – like the widespread destruction of civilian infrastructure – but we won’t be able to do so when trying to deter lesser challenges that rest below the threshold of an allied response. Canada’s cyber-deterrence posture must speak to the specific threats we face and build off a unique blend of homegrown excellence, resources and experience. It should likewise clearly define where our deterrent red lines rest; that is, describe in broad terms the malicious cyber-activities and attacks against which we will pursue retaliatory actions. Canadian cyber red lines should look to the U.S. and U.K. for insight, carving out a Canadian approach that updates traditional notions of infrastructure protection for cyber-space.

Second, from posture we move next to capability. Unlike Cold War deterrence, cyber-deterrence isn’t exclusively about military power, punishment or retaliation. Nor must Canada’s punitive response rest solely in cyber-space. Instead, cyber-deterrence should rely on a range of capabilities that can harm challengers in both cyber- and physical space. Canada must ensure both DND and CSE have the technical capability to respond offensively to cyber-aggression, inside and outside cyber-space, when merited. Adversaries need to believe that Canada has the ability, will, legal right, normative justification and leadership to retaliate if and when needed. Beyond national defence, the RCMP and the Department of Justice can leverage the threat of prosecution; Global Affairs can add the threat of economic sanctions and public retribution, and also promote international cyber-norms by championing Canada’s position at multilateral forums. Shared Services Canada, with CSE and others, can deter attacks by denying adversaries easy access to Canadian cyber-targets. Cyber-deterrence is the sum of these parts and processes.

From posture and capability, we move finally to communication. Deterrence will only work if adversaries appreciate and understand the risks and harms they run in contemplating an attack on Canadian interests. Open and backchannel communications must be developed and used. In the U.S., declaratory deterrence policy is usually reserved for the White House. President Joe Biden’s 2021 Executive Order on Improving the Nation’s Cybersecurity, for instance, provides an updated list of considerations adversaries need to weigh when targeting the U.S. Canada should
follow suit, perhaps via Public Safety or the Privy Council Office, establishing its own approach to
coevasive communication that ties all the other elements of Canadian cyber-deterrence together.

Deterrence and the Information Environment

The nexus between coercion and the information environment (IE) is a perfect example of the
type of research currently being explored by contemporary fifth wave deterrence scholarship,
which crosses between civilian (i.e., safety) and military (i.e., security) applications and rests
“inside and outside of war.” One way to approach deterrence in the IE is through delegitimization.
The objective is to “reduce the challenger’s probability of achieving their goals by attacking the
legitimacy of the beliefs that inform their behavior.” Applying delegitimization to the IE begins by
enshrining norms of behaviour within the IE itself. Norms facilitate deterrence in two ways: by
solidifying acceptable behaviour within a domain and by establishing the bar against which
subsequent kinetic and non-kinetic threats of retaliation will be issued.

On the former, Tim Sweis and Samuel Zilincik note that norms convince “potential transgressors
not to engage” in certain acts by “presenting them with the prospect of social costs.” Canada,
through Global Affairs Canada and other departments, can cultivate delegitimization for the IE
by promoting norms with like-minded states, as it has in the past in the context of norms and
taboo against torture, the targeting of civilians, chemical weapons and other military devices
(e.g., landmines). Over time, IE norms may become passively accepted, shaping behaviour and
providing a context against which collective threats of punishment can be used to convince
transgressors against committing infractions. Challengers to these IE norms may hesitate in
pursuing certain types of behaviour because of moral clarity and conviction and/or out of fear of
international retaliation, condemnation, censure and embarrassment.

On the latter, Canada’s intelligence community, working with a range of departments and civil
society groups, could seek novel ways to punish IE violations by discrediting individuals, leaders
or groups who use IE maliciously. Emerging research has found, for instance, a “strong link”
between the IE, the strategic disclosure of intelligence and the delegitimization and deterrence of
adversaries. Ofek Riemer’s work on public disclosures and “performative use” of intelligence
shows that officials leverage the tactic to “draw global attention to violations of international
regimes and norms.” The release of sensitive information and intelligence is “yet another
instrument capable of inflicting damage on [an] opponent without using force or risking
escalation.”

The U.S. has adopted precisely this strategy during Russia’s war in Ukraine. In an extraordinary
display of public disclosure, Washington has been releasing and discussing declassified
intelligence on a near-daily basis in an attempt to pre-empt and coerce Russia. For instance, in
the lead-up to and during the early phases of hostilities, U.S. intelligence cautioned that Russian
special forces were stationed on Ukraine’s border, warned of imminent military engagement and
even suggested Russia was planning to release a fabricated video of a false flag attack and/or
surreptitiously conduct a chemical weapons attack as a pretext and justification for its war. The
goal was to leverage U.S. intelligence to delay or deter certain Russian behaviour. At other times, American and British officials released intelligence suggesting Putin was being misled by his advisors, that Russian generals were being killed in unprecedented numbers and that Russian troop morale was low. The goal here is to get inside Putin’s head, sow uncertainty, narrow his options and compel him to recalculate his positions and intentions. During a February 11, 2022, press briefing, White House national security adviser Jake Sullivan was clear about U.S. objectives in releasing and discussing sensitive intelligence: “We are trying to stop a war.”

Canadian decision-makers should take note of these developments in information warfare and coercion. GAC, DND, Public Safety, CSE and others should explore the feasibility of developing norms of engagement for the IE, and the practicality of undermining and deterring dis/misinformation campaigns with the timely public disclosure of intelligence.

**Space Deterrence**

Though space deterrence might be thought of as a subset of conventional deterrence, the subject deserves a tailored assessment given space’s unique stature as a domain of conflict. Moreover, space is in flux; it’s increasingly congested and contested. New technologies, including notably LEO satellites, new entrants to the domain, including a multitude of private companies, states and militaries, and ambitious long-term plans to (re)visit and potentially colonize the moon, Mars and other destinations, have rendered space particularly busy. From a defence perspective, as my co-authored research with Kevin Budning and Guillaume Côté exploring Canada’s embrace of novel space technologies finds, “space is used for command and control, situational awareness, surveillance, weather information, navigation, communications, mapping, and search and rescue missions.” Space is likewise critically important to Canada’s alliance commitments and facilitates other economic, environmental and political goals. Recognizing the increasingly tenuous nature of Canada’s space assets, interests and ambitions, and in keeping with similar developments in the U.S., U.K. and elsewhere, in April 2022 the Canadian Armed Forces launched the process that will eventually establish the Canadian Space Division.

Canada’s longstanding position is that conflict in outer space is detrimental to Canadian national interests. Deterrence plays an important role in safeguarding that stability. Implementing deterrence in space pivots on three elements. First, as with deterrence in cyber-space and the IE, Canada should continue working with its international partners, as outlined in SSE, on establishing an enforceable code of conduct for space activities and behaviours. Focus should be placed on solidifying global norms against causing space debris, a concern that touches all governments and militaries alike, against testing and using anti-satellite weapon systems and promoting norms of safe satellite approaches and operations.

Second, Canada must deny adversaries the ability to attack or nullify our space assets. We can do that by enhancing collective defensive space capabilities with our traditional allies as part of the U.S.-driven Combined Space Operations initiative, which calls on Canada to help counter “hostile space activities and to deter, deny, or defeat attacks or interference.” We can also unilaterally...
improve the resilience of our national space assets through improved encryption, engineering and other mitigating techniques.

Finally, most controversially, and despite the fact that doing so could interfere with our larger objective of stabilizing space, Ryder McKeown and I nonetheless find that Canada “must remain open to the possibility that it may eventually need to field counter-space capabilities for deterrence purposes.” At the very least, the topic deserves some thoughtful and strategic recognition. Focus should be placed on exploring whether and how Canadian technological capabilities in lasers, robotics, cyber and other technologies might be repurposed, if and when needed in the midst of a hot war for instance, to deter aggression against Canadian space assets. Under some scenarios, being able to harm others in space may help protect Canadian national interests.

**Deterrence and Emerging Technologies**

Deterrence theory doesn’t sit still. Neither does technology. During the Cold War, technological developments in nuclear science, aviation, space and missile defence led to the exploration of new deterrence scenarios, frameworks, concepts and strategies. Something similar is happening today, pitting a range of new, novel and still emerging technologies against all aspects of deterrence. Scholars are once again probing how the logic, theory and practice of deterrence, compellence and coercion will be influenced by technology in both the near and long term.

For instance: Will hypersonic glide vehicles and cruise missiles, which travel at incredible velocity, undermine certain elements of nuclear deterrence, including assured second-strike capabilities? Similarly, if new underwater detection technologies render the seas transparent, will submarines, including those critical to the stability of nuclear deterrence, become obsolete?

What about direct energy weapons, like lasers or microwaves? Might they provide reliable next-generation ballistic missile defence? What about the rise of sophisticated anti-rocket technology, like Iron Dome? How might either technology influence the interplay between offence and defence in both conventional and nuclear deterrence?

From the field of robotics, will swarms of small, cheap and expendable drones – deployed at sea or in the air – prove useful for precision punishment? Could drone swarms facilitate saturation tactics? What effect would this have on coercion?

From bioscience, could gene-editing techniques, like CRISPR, be used to design next-generation bio-weapons? How might the threat of boutique bio-weapons influence proliferation, and what influence might these types of WMD have on the strategic balance of power?

And from quantum physics and engineering, how might the race between quantum computing, which might undermine contemporary encryption, and cryptographic countermeasures influence national security and inform cyber-deterrence?
To its credit, part of DND’s Innovation for Defence Excellence and Security (IDEaS) program, a $1.6 billion investment in defence research and development announced in SSE, was reserved for research on the theme of “proactive deterrence.” The research cluster hits the mark, asking scholars and scientists alike to “identify novel and innovative strategies, mechanisms and enabling technologies to anticipate and deter potential international crises and war in the 21st Century.” Other IDEaS research challenges focus on tangentially related themes, including improving cyber-attribution, defending satellites and detecting hostile information activities.

IDEaS is generating novel findings on the future of deterrence. For instance, my own research on the nexus between AI and deterrence, which received two rounds of funding from IDEaS under proactive deterrence, has found that the technology risks altering deterrence and coercion in surprising ways. It might change cost-benefit calculations by diminishing the human cost, emotion and psychology of warfare. Or it might recalibrate the balance between offence and defence towards pre-emption, undoing longstanding assumptions embedded to military escalation. Or it could lead to hyper-coercion, the ability to foresee and forestall an adversary’s next move.

To be sure, these findings are inherently speculative, as any thought exercise relating emerging technology to coercion must be. But the larger point is that today’s speculation on the way technology intersects with deterrence is – with time, attention and resources – tomorrow’s novel application of coercion. DND should continue supporting Canadian research on deterrence through funding. It should do so in explicit support of NATO’s latest Strategic Concept (2022), which calls on the alliance to “promote innovation and increase our investments in emerging and disruptive technologies to retain our interoperability and military edge.” Canadian research on deterrence must likewise be provided greater opportunities to test and sandbox new deterrence concepts and frameworks, facilitating their further development and eventual deployment. The latter process will require supporting and fostering a more flexible, nimble and responsive public-industry-academic ecosystem able to bridge the divide between research, development and procurement.

Deterrence comes in various shades; the end of the Cold War expanded the palette. But now that great-power competition is back, it’s time to extend Canada’s approach to deterrence, compellence and coercion across the domains of warfare, combining older lessons with newer innovations towards the nation’s defence.
About the Author

Alex Wilner is an associate professor of international affairs at the Norman Paterson School of International Affairs (NPSIA) and the Director of the Infrastructure Protection and International Security program, Carleton University, Ottawa, Canada. His books include Deterrence by Denial: Theory and Practice (eds., Cambria Press, 2021), Deterring Rational Fanatics (University of Pennsylvania Press, 2015), and Deterring Terrorism: Theory and Practice (eds., Stanford University Press, 2012).

For more information please visit his website: https://www.alexwilner.ca/
The Canadian Global Affairs Institute focuses on the entire range of Canada’s international relations in all its forms including (in partnership with the University of Calgary’s School of Public Policy), 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.