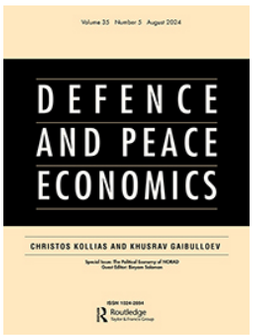

Routledge
Taylor & Francis Group

Defence and Peace Economics

ISSN: 1024-2694 (Print) 1476-8267 (Online) Journal homepage: www.tandfonline.com/journals/gdpe20

NORAD Modernization: Private Benefits to Canada

Ugurhan G. Berkok & Oana Secrieru

To cite this article: Ugurhan G. Berkok & Oana Secrieru (2024) NORAD Modernization: Private Benefits to Canada, Defence and Peace Economics, 35:5, 577-600, DOI: 10.1080/10242694.2023.2228565

To link to this article: https://doi.org/10.1080/10242694.2023.2228565

DEFENCE AND PEACE ECONOMICS
2024, VOL. 35, NO. 5, 577–600
https://doi.org/10.1080/10242694.2023.2228565

NORAD Modernization: Private Benefits to Canada

Ugurhan G. Berkok[a] and Oana Secrieru[b]

[a]Department of Political Science and Economics, Royal Military College of Canada and Department of Economics, Queen's University, Kingston, Canada; [b]Department of Political Science and Economics, Royal Military College of Canada, Kingston, Canada

ABSTRACT

The workhorse of military alliances theory is the joint products model where the prominent existence of private benefits from alliance activities alleviates the free-riding problem. In the case of NORAD Modernization project, there are potentially large private economic benefits accruing to Canada. These benefits may include technology transfers and domestically produced inputs from some sectors exhibiting comparative advantage. In this latter case, the benefits will largely depend on whether a JSF type consortium will undertake the investments efficiently as opposed to the so-called benefits obtainable from Canada's fundamentally inefficient offsets program, Industrial and Technological Benefits (ITB). The article focuses on Canada's Key Industrial Capabilities (KIC), the 17 sectors officially selected as supporting the country's operational capabilities. The width of this selection as well as the procurement and industrial policy interaction are briefly discussed.

ARTICLE HISTORY
Received 21 January 2023
Accepted 20 June 2023

KEYWORDS
NORAD; private economic benefits; alliances; Joint products model

Introduction

The North Warning System (NWS) is an existing early detection mechanism for NORAD (North American Aerospace Defence Command), a bi-national military alliance between Canada and the United States for the aerospace defence of North America. The two neighbours agreed to create NORAD in 1957, in the heat of the Cold War, as a bi-national command, centralizing operational control of continental air defenses against the threat of Soviet bombers.

The predecessor to NWS consisted, at the time, of the Distant Early Warning Line (DEW Line), a chain of 63 radar stations and communication centres, spanning 5,000 km from Alaska through Canadian Arctic to Greenland. In the late 1980s the DEW Line was replaced by the current NWS with 47 radar sites. Since the existing NWS capabilities may not detect incoming modern gliding vehicles and cruise missiles, they have to be modernized to preserve NORAD as a credible deterrent. This modernization requires a multi-domain integrated system of sensors and cyber-safe communications with built-in redundancy.

The modernized system will include more advanced ground-based long-range radars with an over-the-horizon capability (i.e. able to detect targets beyond the limits of the typical radar horizon); dedicated aerial platforms, such as the current Airborne Warning and Control platform like the current AWACs; high-altitude stationary radar blimps or tethered aerostats; maritime-based surveillance systems such as underwater sensors; and space-based systems.[1]

The paper is structured into three parts. Part 1 explains the threats inducing the demand for NORAD modernization. Part 2 introduces the architecture and the corresponding components of the

CONTACT Ugurhan G. Berkok ugurhan.berkok@queensu.ca Department of Political Science and Economics, Royal Military College of Canada and Department of Economics, Queen's University, Kingston, Canada

presumed new NORAD capability. Finally, in Part 3, we identify those Canadian key industrial capabilities (KICs) technologically advanced enough to bid for NORAD Modernization contracts or capable to absorb the advanced American technologies.[2]

Emerging Vulnerabilities and Demand for NORAD Modernization

NORAD, as it exists, has become vulnerable against recently developed hypersonic missiles by China and Russia because its current capabilities were largely installed late in the Cold War and thus may not detect those incoming missiles on time or even at all. Strategically, by escaping NORAD's Northern Warning System (NWS), such a credible threat of incoming missiles can essentially hold North America hostage by targeting critical infrastructures and slowing down deployment in case of conflict overseas.[3]

In particular, after a hiatus in the 1990s and into 2000s, Russia resumed bomber flights into the American and Canadian Arctic regions in 2007 to test NWS responses in the Air Defense Identification Zones (ADIZ). NORAD's current capabilities can defend against a small number of ballistic missiles, such as those of North Korea, but large numbers of incoming missiles with speed and maneuverability, as in the case of hypersonic cruise and glide missiles, can overwhelm the early warning system. This swarming threat thus generates a rivalry issue under NORAD's current capabilities that cannot detect all incoming missiles even if kinetic kill capabilities may exist, which the Modernized NORAD will have to address.[4] Interestingly, this threat might generate a positive relationship between the distribution of the threat, e.g. undetected missiles' intended or perceived targets, and the smaller ally's motivation to contribute.[5]

In terms of the cyber-domain, the existing system is vulnerable to incoming swarms of unmanned aerial vehicles (UAVs) attacking NORAD's Arctic infrastructure that supports NORAD's domain awareness capability.[6] In particular, the current sensors may fail against such swarms accompanied by incoming missiles. This potentially all-spectrum threat requires an expansion of the spectrum of military domains, from submarine threats to cyber and aerospace that a new system has to scan to detect emerging threats.[7]

Beyond the technological ageing of the current system, a spatial challenge arose from the recent expansion of the Canadian ADIZ (CADIZ) in 2018 (see Figure 3 below). The modernized NORAD may not only have to expand its sensors layer to far out into the Arctic but also cope with that challenging environment to surveil with a wide range of threats from multiple adversaries, traditionally Russia and now China with its global ambitions including the Arctic by self-identifying as a Near-Arctic State. Moreover, a new generation of multi-mission sensors that can detect a spectrum of threats have to be installed into harsh climate conditions in vast spaces with no existing infrastructure to support them, well beyond any upgrades to the existing NWS radar stations. While space-based sensors can complement the ground and underwater-based censors in the surveillance of the Arctic, new challenges, and tradeoffs may arise in terms of orbit choice,[8] satellite constellation, and communication securities.[9]

All-domain awareness is a core capability requirement of the modernized NORAD. The multi-layered sensor system that can enable the all-domain awareness must be able to detect, identify, and track all threats, ranging from unmanned aerial vehicles (UAVs) to ballistic to cruise missiles and the new hypersonic glide vehicles.[10] Moreover, the system must detect threats at long distances to shorten the detection and response times. Cruise missiles and hypersonic glide vehicles can be launched over-the-horizon, from well outside the areas currently surveiled by the NWS and they can travel beyond 5 Mach.[11] Thus, the all-domain awareness is all the more important as those offensive weapons can be launched from sea, land, and air all with cyber-prints.[12] While NWS was able to detect ballistic and bomber-launched missiles, the new system must be expanded to include cyber, sea, air, land, and space domains to be surveiled as well as their integration.[13]

The proposed multi-layered all-domain sensors system must satisfy some requirements (See Figure 1 below). First, the system must exhibit redundancy, with additional layers offering

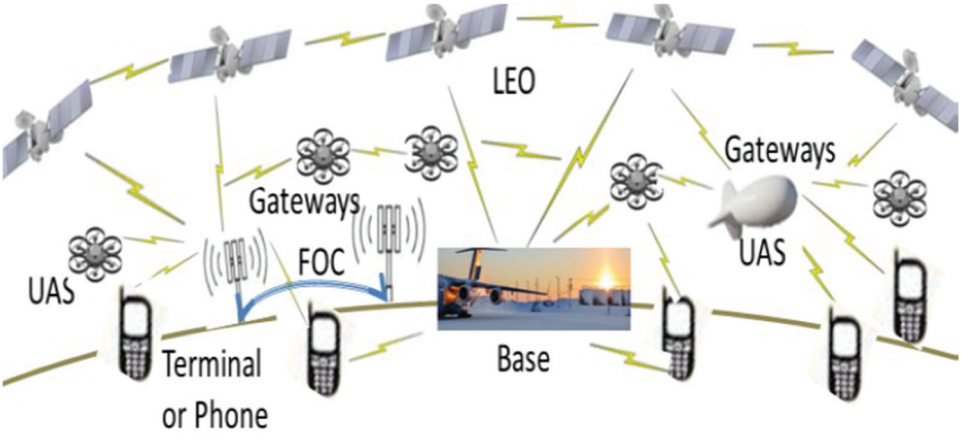

Figure 1. (Labbé 2020b) multi-layered detection system with multi-mission sensors.

enhanced resiliency. Layered redundancy can better absorb an initial damage and might still allow parts of it to fulfill its detection mission. Second, detection sensors must be separate from defeat sensors to reduce complexity and to separate, if necessary, the C2 (command and control) information flow from all-domain awareness information flow hence separating defensive awareness from the response to threat. Third, the layering of the sensors has to be seamless, closing current gaps in coverage that make NORAD so vulnerable to developing threats such as hypersonic glide vehicles and cruise missiles with the existing 47 radar installations. Closing these gaps requires a combination of multi-spectral sensor capabilities (a combination of radar, infrared, radio frequency, acoustics,[14] etc.) given that these missiles can be launched from beyond the horizon as well as from other vehicles, such as submarines. Fourth, all-domain awareness must occur at longer ranges to detect and engage threats as early as possible, i.e. a threat to be identified and tracked from its 'birth.' The new NORAD would thus require a system constituted by such sensors on satellites, ISR aircraft, drones, land, and sea installations, over-the-horizon (OTH) radars to track launches as well as being pushed further north onto the extended CADIZ including the Ellesmere Island.

Figure 1 describes a simplified illustration of the Modernized NORAD. Multi-mission sensors can be mounted on satellites on Low Earth Orbit (LEO) for shorter communication responses (or low latency)[15] as well as on within-atmosphere Unmanned Aerial Systems (UAVs) as well as terrestrial radars, some of which have to be over-the-horizon (OTH)[16] radars that can be connected by fiber optic cables (FOC). As anticipated, another three layers, underwater sensors, possibly fixed-wing Intelligence-Surveillance-Reconnaissance (ISR)[17] aircraft mounted sensors and the cyber dimension will complete the multi-layered detection system.

Since any need for modernization, like retrofits, immediately poses the question as to whether one preserves some legacy components. NORAD Modernization may beg the question as to whether Canadian land mass is critical in the light of modern detection technologies. This question will be addressed in Part 2 below.

The modernized NORAD is being conceived as an integral part of an interception or defeat mechanism structured around a layered 'shoot-assess-shoot' doctrine.[18] The shoot-assess-shoot doctrine optimizes the response with the least number of interceptors to achieve a 'kill' (not including 'left of launch' targeting).[19] Such a mechanism requires longer-range initial intercepts to provide enough battlespace for assessment, tracking, and follow-on shot opportunities. Both layered redundancy and layered shot doctrine become necessary only against great-power adversaries as smaller states may not generate the large volume of fire to overwhelm NORAD.

The Modernized NORAD

The Anticipated Sensor Network

The next-generation sensors, dual-use, modular, and scalable, are expected to have the new capabilities required against the 'swarming' threats where large numbers of drones and missiles may thwart defensive interceptor missiles by successfully identifying armed ones. This strategic necessity generates some requirements. First, the multi-mission sensors[20] should be capable to detect and track more than one threat, different types of threats and even high volumes of threats. Second, the sensor network should be software-defined[21] and use open architecture for quick adaptability and upgradability upon newer technologies. This would also facilitate the integration of layers and support the C2 network without requiring hardware updates, increase the life expectancy of the modernized NORAD and keep down future costs.

The multi-layered sensor network has to integrate detection through to C2 decision nodes. The processed information flow from the network must be relayed to C2 nodes as all-domain awareness data for decisions. This work requires that industry engages in the architecture of how such technologies will enable the military missions from detection to interception. While the related and ongoing U.S. work feeds into the new generation of jet fighters and other networked platforms, the relevant Key Industrial Capabilities (KICs) in Canada[22] have not yet formed R&D clusters presumably because they do not anticipate government action in the form of project definition.

The all-domain awareness paradigm has become tightly mission-focused in the context of NORAD Modernization with the American Joint All-Domain Command and Control (JADC2)[23] project, having shifted away from being about platforms and sensors while these latter remain components of the system. The processed information flow from sensors has to be integrated to C2 and hence to the defeat mechanisms, i.e. a fluidity from data to C2 decision-makers and their decision-making processes can take no more than the time needed 'at the speed of relevance' of the mission. Since system components must necessarily exhibit heterogeneity, the weakest-shot technology in latency may pose a serious constraint on the effectiveness of the system. This speed or latency will depend on computing processes and data structures. A simple representation of this complex network of sensors is given below in Figure 2. An open architecture with reconfigurable sensors may overcome this speed of relevance challenge as the weakest links improve.

In the layered sensor networks, each layer contains nodes with different capabilities. Depending on the environments where these sensors are installed, such as in space, on earth, on aerostats, under water and on drones, the lowest layer contains multi-mission sensors that detect, surveil, and record threats. This is raw data. The middle layer contains the so-called super nodes with higher computational power and longer transmission range so that information flowing from the lowest layer is processed, organized, and then forwarded to the top layer that contains a sink node where it integrates with the C2 network for decisions based on the information generated by the network. Figure 2 yields a simplified illustration of JADC2.

The presence of heterogeneous sensor nodes, i.e. those with different energy capacities and communication capabilities, in a sensor network increases network reliability and its life expectancy. Below, in Figure 3, is a representation of a layered military network, from the forward-most sensors layer to the supernodes layer and, finally, to the C2 layer. The four KICs identified above[25] prominently figure at different as well as across the layers, the NORAD modernization project ought to yield significant industrial and technological benefits to Canada with those industries participating in the design, construction, and maintenance of the capability. Section C below will provide details.

The sensor system must detect not only all well-defined threats but also as early as possible, from 'birth to death', the suspected threats as well. A 'kill' or removal of the threat, whether by kinetic or non-kinetic means, requires a sufficiently quick response time by the kill chain,[27] which, in this case, corresponds to JADC2. The identification of threats to allow a C2 choice of defeat instruments is facilitated by the use of artificial intelligence (AI) over the fusion and

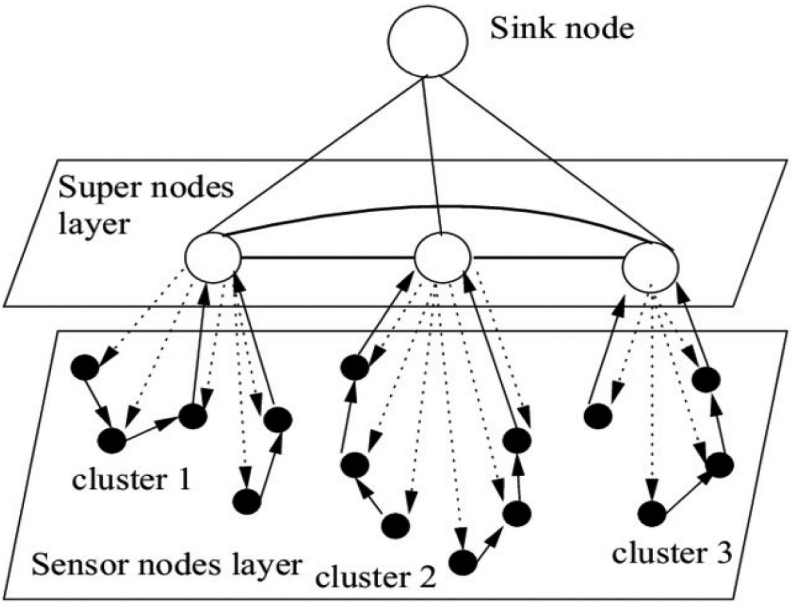

Figure 2. A simple representation of layered sensor networks[24].

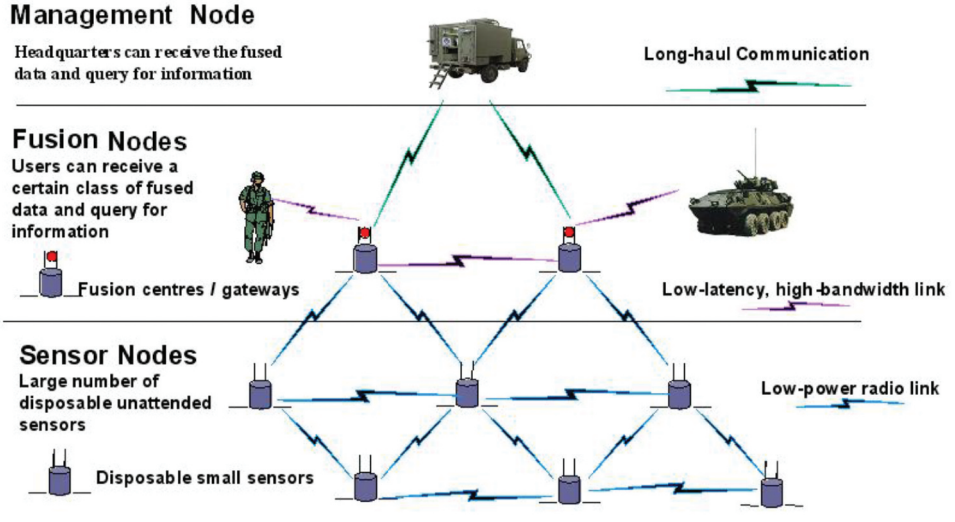

Figure 3. A military C2 integrated layered sensor network[26].

management nodes. This means that some well-defined threats may not have to reach human decision-makers for the activation of defeat mechanisms. Although false positives are possible, the tradeoff is between the false positive and the time and processing gains to assess the less well-defined threats.

The sensor network must build redundancy, not only by sheer numbers of sensors but also by the variety of sensors and their locations in the network. The resiliency of the all-domain awareness requires redundancy by variety. For example, whereas space-based sensors might yield a global view by detecting threats 'from birth', under-water sensors will detect submarines and, conceivably, their payloads. These two informational bits, originating from primary sensor modes, are to be processed

at fusion nodes to yield a possible threat signal to be assessed at the management node. Since the management or decision node in our current context is NORAD, the integrated detection and decision components of the system must be examined with an eye to technological and industrial requirements.

Joint All Domain Command and Control (JADC2)[28]

C2 is normally understood as issuing a command, which sets a standard, and then controlling performance by monitoring and enforcing the standard. In the case of a complex system like the multi-layered sensors fused into a C2 framework, JADC2 discussions must include such concepts as system redundancies, a resilient architecture and the flow of processed information 'at the speed of relevance'. This latter requirement is critical in the performance of such a system simply because the length of time from birth to death of incoming missiles is the window in which C2 will have to detect, identify, and defeat those missiles.

The Strategic Homeland Integrated Ecosystem for Layered Defense (SHIELD)[29] framework, developed by the U.S. Northern Command (NORTHCOM) and to be adapted to NORAD, takes the technologically adaptive approach described above in terms of an open architecture. Consequently, JADC2 will evolve in response to threats as well as its own and ally capabilities. In terms of defeat mechanisms, JADC2 will integrate advanced sensors from all domains and fuse the generated data into an all-domain awareness picture that facilitates identifying over-the-horizon threats without waiting for the threat to approach North America. An efficient intervention mechanism with multiple tools will then defeat a minor threat, upon early detection, with proportionate defeat mechanisms while saving major defeat mechanisms for major threats. The intention is to make JADC2 subsequently available to allies and partners.

This new capability of processing data from every sensor and of making it available to the best defeat mechanism from among all C2 nodes faces three technological challenges. The first relates to data processing to derive the relevant data on which defeat mechanisms can be activated. Although sensors generate abundant data, further data can originate from a wide spectrum of sources such as personnel on the ground who can feed directly into the system or from open sources. The second is the cloud-based data processing architecture through which all the data must be processed. The information thus obtained must be open and accessible to all decision nodes at all levels of C2. The third is the generation of a common picture of the battlefield and how it is made available. This entails the fusion of all feeds from sensors to fusion nodes, from identified threats to friendly troop readiness data and the presentation of the picture for the relevant commander.

Whereas the overcoming of these three challenges may represent a significant step forward for JADC2 capabilities, the sheer volume of data that is fed to C2 can easily overwhelm the cognitive abilities of commanders. Thus, a fourth challenge arises, namely the use of AI in reducing the processing burden to commanders.

The use of AI lessens commanders' cognitive limitations from facing big data. AI will detect patterns and anomalies in big data and, by using the predictive analytics, enable decision-makers to concentrate on decisions at a higher level of information. Moreover, AI may go beyond pattern recognition by producing hypothetical scenarios to yield choice sets. This analytical process is Bayesian, i.e. it corresponds to using historical data but augment it using the present data to build the choice set. This assessment capability determines the best responses to the processed and organized data coming out of machine-learning capabilities in real time.

The use of AI is not intended to replace the human decisions but, instead, enables quicker and clearer human decisions by eliminating the noise, so to speak, from information available to commanders. Machine-enabled insights are thus more than connecting sensors to shooters. The AI-filtered decision space enables commanders to act earlier and, based on filtered, organized, and AI-analyzed information, in real time. Consequently, this JADC2 superiority may even produce a deterrence effect by convincing adversaries not to act and, hence, possibly deescalating crises.

Defeat mechanisms[30]

NORAD's science and technology (J8) section has already produced a white paper to give defence industries the opportunity to propose their defeat mechanism on offer for the short-, medium- and long-term investments as part of the overall NORAD modernization project. The defeat solutions have to address both current and emerging threats as well as the current and expected weaknesses in the solutions. The proposed solutions are to be given opportunities to be tested at demonstrations and tests at events like the Advanced Battle Management System (ABMS) exercises.[31] ABMS testing for JADC2 is thus well underway as a precursor of its integration to the modernized NORAD.[32] Canadian industries, especially those technologically at the frontiers and hopeful to win contracts, are already investing in products. For instance, General Dynamics Mission Systems Canada has been developing The Tactical Network as a Service (TNaaS), which 'addresses the interoperability of data from all domain assets, forming a data-centric foundation, ready for exploitation by artificial intelligence and advanced algorithms, . . .'[33]

While defeat mechanisms are different from all domain awareness and JADC2 solutions, they can and have to be integrated for C2 purposes.[34] While sensors and JADC2 can span the full spectrum of threats, different threats call for different defeat mechanisms. A missile designed to kill a hypersonic glide vehicle at long range is obviously not appropriate for shooting down a small unmanned aerial vehicle (UAV) or a swarm of UAVs. The most pressing threat for NORAD is seemingly the swarms of cruise missiles approaching North America.[35]

Once such a threat is well defined, a few principles to guide the NORAD Modernization project emerge. First, solutions must be purpose-built for North American continental defence rather than transplanting them from other potential theatres. Second, given that launch to impact times have been falling, the Modernized NORAD solution has to reduce the response lag significantly to become a credible deterrent. Third, in order to avoid being taken hostage, as discussed above, the modernized NORAD must concentrate on limited area defences such as to protect critical infrastructure. Last, the modernized NORAD may have to build offensive defeat mechanisms to target adversarial launch platforms at long range as part of a credible deterrent. Such launch mechanisms include mobile platforms like aircraft and submarines. Killing one bomber before it can launch its payload of multiple cruise missiles could well be more efficient.

Modernized NORAD, Canada, and the Defence of North America

Recently, in 2018, Canada's Air defence Identification Zone (CADIZ) was realigned to the outer edge of Canadian Arctic Archipelago to incorporate the Ellesmere Island (See Figure 4 below). However, the NWS does not possess the full capability to look that far north let alone further distances required against the mobile platform launched cruise missiles and hypersonic glide vehicle launched missiles. The current NWS did not need to extend that far north at the time it was installed simply because the threats of the time allowed longer response times from detection. Now that the current threats require earlier detection brings forth the necessity of installing the sensors at the outer edges of CADIZ. New engineering challenges arise,[36] as a result, with radar and sensor installations near the pole. As indicated above, the costs of building infrastructures in the Arctic remain challenging in terms of engineering and hence costs due to the melting permafrost in particular but also to the existing harsh climate conditions. Moreover, short construction seasons and the difficult logistics of transport to the sites add to difficulties as well as to costs.

The current NWS, which provided a single solution for the threat environment of 1980s and into 1990s, now falls short of technical capability requirements against the new threats. For instance, moving the same short- and long-range radar systems farther North in the Canadian Arctic Archipelago cannot be effective against those new threats. Even longer-ranged ground-based radars will not suffice to meet the air-launched cruise missile (ALCM) threats as such missiles exhibit low

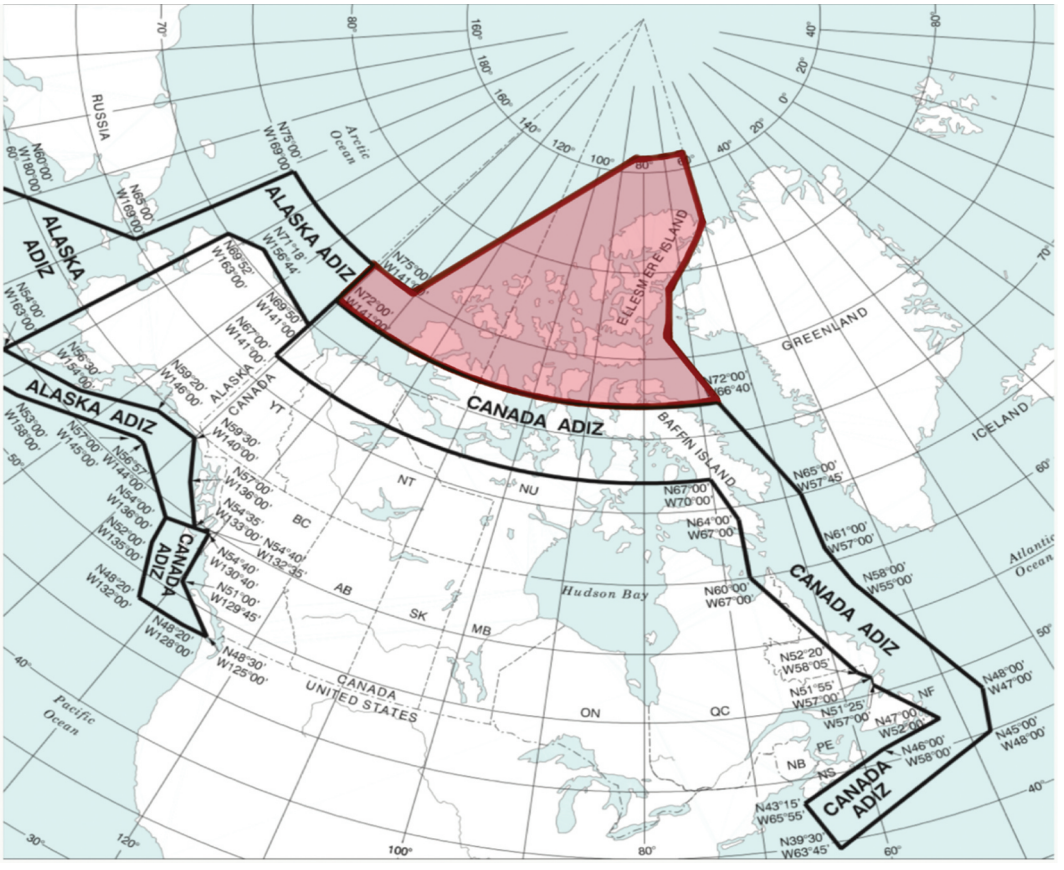

Figure 4. CADIZ after 24 May 2018 expansion (coloured)[37].

signature, higher speeds, and greater maneuverability to escape such detection systems, thus shortening the time span between launch and impact.

Technological advances in cognitive[38] and quantum[39] radars might have improved the performance of NWS but they remain in a single domain. While ground-based radars, both short- and long-range, will remain vital for the time being, both for NORAD as well as for civilian Arctic aviation, they have to be supplemented with the multi-layered and multi-mission sensor networks as part of Modernization. All such modifications must be conceived as part of the comprehensive NORAD Modernization project. Moreover, further supplementation by sensors onboard other systems, namely airborne vehicles, including UAVs and perhaps fixed-wing ISR aircraft, maritime, and space-based assets, have become necessary for the new architecture with redundancies as well as all-domain capabilities.

This brief discussion does not delve into the politically sensitive question on whether the U.S. couldn't go it alone, especially if Canada drags its feet. A broad answer comes in two parts. First, the above discussion of Modernization shows that the removal of land from the architecture is not yet feasible and effective as multi-domain awareness still requires some land-based installations, radars, as well as communications infrastructure. One might even add tethered aerostats as capabilities that come at affordable costs. Second, a related yet a different argument is, still based on multi-domain sensing, the risk-reducing diversity of sensor carrying platforms, from radar to underwater installations. After all, the diversity of domains decreases the likelihood that the system will miss the odd drone or an approaching missile.

In the light of JADC2 debates, the final technical solution will include the existing radar station infrastructure but modernize them. In addition, there will be new sensors and their fixed or mobile carriers in other domains as well as the new spatial domain, i.e. the newly augmented CADIZ. This overall NORAD Modernization carries a current price tag, though probably an underestimate, upwards from $10 billion Canadian. If the Canada U.S. cost sharing arrangement remains similar to the current NORAD, it will be a split of 40% Canadian and 60% US. Whereas Canada's new defence policy, *Strong, Secure and Engaged*, and the 2018 Canadian *Defence Investment Plan* are vague on these costs, the most recent political environment, with the Russian invasion of Ukraine, has produced immense pressure on NATO countries in general and on Canada in particular for additional defence expenditures.[40]

Past data on Canadian political support for NORAD suggested that Canadians were reluctant to embrace offensive weapons or capabilities like the ballistic missile defence (BMD) system, especially French-speaking Québeckers. By contrast, there has been broad political support for Canada to remain a credible ally in continental defence through renewing NORAD's defensive capabilities. Although a more offensive NORAD, including the defeat mechanisms, had until recently being perceived as undermining this support,[41] Russia's more belligerent behaviour, culminating in its invasion of Ukraine, and China's threats to independent Taiwan and its claims to the Arctic, may be positively affecting Canadian attitudes towards the Modernized NORAD with an offensive deterrent with interceptors.[42] The recent Canadian government announcement is evidence of further changes. "In June 2022, Canada's current minister of national defence committed to further modernizing Canada's North Warning System by investing in an Arctic over-the-horizon radar, a polar over-the-horizon radar, a group of sensors called 'Crossbow' located throughout North America, and a space-based surveillance system that will collect intelligence and track threats. Moreover, Canada has recently established a space division (similar to the United States' Space Force) and signed a memorandum of understanding with the US around a NORAD maritime awareness mission."[43] This change will probably be reinforced once the private benefits, as described below, become more apparent.

Canadian Contributions to the Modernized NORAD

Canada's contribution to continental defence consists of financial resources, personnel, and assets to NORAD. Through NORAD, Canada is able to focus on surveillance and operational control over domestic airspace to maintain sovereignty. The bi-national nature of the command allows Canada to respond to threats in a cost-effective way within the collective defence of North America. Whereas NORAD and NWS have operated solely as an aerospace defence against incoming ballistic missiles, the Modernized NORAD will fuse aerospace and cyber defences.

Although today's NORAD operations may be perceived as distinct from Canada's defences, whether aerospace or cyber, the Modernized NORAD will be more demanding in terms of required cyber capabilities inherent in JADC2. The current Canadian cyber defence infrastructure includes the Communications Security Establishment (CSE), the Canadian Centre for Cyber Security (the Cyber Centre), and the Department of National Defence (DND)/Canadian Armed Forces (CAF). CSE is mandated through the *Communications Security Establishment Act* (CSE Act, or see Bill C-59) to protect and defend Canadian cyber systems, acquire foreign intelligence, conduct defensive foreign and active foreign cyber operations, as well as assist domestic law enforcement and security agencies and DND/CAF. The Cyber Centre focuses on defending Government of Canada (GoC) networks from cyber threats and supporting the protection of critical infrastructure (CI) and Canadians online through expert advice, services, and publicly available assessments. The CAF's main cyber unit is the Canadian Forces Network Operations Centre (CFNOC), which is 'tasked to conduct defensive operations within DND/CAF's cyberspace to detect, defeat, and/or mitigate offensive and exploitive actions to maintain freedom of action.'[44]

Whereas Canadian industrial infrastructure can make significant contributions to the Modernized NORAD in most areas, it cannot contribute to defeat mechanisms. Canadian industry does not have the capacity to produce kinetic defeat capabilities and the government investment to create one is unlikely while non-kinetic capabilities that might at times serve the same objective do exist.[45] The next section specifies those areas where Canadian contributions can be substantial and hence they will generate the private benefits from NORAD.

Canadian Industrial Participation and Potential Private Benefits

This section of the paper builds on the joint products model of alliances where private benefits are explicitly modeled[46] and they are shown to alleviate the intrinsic free-riding problem. The NORAD Modernization project can potentially generate significant private benefits to Canada, which ought to strengthen the government's case for fully participating in the project. First, advanced technology transfers from U.S. are clearly possible as for all aspects of the project except the kinetic defeat mechanisms because Canadian industries prove to be at the technological frontiers in nearly all aspects of the project. This signifies that the overall technology absorption capacity is high and Canadian companies are likely to win contracts. Second, if the Modernization project is run like the JSF Consortium, Canadian industries can surely bid and win contracts against American contractors rather than being handed out contracts as in inefficient ITBs, Canada's offsets program. Whereas JSF contracts generated real ITBs, there exists hardly any evidence on long-term benefits generated from contracts under the ITBs policy. The JSF project has been like a club good where the membership allowed member countries' aerospace contractors were qualified to bid. If they won contracts, it was proof of their advanced technological abilities, unlike contracts won under ITBs that provide basically import-substitution protection to domestic contractors. Finally, especially for those radar stations to be built on the Ellesmere Island, new construction technologies will be needed due to a combination of permafrost and thawing permafrost throughout the Arctic.

Table 1 below is a preliminary attempt to establish a mapping from the NORAD Modernization project industrial requirements to Canada's corresponding Key Industrial Capabilities. Since it is likely that contracts will have to go to tender in JSF type bilateral arrangement, companies that happen to be at the frontiers of technology stand a chance of winning.

In terms of private benefits to Canada as a joint-product of a Modernized NORAD, the primary question is whether Canadian defence and security industries can currently deliver components in the detection and the C2 technological solutions.[48] In this regard, the modernized NORAD is

Table 1. Mapping from some NORAD Modernization technologies to Canada's KICs[47].

	Emerging technologies				Leading competencies and critical industrial services		
	Artificial Intelligence	Cyber Resilience	Remotely-piloted Systems & Autonomous Technologies	Space Systems	Aerospace Systems & Components	Electro-Optical /Infrared (EO/IR) Systems	Sonar & Acoustic Systems
Satellites			✓	✓	✓	✓	
UAVs			✓		✓	✓	
Communications	✓	✓	✓	✓	✓		✓
Sensors			✓	✓	✓	✓	✓
Data analytics							
Mission software	✓	✓	✓	✓	✓		✓
ISR	✓		✓	✓	✓		
Forensics	✓	✓					
Advanced materials							✓

envisioned to become an all-domain early warning system, including against cyber threats against its installations and communication systems. For example, the prevention of a potential cyber threat would fall into the cyber resilience KIC. Yet, several other KICs are capable of successfully producing building blocs of the Modernized NORAD[49] other than the rather obvious brick-and-mortar infrastructure as in the case of new radar stations on Ellesmere Island in the High Arctic as well as building underwater sensors in the austere Arctic environments.

Three major questions arise. What off-the-shelf technology is available that can be modified and compete for Modernized NORAD contracts? What current NWS installations can be retrofitted? Can the relevant industries deliver solutions in a timely fashion?

Whereas about a year ago[50] financial resources for NORAD Modernization may not have been readily available as the COVID-19 pandemic started fading and fiscal realities coming to the fore, the rising overall belligerence of Russia and its invasion of Ukraine seem to have modified the Canadian priorities in favour of the project. Moreover, the North Warning System approaching the end of its operational and functional life span, a second urgency imposes. The current sensors are rapidly becoming obsolete and cannot wait for the current 20-year procurement plan. This may well have changed the complexion of the Canadian public policy priorities in favour of an inevitable increase in support for higher defence expenditures including, urgently, the NORAD Modernization.[51]

In terms of the overall Modernization project, one option regarding the path from NSW to Modernized NORAD may well be a transition rather than a complete renewal. Prolonging the service life of useful existing architecture and mixing it with new sensors through the process of incremental improvement to achieve, over time and with a new emphasis on homeland defence, will probably be the way. Such a transitional modernization might pose a different engineering challenge as, instead of the new technologies NORAD modernization requires, this transitional approach may require a systemic approach that would guide the transition.

One of the significant challenges awaiting NORAD modernization is the necessity that project teams have to navigate across the two governments and interact with industry. Better collaboration between government and industry on operational analysis (on sensors, C2, and defeat capabilities) could improve outcomes.

Two critical and related decisions await. First, an overall project director may boost outcomes by drawing attention to NORAD's problems and hence attract industry solutions rather than endless inter-governmental negotiations. Second, perhaps the best example to a competitive bidding environment would be a JSF-like structure where a prime contractor would competitively select the contractors. On this, we would anticipate strong opposition from Canadian politicians with parochial interests in their reluctance to allow an exception to Canada's inefficient offsets program otherwise know as ITBs. Since an overarching Canadian science and technology strategy in defence matters derives from the Key Industrial Capabilities defined a decade ago, the NORAD Modernization project may offer a first real test in assessing how efficient are these KICs.[52]

Further Economic Benefits

There exist several direct and indirect benefits from the NORAD Modernization projects beyond the North American continental security that the modernized system will provide. The following constitute a brief discussion of direct economic benefits obtainable from the construction and installation of Canadian equipment or Canadian-made components of equipment and in-service support of installations and platforms. Indirect benefits will accrue to Canada from development projects in the North that jointly produce benefits to Northern populations in terms of communications, facilities, transport, and jobs.

Federal government's NORAD decisions will inevitably be heavily influenced by the indirect benefits mostly accruing to Canada's North. If dual-use technologies are used in the architecture of the system as technology progresses, what can and cannot be shared in an open architecture system becomes a more difficult policy issue. For instance, if sensors are built as capable of dual use

by military/civilian government agencies, additional value will be generated beyond defence, contributing data for use across the government and possibly in industry. This in itself is one of the private goods produced by the NORAD modernization investments. Moreover, a second economic case for NORAD Modernization can be made based on defence investments into northern infrastructure not only benefiting Indigenous communities but also connecting soon-to-be navigable Northwest Passage to the mainland. Perhaps, a third such benefit would arise if NORAD assumed a maritime warning mission given that the Arctic may slowly be opening to traffic. Since a navigable Arctic will necessarily boost both commercial and passenger traffic, the former in competition with Russian Arctic already with infrastructure, potential environmental threats, such as spills and overuse will arise. If the underwater multi-mission sensors were designed to detect such non-military threats, the cleaner environment, whether due to actual interventions based on detections or by mere deterrence of spills, would generate local public goods as joint products.[53] Finally, Canada's procurement of SPY-7 radars, and the role of Canadian Joint Operations Command (CJOC) working with partners and the commercial sector in providing sensor data as a potential model.

The capabilities of the new NORAD, meaning the new installations equipped with multi-mission sensors within an open architecture framework, may be shared with American and Canadian civilian industries, a large potential benefit will be generated for communications and transport facilities for Northern communities. Moreover, in addition to the deep-water ports under development in Iqaluit, Pond Inlet, and Qikiqtarjuaq, the project may require several more further west along the Northwest passage, not only benefiting the Northern communities but also Canada's sovereignty claims.

Space-based sensors require the right orbit to be effective. The current technology and the industrial capabilities permit a short time frame for the launch of this space component of the SHIELD of the U.S. Air Force that is envisaged as a component part of JADC2. Yet, General Dynamics' TSaaD is fulfilling similar functions. This strongly suggests Canadian companies' or Canada-based U.S. subsidiaries' involvement in the satellite communications aspects of the NORAD Modernization project. As explained above in Figure 1, from a C2 perspective LEO is thought to be the right orbit with its low latency in communications. These are all areas where Canadian industries seem to be excelling.

The critical improvement in the New NORAD is the requirement that the all-domain awareness, C2, and defeat capabilities are integrated and as autonomous as possible without taking human C2 decisions out of the loop. This would allow a seamless 'kill chain' without complete autonomy. That extreme, i.e. taking the human decision off line, reminds one of the mutually assured destruction (MAD) scenario of the 1950s into 1960s, and might remove the flexible response from the set of feasible options. This aspect of the NORAD Modernization is a sensitive political issue in Canada with the rejection, in 2005, of Canada's involvement in ballistic missile defence. However, Russia's invasion of Ukraine seems to have upended a new debate on the issue and NORAD's defeat mechanisms may gain easier acceptance in the Canadian public debates. We note, in Appendix B, the potential involvement of Canadian industries in this offensive deterrence capability.

Canada possesses industrial capabilities to engage across the spectrum of JADC2 development. For instance, General Dynamics' TNaaSD is a version developed for the Canadian Army. However, lower Canadian threat assessment and political will, and the sticky procurement practices, may place Canadian industries at an immediate disadvantage relative to their American counterparts. Moreover, pandering to industries and regions may hinder industry from actively participating in JADC2 partly due to weaker willingness to spend in defence.[54] However, the significant private benefits of this project might convince many on its local infrastructure and technological benefits. For instance, using dual-use technologies, this infrastructure project may connect Canadians to the digital economy across the vastness of the country. Remote communities in the North will particularly benefit from this infrastructure, especially from connectivity facilitated by new space-based assets feeding data to JADC2. For example, this connectivity with dual-use may well bring high-speed internet communications to northern communities.[55]

Data integrity proves critical both for the deterrence objective within NORAD but also potentially further uses of the infrastructure. This depends on whether sensors communicate safely and reliably amongst themselves within smaller loops as well as between layers so that all-domain awareness capability is not compromised.[56] Given the sophistication of adversaries, the ubiquitous need of information sharing across layers as well as within layers requires building cyber secure environments. If the current radar stations are upgraded and new ones added further north onto Canadian Arctic archipelago, beyond facility building and maintenance work, the work on the actual layered sensor network will require work by several of the sectors identified as KICs.

Regarding the JADC2 or the digital communications, AI and software design technologies, there seem to exist two policy challenges. First, the relevant high-technology non-traditional industries' full participation in NORAD Modernization, a defence project, may require incentives to join JADC2 development. This also means, as the second policy challenge, finding a solution to American security classification processes that act as a barrier to participation. How can Canadian companies receive appropriate classifications in a timely manner that allows for their participation whilst preserving the protections that these classifications offer? This may require adjustments to the NORAD Modernization project in somewhat similar ways to the JSF project where companies from participating countries can bid for contracts. The Canadian government will therefore swiftly engage with American authorities to allow for enhanced data and technology sharing between American and Canadian players in a less burdensome fashion.

Design Considerations for Canadian Industry

Assuming that Canada may not be interested in anti-missile kinetic interceptors as defeat mechanisms, there will still be plenty of opportunities for Canadian defence and security industries elsewhere in the project. The multi-layered sensor network requires many types of multi-mission sensors and communication links within and across layers. Moreover, layers will include such platforms for sensors as satellites and drones that the industry will find challenging to design and manufacture. Finally, JADC2 capabilities will require not only communication requirements but also artificial intelligence[57] capabilities to speed up the data processing, information transmission and, at times, autonomous decision-making.[58]

Given the emerging technologies from NORAD's science and technology (J8) section, related Canadian industries will be compelled to intensify their Research & Development (R&D) activities as the new network will have to be at the frontiers of technology and they have to compete against the corresponding American firms. Clear government guidance and policy can help direct and prioritize these R&D activities by providing clear threat assessments so that the industry can understand the industrial targets and, if necessary, follow industrial R&D policies within the parameters of the North American trade agreements. For instance, cruise and hypersonic missiles are umbrella terms for a wide variety of weapons and there exists evidence that a certain potential exists in Canada for the industry to reorient itself to participate in that market's activities.

From small business perspective on NORAD's modernization, the major challenge will consist of integrating smaller components into the larger architecture supporting NORAD. Though there will be plenty of such opportunities through an open architecture for NORAD Modernization, access by small firms will have to overcome some informational barriers on what exactly the project requires. This would require a technology infrastructure with specifications that are public as opposed to proprietary. Such an open architecture will also benefit the technological capabilities at large by enabling a wider range of businesses to refresh NORAD's capabilities continuously. Small Canadian businesses should be looking at non-kinetic defeat mechanisms such as electronic warfare and signals technology where Canada possesses a robust Cyber Resilience industry, another KIC.

Layer Upon Layer

Deterrence being the goal of NORAD Modernization, enhancing NORAD's deterrence by denial – its ability to block an adversary from achieving its objective – was a necessary part of increasing the overall credibility of its deterrent. Layering sensors along the approaches to North America is the first element of deterrence by denial. NORAD can achieve this objective with at least three layers of sensors for a starter (as illustrated in Figure 3 above), granting the command its all-domain awareness capability.

The farthest layer, spatially speaking, is composed of space-based sensors, providing NORAD a vantage point from 'the highest of high grounds.' However, as explained above, the satellite constellation will use LEO, the closest orbit in near-Earth space responding to the lowest latency requirement. The second layer is made up of forward deployed sensors like UAVs and ISR aircraft. The third layer is terminal sensing by dedicated systems, including the High Arctic expansion of the NWS and modernization of the existing sensor installations. Finally, particularly against submarine incursions, underwater sensors will form the final layer. The benefits of layered sensors are that they allow NORAD to be more conservative with its expensive kinetic interceptors but more sensors place greater coordination demands on NORAD's JADC2. The better the JADC2, the more layers of sensors could be added to NORAD. From satellites to aircraft to Arctic sensor installations, domestic industries should be able to bid successfully given the fact that Canadian KICs include Aerospace Systems and Components, Sonar and Acoustic Systems, Aerospace Systems and Components, and Space Systems. Moreover, AI and in-service support capabilities may augment domestic industry participation. Industry needs to invest in data sciences, which in this case extends from multi-mission sensors' data collection capabilities to communications, their security, and the processing of information at appropriate levels before processed information becomes available to commanders, to boost JADC2 capability by additional layers of sensors.

Offensive Deterrence Capability

The aim of JADC2 with current technology was to enable 'engage on remote' in military jargon, making the most of the defeat mechanisms that NORAD already has. The layered sensor network can tell a fighter to shoot its missiles early at a target, beyond that aircraft's radar coverage, so that the missile's maximum range is the point of intercept. This 'engage on remote' capability not only extends the effective range of the weapon, it also introduces more layers and greater effectiveness. This 'engage on remote' capability, strengthened by AI pulling data from as many sensors in the network as possible can achieve the 'best sensor, best shooter' offensive deterrence capability which, in turn, can generate a deterrence by denial effect. Canadian industries, from AI to sensors and various platforms might find a niche in this familiar terrain as several of them are at the frontiers of technology just as the Canadian aerospace sector found several niche areas in the JSF project.

Data demands are likely to shape how JADC2 evolves. The 'Five Eyes' intelligence community and NATO all have capabilities that can contribute to JADC2's global all-domain picture. The sharing of data between allies brings with it the challenge of contributing to the maintenance and updating of architecture across JADC2. A good model for this future burden sharing can be found in the American nuclear command and communications (N3) world, as the different services invest appropriately across N3 to maintaining and renewing the nuclear deterrent.

The second element of deterrence by denial is the layered 'shoot-assess-shoot' doctrine developed by the U.S. Air Force. This concept can be expanded to include the space domain and non-kinetic defeat mechanisms. Since non-kinetic defeat mechanisms are adjacent to Cyber Resilience, another KIC, as an area in which the relevant KICs should take greater interest. Non-kinetics are critical and must work in tandem with kinetics in a layered fashion, presenting enough uncertainty to an adversary as to which deterrent might be used to deter their first attack. The technology to integrate kinetics and non-kinetics does not yet exist, but if detection, identification, and tracking

improve, non-kinetics can be used to save expensive interceptors. Used in a shoot-assess-shoot doctrine, 'non-kinetics become magazine extenders.' Non-kinetics may thus enable the Modernized NORAD to reduce the costs of deterring BMDs, cruise missiles to UAVs. The technology might develop to allow NORAD to choose whether to commit a kinetic defence at all, relying solely on non-kinetic solutions to achieve a kill.

More Than Missiles for Canadian Industries

Whilst Canadian defence industries have no capability to produce kinetic defeat mechanisms, the industry may still contribute as sub-contractors by seizing one of the major opportunities for participating in defeat mechanisms. First, industry can develop the sensor and communication links that are essential to enabling defeat mechanisms over the near-term time horizon as, after all, the Canadian-made optical systems of the Turkish-made Bayraktar UAVs effectively used in the war between Armenia and Azerbaijan by the Azerbaijanis as well as by Ukrainians against the current Russian invasion. Second, industry can continue investing in non-kinetic defeat mechanisms. Focusing on electronic warfare and signals, this technology has the capacity to grow with time from being 'magazine extenders' to likely the primary method of defeating incoming fire outright. Lastly, Canadian industries can pursue the development of direct energy weapons to be directed towards guidance mechanisms of the incoming hypersonic missiles. While not a near-term solution for NORAD, such mechanisms can be integrated into NORAD's evolving layered defeat mechanisms in the long term. Pursuing all of these defeat mechanism options, industry must remain cognizant of how their solutions will thin the volume of incoming fire through NORAD's renewed layered defence and thus generate a deterrence by denial effect.

The spectrum of JADC2 requirements presents an excellent opportunity to bring Canada's diverse advanced technology industry – a non-traditional defence player – into the process. While larger Canadian technology companies specialize in network communications and telecommunications, many smaller- and medium-size advanced technology firms work in quantum computing, data analytics, and AI – the very technologies that will enable JADC2.[59] Since they will need to collaborate with the Canadian and American governments to qualify, non-traditional defence companies will have to acquire the appropriate security classifications necessary to participate in bidding for various components of the project. To reiterate, since the NORAD Modernization project will be a joint U.S.-Canada endeavor, it is likely to be run like the JSF project.

Summary and Further Work

If the Canadian procurement practices were to provide us an indication, one would have expected an incremental process rather than a full-blown open architecture for an effective JADC2 capability. However, since the project is bilateral with U.S. and an urgency to complete the project exists, the process may take a test-build-test path with experimentation. Since open architecture allows for 'plug and play' of various components across the entire system, this experimentation can proceed. Now that the political realities have become more conducive to NORAD Modernization upon Russia's invasion of Ukraine,[60] another reason why the project can progress faster is the high likelihood that Canada cannot impose its inefficient and delay-prone offsets or ITB policy, due to the bilateral nature of NORAD. One might expect a JSF (Joint Strike Fighter) type program where a prime contractor will choose the best builders and the equipment technologically specified for the project rather than politically divided up contracts awarded to satisfy politically tainted industrial policy objectives.

As we described above, the project may provide civilian communications networks by dual-use sensors and other benefits to Northern communities such as telemedicine over the broadband networks. On a wider scale, the massive amounts of data collected by sensors will also have civilian applications. For example, weather data inform the insurance industry by offering predictive data on storm damage and other weather events. Moreover, underwater sensors may collect data on the

health of the environment and, together with the other sensors in the system, real-time information on polluters, transiting ships once Northwest Passage becomes navigable.

Here are two examples of how the challenge of sharing data with the civilian world could be managed. Operation Olympic Defender[61] brings together allies to provide joint C2 for space. Data is pooled from and shared across multiple allied communities. The space community also has the Unified Data Library (UDL) that captures data on space objects. The UDL classifies and partitions this data, allowing for those with the requisite security clearances to draw from it as needed. Data sharing increases the risk of compromising JADC2 but in terms of data security, industry might want to learn from banks and credit card companies that securely handle tremendous volumes of financial transactions. To prevent financial data from being exploited, these companies take two measures. First, they segment their data so that segments have to be correctly combined for complete pictures. Second, they rely on Robotic Process Automation (RPA) to process vast amounts of data, freeing up people to do other things. Similarly, NORAD must pursue segmented data and RPA to transport and process data for JADC2.

While JADC2 can be applied across the globe, users should be able to customize their interface at the tactical level to give them the data they need, tailoring needs to match geographic demands. The industry must make the architecture modular so that users can tailor JADC2 for specific missions yet, on the downside, excessive customization adds to the complexity of the system, running the risk of inhibiting decision-making.[62]

This paper is just a preliminary study of the private benefits for Canada from NORAD Modernization. First, we have not included any study of the private benefits to the U.S., thinking that NORAD means so much more to U.S. in terms of the public good it provides, i.e. by deterring the incoming missiles, which the U.S. private benefits are not strong enough to matter for U.S. decisions. Second, our study of the Canadian industries capable of bidding for components of the project is rather cursory. A deeper analysis may provide more precise and policy-relevant information to the federal government regarding the benefits from technology transfers as well as more immediate benefits in terms of contracts likely to be obtained by Canadian companies that exhibit comparative advantages. In this regard, several further questions about the Canadian-ness of Canadian defence contractors arise. For one, a significant number of Canadian defence contractors are subsidiaries of American contractors. The structure of the industry, mostly 2nd and 3rd tier contractors to major American prime contractors, can be traced back to Production Sharing Agreements of the two countries in the 1950s. This matters significantly in terms of technology transfers as potentially providing significant private benefits but that some emerging solely Canadian firms not being able to seamlessly accessing advanced technology not have access to some of the technology transfer. Moreover, this technology transfer issue may necessitate the formation of a consortium in order to assure the security of technology transfers, which might concern particularly the U.S. given the strategic competition with China. Finally, as a separate but related issue, a further study of the implications of JADC2 and the new NORAD hardware on the future requirements for Canadian Armed Forces would be suggestive in terms of defence budget allocations as defence spending will be inching up towards NATO's 2% benchmark.

Notes

1. Fergusson (2020), Budning et al. (2021a).
2. Jenkins (2013).
3. Heal et al. (2002) introduced the concept of interdependent security.
4. Further rivalry or publicness issues will arise for the non-security joint products, to be discussed in Part 3. Charron & Fergusson (2020).
5. Berkok et al. (2023), Fetterly & Solomon (2021).
6. Verklan (2021).
7. RADA (2020).
8. Anticipated to be a low-earth orbit (LEO).

9. Labbé (2020b), Lamont et al. (2011), Lackenbauer & Bouffard (2021).
10. Brockmann and Schiller (2022), Kunertova (2022).
11. Bouffard and Lajeunesse (2022).
12. Csenkey and Genest (2021), Ball et al. (2016), CDAI (2020a).
13. Budning et al. (2021b).
14. Acoustic multi-mission sensors.
15. Labbé (2020b).
16. Labbé (2020a).
17. Brown (2014).
18. Shoot-assess-shoot doctrine is 'a defensive plan that entails shooting one interceptor and assessing its success before firing others obviates the need to fire large salvos of very expensive interceptors. This "shoot-assess-shoot" doctrine led to the MDA's concept of early intercept, emphasizing the first intercept attempt during the first half of the threat's flight path. Unfortunately, such an approach necessitates tracking sensors and interceptor launch sites well forward of the defended area (or in space).' Corbett (2013); also in Russell (2021).
19. Corbett (2013).
20. RADA 2020.
21. Software-Defined Network (SDN): Such a network exhibits an architecture that the network can be centrally controlled or 'programmed,' using software applications. This enables C2 to manage the network consistently with the strategic objectives in mind.
22. These industries would be artificial intelligence, cyber resilience, sonar and acoustic systems, and electro-optical /infrared (EO/IR) systems (Jenkins 2013; Jones and Perron 2022; White 2022).
23. CRS (2022b), McDonald (2020).
24. Lamont et al. (2011).
25. Footnote 15.
26. Lamont et al. (2011).
27. A kill chain consists of detecting, identifying, and stopping adversary activity.
28. CDAI 2020c.
29. Russell (2021), Sherman (2021), Verklan (2021).
30. CDAI 2020b.
31. CRS (2022a).
32. Pope (2020).
33. White (2022).
34. The Joint All-Domain Command & Control (JADC2) is the U.S. initiative to replace the current domain and control systems with one that connects the existing sensors and shooters, i.e. commanders in control of defeat mechanisms, and distribute the available data to all domains (sea, air, land, cyber, and space) and forces that are part of the U.S. military. The system originated in the U.S. Air Force. Through NORTHCOM it will be adapted to the Modernized NORAD.
35. CDAI 2020b.
36. Building in High Arctic and generating energy will require technological innovations.
37. Charron et al. (2019).
38. Labbé (2020a).
39. Cho (2020).
40. Charron et al. (2019), Anand (2022), Raymond (2022), Raymond & Munier (2021).
41. Brewster (2021), Chase and Fife (2022), Gilmour (2021), Glesby et al. (2021), Ibbitson (2022), Kieley (2021).
42. Berthiaume (2022).
43. Budning, Wilner, and Côté (2022).
44. Csenkey and Genest (2021).
45. Csenkey and Genest (2021).
46. Berkok, Secrieru, and Peyrow (2023).
47. Austere environment advanced construction materials in High Arctic as well as deep-water ports in the Arctic.
48. Mallory (2018).
49. See Appendix A listing the KICs and, in particular, describing those directly relevant to the Modernized NORAD.
50. At the time of writing the first draft of this paper about a year ago, the world may have entered what some are terming as 'post-post-Cold War' era with Russia emerging, beyond any reasonable doubt, as a belligerent military power with a powerful nuclear arsenal. Moreover, the self-proclaimed 'Near-Arctic' China's Arctic interests and activities are rising unabated.
51. Mason (2022).
52. Appendix A draws attention to those KICs that are most technologically relevant to the transition.
53. Droff & Malizard (2020), Engerer (2011).
54. See footnote 28.
55. Davis (2022), Dean (2022), Haney (2020).

56. Hare and Goldstein (2010).
57. Canada is ranked 5th amongst 29 top countries in AI by Stanford University's Global AI Vibrancy index, https://aiindex.stanford.edu/vibrancy/ (accessed 23 December 2022).
58. Appendix A describes industries competing in these markets. For instance, Electro-Optical/Infrared (EO/IR) Systems and Cyber Resilience sectors.
59. CDAI (2020b).
60. As well as China's hardening stance on Taiwan.
61. A U.S. Strategic Command effort to cooperate with America's closest allies in space. Under Operation Olympic Defender, America is leading a coalition of allied space-faring nations to work together to deter hostile acts in space, strengthen deterrence against hostile actors and reduce the spread of debris orbiting Earth.
62. CDAI (2020b). Also see Raymond (2022).
63. Jenkins (2013). We note that the 17th capability, Clean Technology, has just been added.

Acknowledgments

We gratefully acknowledge very relevant, extensive, and constructive comments from the referees. Moreover, we thank the significant research assistance by Lt(Navy) Kevin Kodis to Part 3 of the paper entitled Canadian industrial participation and potential private benefits.

Disclosure statement

No potential conflict of interest was reported by the author(s).

Funding

This article benefited from funding by Defence Research and Development Canada (DRDC) under research grant 2022-11246.

References

Anand, A. 2022, "Minister of National Defence Announces Canada's NORAD Modernization Plan", Accessed December 25, 2022. https://www.canada.ca/en/department-national-defence/news/2022/06/minister-of-national-defence-announces-canadas-norad-modernization-plan.html.

Ball, M. G., B. Qela, and S. Wesolkowski. 2016. "A Review of the Use of Computational Intelligence in the Design of Military Surveillance Networks." DRDC-RDDC-2015-P046, Accessed March 21, 2022. https://www.researchgate.net/publication/291167525_A_Review_of_the_Use_of_Computational_Intelligence_in_the_Design_of_Military_Surveillance_Networks.

Berkok, U. G., O. Secrieru, and K. Peyrow. 2023. *On Distinguishing Defence Inputs in an Alliance – the Case of NORAD"*. forthcoming. Defence & Peace Economics.

Berthiaume, L. 2022. "Canada Weighs Whether to Rejoin U.S. Ballistic Missile Defence of North America." *The National Post*, May 12.

Bouffard, T., and A. Lajeunesse [2022], "NORAD Modernization: Next Steps", *Vanguard*, Accessed November 24, 2022. https://vanguardcanada.com/norad-modernization-next-steps/.

Brewster, M. [2021], "Plan to Rebuild Defence Early-Warning System Means Political, Fiscal Headaches for Trudeau Government", Accessed March 26, 2022. https://www.cbc.ca/news/politics/norad-shield-defence-ballistic-missile-bmd-1.5887192.

Brockmann, K., and M. Schiller [2022], "A Matter of Speed? Understanding Hypersonic Missile Systems", Accessed February 23, 2022. https://www.sipri.org/commentary/topical-backgrounder/2022/matter-speed-understanding-hypersonic-missile-systems?utm_source=phpList&utm_medium=email&utm_campaign=SIPRI+Update+February+2022%3A+SIPRI+at+MSC%2C+hypersonic+missile+systems%2C+avoiding+nuclear+war%2C+the+Anthropocene+and+more&utm_content=HTML.

Brown, J. M. 2014. "Strategy for Intelligence, Surveillance, and Reconnaissance." *Joint Force Quarterly* 72:39–46.

Budning, K., A. Wilner, and G. Côté. 2021a. "Connecting the Dots on Canada's Connected Battlespace." *International Journal* 76 (1): 154–162. https://doi.org/10.1177/0020702021992855.

Budning, K., A. Wilner, and G. Côté. 2021b. "A View from Above: Space and the Canadian Armed Forces." *International Journal* 76 (4): 594–605. https://doi.org/10.1177/00207020211067944.

Budning, K., A. Wilner, and G. Côté. 2022. "From Physical to Virtual to Digital: The Synthetic Environment and Its Impact on Canadian Defence Policy." *International Journal* 77 (2): 335–355. https://doi.org/10.1177/00207020221135302.
CDAI 2020a, "First Report: Domain Awareness & Sensors", NORAD Modernization Forum, Accessed January 31, 2022. https://cdainstitute.ca/norad-modernization-report-one-awareness-sensors/.
CDAI 2020b, "Second Report: Defeat Capabilities", NORAD Modernization Forum, Accessed January 31, 2022. https://cdainstitute.ca/norad-modernization-report-two-defeat-capabilities/.
CDAI [2020c], "Third Report: JADC2/JADO", NORAD Modernization Forum, Accessed January 31, 2022. https://cdainstitute.ca/norad-modernization-report-three-jadc2-jado/.
Charron, A., and J. Fergusson. 2020. "Out of Sight, Out of Mind NORAD Vis-à-Vis CANUS Politics." *Canadian Foreign Policy Journal* 26 (2): 137–151. https://doi.org/10.1080/11926422.2019.1670221.
Charron, A., J. Fergusson, J. Jockel, C. Sands, and J. Sokolsky 2019, "NORAD: Beyond Modernization", Centre for Defence and Security Studies, University of Manitoba, https://umanitoba.ca/centres/cdss/papers/2201.html.
Chase, S., and R. Fife 2022, "Canada to Unveil 'Robust package' to Modernize NORAD, Defence Minister Anita Anand Says", Accessed march 26, 2022. https://www.theglobeandmail.com/politics/article-canada-to-unveil-robust-package-to-modernize-norad-continental-defence/.
Cho, A. 2020. "The Short Weird Life—And Potential Afterlife—Of Quantum Radar." *Science: Advanced Materials and Devices* 369 (6511): 1556–1557. https://doi.org/10.1126/science.abe9362.
Congressional Research Service (CRS). 2022a, "Advanced Battle Management System", https://crsreports.congress.gov. (Accessed March 27, 2022)
Congressional Research Service (CRS). 2022b, "Joint All-Domain Command and Control (JADC2)", https://crsreports.congress.gov/search/#/?termsToSearch=Joint%20All-Domain%20Command%20and%20Control%20JADC2&orderBy=Relevance.
Corbett, M. 2013 March-April. "A New Approach to Ballistic Missile Defense for Countering Antiaccess/area-Denial Threats from Precision-Guided Weapons." *Air & Space Power Journal*, 83–106.
Csenkey, K., and D. P. Genest 2021, "An Opportunity for NORAD Modernization in a Joint CA-US Cyber Component", Strategic Perspectives, North American and Arctic Defence and Security Network, Accessed March 21, 2022. https://www.naadsn.ca.
Davis, C. 2022, "Modernizing NORAD is Key to Supporting Economic Reconciliation in the North", The Globe & Mail, June 23, Accessed December 26, 2022. https://www.theglobeandmail.com/opinion/article-modernizing-norad-is-key-to-supporting-economic-reconciliation-in-the/.
Dean, T. 2022, "Defence Upgrades in Canada's Arctic Should Have Collateral Social and Economic Benefits", Accessed December 26, 2022. https://sencanada.ca/en/sencaplus/opinion/defence-upgrades-in-canada-s-arctic-should-have-collateral-social-and-economic-benefits-senator-dean/.
Droff, J., and J. Malizard. 2020. "Menaces, biens publics et demande de défense européenne." *Revue Défense Nationale* 828 (3): 95–100. https://doi.org/10.3917/rdna.828.0095.
Engerer, H. 2011. "Security as a Public, Private or Club Good: Some Fundamental Considerations." *Defence and Peace Economics* 22 (2): 135–145. https://doi.org/10.1080/10242694.2011.542333.
Fergusson, J. 2020. *Missed Opportunities: Why Canada's North Warning System is Overdue for an Overhaul*. Macdonald-Laurier Institute, Commentary. https://macdonaldlaurier.ca/canadas-north-warning-system-needs-overhaul-new-mli-commentary/.
Fetterly, R., and B. Solomon 2021, "North American Aerospace Defense Command (NORAD) Burden Sharing", Accessed March 26, 2022. https://cradpdf.drdc-rddc.gc.ca.
Gilmour, J. G. [2021], "NORAD: Renewal of the North Warning System by Canada – or Not?" Naval Association of Canada, Backgrounders, Accessed January 31, 2021. https://www.navalassoc.ca/naval-affairs/from-the-past/ .
Glesby, N., D. Kiesman, J. Barclay, and A. Charron [2021], "NORAD Modernization Closed Door Workshop Report", Centre for Defence and Security Studies, https://umanitoba.ca/centres/cdss/papers//2201.html.
Haney, S. 2020, "Low-Earth Satellites Getting Closer to Delivering High Speed Rural Internet", *RealAgriculture*, Accessed December 26, 2022. https://www.realagriculture.com/2020/09/low-earth-satellites-getting-closer-to-delivering-high-speed-rural-internet/.
Hare, F., and J. Goldstein. 2010. "The Interdependent Security Problem in the Defense Industrial Base: An Agent-Based Model on a Social Network." *International Journal of Critical Infrastructure Protection* 3 (3–4): 128–139. https://doi.org/10.1016/j.ijcip.2010.07.001.
Heal, G., H. Kunreuther, and P. R. Orszag 2002, "Interdependent Security: Implications for Homeland Security Policy and Other Areas", Policy Brief #108, Accessed March 26, 2022. http://www.brookings.edu/research/papers/2002/10/defense-kunreuther.
Ibbitson, J. [2022], "In a Dangerous World, Canada is Unprepared on Every Front. It Needs to Come to Its Own Defence", Accessed February 21, 2022. https://www.theglobeandmail.com/politics/article-in-a-dangerous-world-canada-is-unprepared-on-every-front-it-needs-to/.
Jenkins, T. [2013], "Canada First: Leveraging Defence Procurement Through Key Industrial Capabilities", Accessed March 27, 2022. https://www.ic.gc.ca/eic/site/086.nsf/eng/h_00175.html.

Jones, D., and B. Perron [2022], "Joint All Domain Command and Control: Is There a CAF Approach?" Accessed December 19, 2022. https://www.disruptingdefence.com/post/joint-all-domain-command-and-control-is-there-a-caf-approach.

Kieley, M. 2021. "No Umbrella for the Rain: Canadian Implications Following the Global Revolution in Reconnaissance-Strike Technologies." *International Journal* 76 (2): 221–237. https://doi.org/10.1177/00207020211019301.

Kunertova, D. [2022], "New Hypersonic Weapons: Same but Different", Policy Report 20, Network for Strategic Analysis, Accessed December 26, 2022. https://ras-nsa.ca/new-hypersonic-weapons/.

Labbé, P. [2020a], "Cognitive Radars Could Improve Target Engagement Success Rate", SPACOMM 2020, The Twelfth International Conference on Advances in Satellite and Space Communications, Accessed December 17, 2022. http://thinkmind.org/articles/spacomm_2020_1_30_20038.pdf.

Labbé, P. [2020b], "LEO Satellite Constellations: An Opportunity to Improve Terrestrial Communications in the Canadian Arctic", SPACOMM 2020, The Twelfth International Conference on Advances in Satellite and Space Communications, Accessed December 17, 2022. https://cradpdf.drdc-rddc.gc.ca/PDFS/unc372/p813798_A1b.pdf.

Lackenbauer, W., and T. Bouffard. 2021. "The Arctic and North American Defence: Reflections on 2021." *North American and Arctic Defence & Security Network*. https://www.naadsn.ca/wp-content/uploads/2021/12/21-dec-PWL-TJB-The-Arctic-and-North-American-Defence-2021-final.pdf.

Lamont, L., et al. [2011], "Tiered Wireless Sensor Network Architecture for Military Surveillance Applications", *SENSORCOMM 2011 : The Fifth International Conference on Sensor Technologies and Applications, Proceedings*, Accessed March 23, 2022. https://www.researchgate.net/publication/268350779_Tiered_Wireless_Sensor_Network_Architecture_for_Military_Surveillance_Applications.

Mallory, K. [2018], "New Challenges in Cross-Domain Deterrence", RAND Corporation, Accessed February 21, 2022. https://www.rand.org/search.html?query=New+Challenges+in+Cross-Domain+Deterrence.

Mason, G. [2022], "Russia Has Designs on the Arctic. How Will Canada Respond?", Accessed March 30, 2022. https://www.theglobeandmail.com/opinion/article-russia-has-designs-on-the-arctic-how-will-canada-respond/.

McDonald, G. [2020], "NORAD at the Crossroads", KPMG, Accessed December 26, 2022. https://home.kpmg/ca/en/home/insights/2021/01/norad.html.

Pope, C. [2020], "Advanced Battle Management System Field Test Brings Joint Force Together Across All Domains During Second Onramp", Accessed March 27, 2022. https://www.af.mil/News/Article-Display/Article/2336618/advanced-battle-management-system-field-test-brings-joint-force-together-across/.

RADA [2020], "Tactical Multi-Mission Sensors in the Defense Environment", Accessed March 21, 2022 https://radausa.com/blog/multi-mission-sensors.

Raymond, C. [2022], "New Technologies, Climate Change and War in Ukraine: What Impacts on NORAD Modernization?", Policy Report 16, Network for Strategic Analysis, Accessed December 26, 2022 https://ras-nsa.ca/new-technologies-climate-change-and-war-in-ukraine-what-impacts-on-norad-modernization/.

Raymond, C., and M. Munier 2021, "Continental Defence Modernization and the Future of Canadian Defence Policy", Policy Brief 13, Network for Strategic Analysis, Accessed December 26, 2022. https://ras-nsa.ca/continental-defence-modernization-and-the-future-of-canadian-defence-policy/.

Russell, S. A. [2021], "Diverging Objectives - Maintaining Strategic Stability with Russia While Expanding Global Missile Defense", Wright Flyer papers, Air University Press, Accessed March 21, 2022. https://www.airuniversity.af.edu.

Sherman, J. [2021], "Forging a SHIELD for the Homeland", Accessed March 26, 2022. https://www.airforcemag.com/article/forging-a-shield-for-the-homeland/.

Verklan, C. [2021], "NORAD Modernization: Considering the Threat of Small UAS to (Integrated) Air and Missile Defence", Policy Primer, North American and Arctic Defence and Security Network, Accessed January 31, 2022 https://www.naadsnca.

White, J. [2022], "Joint All Domain Command and Control Data Driven Decision Making", Accessed December 19, 2022 https://vanguardcanada.com/joint-all-domain-command-and-control-data-driven-decision-making/.

Appendix A

Canada's 17 Key Industrial Capabilities[63]

(***Bold+Italic*** industrial capabilities are likely to be in contention to bid for NORAD Modernization contracts.)

Emerging Technologies

- ***Advanced Materials***
- ***Artificial Intelligence***

Artificial Intelligence (AI) spans a range of technologies that allow machines to execute tasks that normally require human intelligence, such as pattern and speech recognition, translation, visual perception, and decision-making. AI develops or draws on disciplines such as search and mathematical optimization, machine learning, deep learning, self-learning, and neural networks. AI can reduce operator workload and automate easily repeatable tasks that otherwise require significant human involvement. AI promises enhanced efficiency in the use of trained personnel, less exposure of humans to dangerous environments, and more rapid responses to changes in the military operating environment. It can also permit the analysis of large volumes of data in support of intelligence analysis, mission planning and rehearsal, logistics and business management, cyber security and resilience, and many other activities. AI is relevant across a broad set of both defence and non-defence domains.

- ***Cyber Resilience***

Cyber resilience spans every element of the domestic commercial, civil, and national security sectors and addresses the vulnerabilities created by the expansion of information technology and the knowledge economy. Activities in this segment include design, integration, and implementation of solutions that secure information and communication networks. These and other technologies should focus on achieving effective development of the following cyber capabilities:

- **Information security**

The practice of defending electronic and digital data and information from unauthorized access/intrusion, use, disclosure, disruption, modification, perusal, inspection, recording, or destruction;

- **IT security**

Secure content and threat management (endpoint, messaging, network, web, and cloud), security, vulnerability and risk management, identity and access management and other products (e.g. encryption/tokenization toolkits and security product verification testing), and education, training services and situational awareness;

- **Operational technology (OT) security**

Monitoring, measuring, and protecting industrial automation, industrial process control and related systems. Cyber resilience may involve the development of tools and the integration of systems and processes that permit hardening of tactical systems or broader networks, encryption, cyber forensics, incident response, and others. Capabilities developed in this domain may increasingly draw on AI as an enabling technology; for example, networks may autonomously and dynamically defend against intrusions and repair themselves if disrupted.

- ***Remotely-piloted Systems and Autonomous Technologies***

These are platforms and systems, which make use of autonomous machine operations, including completely unmanned aerial, marine, or ground vehicle systems, and employ AI technologies to enable increasingly autonomous operations in both the military and commercial domains. These technologies rely on various forms of artificial intelligence, including (but not limited to) machine learning, self-learning, and neural networks, in order to increase operational speed or duration, reduce operator exposure to dangerous environments, and enhance overall mission effectiveness.

- ***Space Systems***
- Earth Observation Software Applications

Software and value-added services leveraging terrestrial satellite imagery and geospatial information. These solutions may be developed for a variety of applications, including navigation, surveillance and intelligence gathering, mapping, climate observation, or other military or civil purposes. These solutions may increasingly draw on capabilities contained in the AI domain to autonomously process data and execute preliminary analysis.

- Satellite Systems

Design and manufacture of a wide array of satellite and other spacecraft sub-systems encompassing both space and ground segments. These include (but are not limited to) satellite buses, communications or imagery payloads, propulsion and power systems. Critically, this category also spans the ground control infrastructure needed to operate satellites and manage the data they produce.

Leading Competencies and Critical Industrial Services

- ***Aerospace Systems and Components***

Design, fabrication, assembly, and integration of aircraft structural elements, control surfaces, systems, sub-systems, parts, and components of manned aerial platforms, and complete manned aerial platforms. This includes the following systems and components: landing gear (e.g. wheels, shock absorbers, and related parts for the retraction and extension of aircraft landing gear, helicopter pontoons); flight control actuators; avionics; and propulsion and power systems for military aircraft (e.g. aircraft gas turbine engines, compressors, and fuel systems).

- Armour
- *Defence Systems Integration*
- *Electro-Optical/Infrared (EO/IR) Systems*

Design, manufacture, and integration of electro-optical and infrared systems for surveillance, reconnaissance, night vision, and targeting. This category also includes components and assemblies that significantly drive system capability, as well as software that enhances system performance or contributes to superior exploitation of collected sensor information. Applications for these systems are either military or civil, and feature in multiple media, including airborne platforms, satellites, ground vehicles, ships, and submarines, or in fixed infrastructure.

- Ground Vehicle Solutions
- *In-Service Support*
- *Marine Ship-Borne Mission and Platform Systems*
- Munitions
- Shipbuilding, Design, and Engineering Services
- *Sonar and Acoustic Systems*

This includes the design, manufacture, and integration of sonar and/or acoustic systems used for navigation, surveillance, fire control, survey, scientific, and other purposes, both military and civil. This spans both the 'dry side' signal processing and system management capabilities, and the 'wet side' sensor arrays.

- Training and Simulation
- Clean Technology

Appendix B Defence & security companies likely to bid in NORAD Modernization project

A relevant subset of Top 100 Canadian companies 2022 (Canadian Defence Review, https://www.canadiandefencereview.com/2022-top-100-defence-companies) are listed below and classified into KIC in Table A1.

(1) **Lockheed Martin Canada**
Surveillance/detection capabilities like the SPY-7 radar (capable of tracking multiple sophisticated ballistic missile threats).

Table A1. Canadian defence & security companies as potential bidders in NORAD Modernization.

	Emerging technologies				Leading competencies and critical industrial services		
	Artificial Intelligence	Cyber Resilience	Remotely-piloted Systems & Autonomous Technologies	Space Systems	Aerospace Systems & Components	Electro-Optical /Infrared (EO/IR) Systems	Sonar & Acoustic Systems
Satellites			09	19			
UAVs			18				07[58]
Communications							
Sensors	13		05	12			23
Data analytics				17	15		22
Mission software		02	06		21	16	11
ISR		14		01			
Forensics/ detection		19	04				20
Advanced materials							07

(2) **L3Harris Technologies Canada**
Capabilities in air/land/sea/space/cyber/multi-domain environments: Missile warning anddefence (including space-based), signals intelligence systems, defensive cyber systems (Agile Guardian).

(3) **Chantier Davie Canada**
Building/maintaining Canada's polar icebreaker fleet.

(4) **MDA**
Robotics, satellite systems, geo-intelligence, Glide Phase Interceptor.

(5) **Raytheon Technologies**
OTH-radar, C2 systems, C4ISR network, JADC2 architecture.

(6) **General Dynamics Mission Systems**
Canada TNaaS (Tactical Network as a Service), C4ISR, and defence electronics producer.

(7) **IMP Aerospace & Defence**
In-service support for airframes and platforms, structural/electronic manufacturing capabilities in air land sea and space domains.

(8) **Irving Shipbuilding**
Shipbuilder frigates (Canadian Surface Combatants).

(9) **QinetiQ Group Canada**
Defence and aerospace technical expertise, R&D, test & evaluation, engineering solutions, training & assurance.

(10) **Airbus**
Earth observation data and services to government, military and commercial users. Geostationary telecommunications satellites to Telesat (satellite operator in Ottawa). Military satellite communication terminal equipment/secure communications services.

(11) **Kraken Robotic Systems**
Underwater imagery/sonar, underwater unmanned systems.

(12) **Kongsberg Geospatial**
Works with Canadian Space Agency in developing real-time C2 systems for the Artic via satellite sensors. RAVENS tool: Provides unclassified, multi-domain situational awareness and communications to support SAR/sovereignty/ humanitarian and disaster relief efforts.

(13) **ATCO Frontec**
Real-life support/operation and maintenance, heavily involved with the NWS.

(14) **Contextere**
Data extraction, AI, natural language processing to deliver actionable intelligence for front-line service workers (potential in-service support applications).

(15) **RaceRocks**
Traditional/e-learning/VR/AR/media/story/game-based training development tools, data analytics for aerospace defence.

(16) **Avalon Holographics**

Holographic Display Company provided the RCN with display for hunting submarines.

(17) **Terris (formerly 3D Planeta)**
Collates data (visual, UV/IR, radar, LIDAR, sonar) from space, air, ground, and sea (above/sub surface) for monitoring purposes.

(18) **Cleeve Technology**
Aerospace/defence electrical interconnectivity solutions.

(19) **Sapper Labs Cyber Solutions**
Cyber defence projects: Cyber attribution capability in defence operational setting, detection of advanced threats.

(20) **GeoSpectrum Technologies**
Developer of underwater acoustic detection systems.

(21) **Magellan Aerospace**
Rockets/rocket propellant potential for missile defence capabilities.

(22) **Global Spatial Technology Solutions**
OCIANA DND's maritime portion of NORAD Modernization Program and pursue DND's Defence Enhanced Surveillance from Space Project procurement opportunity." AI/big data analytics tools in a maritime environment

(23) **D-TA Systems**
Radio, radar, communications, sonar and test and measurement applications for the defense, aerospace and wireless markets, acoustic signals, high-speed networks, real-time recording and playback, multi-core software processing, sensor processing with separation of signal acquisition and processing over long distances, permitting signal digitization.