CDA INSTITUTE

NORAD MODERNIZATION FORUM

FIRST REPORT

AWARENESS & SENSORS

Introduction

The CDA Institute, in partnership with NDIA and NORAD/USNORTHCOM hosted a three-part virtual roundtable focused on NORAD modernization. The goal was to allow experts from industry, academia, and government to break down silos and engage in direct conversations about North American continental defence challenges and what form NORAD modernization might to address them. The forum was created to imagine the art of the possible. More specifically, the goal of these three events were to identify security gaps and brainstorm actionable solutions to the issues identified during the discussions.

- **12 August 2020: Domain Awareness/Sensors**
- **26 August 2020: Defeat Capabilities**
- **9 September 2020: JADC2/JADO**

This report is focused on the first of these three events and will be followed up by two upcoming exposés of the conversations that took place during the subsequent panels.

The Domain Awareness / Sensors event was 2 hours in length and took place on 12 August 2020. **NORAD Deputy Commander L. Gen Pelletier** provided introductory remarks. This was followed by a white paper overview from **Dr. Thomas Walker** of Lockheed Martin. Director of the Centre for Defence & Security Studies and University of Manitoba's, **Dr. Andrea Charron** served as a guest speaker, providing an overview and context for the discussion that would follow. Director, Operations for NORAD HQ, **Brig Gen Pete. M Fesler** also helped set the scene with a short presentation. Following this, **LGen (Ret'd) Guy Thibaut**, Chair of the CDA Institute moderated a panel discussion on awareness and sensors with several industry representatives. The panel consisted of:

- **Sunil Chavda**, Director, New Satellite Systems Development, Telesat Canada
- **Ravi Ravichandran**, Vice President, CTO BAE Systems
- **Mike Walsh**, Chief Engineer, Radar and Sensor Systems, Lockheed Martin
- **Jerome Dunn**, Chief Architect, NG Counter Hypersonics Campaign Launch & Missile Defense Systems, Northrop Grunmman
- **Mark Rasnake**, Boeing

The following report will outline the major points of consensus and contention reached by participants during the webinar, a backgrounder on the case for NORAD modernization, sections on obstacles to renewal, all domain awareness requirements, design considerations for Canadian industry, and data plans. This report was created by the CDA Institute and is intended to read as an overview of the key points made by our invited experts. The report was produced by rapporteurs from the North American and Arctic Defence and Security Network (NAADSN), a Department of National Defence MINDS Collaborative Network.

Executive Summary

NORAD's defences are challenged by advanced new weapons like hypersonic glide vehicles. These new weapons have proliferated across all military domains, designed to threaten North America and place its political autonomy and financial stability at risk. North American homeland defence needs to modernize to meet these new threats. A major component of this new thinking is the development of All Domain Awareness capabilities provided by a multi-layered sensor system (an ecosystem) that can detect, identify, and track these and other new threats at great distances and provide the right information to the right assets at the right time.

High financial costs and tight timelines are major obstacles to NORAD implementing an All Domain Awareness capability. These factors necessitate an approach to All Domain Awareness that emphasizes the technological readiness levels of industry. What 'off the shelf' technology is available that can be modified and brought to bear quickly?

Experts from across the defence industry elaborated on the design of the multi-layered sensor system that will enable a future All Domain Awareness capability. Sensors should be multi-mission, able to detect, identify, and track more than one threat from "birth to death". These sensors should be modular, scalable, and software-defined with an open architecture for quick adaptability and upgradability. Throughout the discussions, the need to integrate these multi-layered sensors into a holistic system was emphasized. The goal is to create All Domain Awareness that seamlessly converges with renewed Command and Control (C2) and defeat capabilities to enable NORAD's deter, detect, and defeat mission.

Many decisions have yet to be made that will drive the design of the multi-layered sensor system. Where should these sensors be placed that provides the best coverage? Furthermore, the data this system provides will be valuable and could be partly shared with allies and industry. How can industry ensure the integrity of this data? Lastly, where and how does human decision-making come into a largely autonomous system.

Points of Consensus

- All Domain Awareness is paramount to enabling NORAD's deter, detect, defeat mission.
- A renewed multi-layered system will be a combination of new, old, and repurposed equipment.
- Solutions will favour "off the shelf" technology that can be modified and upgraded.
- Most of the sensor technology to meet NORAD requirements exists today or will shortly.
- The system must have seamlessly layered sensors to detect, identify, and track full spectrum of threats across All Domains, from ballistic missiles to advanced hypersonic glide vehicles to cheap aerial drones.
- Data must be shared widely to be effective, but policy must be developed to ensure that information can be shared to the right people at the right time.
- Multi-layered sensors should be able to detect and identify a threat at its 'birth' and track until its 'death.'
- The Arctic poses unique challenges for remote ground-based sensors and space-based sensors in polar orbits.
- The NWS is nearing its end of serviceable life, but a replacement is not possible yet. Instead, the life of the NWS will need to be extended in parallel with new systems and capabilities.

Points of Contention

- How much of the world, beyond North America and its approaches, will All Domain Awareness have to cover to be effective?
- The disposition of the renewed all domain awareness sensor network, with debate over how much of it should be space or terrestrially based.
- Where does the human decision-making process to 'not shoot' or chose other options (such as to exploit, probe, surveille) come into a largely autonomous 'kill chain'?
- Extent of compatibility/upgradability of older Cold War Domain Awareness architecture to work with new systems.
- Integrity of sensor data. Could it be tampered with?

The Case for NORAD Modernization

In opening the webinar, NORAD Deputy Commander LGen Alain Pelletier presented the broad challenge facing NORAD. Following 9/11 the command focused on violent extremist organizations, putting its energies into looking inward across North American airspace to prevent such a terror attack from happening again. This reorientation of NORAD has since been exploited by adversaries, with China and Russia having developed new capabilities specifically to bypass NORAD's largely Cold War-era defences. As the world shifts towards a state of great power competition, this threat becomes more acute. By being able to defeat NORAD, these states can essentially hold North America hostage, preventing it from intervening in conflict overseas.

Brig Gen Pete M. Fesler, Deputy Director of Operations at NORAD's Headquarters, explained that America's long mobilization times have been noted as a vulnerability. By exploiting seams, adversaries can target military bases, airports, and seaports from far away, greatly disrupting the long and complex mobilizations required to project military power abroad. Future overseas conflict involving the great powers will thus see North America struck to delay its forces from intervening abroad, buying time for an adversarial victory.

LGen Pelletier stated that NORAD's adversaries are agile, rapidly evolving their capabilities to exploit vulnerabilities in the command's aging defences or circumventing these defences entirely. Jerome Dunn of Northrop Grumman elaborated on how these new threats can avoid NORAD's current sensors and that they can come in quantity. While NORAD's current defences are designed to deal with a few ballistic missiles from a rogue state, such as North Korea, these defences can be easily overwhelmed by large numbers of aerospace threats from a power like Russia. NORAD must address advanced new aerospace weapons such as hypersonic glide vehicles. A requirement to defend against sophisticated cyber-attacks was repeatedly emphasised throughout the seminar. Lockheed Martin's Mike Walsh also pointed out that NORAD needs a response for swarms of cheap unmanned aerial vehicles (UAVs) that can attack vulnerable Arctic infrastructure that supports NORAD's current Domain Awareness capability. A diversity of threats to NORAD have proliferated across the spectrum of military domains, from cyberspace to aerospace.

Ultimately, NORAD's defences have been overtaken by advancing technology. LGen Pelletier made clear that with aging systems and just two percent of NORAD's original force strength to draw upon from Cold War peak, the command can no longer deter great power adversaries as it had during the Cold War. This potentially places Canada into the 'hostage situation' outlined above, putting its political autonomy and economic growth and stability at unacceptable risk. With its ability to meet its mission statement to deter, detect, and defeat threats against the United

States and Canada degrading, NORAD cannot continue its current course. NORAD must be modernized.

Obstacles to the modernization of NORAD and the defence of North America

Dr. Andrea Charron, Director of the Centre for Defence and Security Studies (CDSS) and co-lead of the North American and Arctic Defence and Security Networks cautioned not to expect that endless financial resources will be available. The COVID-19 pandemic, she highlighted, has placed great strain on federal budgets, creating new fiscal realities and old agreements about cost splitting connected to the NWS are likely to change. CDAI Chair LGen (ret'd) Guy Thibault also emphasized this point. COVID-19 will put future pressure on Ottawa's coffers as the pandemic unfolds, making NORAD modernization spending uncertain. Dr. Charron also raised the importance of meaningful consultations with indigenous peoples about the old and potential new sensors that are located in

indigenous territories.
Aside from the growing fiscal challenges are the looming time constraints facing NORAD modernization. Dr. Charron stated the obvious, "the North Warning System, are on borrowed operational time." Brig Gen Fesler elaborated that there were multiple systems coming to the end of their useful lives. These sensors are rapidly becoming obsolete and cannot wait for a twenty-year procurement plan. Both Charron and Fesler emphasized to the audience that these two factors were driving the overall approach to NORAD modernization: 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 defense All Domain Awareness. Telesat's Sunil Chavda observed that the subsequent engineering challenge was not in the new technologies NORAD modernization requires, but in bringing this eclectic approach together as a holistic system.

LGen Pelletier made clear that while NORAD would have to push its all domain sensors far out into the world, covering the Arctic is the most challenging of the command's environments to surveille. Walsh elaborated on these challenges, pointing out the wide range of threats from multiple adversaries passing through the Arctic. The sensors that are needed to address these threats will be placed into "a resource constrained space," characterized by vast distances with little infrastructure to support them. These remote sensors will have to be able to reliably cope with the Arctic's harsh climate and severe weather. Walsh stated that while space-based sensors will be helpful to surveille the arctic there

are constraints imposed by what orbit the satellite is in. Fidelity can be sacrificed for distance as well.

All Domain Awareness Requirements

Dr. Thomas Walker of Lockheed Martin stated that the primary concern of NORAD modernization is the technology readiness levels of industry, the command wanting solutions now. What 'off the shelf' technology is available that can be modified and brought to bear quickly? What current NORAD systems can be retrofitted? Walker conveyed that NORAD was open to making all sorts of solutions work so long as they emphasised little to no development timelines and speed of implementation.

All Domain Awareness is a core capability requirement of NORAD. Dr. Walker emphasized that the multi- layered sensor system NORAD needs to develop to enable this capability must be able to detect, identify, and track all types of missiles ranging from ballistic to cruise missiles and new hypersonic glide vehicles. He also stressed that this new sensor system must detect threats at great distance to increase warning and reaction times as much as possible, both of which are central to decreasing the risk these weapons pose to Canada.

Brig Gen Fesler elaborated that the proposed multi-layered sensor system must ensure that detection sensors are separate from defeat sensors. Ballistic Missile Defence (BMD). 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. Closing these gaps requires a combination of multi-spectral sensor capabilities (a combination of radar, infra-red, radio frequency, acoustics, etc.). Lastly, he emphasised Dr. Walker's point that All Domain Awareness must occur at longer ranges to detect and engage threats as early as possible. Preferably the extent of Domain Awareness would allow for a threat to be identified and track from its 'birth.'

Design Considerations for Canadian Industry

Lockheed Martin's Mike Walsh, working on next generation sensors, presented three considerations for NORAD modernization. The first was the concept of multi-mission sensors that could detect and track more than one threat. These sensors could adapt what they do and where they do it to handle a high volume of threat. Second, sensors should be software defined and open architecture for quick adaptability and upgradability. This would facilitate C2 networking without requiring a hardware update, increasing the lifespan of the renewed system and keeping down future costs. Lastly, industry should provide sensors that are modular and scalable. This means adapting sensors developed for other parts of the world for use with NORAD, making the renewed system quick to install, cheap, and easily upgradable.

Chavda, who works on satellite systems development, emphasized the need to

integrate the proposed multi-layered sensors into a holistic system. This requires a paradigm shift. How is the processed data displayed for action? He pointed out that there is limited development and no superclusters working on this. This means bringing in the commercial sector to tackle how information is managed, providing new opportunities for industry products and services.

Ravi Ravichandran of BAE Systems, with an extensive background in technology development, asked industry to consider how technology enables a mission. The language surrounding Domain Awareness has become mission-focused, having shifted away from being about platforms and sensors. Domain Awareness cannot be considered in isolation, it has to be connected to C2 and defeat mechanisms. Data to decision-makers and their thinking needs to happen 'at the speed of relevance,' which means understanding computing and data structures. Faster computing is required, the processing behind complex systems having struggled in the past. He agreed that sensors should be reconfigurable in real time, supported by an open architecture. He concluded that the ability to anticipate battle management demands should drive Domain Awareness.

Dunn, working on countering hypersonic threats for Northrop Grumman, stressed that the architecture of the sensor system must be able to account for all threats, from 'birth to death.' Engag on Remote to engage a threat as early as possible is of paramount importance for a successful defeat outcome since this allows a Shoot Asses Shoot shot doctrine. Dunn emphasized that new ways of engaging these threats are needed, including Artificial Intelligence (AI) weapons. Engaging threats remotely could represent another paradigm shift in thinking. He posited that 'kill chains' could be forged on the fly rather than pre-planned, leading to the combination of "any sensor, best shooter." Lastly, he wanted industry to consider building in systems redundancy; All Domain Awareness cannot just rely upon space assets.

Punch Moulton argues that terrestrial sensors cannot provide All Domain Awareness alone; the sensor system must be based mostly in space. This will provide NORAD with the global level awareness needed to detect threats originating outside of North America 'from birth.' Second, he suggests participants should consider that NORAD states are also a part of NATO. Tying the two organizations together should help NORAD address deficits in awareness across the North Atlantic whilst giving the command a chance to secure NATO funding for its modernization. Lastly, he stressed the necessity of integrating a holistic multi-layered sensor system with the C2 and defeat mechanisms; the best shooter is the weapon that gets the right information at the right time. The goal should be 'best sensor, best shooter.'

Data Plans

A major theme of the webinar was the sharing of sensor data with allies and industries. Moulton largely considers the sharing of data to be a policy question – one that should be tackled from the beginning – using the example of NORAD sharing US-Canada 'Two Eyes' data with the other twenty-eight members of NATO. He also raised this issue in relation to dual-use technology that can be shared with American and Canadian civilian departments and industries. As the technology goes forward, he cautions that the policy needs to be in place that

collectively says what can and cannot be shared in an open architecture system. Dr. Charron argues that sensors should be capable of dual use by military/civilian government agencies. This generates additional value beyond defence, contributing data for use across government and possibly the commercial sector. LGen Thibeau commented that such an approach improves the economic case for NORAD modernization as this type of defence investment could be seen as developing northern infrastructure. Similarly, LGen Pelletier commented sharing this data across departments and agencies means "everyone is a contributor" to NORAD modernization. Dr. Charron recommended creating a lexicon to facilitate the sharing of data due to the number and diversity of potential beneficiaries. She also suggests there may be lessons that can be taken from NORAD assuming its maritime warning mission. Similarly, LGen Thibault offered the example of 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.

Walsh raised the significant challenges NORAD modernization poses to project teams having to work across governments and industry. He highlighted the need for more collaboration between government and industry on operational analysis (on sensors, C2, and defeat capabilities) which could improve this working relationship. It was

noted, however, that more industries are declining to work with the military – a challenge that needs to be resolved. Dr. Charron recommend that the Canadian government send a 'finishing advocate' to NORAD. Such an advocate would increase the success rate of projects by matching the 'hoovering' practice of attracting ideas and technology to NORAD's particular problems, seeing them through to fruition. She recommended this advocate approach as part of an overarching Canadian science and technology strategy.

Another major theme of the webinar was that the sensor did not matter so much as the actionable data it provided. What does matter is where the sensor is placed to provide the best coverage. Chavda stated that getting the technology into the right place was a challenge. Dunn stressed this point with respect to space-based sensors, emphasizing that they have to be put in the right orbit to be effective. He projects that some operational ability will be flying in two to three years.

The expert panel agreed that most of the technology to make the types of sensors envisioned exists today. For technology that must be developed, both Dunn and Chavda argued that rapid prototyping must be able

to fail early and more often for best results, especially for space-based sensors. Physical demonstrations are important. Ravichandran pointed out that digital prototyping is getting better, driving down development costs. Digital prototyping is beginning to allow for digital demonstrations – not just of components, but of systems as well. Such an approach will allow for system designs to be tested before being physically built and put into place.

A common element running throughout the discussion was that NORAD should have its All Domain Awareness, C2, and defeat capabilities fully converge and be as autonomous as possible. Dunn explained that a full convergence system would see sensors push data to C2, with the sensors changing with the defeat needs for intercept, thus completing a seamless 'kill chain.' Dr. Charron asked what would happen if NORAD did not want to shoot at a particular threat that it detects (which could leave room for a diplomatic solution). I.e. the sensors cannot only feed information that leads only to the defeat of a target. The sensors must provide information that allows for flexible responses including the exploitation, tracking or gathering of intelligence of a target, not just its defeat. The human decision-making process within this tightly knit kill chain was largely omitted from discussion but the participants concurred that it was an important subject for consideration and future discussion.

Lastly, LGen Pelletier raised the issue of data integrity during his closing remarks. Could he trust that the data he was being provided by sensors was safe, secure, and reliable? Could All Domain Awareness capability be tampered with? This question is salient given the sophistication of adversaries, the core importance of information sharing, and the long supply chains of contractors and sub-contractors needed to build and maintain NORAD's All Domain Awareness capability.

Special thanks to our NAADSN rapporteurs:

Ryan Dean and Dr. Nancy Teeple