

MAY 15, 2024

Enhancing Arctic Intelligence, Surveillance and Reconnaissance (ISR) in *Our North, Strong and Free*

Benjamin T. Johnson
NAADSN Fellow

Background

The Government of Canada's recent defence policy update, *Our North, Strong and Free: A Renewed Vision for Canada's Defence* (ONSF), in many ways reflects a different world than the one described in the federal government's 2017 defence policy *Strong, Secure, Engaged* (SSE). As Defence Minister Bill Blair states pointedly in his opening message to *ONSF*, “[t]he world is at an inflection point.” Notably, there is broad agreement that the Arctic, a region of immense strategic importance, is at the front and centre of this changing world, as evidenced by *ONSF*'s focus on the region.

Despite this changing world, *ONSF*'s Arctic focus continues what is discussed in *SSE* in several ways. Canada's Arctic territory spans over 1.4 million square kilometres of diverse geography and environmental conditions and over 160 thousand kilometres of coastline, exposing the country to expansive maritime and aerospace approaches. This geography has consistently challenged the Canadian state's ability to monitor and control its Arctic territory, mainly as human settlement and infrastructure development is sparse relative to its southern territory. For instance, the harsh weather conditions and vast distances in the Arctic make it difficult to maintain a continuous surveillance presence, and the sparse population and lack of infrastructure make it challenging to gather real-time intelligence.

These dynamics have led to repeated attempts to develop advanced intelligence, surveillance, and reconnaissance (ISR) capabilities through technological innovation, particularly during the Cold War, including underwater monitoring systems that never fully delivered on their promised outcomes. [NATO defines ISR](#) as “the foundation of all military operations,” with surveillance and reconnaissance

encompassing all forms of manual and electronic observations and intelligence being the “final product derived from surveillance and reconnaissance, fused with other information.”

While efforts to enhance Canada’s Arctic ISR capabilities largely stalled in the immediate post-Cold War years, the Harper era ushered in modest efforts to reengage with research and development (R&D) focusing on Arctic surveillance technologies. These efforts have continued under the Trudeau government and have only become more critical.

ISR in the Contemporary Era

Several developments have occurred since *SSE* was published that are affecting the Circumpolar Arctic region and Canada’s Arctic territory in particular. Specifically, three broad trends underpin our contemporary inflection point: climate change, geopolitical contestation, and rapid advancements in technological innovation. Also notable is the speed and scale of these dynamics, demonstrated, for instance, by the record-setting wildfire season in the summer of 2023, NORAD’s interception of Chinese surveillance balloons that same year, and Russia’s invasion of Ukraine in 2022, the latter of which effectively dissolved much of the regional cooperation undertaken through the Arctic Council.

These dynamics create an urgent need to enhance the Canadian Armed Forces’ (CAF) ability to possess sufficient ISR capabilities to produce all-domain awareness across Canada’s maritime, land, air, space, and, more recently, cyber fronts. Indeed, such awareness is crucial to realizing the defence vision outlined in *ONSF*, including in relation to continental defence under NORAD and NATO’s security.

The complexity and uncertainty of the contemporary threat environment puts a premium on distance and speed, thus requiring greater persistent awareness and the ability to make rapid decision-making and action. ISR is prioritized to enable the timely and flexible application of military power much quicker (including pre-emptively) to overwhelm and deny adversarial capacity. *ONSF* states that, “to address new threats through, to and in the Arctic and North, we will prioritize detecting an understanding threats across all military domains, increasing our military’s presence, mobility and responsiveness in the Arctic, and robustly responding to threats when and where they materialize.” In the ISR field, technological developments in automation via artificial intelligence (AI) and quantum technology are reshaping, or are expected to contribute significantly to, remote sensing and other surveillance efforts.

NORAD modernization efforts focus on the air and maritime approaches, where *ONSF* explains that new Arctic and Polar over-the-horizon-radar systems will support surveillance. DND affirms that it is also investing in undersea surveillance, cyber, and space-based capabilities while leveraging AI and cloud computing for rapid decision-making systems. Investment in research and development for these technologies will be provided in several areas, including NATO’s *Defence Innovation Accelerator for the North Atlantic* and the *NATO Innovation Fund*, along with research funds committed in earlier budgets and programs, such as the *All Domain Situational Awareness (ADSA) program*.

Conceptually, DND envisions a networked array of sensors that enable monitoring across Canada's expansive Arctic domains and which allows for rapid responses, especially to climate-related disasters (such as wildfires and floods) and contributes to national defence efforts. In the near to medium term, DND will focus on augmenting and updating existing assets and ISR resources. While NORAD modernization encompasses many of the significant surveillance-related projects being pursued, *ONSF* notes several other efforts and interests that DND/CAF will investigate for their potential contributions to all-domain awareness. For instance, the *ONSF* commits to exploring options to expand and renew its conventionally-powered submarines, and will acquire specialized maritime sensors deployed on the *Harry DeWolf*-class Arctic and Offshore Patrol Vessels for ocean surveillance. New satellite ground stations are also expected to support space-based ISR.

Challenges Ahead

Much of the surveillance and intelligence initiatives discussed in *ONSF* need to be better defined and, like much of the vision outlined, remain aspirational – particularly regarding the role of AI and quantum technologies in enhancing ISR capabilities. This ambiguity is not surprising, given that these technologies are in their early stages of development and will not mature for years or decades. However, their potential to revolutionize ISR is immense, and it is crucial to anticipate and understand the challenges and limitations that they may present.

Canada is in a favourable position to contribute to R&D in these areas as it has a well-established industrial network and research centres focusing on AI and quantum technology, partially due to earlier investments made by the federal government. The Government of Canada is also thinking about these issues elsewhere, as evidenced by its [National Quantum Strategy](#) and DND's complementary [Quantum Science and Technology Strategy](#).

Nevertheless, *ONSF* is largely silent on specific challenges that are likely present themselves along the path to achieving a modern ISR network. These challenges include technological limitations, regulatory hurdles, and the need for international cooperation. Understanding and addressing these challenges will be crucial for successfully developing Canada's ISR capabilities.

For instance, while a modern ISR architecture will be highly digitized and rely on advanced technologies, humans will remain essential to the practices associated with ISR, even if they are augmented by machines (machine teaming). While *ONSF* notes the current and future CAF personnel requirements, digital literacy and diverse skill sets will remain critical. Moreover, this ongoing reliance on humans involves its own risks, including human error, cognitive biases, and limitations, which may continue to produce or amplify automation biases (the over-confidence in decisions made by automated processes). In short, while promising, human-machine teaming involves its own sets of complex challenges that require immediate and careful attention.

Moreover, ISR modernization will require significant infrastructure, both conventional and digital. The infrastructure gap in Canada's Arctic is well documented, including access to reliable broadband. Addressing this gap will require large sums of money and effort over the long term (likely facing added budgetary pressures), as well as collaboration and engagement with Indigenous partners.

As mentioned, much of the technology envisioned in *ONSF* remains speculative. The technical issues involving AI and quantum capabilities are particularly apparent. However, sensors are an area where these capabilities are more developed and potentially ready for wider deployment in the near term. Nonetheless, it is recognized that some or much of the desired outcomes of these technologies may not be realized, as the history of developing Arctic surveillance technologies attests.

Other challenges will persist even if AI and quantum significantly contribute to ISR capabilities. For example, the ethical implications of possessing more intensive ISR capabilities domestically and beyond national borders generate tensions related to sovereignty, privacy, and data governance. These capabilities also create a paradox whereby realizing greater domestic security might undermine international stability through its disruptive capacity. For example, quantum sensing might offer unparalleled data on environmental conditions and support weather pattern modelling (helping combat forest fires and plan evacuation routes), but could simultaneously undermine nuclear deterrence by illuminating the oceans and the locations of nuclear submarines (though many experts note that this is unlikely in the near future). These tensions and contradictions need to be explored further.

Lastly, the layered or systems-of-systems ISR network that DND and allied states envision will require close cooperation for development and interoperability, particularly related to NORAD and NATO systems. These requirements may be affected by geopolitical considerations involving sovereignty and economic competition prioritizing domestic investment. Navigating these challenges will require ongoing negotiation with industry partners and allies.

The Government of Canada, and DND/CAF more specifically, recognize various pan-domain risks and threats in the current security environment and the rapid pace at which that environment is changing. This recognition is encouraging, as is DND's commitment to produce defence updates every four years, given the speed of technological evolution. As they research and grow their ISR capabilities, ongoing consideration and thoughtful discussion will be more important than ever to overcome emerging challenges.