North America's Imperative: Strengthening Deterrence by Denial

Andrea Charron
James Fergusson

In today's threat environment, adversaries can hold the continent hostage unless leaders can bolster its deterrence posture. Rather than deterrence by punishment, however, the focus of NORAD, USNORTHCOM, and the Canadian Joint Operations Command must be on deterrence by denial and increasing the costs of actions by adversaries should they pursue an attack on North America.

To ensure credible deterrence by denial, the North American Aerospace Defense Command (NORAD) and the Canada-US (CANUS) defense relationship needs modernizing. Not only do sensors need to be updated and significant expenditures made, but the entire approach to the defense of North America needs to materially change. We must rethink the domains that require defending and how deterrence by denial moves beyond the current outdated Cold War mindset that evolved in an ad hoc manner.

Beginning with General Charles H. Jacoby Jr., USA—dual-hatted as commander of United States Northern Command (USNORTHCOM) and NORAD from 2011 to 2014—and the 2013 *NORAD Next* study, successive dual-hatted commanders have raised concerns about the vulnerability of North America. A new generation of advanced strike weapons, two peer US competitors, and violent extremists seek to exploit all domains to undermine the credibility of US and allies' defenses.

Deterrence is fore of mind for security analysts, but rather than punishment and imposing a cost on adversaries in the form of nuclear annihilation, the focus is on denial and raising an adversary's costs of action. The question is, What does credible deterrence by denial look like for North America in the 2020s?

This analysis briefly examines the strategic logic underpinning the need to modernize North American defense, focusing primarily on NORAD and deterrence by denial. It is vital that structural changes to the North American deterrence posture, including necessary investments, are made to alter adversarial perceptions so that North America cannot be held hostage. Beyond the need to modernize NORAD's early warning and defense control capabilities to meet the new threat environment, both countries

must modernize NORAD—the organization—and rethink the importance of protecting the North American homeland.

The Strategic Rationale for Modernization

In the immediate post–World War II era, the United States and Canada paid significant attention to and made resource investments in North American air defense cooperation. This focus led to the creation in 1957 of a binational command—the North American Air Defense Command, which centralized operational control of continental air defenses against the threat of Soviet bombers. Attention to NORAD waned, however. The defense of North America and NORAD's contribution to that mission, especially since the end of the Cold War, have largely taken a backseat to Canadian and American strategic priorities and investments.[1]

North America has not been entirely neglected. As evidence, in the 1980s, the 1950s-era Distant Early Warning Line radar system was modernized to create the existing North Warning System (NWS)—a series of uncrewed long- and short-range radars stretching from Alaska, through Canada's Arctic, and down the East Coast.

Moreover, in the wake of 9/11, internal air radar feeds from the Federal Aviation Administration and NAVCanada were integrated with NORAD's NWS feeds to warn of approaching threats, creating a more complete air picture for the NORAD and USNORTHCOM Command and Control Center. Now, NORAD monitors the internal air picture and the (usual) air approaches to North America. Nonetheless, continental defense (Canadian parlance)/defense of the homeland (US parlance) has not been a priority. Two factors explain this situation.

First, drawing from the interwar and World II experience and the demands of the Cold War, the strategic priority of both countries continues to be overseas commitments or forward defense (the "away" game).[2] Second, beginning in the 1960s with the development and deployment of long-range intercontinental and submarine-launched ballistic missiles, with no defense possible at the time, the focus was on deterrence by punishment.

Beyond the need to have early warning of a strategic attack, a mission assigned to NORAD, defense of North America was based on the offensive threat of American strategic nuclear retaliation. Indeed, it was largely assumed that any Soviet Union attack against North America could quickly escalate into a nuclear exchange because of the deterrence by punishment logic—a defense, of sorts, for North America. Air defense was not entirely forgotten or ignored but became a secondary concern to early warning of an attack.[3] In the 1960s, the famous hardened Combat Opera-

tions Center in the Cheyenne Mountain Complex in Colorado Springs was completed to withstand a nuclear attack, and a series of radars, radar nets, and other early warning attack systems were brought online.[4]

Today, the overseas priority has not changed (consider, for example, the pivot to the Indo-Pacific), but the North American threat environment has changed significantly. Successive NORAD and USNORTHCOM commanders have raised concerns about the vulnerability of North America—emanating from Russia and China primarily—linked to a new generation of advanced strike weapons.

Most recently, the former commander of NORAD and USNORTHCOM, General Terrence J. O'Shaughnessy, USAF, and the deputy director of NORAD operations, Major General Peter M. Fesler, USAF, provided the fundamental strategic logic for significant investments in North American and NORAD defense modernization. As the American way of war has focused on large deployments overseas to project overwhelming force, the solution for adversaries "is to prevent deployment in the first place."[5] North America thus becomes a primary target and will be vulnerable to subversion and coercion as well as conventional and nuclear attacks. The requirement to raise the costs of action by adversaries against North America is paramount.

Emphasizing North America is no longer a sanctuary, O'Shaughnessy and Fesler argued a credible deterrence by denial posture is vital to support the credibility of the American strategic deterrence posture overseas. North American vulnerability may embolden China or Russia to challenge the status quo in the Asia-Pacific or European theaters, generating a major crisis and possibly war. Specifically, new strike capabilities (including hypersonic weapons) enable competitors to threaten, and, in a worst-case scenario, destroy North American military bases and embarkation points vital for reinforcing forward-deployed forces.

With few extant defensive capabilities at home to meet this threat, the willingness of the United States to stand firm in a crisis overseas would be at issue. Ensuring the capacity to detect, deter, defend, and defeat such threats to North America via denial is essential to reduce incentives for Russia and China to challenge the overseas status quo by threatening the homeland.

Of course, issues surrounding deterrence postures and credibility, both globally and for North America, are complicated and contentious in the new world of great power rivalry. Among others, the threats posed by new, dual-capable nuclear and conventional strike systems will be center stage in future debates about North American and NORAD defense modern-

ization. Nonetheless, the vital issue is to recognize and detail North American deterrence-by-denial requirements, including the need to go beyond simple resource investments to modernize the Canada-US defense relationship and NORAD's place within it.

North American Deterrence Requirements

Any evaluation of deterrence requirements must first recognize the objective is North America, not Canada or the United States separately per se. A threat to either is a threat to both. From this starting point, the current structure of the defense relationship underpinning a credible North American deterrence-by-denial posture is itself problematic. The relationship, at its strategic and operational levels, is divided in several ways with no overarching true central structure to provide unity of effort and command for North America. Part of the relationship is binational as embodied in NORAD with its functional responsibility for aerospace (air and ballistic missile) and maritime warning and aerospace control (air).[6] The remaining parts are bilateral.

Overall cooperation and coordination are implemented through the tri-command arrangement consisting of NORAD, USNORTHCOM, and Canadian Joint Operations Command (CJOC)—N2+C—established roughly a decade ago.[7] It is at best an informal command arrangement, and whether it will evolve to become a more formal, centralized North American command depends on political will.

Moreover, the N2 legs of the arrangement are devoted strictly to North America, while CJOC is responsible for all Canadian military operations, home or abroad, that do not involve NORAD or special forces. At one time, CJOC devoted most of its attention and limited resources to overseas operations. Today, due to climate change, COVID-19, and the need to provide assistance to Canadian civilian agencies, the split in terms of resources and attention is 50 percent at home and 50 percent overseas.[8]

Seams to Consider

First identified by the now defunct Binational Planning Group stood up after 9/11 to consider how best to defend North America, N2+C, along with the mixed binational and bilateral components of the North American defense relationship, have created North American command "seams" with implications for deterrence credibility. For example, while NORAD can warn of a maritime threat to North America, the US Navy and Royal Canadian Navy operate unilaterally and bilaterally and under US-

NORTHCOM and CJOC commands, respectively, with different areas of responsibility and jurisdiction. An adversary need only find the seams between CJOC and USNORTHCOM areas of responsibility, and precious response time will be lost coordinating an ad hoc, bilateral solution to fortify the command and geographic seams.

Another seam—between denial and punishment or raising versus imposing costs—is directly related to the concept of deterrence. The North American command components (N2+C) operate in the denial sphere. The United States' punishment authority and capabilities relative to North America are assigned to US Strategic Command (USSTRATCOM), another command within the US Unified Command Plan.[9] Canada has no such capability other than via its Ally status with the United States and via NATO.

Regional commands in the Unified Command Plan, including USNORTHCOM, possess both denial and punishment authority and capabilities; NORAD does not. For example, NORAD warns of an inbound ballistic missile, but the defeat decision and capability rest entirely with USNORTHCOM with no Canadian input. Therefore, Canadian personnel assigned to NORAD on the NORAD and USNORTHCOM Command and Control Center watch floor will see and warn of an attack. But then they will step aside for USNORTHCOM US personnel to decide how best to react.

Certainly, such defeat authority and capabilities could be given to NORAD as they partially once were when US Space Command (USSPACECOM) and NORAD were situated under the same commander with punishment authority. (After 9/11, USSPACECOM was separated and dissolved and its responsibilities folded into United States Strategic Command.[10]) Successive Canadian governments, most notably the Martin government in 2005, have long ceded punishment to the United States for domestic political reasons.

In terms of the US part of the deterrence equation, USNORTHCOM also confronts horizontal, geographic seams as a function of the Unified Command Plan. It shares Alaska with US Indo-Pacific Command (USINDOPACOM), and many of USNORTHCOM's capabilities are held by USINDOPACOM (fig. 1). There are three geographic combatant command seams in the Arctic approaches to North America—USNORTHCOM, USINDOPACOM, and US European Command (USEUCOM). Three geographic combatant command seams also impact North America as a whole—the Atlantic and USEUCOM, the Pacific and USINDOPACOM, and the south via US Southern Command.

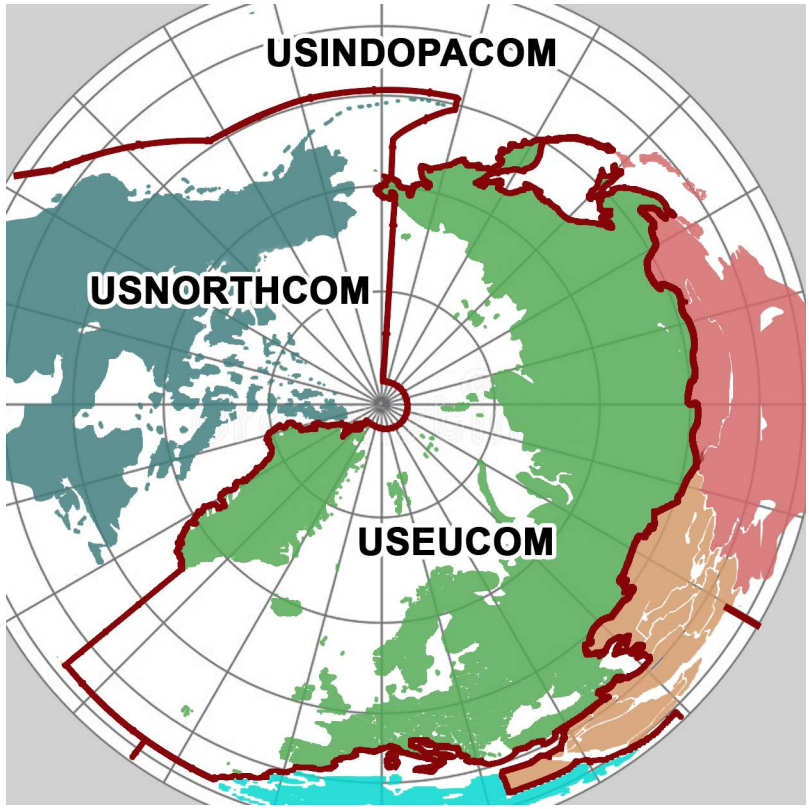

Figure 1. North America Unified Command Plan seams (courtesy of US Department of Defense)

In addition to jurisdictional, authority, and geographic seams, North American deterrence also confronts domain seams. Reflective of the military service structure, the geographic domains of air, land, maritime, and space remain conceptually and structurally separate even though these domains increasingly blur together as a function of technological change and hybrid tactics. Thus, for example, a maritime threat as a function of cruise missile technology can quickly transition into an air-breathing threat.

The United States' solution is to adopt Joint all-domain command and control (JADC2) to connect sensors from all military services—Air Force, Army, Marine Corps, Navy, and Space Force—into a single network.[11] The implications for the North American deterrence structure remain to be seen, but JADC2 implies the potential merger of punishment and denial. A long list of obstacles remains to achieve this concept within the US military, let alone the challenges involved in including the Canadian military. Ideally, some level of discussion and engagement with Canada in

JADC2 development is necessary versus the traditional approach wherein the US decides on a course of action, and Canada reacts.

Two additional domains require consideration. The first is not a traditional domain per se but involves violent extremists. Violent extremism (formerly terrorism) has significantly receded from defense and security agendas (even at a time when there is a rise of right-wing, national violent extremism as opposed to foreign and mainly radical Islamic forms of terrorism).[12] Moreover, many national security decision makers today question whether terrorists can truly be deterred.[13]

But this domain cannot be ignored, as it resides in the seam between military and civil security agencies. The other domain—cyber—has risen noticeably on the defense and security agenda and with it, the cognitive domain (think misinformation, disinformation and malinformation campaigns). In these worlds, denial and punishment are also separated—punishment in the cyber world appears to be the exclusive domain of US Cyber Command—but denial entails the military, civilian security agencies, and the private sector.

Capability Gaps

Beyond structural seams, notable capability deficiencies—gaps—are identified in several reports, including the Heritage Foundation's *2021 Index of US Military Strength*, which graded all services' capabilities as "marginal."[14] Further, the Heritage *Index*, reflective of many studies on the US military, does not consider North America: only suitability for operations in Europe, Asia, and the Middle East are assessed. United States Northern Command and NORAD employ the concepts of detection, denial, defense, and defeat. Although these elements are not necessarily understood to be linear, detection and defense are the key concepts to evaluate capability deficiencies. In this regard, a credible capacity to detect and defend equates to a credible deterrence-by-denial posture.

Detection

Detection is the first ingredient of denial credibility and is central to NORAD's mandate. The North American aerospace warning mission is essential as is its maritime warning mission. Both missions have complicated national and bilateral elements embedded in their processes, especially in the maritime domain. Three key deficiencies stand out. First, NORAD's air warning component is almost exclusively defined as syn-

onymous with the information provided by the North Warning System rather than a North American warning system.[15]

The NWS is technically obsolete; as a result and notwithstanding new artificial-intelligence-inspired additions, NORAD's air warning capability is potentially on the precipice of failing. Because of its 1970s technology and physical location, the NWS is challenged to detect long-range air- and sea-launched cruise missiles, not to mention drones that fly at speeds and altitudes not envisioned for 1970s air threats.

All relevant parties recognize these deficiencies. In response, a binational structure is in place to identify sensor solutions and requirements to move and filter large quantities of sensor data into NORAD for analysis and action (NORAD modernization). Nevertheless, there seems to be no pressing urgency to move forward. In 2017, in the joint statement released after the summit between Canadian Prime Minister Justin Trudeau and US President Donald Trump, and reiterated in the first, virtual summit with US President Joe Biden, the leadership of both countries placed North American defense and NORAD modernization among their priorities. To date, too few significant investments have occurred.[16]

Certainly, as the future North Warning System is likely to entail a complex array of ground-, air-, maritime-, and space-based sensors, technology hurdles do exist, especially in terms of systems integration. The danger lies in waiting for the final, perfect solution rather than building the system as partial solutions come online. Such a delay will leave a major detection gap for some time to come. Indicative of this trend, the current NWS radars that will reach the end of their life cycle in 2025 are already set to be extended until 2035.

Second, the future NWS/North American Warning System sensor system remains largely conceptualized as a perimeter system, looking outward from the continent (fig. 2). In the wake of 9/11, NORAD acquired an internal air picture of North America through its link to the US Federal Aviation Administration and NAVCanada radars. But it is unclear whether these internal radars possess a cruise missile detection and tracking capability and/or future improved drone-tracking technology. A perimeter system must be augmented by internal detection capabilities, in the very least as assurance should the defense side of the equation fail at the perimeter.

Figure 2. NORAD radar coverage

Third, the detection domains remain largely separate rather than integrated into an all-domain detection and thus analysis structure. While NORAD has air and ballistic missile warning functions, and with the latter, a space-tracking function as well, these appear to be largely independent, reflecting the traditional division between air and outer space. Yet, as the future North American Warning System will likely comprise a significant space-based component, threat detection against these key space-based assets is essential. Moreover, threats to these components also extend to a wide range of space-based assets vital to the military and the economy, especially in low Earth orbit.

Clearly, such threats (especially to space-based assets) are in fact threats to the North American homeland. Moreover, attacks against these assets are not just a physical attack against the territorial homeland but could involve the direct loss of life. Adversary calculations of the repercussions of their attacks on assets alone will be distinctly different from a direct threat or attack against North America. This factor does not imply NORAD should acquire a space defense mission per se; rather, NORAD's

ballistic missile warning mission should include detecting threats against space-based assets. Detecting these threats should also be part of its integrated tactical warning/attack assessment function.

In addition, the development of hypersonic weapons technology foreshadows the merger of space and air into a true "aerospace" domain. As with the maritime domain, the ballistic threat of maneuverable hypersonics may transition into a maneuverable air threat operating between space and air. That is, the space, aerospace, and air domains need to be integrated into a single detection domain, along with the maritime domain, to generate an integrated, all-domain North American common operating picture. The final geographic domain—land—is less important to include: three oceans effectively mitigate a land-invasion scenario. The cyber domain, however, is vital.

The Cyber Complication

Threats emanating from the cyber world have attracted growing attention over the last several decades. For many years, the air forces of the United States and Canada (and to a lesser degree NORAD) have made a claim on the domain, notwithstanding US Cyber Command and its unclear role in the North American deterrence equation. Regardless, central to the detection problem in the cyber domain and distinct from the other domains, attribution of a cyberattack is extremely problematic. Due to the complexities of the internet and the ability of states such as China and Russia to employ—implicitly or explicitly—private actors, it is difficult to ascertain whether any attack has been motivated just for mischief, for criminal purposes, and/or for state purposes.

Moreover, this domain is structurally more complicated than the maritime domain. It involves not only the military relative to its own systems and other government agencies but also private actors within the economic system. The overwhelming majority of cyber critical infrastructure resides in private hands within the integrated North American economy. In this regard, private business interests related to corporate viability act to some degree as disincentives to report cyberattacks.

So long as North American officials continue to emphasize cyber vulnerabilities and fear the consequences, adversaries have incentives to exploit the cyber world. Whether the attempt by Russia, as attributed, to influence the 2016 US presidential election had any real impact on its outcome is a moot question. It is the attempt itself and the fears it generated of other, potentially more devastating attacks that Russia uses to its advantage. At the core of this problem is detection and attribution.

A cyberattack occurs in near real time, usually with no warning or with such obfuscation that targets may not even realize they are under attack. In contrast, the kinetic world provides, to varying degrees, early warning signals due to advanced intelligence and surveillance capabilities. One can expect, for example, that long-standing, normal patterns of military activity will be altered in preparation for employment (e.g., mobilization of personnel and assets).

Such deviations do not necessarily mean a decision to use force has been made. In some cases, preparations may simply be a means of threat signaling to alter adversarial responses, with no intent to escalate to the use of force. Political contexts that suddenly change or evolve over time also provide signals. Regardless, in the kinetic world, the probability or fear of a bolt from the blue is less likely.

Cyberattacks and probing are, however, a world of "bolts from the shadows." As an element of deterrence, in this case by punishment, state-sponsored or directed deterrence attacks may simply be intended to demonstrate what an adversary can and might do in the future to alter calculations. In other cases, these attacks are meant to disrupt a state's ability to track and react at a later point in the decision-making process or to obfuscate an adversary's actions.

Operating at a low level of effect and thus having only a temporary, limited, and marginal impact—shutting down a website or a pipeline—the act is meant to indicate the potential to do more damage. Moreover, at least to date, these attacks are calculated as insufficient to generate a kinetic response. Furthermore, the problem of attribution and thus plausible deniability also adds complexity to the detection side of the equation. This complexity is compounded further with the potential for embedded computer viruses, such as the case of Stuxnet in Iran, that may remain undetected until triggered under certain conditions—a potential attack in the making.

Political warning signals, too, can emerge to challenge the status quo and can be generated and transmitted across the complicated North American cyber world, requiring greater vigilance. Additionally, ongoing analysis to discern potential patterns of cyberattacks over time and space may provide some modicum of prediction and thus detection. Ultimately, however, detection is exclusively in the hands of the owners of the private, public, and military networks. As a result, detection capabilities, and thus vulnerabilities, vary widely across the North American cyber world.

While one cannot expect every network in the North American cyber world to implement a common standard, and apart from the problem of

determining what critical infrastructure is and is not, critical infrastructure across North America needs to adopt a common detection standard in terms of detection software. In addition, intelligence or information sharing must be formalized across the private, public, and military divides following cyberattacks.

The state of the cyber domain in North America is reminiscent of the state of the intelligence world prior to 9/11 and of the maritime domain prior to the undertaking of significant steps in the years following those attacks. Improvements to threat detection in the maritime domain included NORAD's acquisition of a maritime warning mission, the creation of the US National Maritime Integration Intelligence Office, and the establishment of Canada's Marine Security Operations Centres.

In this regard, a NORAD or perhaps N2 cyber detection mission for North America might be conceptualized based on maritime warning and its protocols. Designed not to duplicate existing and evolving private/public actors and processes, this mission would provide a centralized analytical function based upon its integrated tactical warning/attack assessment function. This mission would serve as the only North American eyes at the end of the intelligence collection process as it currently exists nationally and bilaterally. As NORAD was a key promoter and supporter of greater interagency cooperation to enable its maritime warning mission, it may also act to spur greater intelligence cooperation and information sharing across North America as a whole.[17]

Defense

Alongside detection, defense is the second capability component of a credible North American denial deterrent. As with detection, existing gaps may affect adversary and North American (Canada and the United States) deterrence calculations. Several stand out in the traditional defense domains. Assuming Canada agrees on a CF-18 replacement and given the presence of US anti-cruise missile interceptors, the question becomes whether intercept density relative to NORAD's assigned assets is sufficient to defend against cruise missile threats.

NORAD is also looking at existing northern forward operating locations and other possible locations farther south to meet maritime threats and potentially provide some form of layered defense. Additionally, there is a recognized requirement for in-flight refueling capabilities, and the deployment of anti-cruise missile point defenses must be considered. These factors strongly suggest more resources need to be dedicated to the

air defense component of North American deterrence and then integrated into the detection side of the equation.

Related to air defense requirements, the aforementioned merger of air and space into a true aerospace domain raises the subject of combining air and missile defense capabilities. This process is already underway with the US Army developing the Integrated Air and Missile Defense Battle Command System.[18]

Merging these capabilities raises the thorny issue of Canadian participation and with it, concerns related to intercept priorities and centralized command and control, which in part derailed Canada's participation in ballistic missile defense (BMD) in 2005.[19] A reversal of Canada's "not yes" to missile defense is likely to entail assigning command and control to NORAD. Doing so ensures Canada's direct participation in decision making per the binational agreement and potentially clears the way for the merger of the J-3 position in the NORAD-USNORTHCOM command center—the only position currently not combined. Otherwise, the credibility of the North American denial posture is undermined, with Canadian vulnerability providing a venue for an adversary to exploit.

Relatedly, assuming the United States proceeds with a third continental missile defense site in the Northeast, its requirements may entail an advanced tracking and cueing radar deployed to Canada. Such a radar, in turn, would also likely serve other valuable detection functions related to North American defense.

Maritime Complexity

Turning to the maritime domain, beyond the logic of evolving the current bilateral structure of the Canada-United States (CANUS) naval relationship into a binational one, the defense equation is problematic. Naval preferences are currently forward-defense oriented against cruise-missile-capable surface and subsurface ships (*Archer* class) rather than homeland-defense oriented against sea-launched cruise missiles (the Arrows). While not ignoring the defense value of this preference, the *Archers* are located outside the Royal Canadian Navy and USNORTHCOM's areas of responsibility. Defense against the Arrows is secondary when it should be primary for North American deterrence.

In this regard, major surface combatants (including the future Royal Canadian Navy combat vessel) need to deploy sufficient anti-cruise missile air defenses, and these defenses need to be integrated into NORAD's air defense assets. At a minimum, the role of maritime assets must be fully

integrated into NORAD exercises to bolster North American deterrence requirements.

Other Domains and Resilience

In the terrorism and cyber domains, defense has long been outside the military mandate. The military has been assigned the role of second responder to deal with the consequences of an attack. Defense is in the hands of police forces and bilateral cooperation between Canada and the United States. There appears to be no reason to change the military's role except to ensure protocols governing the provision of mutual support are fully developed in response to a major incident. In this regard, the concept that has recently emerged is deterrence by resilience. Simply stated, capabilities are developed to mitigate the consequences of a major terrorist or cyber event quickly and effectively, thereby reinforcing deterrence credibility.

In many ways, deterrence by resilience is not a denial posture. Rather, it is a recognition that denial is not possible. In traditional military jargon, it is a damage limitation posture that serves to enhance credibility, demonstrating to an adversary that its attack will unlikely reap expected benefits. Canada and the United States need to enhance their ability to assist civil agencies. Furthermore, this assistance should not be constrained by the border, and, at a minimum, such requirements should be a priority for the tri-command structure.

Conclusion

From the perspective of North American homeland defense and security, the current CANUS command structure and capabilities are locked into an exclusive deterrence-by-denial posture. Punishment as an alternative is not an option, which does not mean that an adversary does not confront a credible punishment threat. Rather, the punishment threat and thus punishment capabilities reside elsewhere and are exclusively American. The question then is whether the CANUS part of the equation is adequately structured and resourced to present a credible denial threat to an adversary. Arguably, an adversary could be dissuaded from directly threatening or attacking independent of a punishment threat conceived of as a last resort.

Importantly, any adversary, regardless of perceptions of denial credibility, cannot ignore or simply discount punishment given the reality of US strategic conventional and military capabilities. Of course, as a psychological theory designed to alter adversarial thinking and calculations, it is

extremely difficult to know or predict how an adversary thinks and responds to a deterrence posture. Perhaps, then, what is more significant is how North American decision makers think about their own credibility. It is here that the North American conundrum resides.

The North American component of the US-led Western global deterrence posture should exist as the central deterrence hub such that an adversary does not perceive it as a vulnerability that could be exploited to deter US-led responses to regional challenges. Yet it is questionable whether US and Canadian decision makers even think in these terms about the homeland.

Both arguably remain fixated on the overseas components, with North America as an afterthought despite the rhetoric.[20] Moreover, beyond NORAD and USNORTHCOM and to a much lesser degree CJOC, two different viewpoints exist. The American view is that neither Russia nor China would dare strike North America due primarily to its overarching military superiority and last-resort strategic punishment capabilities. The Canadian view is really a nonview. Essentially, Canada does not really think in deterrence terms because it lacks the capabilities to deter credibly and because deterrence is an American responsibility, with Canada helping and warning where it can.

The net result may be a (vicious) feedback loop. An adversary comes to believe it can exploit homeland vulnerability, thus emboldening it to undertake a regional challenge by threatening actions short of war to deter a regional overseas response by North America. The United States and, to a lesser degree, Canada quickly recognize their vulnerability (and that of vital overseas Allies and partners) and are unwilling to respond effectively, being forced to fall back on a strategic punishment threat to deter. This approach, in turn, emboldens the adversary to initiate further challenges, raising doubts among overseas Allies and partners that the United States will defend them.

The basic answer is to alter deterrence thinking in North America. Structural changes, including necessary investments, to the North American deterrence posture must be made to alter adversary perceptions so that North America cannot be held hostage. In fact, the current North American deterrence-by-denial posture remains embedded in an outdated Cold War mindset that has largely evolved in an ad hoc manner.

These changes are obviously easier said than done. Despite the best efforts by senior NORAD and USNORTHCOM officials to communicate this message, it may take an unexpected overseas regional challenge resulting in a major crisis in which the lack of North American denial credibil-

ity comes to the fore. Unfortunately, by then, it may be too late. The need to refocus on denial is paramount. SSQ

Andrea Charron

Dr. Andrea Charron is an associate professor of international relations and director of the Centre for Defence and Security Studies at the University of Manitoba in Winnipeg, Manitoba, the home of Canada's NORAD headquarters.

James Fergusson

Dr. James Fergusson is a professor of international relations and deputy director of the Centre for Defence and Security Studies at the University of Manitoba. His latest book is *Beyond Afghanistan: An International Security Agenda for Canada* (2016).

Notes

1. Andrea Charron and James Fergusson, "Out of Sight and Out of Mind: NORAD vis-à-vis CANUS politics," *Canadian Foreign Policy Journal* 26, no. 2 (2020), https://doi.org/.
2. Terrence J. O'Shaughnessy and Peter M. Fesler, *Hardening the Shield: A Credible Deterrent and Capable Defense for North America* (Washington, DC: Wilson Center, September 2020), https://www.wilsoncenter.org/.
3. Joseph T. Jockel, *Canada in NORAD, 1957–2007: A History* (Montreal/Kingston, QC: McGill-Queen's University Press, 2007).
4. Office of the Command Historian, NORAD, "A Brief History of NORAD," May 13, 2016, 19–21, https://www.norad.mil/.
5. O'Shaughnessy and Fesler, *Hardening the Shield*, 3.
6. Andrea Charron, James Fergusson, and Nicolas Allarie, *Left of Bang: NORAD's Maritime Warning Mission and Maritime Domain Awareness* (Winnipeg, MB: Centre for Defence and Security Studies, 2015), https://umanitoba.ca/.
7. Andrea Charron, *The Permanent Joint Board on Defence (PJBD); How Permanent and Joint? Celebrating 80 Years of Cooperation* (Winnipeg, MB: Centre for Defence and Security Studies, February 25, 2020), https://umanitoba.ca/.
8. Government of Canada, Canadian Armed Forces, "Current Operations and Joint Military Exercises List: Canada and North America," accessed September 2021, https://www.canada.ca/.
9. Thomas Nilsen, "B-52 Flights Close to Homeport and Patrol Areas for Russia's Ballistic Missile Subs," Barents Observer, November 8, 2019, https://thebarentsobserver.com/.
10. Joseph T. Jockel, "Four US Military Commands: NORTHCOM, NORAD, SPACECOM, STRATCOM—The Canadian Opportunity," Institute for Research on Public Policy (IRPP) working paper 2003-03 (Montreal, QC: IRPP, November 13, 2003), https://irpp.org/.
11. John Hoehn, "Joint All-Domain Command and Control," IF14933 (Washington, DC: Congressional Research Service [CRS], July 2021), https://fas.org/.
12. Bruce Hoffman and Jacob Ware, "Are We Entering a New Era of Far-Right Terrorism?," War on the Rocks, November 27, 2019, https://warontherocks.com/.

13. See Alex Wilner, "Contemporary Deterrence Theory and Counterterrorism: A Bridge Too Far?," *New York University Journal of International Law and Politics* 47, no. 2 (2015), https://nyujilp.org/; Paul K. Davis and Brian Michael Jenkins, *Deterrence and Influence in Counterterrorism: A Component in the War on al Qaeda* (Santa Monica, CA: RAND Corporation, 2002), https://www.rand.org/; and Andrew R. Morral and Brian A. Jackson, *Understanding the Role of Deterrence in Counterterrorism Security* (Santa Monica, CA: RAND Corporation, 2009), https://www.rand.org/.

14. "Executive Summary: 2021 Index of Military Strength" (Washington, DC: Heritage Foundation, November 17, 2020), https://www.heritage.org/.

15. Agreement Between the Government of Canada and the Government of the United States of America on the North American Aerospace Defense Command, April 2006, art. IId, Government of Canada website, https://www.treaty-accord.gc.ca/.

16. "Joint Statement from President Donald J. Trump and Prime Minister Justin Trudeau" (remarks, Washington, DC, February 13, 2017), Prime Minister of Canada website, https://pm.gc.ca/; and "Remarks by President Biden and Prime Minister Trudeau of Canada in Joint Press Statements," press release, White House, February 23, 2021, https://www.whitehouse.gov/.

17. Charron, Fergusson, and Allarie, *Left of Bang*, 42–44.

18. Missile Defense Project, "Integrated Air and Missile Defense Battle Command System (IBCS)," *Missile Threat*, Center for Strategic and International Studies, November 3, 2016, last updated June 7, 2021, https://missilethreat.csis.org/.

19. James Fergusson, *Canada and Ballistic Missile Defence 1954–2009: Déjà Vu All Over Again* (Vancouver: University of British Columbia Press, 2010).

20. CRS, *Renewed Great Power Competition: Implications for Defense—Issues for Congress* (Washington, DC: CRS, September 9, 2021), https://crsreports.congress.gov/.